



INSTITUTO NACIONAL DO SEGURO SOCIAL
Comitê Estratégico de Governança

DESPACHO

Comitê Estratégico de Governança, em 27/02/2020.

Ref.: Processo nº 35014.047735/2020-84

Int.: DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO

A s s . : Instrução de processo para proposição de resoluções do CEGOV para instituição de normas de segurança da informação e comunicação, em atendimento ao Decreto nº 9.637, de 26 de dezembro de 2018, que trata da Política Nacional de Segurança da Informação do Poder Executivo Federal.

1. Trata-se de processo para proposição de atos normativos para instituição de políticas e normas de segurança da informação e comunicações do Instituto Nacional do Seguro Social - INSS, de competência do Comitê Estratégico de Governança - CEGOV, conforme previsto no Art. 5 da Portaria nº 3.213/PRES/INSS/2019 (inciso VIII e parágrafo único).

2. Na Reunião CEGOV nº 1/2020 (vide processo SEI nº 35014.012037/2020-68) foram apresentadas e discutidas as minutas das normas de segurança da informação abaixo relacionadas:

- 2.1. Política de Segurança da Informação e Comunicações - POSIC;
- 2.2. Política de Controle de Acesso Lógico;
- 2.3. Norma de criação da Equipe de Tratamento de Incidentes de Redes – ETIR;
- 2.4. Norma de acesso à Internet.

3. Na oportunidade, o CEGOV deliberou pela realização de ajustes nas normas propostas, de acordo com a ata da reunião, registrada no documento SEI nº 0368652. Ademais, foi acordado que as normas seriam circularizadas por e-mail para coleta de sugestões finais, que seriam consolidadas pela Diretoria de Tecnologia da Informação e Comunicações - DTI.

4. O e-mail supracitado foi enviado no dia 19/02/2020, e consta do documentos SEI nº 04110459, anexado ao presente processo. As normas que foram submetidas à apreciação dos integrantes do CEGOV constam dos documentos SEI nº 04110468, 04110474, 04110479 e 04110495.

5. Dando prosseguimento ao decidido na Reunião CEGOV nº 1/2020, vem-se solicitar que a DTI instrua o presente processo com:

5.1. Nota técnica que justifica a necessidade de edição das normas em tela, bem como o fluxo de elaboração e aprovação dos normativos propostos;

5.2. Documentos que registrem as eventuais demandas de ajustes solicitados pelas áreas, conforme indicado no item 4 do presente despacho;

5.3. Minuta de resolução para instituição da Política de Segurança da Informação e Comunicações - POSIC, consolidando os ajustes citados nos itens 3 e 4 deste despacho;

5.4. Minuta de resolução para instituição da Política de Controle de Acesso Lógico, consolidando os ajustes citados nos itens 3 e 4 deste despacho;

5.5. Minuta de resolução para instituição da norma de criação da Equipe de Tratamento de Incidentes de Redes – ETIR, já consolidando os ajustes citados nos itens 3 e 4 deste despacho; e

5.6. Minuta de resolução para aprovação da norma de acesso à Internet, também consolidando os ajustes citados nos itens 3 e 4 deste despacho.

6. Registra-se que as deliberações do CEGOV serão editadas por meio de resolução, em consonância com o disposto no inciso II do art. 2º do Decreto nº 10.139, de 28 de novembro de 2019.

7. Após o feito, solicita-se que os autos sejam retornados à Secretaria-executiva do CEGOV, para encaminhamentos posteriores, conforme Resolução nº 708/PRES/INSS, de 6 de novembro de 2019.

CIBELLE CESAR DO AMARAL BRASIL

Coordenadora-Geral de Governança
Secretaria-Executiva do CEGOV



Documento assinado eletronicamente por **CIBELLE CESAR DO AMARAL BRASIL**, **Coordenador(a) Geral**, em 27/02/2020, às 15:42, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0409817** e o código CRC **6B83DD9A**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 0409817

Cibelle Cesar do Amaral Brasil

De: Renata Cesario de Oliveira Gomes <renata.cgomes@inss.gov.br>
Enviado em: quarta-feira, 19 de fevereiro de 2020 20:59
Para: cibelle.brasil@inss.gov.br; adler.alves@agu.gov.br;
alessandro.ribeiro@inss.gov.br; clovis.decastro@inss.gov.br;
flaviof.santos@inss.gov.br; jobson.sales@inss.gov.br;
leonardo.rolim@inss.gov.br; pedro.rosario@inss.gov.br;
rodrigo.barreto@agu.gov.br; vitor.dasilva@inss.gov.br;
william.guedes@inss.gov.br
Cc: alexinaldo.cerqueira@inss.gov.br; claudio.ferraz@inss.gov.br;
katia.macarini@inss.gov.br; lorena.mferreira@inss.gov.br;
nelson.jacinto@inss.gov.br; roberto.dalfilho@inss.gov.br;
roberto.rufino@inss.gov.br; sidarta.souza@inss.gov.br;
ziana.santos@inss.gov.br
Assunto: Re: Minuta da Ata de Reunião CEGOV nº 1/2020
Anexos: SEI_INSS - 0369782 - Minuta de Resolução_normas_internet.pdf; SEI_INSS - 0369776 - Minuta de Resolução_ETIR.pdf; SEI_INSS - 0369764 - Minuta de Resolução_PCAL.pdf; SEI_INSS - 0369749 - Minuta de Resolução_POSIC.pdf

Prezados,

De ordem do Diretor de Tecnologia da Informação e Inovação, encaminho as minutas das normas de segurança que foram revisadas de acordo com o que foi solicitado em reunião.

Respeitosamente,

Renata Cesário de Oliveira Gomes

Instituto Nacional do Seguro Social – INSS

Diretoria de Tecnologia da Informação e Inovação - DTI



Só imprima o necessário. Preserve o meio ambiente

Em 17/02/2020 18:23:29, Cibelle Cesar do Amaral Brasil escreveu:

Prezados Senhores,

Envio, em anexo, minuta da ata de Reunião CEGOV nº 1/2020, realizada hoje. Solicito, por favor, que enviem contribuições até amanhã, no final do dia.

Após ajustes, a ata será disponibilizada em bloco de assinaturas no SEI, para que os membros do CEGOV a assinem digitalmente.

Respeitosamente,

--

Cibelle Cesar do Amaral Brasil

Coordenadora-Geral de Governança - Matr. 1659631

Diretoria de Integridade, Governança e Gerenciamento de Riscos - DF

Tel.: (61)2323-3720



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 2/CEGOV/INSS, DE DE DE 2020

Atualiza a Política de Segurança da Informação e Comur POSIC-INSS.

O **COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS**, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída no âmbito do INSS e nos termos do Anexo a esta Resolução, a Política de Segurança da Informação e Comunicações – POSIC-INSS.

Art. 2º Esta Resolução entra em vigor na data de sua publicação e seu Anexo será publicado em Boletim de Serviço.

Art. 3º Fica revogada a Resolução nº 672/PRES/INSS, de 27 de dezembro de 2018.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

MÁRCIA ELIZA DE SOUZA
Diretora de Benefícios

CLÓVIS DE CASTRO JÚNIOR
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

GUSTAVO PAULO LEITE DE SOUZA
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação

ANEXO I

RESOLUÇÃO Nº 2/CEGOV/INSS, DE DE DE 2020

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO INSTITUTO NACIONAL DO SEGURO SOCIAL – POSIC-INSS

Art. 1º A Política de Segurança da Informação e Comunicações do Instituto Nacional do Seguro Social – POSIC-INSS, tem por objetivo estabelecer e difundir diretrizes e princípios de Segurança da Informação e Comunicações – SIC, com vistas à orientação para uso e proteção adequados das informações produzidas e custodiadas pelo Instituto, preservando sua disponibilidade, integridade, confidencialidade e autenticidade.

Parágrafo único. A Política de que trata o **caput** e suas normas complementares aplicam-se a todos os agentes públicos que têm vínculo direto e/ou indireto com o Instituto.

Art. 2º Para os efeitos da POSIC-INSS, entende-se:

I - agente público: todas as pessoas físicas que manifestam, por algum tipo de vínculo, a vontade do Estado, abrangendo servidores, ocupantes de cargo comissionado ou em comissão, prestadores de serviço e estagiários;

II - dado: é o registro do atributo de um ente objeto ou fenômeno onde registro indica o ato de registrar, ou seja, é a gravação ou a impressão de caracteres ou símbolos que tenham um significado em algum documento ou suporte físico;

III - Informação: é a resultante do processamento, manipulação e organização de dados;

IV - ativos de informação: meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

V - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

VI - necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para que uma pessoa possuidora de credencial de segurança tenha acesso a dados ou informações sigilosas;

VII - riscos de segurança da informação e comunicações: potencial associado à exploração de uma ou mais vulnerabilidades nos ativos de informação, em razão de ameaças, com impacto negativo às atividades do Instituto;

VIII - segurança da informação e comunicações – SIC: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e autenticidades das informações;

IX - vínculo direto: agentes públicos contratados diretamente pelo INSS;

X - vínculo indireto: agentes privados ou públicos pertencentes a órgãos ou unidades da Administração Pública Federal, Estadual ou Municipal que mantenham contrato, convênio, acordo de cooperação técnica ou instrumento congênere com o INSS; e

XI - gestor de Segurança da Informação e Comunicações: é o responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF.

Art. 3º Esta POSIC-INSS foi elaborada com base nos seguintes documentos:

I - Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;

II - Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto na Constituição Federal;

III - Decreto nº 7.724, de 16 de maio de 2012, regulamenta a Lei nº 12.527, de 18 de novembro de 2011;

IV - Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

V - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

VI - Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

VII - Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008, que disciplina a gestão de segurança da informação e comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

VIII - Normas Complementares nº 01 a 21/IN01/DSIC/GSIPR;

IX - NBR ISO/IEC 27002:2013, que institui código de melhores práticas para a Gestão de Segurança da Informação;

X - Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais; e

XI - Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Art. 4º Esta POSIC-INSS foi elaborada com base nos seguintes princípios:

I - a preservação da imagem do Instituto e de seus agentes públicos;

II - a salvaguarda das informações do cidadão;

III - ações de segurança orientadas pela gestão de riscos;

IV - continuidade assegurada dos serviços ao cidadão;

V - o alinhamento com a missão institucional e seu planejamento estratégico; e

VI - respeito à natureza e finalidade de cada área do Instituto.

Art. 5º São diretrizes gerais da POSIC-INSS:

I - Tratamento da Informação:

- a) toda informação produzida pelos agentes públicos, no exercício de suas atividades, é de propriedade do INSS e deve ser protegida;
- b) informações produzidas, armazenadas e tratadas pelo Instituto, especialmente as informações pessoais e custodiadas, devem receber o devido tratamento para assegurar sua proteção durante todo o ciclo de vida; e
- c) somente os canais de comunicação disponibilizados pelo INSS devem ser utilizados para trafegar informações institucionais.

II - Tratamento de Incidentes de Segurança da Informação (SIC):

- a) todo incidente de segurança da informação deve ser imediatamente relatado à área responsável pela gestão de segurança da informação de TIC, observando-se a apropriada coleta de evidências.

III - Gestão de Riscos de Segurança:

- a) os riscos de segurança da informação devem ser identificados e tratados; e
- b) os critérios para a gestão de risco devem ser definidos e comunicados a toda instituição.

IV - Gestão de Continuidade:

- a) os ativos de informação que suportam as atividades críticas do Instituto devem ser suportados por ambiente de alta disponibilidade e ter capacidade de recuperação em prazos e condições previamente definidos para situações de contingência, em conformidade com o processo de continuidade; e
- b) a continuidade das operações e serviços de Tecnologia da Informação e Comunicações – TIC, deve estar prevista nos contratos, assim como os prazos e condições devem estar formalmente estabelecidos.

V - Controles de Acesso:

- a) todo acesso à informação deve ser motivado pela necessidade de conhecer;
- b) os sistemas de informação e as instalações físicas devem ter capacidade de controlar os acessos, com fins de responsabilização pelo seu uso; e
- c) as autorizações de acesso às informações, sistemas e instalações físicas devem ter critérios de acesso definidos e divulgados a todos da instituição.

VI - Recursos Computacionais:

- a) correio eletrônico:
 - 1. o correio eletrônico, *e-mail*, é uma forma de comunicação oficial e deve ser utilizado exclusivamente no desempenho das atividades funcionais; e

- 2. ao produzir, responder ou encaminhar mensagem em caixa de correio eletrônico institucional, o servidor deverá se identificar, subscrevendo, ao menos, seu nome, cargo e telefone de contato institucional.

- b) Acesso à Internet:

- 1. o acesso à Internet, por meio da rede de dados do INSS, é uma concessão e deve ter seu uso orientado para a execução das atividades do Instituto; e

- 2. os acessos serão liberados de acordo com perfis previamente definidos pelo órgão responsável pelos serviços de TIC.

- c) Gestão de Mudanças de TIC:

- 1. toda mudança nos sistemas de informação do INSS deve ser previamente e formalmente autorizada; e

2. a gestão de mudanças deve prever, no mínimo, a guarda dos registros, realização de testes e a possibilidade de recuperação do ambiente.

VII - Educação e Conscientização:

- a) esta Política e seus normativos complementares devem ser periodicamente divulgados a todos os agentes públicos do Instituto;
- b) o Instituto deve manter programa contínuo de conscientização dos agentes públicos em Segurança da Informação e Comunicações – SIC; e
- c) deve ser mantido plano de capacitação especializado aos profissionais que atuam na gestão de SIC.

VIII - Auditoria e Conformidade:

- a) o cumprimento desta Política e de suas normas complementares deve ser avaliado periodicamente, por meio de verificações de conformidade; e
- b) o uso dos recursos de TIC disponibilizados pelo Instituto é passível de monitoramento e auditoria.

IX - Responsabilidade na gestão das informações:

Parágrafo único. O Comitê Temático de Gestão da Informação é responsável pela aprovação de procedimentos e de normas internas que orientem o compartilhamento de dados sob gestão do INSS e pela aprovação da categorização dos níveis de compartilhamento de dados com outras entidades públicas (federais ou de outras esferas e poderes) da sociedade civil (Vide atribuições do CTGI, no Art. 6º do Anexo da Portaria nº 3.213/PRES/INSS/2019).

Art. 6º A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas, cíveis e penais, previstas na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), no Código Penal, no Código Civil, e, ainda, em legislação que regule ou venha regular a matéria.

Art. 7º Competências e Responsabilidades:

I - Cabe ao Gestor de Segurança da Informação e Comunicações:

- a) promover cultura de segurança da informação e comunicações;
- b) acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
- c) propor os recursos necessários à implementação das ações de SIC;
- d) coordenar o CSIC e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR do INSS; e
- e) propor o detalhamento das diretrizes desta Política, por meio de normas e procedimentos, e acompanhar sua implementação.

II - Cabe ao Presidente do Instituto nomear o Gestor de SIC;

III - Caso o Gestor de SIC não seja nomeado, as atribuições relacionadas no item 7.1 serão desempenhadas pelo Diretor de Tecnologia da Informação e Inovação;

IV - A ETIR-INSS deve analisar e propor respostas a notificações e atividades relacionadas a incidentes de SIC, no âmbito do Instituto; e

V - É responsabilidade de todos os agentes públicos, diretos e indiretos, conhecer e cumprir as diretrizes desta Política e demais normas e procedimentos complementares de SIC.

Art. 8º Esta Política deve ser revisada sempre que necessário, não excedendo o período máximo de três anos.



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 3/CEGOV/INSS, DE DE DE 2020

Define regras para a emissão de credenciais de acesso lógico no âmbito

O **COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS**, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída a Norma de Controle de Acesso Lógico - NCAL, do Instituto Nacional do Seguro Social – INSS.

Art. 2º Esta Resolução, bem como seus anexos, serão publicados em Boletim de Serviço, nos termos do Art. 15, § 2º, Inciso I da Resolução 70/INSS/PRES, de 06 de outubro de 2009.

Art. 3º Revogar a RESOLUÇÃO Nº 413/PRES/INSS, DE 20 DE MAIO DE 2014.

Art. 4º Esta Resolução entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

MÁRCIA ELIZA DE SOUZA
Diretora de Benefícios

CLÓVIS DE CASTRO JÚNIOR
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

GUSTAVO PAULO LEITE DE SOUZA
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação

ANEXO I

RESOLUÇÃO Nº 3/CEGOV/INSS, DE DE DE 2020

NORMA DE CONTROLE DE ACESSO LÓGICO – INSS

Art. 1º Os termos definidos nesta norma aplicam-se a todos os agentes públicos e privados com vínculo direto ou indireto, permanente ou temporário com o INSS.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União – AGU que atuarem na consultoria e no assessoramento jurídico, e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta Norma de Controle de Acesso Lógico são estabelecidos os seguintes conceitos e definições:

I - administrador de Domínio: Usuário responsável pela administração de um domínio por meio da aplicação de políticas globais, criação, edição e exclusão de usuários e grupos, e instalação de programas em um grande número de estações de trabalho;

II - administrador Local: Usuário responsável pela administração de partes de um domínio (geralmente restrito a um setor ou abrangência), por meio de políticas locais, edição de grupos e usuários locais, e instalação de programas em estações de trabalho limitadas a um setor ou abrangência;

III - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta;

IV - dado: é o registro do atributo de um entre objeto ou fenômeno onde registro indica o ato de registrar, ou seja, é a gravação ou a impressão de caracteres ou símbolos que tenham um significado em algum documento ou suporte físico;

V - Informação: é a resultante do processamento, manipulação e organização de dados;

VI - ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VII - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

VIII - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

IX - contas de serviço: contas de acesso à rede corporativa de computadores, necessárias para a execução de procedimentos automáticos (aplicação, script, etc) sem qualquer intervenção humana no seu uso;

X - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

XI - credenciamento: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer;

XII - credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física, como crachá, cartão e selo ou lógica como identificação usuário e senha;

XIII - domínio: agrupamento lógico de computadores em rede que compartilham recursos em um banco de dados de segurança, comum, onde a administração e autenticação são centralizadas. Desta forma um usuário precisa de uma conta para ter acesso ao domínio e aos recursos compartilhados;

XIV - endereço IP: sigla em inglês para *Internet Protocol*. Trata-se de endereço lógico que identifica a localização de determinado ativo na rede;

XV - entidade externa: Organização governamental, não governamental ou privada amparada por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica ou instrumento congênere com o INSS;

XVI - e-SIC: Sistema Eletrônico do Serviço de Informações ao Cidadão, aplicação disponibilizada na internet, que centraliza todos os pedidos de informações dirigidos ao Poder Executivo Federal;

XVII - estagiário: educando que esteja frequentando o ensino regular, em instituições de educação superior, de educação profissional, de ensino médio, de educação especial e dos anos finais do ensino fundamental, na modalidade profissional da educação de jovens e adultos, que desenvolve as atividades relacionadas à sua área de formação profissional junto as pessoas Jurídicas de Direito Privado, órgãos da Administração Pública e Instituições de Ensino, que tenham condições de proporcionar experiência prática na sua linha de formação;

XVIII - estágio Supervisionado: ato educativo escolar supervisionado, desenvolvido no ambiente de trabalho, que visa a preparação para o trabalho produtivo de educandos;

XIX - ferramenta de gestão de acessos: Software que possibilita a gestão integrada de papéis e permissões de acesso dos usuários nos sistemas corporativos;

XX - gestor da informação: usuário que gerou a informação, que responde pelo seu conteúdo ou que foi formalmente designado para definir, alterar a sua classificação nos graus de sigilo e perfil de acesso dos demais usuários e processos;

XXI - gestão de identidades: Combinação de sistemas técnicos, regras e procedimentos que definem a posse, utilização e segurança de uma identidade. Seu objetivo primário é estabelecer a confiança na associação de atributos a uma identidade digital e conectar esta identidade com uma entidade individual;

XXII - necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação;

XXIII - perfil de Acesso do Usuário: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

XIV - recursos de rede: Dispositivos (impressoras, scanners, multifuncionais, etc) ou serviços (sistemas, portais, etc) disponibilizados para os usuários por meio de uma rede de dados;

XXV - serviço de diretório: serviço que armazena e organiza informações relativas a recursos disponíveis e usuários de uma rede de dados. Permite que o administrador da rede gerencie o acesso de usuários e sistemas aos recursos disponíveis;

XXVI - sistemas corporativos: sistemas de operação, ou finalísticos, que se coadunam com os fins da Previdência Social. Assim, entende-se que este conceito comporta o conjunto de sistemas e subsistemas que garantem a operação dos regimes geral e próprio de previdência social, inclusive de previdência complementar;

XXVII - sistemas legados: compreendem o conjunto de aplicações desenvolvidas com tecnologias obsoletas que permanecem em operação no INSS;

XXVIII - usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal-APF, formalizada por meio da assinatura do Termo de Responsabilidade;

XXIX - usuário interno: servidor do quadro do INSS lotado em uma Unidade Orgânica – UO, que se utiliza dos sistemas corporativos do Instituto;

XXX - usuário externo: usuários vinculados a uma Entidade Externa, que se utiliza dos sistemas corporativos do Instituto por meio de um perfil de acesso concedido por um Gestor de Acesso Externo;

Art. 3º São diretrizes desta NCAL-INSS:

I - o acesso à rede e aos sistemas corporativos do INSS dar-se-á por meio de autenticação integrada de domínio baseado em serviço de diretório, administrado por meio de uma ferramenta de gestão de identidades;

II - as concessões de acesso à rede de dados e aos sistemas corporativos são distintas. Sendo assim, o usuário pode obter permissão de acesso apenas à rede de dados, ou apenas a determinado(s) sistema(s) corporativo(s);

III - as credenciais de acesso a rede de dados e aos sistemas corporativos do INSS são conferidas aos usuários com base na necessidade de conhecer, para viabilizar o exercício de suas atribuições funcionais e atividades a serem desenvolvidas no âmbito do INSS; e

IV - o uso indevido de informações dos sistemas corporativos do INSS sujeitará o agente às penalidades previstas na legislação.

Art. 4º Base Cadastral:

I - as bases de dados do Serviço de Diretórios (acesso à rede de dados), do Sistema de Gestão de Acessos (sistemas corporativos) e sistemas legados devem ser alimentadas por informações disponibilizadas pelo INSS;

II - para tanto, a área responsável pela gestão de pessoas do INSS disponibilizará periodicamente as informações extraídas do Sistema Integrado de Administração de Recursos Humanos – SIAPE para a área responsável pela gestão de TIC do INSS (não ultrapassando o prazo de sete dias), contendo, minimamente, os seguintes dados:

Tabela 1: Informações Usuários

Item	Informação	Campo	Descrição
1	GR-MATRICULA	N 0012	GRUPO NUMÉRICO COMPOSTO DE NÚMERO DO ÓRGÃO (N0005) E NÚMERO DE MATRÍCULA DO SERVIDOR (N0007)
2	IT-NU-IDEN-SERV-ORIGEM	A 0008	NÚMERO DE IDENTIFICAÇÃO DO SERVIDOR NA ORIGEM - NÚMERO VINCULADO AO CARGO EFETIVO OU EM COMISSÃO
3	IT-NO-SERVIDOR	A 0060	NOME
4	IT-DA-NASCIMENTO	N 0008	DATA DE NASCIMENTO
5	IT-NU-CPF	N 0011	NÚMERO DO CPF
6	IT-NU-PIS-PASEP	N 0011	NÚMERO DO PIS
7	IT-IN-SUPRESSAO-PAGAMENTO	A 0001	INDICATIVO DE SUPRESSÃO DE PAGAMENTO
8	IT-CO-SITUACAO-SERVIDOR	N 0002	CÓDIGO DE SITUAÇÃO FUNCIONAL DO SERVIDOR
9	IT-CO-GRUPO-OCOR-AFASTAMENTO	N 0002	CÓDIGO DE OCORRÊNCIA DE AFASTAMENTO
10	IT-DA-INICIO-	N 0008	DATA DO INÍCIO DA OCORRÊNCIA DE AFASTAMENTO

	OCOR-AFASTAMENTO		
11	IT-DA-TERMINO- OCOR-AFASTAMENTO	N 0008	DATA DE TÉRMINO DA OCORRÊNCIA DE AFASTAMENTO
12	IT-CO-GRUPO- OCOR-EXCLUSAO	N 0002	CÓDIGO DE OCORRÊNCIA DE EXCLUSÃO
13	IT-CO-UORG- LOTACAO-SERVIDOR	N 0009	CÓDIGO DA UORG DE LOTAÇÃO DO SERVIDOR
14	IT-CO-ORGAO- REQUISITANTE	N 0005	CÓDIGO DO ÓRGÃO REQUISITANTE

III - a Empresa de Tecnologia e Informações da Previdência Social - Dataprev, procederá com a atualização dinâmica das bases cadastrais do serviço de diretórios e dos sistemas corporativos, bem como realizará a validação das informações disponibilizados pelo INSS por meio de outras bases, na periodicidade do envio das informações; e

IV - a área responsável pela gestão de pessoas do INSS poderá acordar, com a área responsável pela gestão de TIC do INSS, a inclusão de outras informações necessárias à administração de contas de usuários.

Art. 5º Credenciais e perfis de acesso:

I - a emissão de uma credencial permite ao usuário acessar a rede de dados corporativa do INSS. Para que o mesmo obtenha acesso aos sistemas corporativos a credencial deve ser associada a um perfil de acesso;

II - o processo de credenciamento de usuário aos ativos de informação deve ser feito observando os seguintes critérios:

- a) a credencial de acesso concedida para acesso à rede de dados e sistemas corporativos do INSS é de caráter pessoal e intransferível;
- b) as credenciais de acesso devem ser concedidas após a data de contratação ou entrada em exercício do usuário; e
- c) as mesmas credenciais de acesso devem ser utilizadas para o acesso à rede de dados e aos sistemas corporativos do INSS, mediante autenticação que permita ao usuário acessar vários sistemas, por meio de ferramenta de gestão de identidades e acessos.

III - os servidores lotados nas áreas responsáveis pela gestão de pessoas do INSS deverão utilizar os canais de atendimento disponibilizados pela Dataprev, ou outro canal informado pela DTI, para:

- a) solicitar, se necessário, o credenciamento de usuários, contratados ou requisitados, para compor o quadro de servidores do INSS, após o ato da posse, e de estagiários, após assinatura do contrato de prestação de serviço, para acesso à rede;
- b) solicitar a inativação imediata do perfil de acesso dos servidores cedidos a outros órgãos, inativos ou exonerados do quadro de servidores do INSS na data da publicação do ato;
- c) solicitar a suspensão imediata do perfil de acesso dos servidores afastados ou com licença programada de suas funções por mais de sessenta dias ininterruptos; e
- d) solicitar a exclusão do acesso de estagiários, cujo vínculo com o Instituto tenha sido encerrado, tão logo a rescisão do contrato seja efetivada.

IV - quanto ao processo de formação das credenciais de acesso fica estabelecido que:

a) o nome do usuário será composto de acordo com os padrões estabelecidos no Guia de Interoperabilidade do Governo Eletrônico – e-Ping, mais especificamente no documento “Caixas Individuais-Fundacionais no Governo Federal” (Rede do Governo, 2010) que define regras de formação de nomes para a composição de endereços eletrônicos;

b) quanto às senhas de acesso:

- 1. deverão ter no mínimo oito caracteres e conter, obrigatoriamente, caracteres alfanuméricos (combinação de letras e números). O usuário poderá acrescentar caracteres especiais (espaços em branco, símbolos, sinais de pontuação, etc);
- 2. é vedada a reutilização das últimas quatro senhas utilizadas pelo usuário;
- 3. podem ser alteradas sempre que preciso ou quando o usuário achar necessário;

4. o prazo de validade não deve ultrapassar noventa dias; e

5. o usuário receberá por meio de comunicado direto (via interface do sistema ou por mensagem no correio eletrônico) a informação do prazo próximo de vencimento da senha, quando esta estiver a 15 dias da sua data de expiração.

V - os perfis de acesso aos sistemas corporativos deverão contemplar um conjunto de permissões e ações vinculadas às atividades desenvolvidas pelo usuário;

VI- caberá à área responsável pela gestão de TIC do INSS estabelecer, em conjunto com as áreas responsáveis pela gestão dos sistemas corporativos, a política de criação dos perfis de acesso;

VII - as áreas responsáveis pela gestão dos sistemas corporativos, são responsáveis pelas permissões, transações e ações que devem compor cada perfil de acesso;

VIII - os perfis de acesso e perfis de gestão concedidos para usuários deverão ser objeto de revisão contínua pelos gestores responsáveis, não podendo ultrapassar o prazo máximo de 24 (vinte e quatro) meses;

IX - quanto à utilização das credenciais e perfis de acesso, o usuário:

a) deve ter conhecimento prévio desta Política de Controle de Acesso Lógico e preencher os requisitos estabelecidos na mesma;

b) deve estar devidamente autorizado a utilizar a rede corporativa e/ou os sistemas corporativos, de acordo com os requisitos estabelecidos nesta Política;

c) deve utilizar os serviços e as informações obtidas, por meio do perfil de acesso, única e exclusivamente em razão do exercício da função pública e para os fins que lhe foi designado, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal;

d) não pode divulgar, nem mesmo compartilhar, os códigos de segurança que lhe forem atribuídos (credenciais de acesso), os quais são pessoais e intransferíveis;

e) não pode utilizar as credenciais para acessar os recursos disponíveis em mais de uma estação de trabalho simultaneamente;

f) não pode fazer uso das credenciais de acesso de outros usuários;

g) deve fornecer informações acessadas nos sistemas e na rede de dados corporativos do INSS somente mediante demanda formalizada de quem tenha competência para tal;

h) deve comunicar a chefia imediata ou responsável pela administração do sistema ou rede corporativa quaisquer violações ou incidentes referentes à proteção do equipamento utilizado, do software ou de outros ativos da informação; e

i) deve, sempre que for necessário afastar-se da estação de trabalho, certificar-se de que a sessão de rede ou acesso ao sistema corporativo esteja encerrado ou bloqueado.

X - a autenticação dos usuários será feita por meio de credenciais de acesso baseadas em nome de usuário e senha e, quando disponível, aliada ao uso certificação digital padrão ICP-Brasil e/ou uso de dados biométricos;

XI - o usuário deverá, obrigatoriamente, efetuar processo de alteração da sua senha em seu primeiro acesso à rede de dados corporativa; e

XII - no ato do primeiro acesso, bem como após cada atualização desta Política, o usuário deverá manifestar concordância com os termos dispostos na mesma.

XIII - Credenciamento de Usuários Internos:

a) o cadastro de novos servidores ou ocupantes de cargo em comissão, no âmbito do Instituto, pode ser solicitado por servidor vinculado à área responsável pela gestão de pessoas ou pela chefia imediata do usuário; e

b) esse cadastro deve ser solicitado por meio dos canais de atendimento da Dataprev ou outro informado pela DTI.

XIV - credenciamento de estagiários:

a) a emissão de credencial de acesso se dará tendo como requisito as seguintes condições:

1. a empresa que atuar como agente de integração do estágio supervisionado deve manter contrato com o INSS; e

2. o contrato de estágio supervisionado deverá conter cláusula de confidencialidade e sigilo de informações preestabelecidos com a Administração Pública.

b) para viabilizar o acesso de estagiários aos sistemas corporativos, os gestores dos sistemas corporativos deverão criar perfis específicos e restritos às atividades do estagiário;

c) é vedada a concessão de perfis de acesso aos sistemas corporativos para estagiários com permissão de alteração das bases de dados institucionais;

d) o acesso será concedido mediante solicitação expressa de servidor do quadro do INSS, responsável pela supervisão do estágio, que deverá:

1. avaliar os riscos de utilização indevida de informações institucionais e as eventuais restrições referentes aos dias e horários para a realização dos acessos.

e) o acesso será precedido da assinatura do Termo de Confidencialidade e de Manutenção de Sigilo – TCMS, Anexo II, o qual deverá ser firmado pelo estagiário ou pelo estagiário e seu responsável legal, no caso de se tratar de estagiário menor de dezoito anos;

f) as solicitações de acesso à rede para estagiários devem ser procedidas por meio dos canais remotos de atendimento da Dataprev ou outro canal informado pela DTI, pela unidade de gestão de pessoas, pela chefia imediata do educando ou pelo responsável por sua supervisão;

g) os gestores de sistemas devem criar perfis diferenciados para estagiários de nível médio e nível superior;

h) o supervisor do estagiário deverá, periodicamente, orientá-lo quanto ao uso responsável e adequado do acesso aos sistemas corporativos;

i) o acesso do estagiário limitar-se-á à data final do contrato ou imediatamente cessado na hipótese de rescisão antecipada do estágio, cabendo ao supervisor do estagiário, em quaisquer dos casos, adotar as providências necessárias ao bloqueio do acesso, tão logo finde a contratação.

XV - credenciamento de usuários externos:

a) as credenciais de acesso para usuários externos devem ser emitidas tendo em vista o interesse do INSS, devidamente justificadas e previstas no convênio, acordo de cooperação técnica ou instrumento congênere;

b) as solicitações de emissão de credenciais de acesso à rede corporativa para usuários amparados por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica, contrato ou instrumento congênere devem:

1. ser feitas pelo gestor da unidade/área responsável pela gestão do instrumento legal; e

2. ser atendidas somente após validação das credenciais do gestor solicitante do Instituto, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700) ou outra base de dados indicada pela área responsável pela gestão de pessoas, a qual contenha informações referentes à estrutura organizacional do Instituto.

c) a emissão de credenciais de acesso à rede corporativa para prestadores de serviço terceirizados ou equiparados nas dependências do INSS, quando necessária, será provida unicamente pelo interesse do INSS. Para tanto, devem ser atendidos os seguintes requisitos:

1. a organização a qual o usuário é vinculado deve manter contrato, acordo de cooperação, convênio ou instrumento congênere vigente com o INSS;

2. instrumento deve conter cláusulas prevendo:

2.1. necessidade e justificativa para acesso à rede corporativa;

2.2. a confidencialidade e sigilo de informações preestabelecidas junto ao Instituto;

2.3. a obrigatoriedade da organização ou do ente contratado informar previamente ao representante legal do INSS, responsável pela gestão do contrato, quaisquer alterações em seu corpo de colaboradores que impacte na emissão/exclusão das contas de acesso;

2.4. a organização ou ente contratado também deverá manter com seus colaboradores Termo de Confidencialidade de Manutenção de Sigilo – TCMS; e

2.5. o gestor do contrato pelo INSS deve fundamentar a necessidade do acesso à rede para prestadores de serviço terceirizados ou equiparados, definindo os recursos que devem ser disponibilizados e eventuais restrições a dias e horas para realização do acesso à rede.

3. os TCMS deverão ser arquivados junto aos instrumentos assinados com o INSS e uma cópia ou link eletrônico deverá ser encaminhada ao Gestor do Contrato. O mesmo deve ocorrer para quaisquer alterações ocorridas na vigência dos contratos, acordos ou convênios;

3.1 caso os Termos sejam gerados de forma eletrônica, deverá ser disponibilizado o arquivo correspondente, atendendo aos requisitos necessários para garantia de integridade e disponibilidade de acesso, assim como os requisitos específicos previstos em contrato; e

4. a emissão de credenciais de acesso poderá ser feita pelo gestor do contrato, representante legal do INSS, ou pelo gestor da unidade responsável pela gestão do contrato, convênio, acordo de cooperação técnica ou instrumento congênere e serão atendidas somente após validação das credenciais do solicitante, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700) ou outra base de dados indicada pela área responsável pela gestão de pessoas, a qual contenha informações referentes à estrutura organizacional do Instituto.

d) o acesso aos prestadores de serviço vinculados à Central de Atendimento 135 se dará observando as seguintes condições:

1. a empresa deve manter contrato com o INSS;
2. o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;
3. a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade - TCMS;
4. o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte do INSS, definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;
5. os acessos deverão ser realizados única e exclusivamente por necessidade de serviço; e
6. o INSS pode disponibilizar, de forma restrita, às centrais 135 uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

e) nos casos referentes a prestadores de serviço vinculados à Ouvidoria-Geral da Previdência Social – OUGPS, o acesso se dará observando-se as seguintes condições:

1. a empresa deve manter Contrato direto com a Ouvidoria-Geral da Previdência Social;
2. o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;
3. a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade;
4. o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte da OUGPS, definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;
5. os acessos deverão ser realizados única e exclusivamente por necessidade de serviço; e
6. o INSS pode disponibilizar, de forma restrita, à OUGPS uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

f) o acesso à rede corporativa por servidores vinculados a órgãos de controle externo, envolvidos em ações de auditoria no âmbito do INSS, será concedido mediante apresentação da equipe de auditoria por meio de documento formal que conste:

1. dados necessários ao cadastro de usuários externos;
2. informações acerca dos objetivos dos trabalhos a serem executados;
3. os prazos envolvidos; e
4. informações complementares.

g) este tipo de acesso deverá observar as parcerias institucionalmente estabelecidas entres esses órgãos e o INSS no que tange à cobertura/previsão de acesso à rede corporativa do Instituto; e

h) o atendimento de pedido de solicitação de informações advindo de pessoas físicas ou jurídicas externas, respeitadas as restrições de acesso às informações previstas na Lei nº 12.527, de 18 de novembro de 2011, serão analisadas pela área designada para responder as demandas dos cidadãos por meio do e-SIC.

XVI - os procedimentos referentes às solicitações de inclusão, exclusão, inativação e suspensão de contas de acesso de usuários devem ser executados tendo como premissa a preservação dos registros para efeito de auditoria.

XVII - bloqueio administrativo:

a) os responsáveis pela Corregedoria-Geral do INSS, quando necessário, poderão solicitar a suspensão, bloqueio ou inativação imediata de contas de acesso de usuários que estiverem envolvidos em inquérito penal, em Processo Administrativo Disciplinar – PAD – ou em Sindicância, decorrente de infrações cometidas no exercício das atribuições do cargo;

b) estas solicitações deverão ser efetuadas mediante comunicação formal da Corregedoria-Geral para a Dataprev, ou outro canal informado pela DTI, a qual procederá a imediata implementação da mudança.

c) para disciplinar o disposto no item 5.17.1, é considerado envolvido em Processo Administrativo Disciplinar ou Sindicância, o usuário que estiver na seguinte situação:

1. afastado temporariamente do cargo ou função pública em razão de ato que se encontra sob apuração;

2. indiciado em processo administrativo disciplinar, por incursão nos incisos IX, XI, XII, XV, XVI e XVII do art. 117 e arts. 130 e 132 da Lei nº 8.112, de 11 de dezembro de 1990, ou cuja proposta pela Comissão Processante, no relatório final, seja pela aplicação de penalidade a partir de suspensão de trinta dias; e

3. submetido à prisão em flagrante, temporária ou preventiva decorrente do cometimento de infração no exercício das atribuições do cargo, enquanto estiver em apuração de inquérito policial ou pelo Ministério Público Federal.

d) o bloqueio de acessos, tratados nas situações do item 5.17.3, será efetivado no âmbito da ferramenta de gestão de acessos nas seguintes situações:

1. usuário afastado temporariamente do cargo ou função, enquanto durar o afastamento; e

XVIII - usuário indiciado nos termos do subitem 5.17.3.2, desta Política, até o efetivo cumprimento da penalidade porventura aplicada ou, em caso de não aplicação de penalidade, enquanto durar o processo.

Art. 6º Rede de Dados Corporativa:

I - infraestrutura de rede:

a) a infraestrutura de rede do INSS é disponibilizada para uso Institucional. Sendo assim, apenas equipamentos de propriedade do Instituto são autorizados e devem ser conectados à rede corporativa;

1. em casos excepcionais, a conexão de equipamentos particulares à rede corporativa deve ser feita em razão do interesse do Instituto e sob prévia autorização do responsável pela gestão da unidade em que o equipamento estiver localizado.

b) o INSS poderá disponibilizar o acesso à rede de dados corporativa por meio de tecnologia *Wireless* (sem fio). Para tanto os seguintes critérios deverão ser adotados:

1. os projetos que envolvam a utilização de pontos de acesso sem fio à rede corporativa no âmbito do Instituto deverão ser devidamente registrados e aprovados pela área responsável pela gestão de TIC do INSS;

2. os pontos de acesso à rede de dados corporativa sem fio poderão ser objeto de testes periódicos de penetração e de auditoria a critério da área responsável pela gestão de TIC no INSS;

3. as conexões à rede sem fio serão avaliadas pela área responsável pela gestão de TIC do INSS em relação aos requisitos de segurança e deverão atender ao princípio do privilégio mínimo;

4. a área responsável pela gestão de TIC do INSS poderá disponibilizar rede sem fio com regras específicas de acesso para visitantes nas diversas unidades do Instituto;

5. os dispositivos conectados à rede do INSS por meio de conexão sem fio deverão suportar configurações de criptografia estabelecidas pela área responsável pela gestão de TIC no âmbito do INSS; e

6. qualquer tecnologia de acesso sem fio implementada no INSS deverá suportar autenticação forte, com possibilidade de efetuar checagens em bancos de dados externos.

c) a área responsável pela gestão de TIC do INSS deve dispor de mecanismos automáticos que possibilitem:

1. a detecção e bloqueio de equipamentos externos conectados à rede corporativa; e
2. a identificação e rastreamento dos endereços IP de origem e destino, bem como os serviços utilizados na rede corporativa inclusive nos acessos remotos.

II - administração da rede corporativa:

a) a administração da rede do INSS é realizada pela Empresa de Tecnologia e Informações da Previdência Social - Dataprev;

1. os ativos e serviços que compõem a rede de dados corporativa são providos, gerenciados e operacionalizados pela empresa; e
2. os acessos à rede de dados corporativa realizados pelos usuários do INSS são gerenciados e monitorados pela Dataprev, contudo seguem as regras desta política.

b) quanto ao processo de geração de contas de serviço fica estabelecido que:

1. os critérios para a emissão de contas de serviços serão vinculados a um processo formal estabelecido pela área responsável pela gestão de TIC do INSS;
 2. a concessão de contas de serviços deve ser feita conforme a necessidade de uso de acordo com os critérios estabelecidos nesta Política de Controle de Acesso;
 3. o direito de acesso privilegiado, por meio de contas de serviços, associado a sistemas ou processos, deve ser identificado;
 4. deve ser viabilizada ferramenta que possibilite a gestão das contas de serviço de forma automatizada, possibilitando o registro e verificação de todos os privilégios concedidos;
 5. as contas de serviço fornecidas devem ser utilizadas exclusivamente para os fins aos quais foram concedidas;
 6. as contas de serviço emitidas devem ser revalidadas periodicamente com base na função exercida e na área de atuação do servidor;
- e
7. as contas de serviço com credenciais de acesso de uso compartilhado devem ter suas senhas alteradas periodicamente, conforme estabelecido nesta Política de Controle de Acesso Lógico, ou sempre que ocorrerem mudanças no grupo de usuários que utilizam as mesmas.

C) é vedado o uso da rede corporativa para:

1. acesso por meio de equipamento não homologado ou não autorizado pelo INSS;
2. fazer download, instalar e/ou utilizar sistemas ou aplicativos não homologados pela área responsável pela gestão de TIC do INSS nos equipamentos de propriedade do Instituto;
3. a utilização de softwares particulares em equipamentos do INSS sem autorização expressa;
4. a instalação e conexão de equipamentos particulares à rede corporativa do Instituto sem a prévia autorização do gestor responsável pela unidade ou da área responsável pela gestão de TIC do INSS;
5. o uso dos recursos de rede para fins particulares ou de terceiros alheios aos interesses do INSS, em especial quando tal procedimento prejudique o tráfego da rede de dados;
6. o uso para fins de divulgação ou distribuição de material que não possua vínculo com as atividades desenvolvidas pelo Instituto;
7. a instalação ou utilização de ferramentas de monitoramento de rede sem a anuência e autorização expressa da área responsável pela gestão de TIC no Instituto;
8. a instalação de dispositivos de comunicação ou de compartilhamento de dados sem fio, particulares, à rede corporativa do Instituto, sem autorização expressa da área responsável pela gestão de TIC do INSS; e

9. burlar as regras a internet configuradas em proxy ou ferramenta similar de gerenciamento de conteúdo web;

d) cabe a área responsável pela gestão de TIC no âmbito do INSS definir os aspectos relacionados à plataforma tecnológica, gestão operacional, forma de autenticação e sustentação do domínio de rede do INSS.

Art. 7º Gestão do Acesso aos Sistemas Corporativos:

I - sistemas legados:

- a) as regras estabelecidas nesta norma devem ser aplicadas, guardando-se as devidas limitações tecnológicas, aos sistemas legados; e
- b) o controle de acesso aos sistemas legados é efetuado por base própria.

II - sistemas de apoio à administração:

- a) os ambientes de hospedagem desses sistemas são suportados por terceiros;
- b) o ambiente deverá ser gerenciado e operacionalizado pela área de gestão de TIC do INSS;
- c) o acesso pelos usuários a esses sistemas deverá ser autenticado pelo serviço de diretório utilizado pelo Instituto; e
- d) as regras de hospedagem de sistemas serão definidas, em ato próprio, pela área de gestão de TIC do INSS.

III - armazenamento de registros logs:

a) as áreas responsáveis pela gestão de sistemas corporativos e demais aplicações devem definir, em conjunto com a área responsável pela gestão de TIC, a temporalidade de registro dos logs de acesso e transações, e quais registros devem ser armazenados por um período maior que o estipulado no item 8.1 desta Política; e

b) o INSS poderá alterar a temporalidade destes dados em norma específica.

IV - administração da ferramenta de gestão de acesso:

a) com o objetivo de operacionalizar a gestão dos acessos aos sistemas corporativos no âmbito do INSS, serão criados os seguintes papéis:

1. administrador de sistema INSS: Servidor do quadro, lotado na área responsável pela gestão de TIC, designado por meio de Portaria do Diretor de Tecnologia da Informação e Inovação, a ser publicada em Boletim de Serviço – BS, responsável pela administração da ferramenta de gestão de acesso aos sistemas corporativos no âmbito do INSS;

2. gestor de sistema: Servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em Boletim de Serviço, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedoria-Geral e Procuradoria Federal Especializada. É responsável pela implementação de sistemas corporativos no âmbito do INSS;

3. gestor de acesso central: Servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em Boletim de Serviço, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedoria-Geral e Procuradoria Federal Especializada. É responsável pela manutenção dos perfis de gestão dos usuários nas áreas que compõem a Administração Central e, quando necessário, dos gestores de acesso das Superintendências Regionais;

4. gestor de acesso interno: Servidor do quadro, lotado na Administração Central, Superintendência Regional, Gerência Executivo, Agência da Previdência Social, indicado pelo Gestor de Acesso Central ou por um Gestor de Acesso, responsável pela atribuição do perfil de acesso e de gestão dos usuários no INSS; e

5. gestor de acesso externo: Pessoa formalmente indicada, por documento previsto no instrumento legal que firmou a parceria ou por meio de Ofício de lavra do representante máximo de uma Entidade Externa, responsável pelo cadastro de usuários externos e a gestão dos acessos aos sistemas corporativos do Instituto.

b) a indicação e processo de substituição dos responsáveis pela gestão dos acessos aos sistemas corporativos no âmbito do INSS poderá ser procedida das seguintes formas:

- 1. a autoridade responsável pela indicação do gestor de acessos pode indicar opcionalmente o substituto;

2. o próprio gestor de acessos pode designar, a qualquer momento, por meio da ferramenta de gestão de acessos um substituto; ou

3. quando não houver um gestor responsável, ou substituto, por uma unidade devidamente designado, a gestão dos usuários será transferida, preferencialmente de forma automática, para o responsável pela área da abrangência daquela unidade e assim subsequentemente; e

4. o Gestor de Acesso é corresponsável com os perfis de gestão ou acesso que ele atribuir aos usuários.

c) ao usuário interno cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Política de Controle de Acesso Lógico e suas normas complementares;

2. solicitar, ao Gestor de Acesso responsável pela gestão da unidade de lotação a qual é vinculado, a suspensão do seu perfil de acesso nos períodos de afastamento do serviço por mais de trinta dias consecutivos;

3. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e

4. ter conhecimento e estar de acordo com o disposto nesta Política.

d) ao usuário externo cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Política de Controle de Acesso Lógico;

2. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e

3. ter conhecimento e estar de acordo com o disposto nesta Política.

e) ao administrador do sistema INSS cabe:

1. criar os sistemas e subsistemas, devidamente homologados pela área de negócio responsável, no ambiente de produção, por meio de ferramenta de gestão de acesso;

2. mediante apresentação de Portaria de designação para Gestores de Acesso Central, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores quanto à atribuição dos perfis de gestão; e

3. mediante apresentação de Portaria de designação para Gestores de Sistema, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores acerca do processo de implementação dos sistemas corporativos no âmbito do INSS.

f) ao gestor de sistema cabe:

1. efetuar os procedimentos de importação, inclusão, alteração e exclusão de papéis e permissões nos sistemas corporativos em ambiente de produção; e

2. atuar, em conjunto com o Administrador do Sistema INSS e a Dataprev, no planejamento e execução do processo de implementação dos sistemas corporativos dos quais for designado responsável.

g) ao gestor de acesso central cabe:

1. efetuar o credenciamento, suspensão ou exclusão de perfis de gestão dos sistemas corporativos aos Gestores de Acesso na Administração Central e, quando necessário, dos Gestores de Acesso da Superintendência Regional, Gerência Executiva, Agência da Previdência Social e demais usuários de sua abrangência; e

2. orientar os usuários de sua abrangência e os gestores da Administração Central e Superintendências Regionais, Gerências Executivas e Agências da Previdência Social acerca das regras para o acesso aos sistemas corporativos do INSS.

h) ao gestor de acesso interno cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários da Administração Central, Superintendência Regional, Gerência Executiva, Agência da Previdência Social;

2. atribuir, alterar ou excluir os perfis de acesso aos usuários da Administração Central, Superintendência Regional, Gerência Executiva, Agência da Previdência Social; e

3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS.

i) ao gestor de acesso externo cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários do seu Órgão/Entidade;

2. atribuir, alterar ou excluir os perfis de acesso aos usuários do seu Órgão/Entidade; e

3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS.

V - configura-se mau uso, sujeito a responsabilidade penal, civil e disciplinar:

a) a divulgação, sem autorização expressa da chefia imediata ou do gestor de acesso de sua abrangência, de informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS;

b) acessar sistemas corporativos sem autorização prévia, de acordo com os requisitos estabelecidos nesta Política;

c) utilizar-se das informações obtidas por meio de acesso concedido em desacordo com os procedimentos dispostos nesta Política e demais normas vigentes na Administração Pública Federal;

d) compartilhar ou fazer uso das credenciais de acesso, aos sistemas corporativos, de outros usuários;

e) a instalação de sistemas corporativos em equipamentos particulares; e

f) em casos excepcionais, a área responsável pela gestão de TIC do INSS, mediante ato formal, poderá autorizar o contido no Art.8º, III.

Art. 8º Disposições Gerais:

I - todo acesso à rede de dados e aos sistemas corporativos deve ser registrado e monitorado de modo que permita a rastreabilidade, a identificação e o bloqueio de usuários e equipamentos não autorizados. Estas informações devem ser armazenadas por um período de, no mínimo, 30 (trinta) meses;

II - as ocorrências de mau uso do acesso aos recursos disponíveis na rede e sistemas corporativos não previstas nesta norma e os casos omissos serão encaminhados para a área responsável pela gestão de TIC no âmbito do INSS para análise e pronunciamento;

III - identificada irregularidade de mau uso dos recursos de rede poderá ocorrer:

a) o bloqueio preventivo do acesso pela DTI, o encaminhamento de dossiê com as informações para a Corregedoria-Geral do INSS ou Corregedorias Regionais, nas suas áreas de abrangências, a fim de que seja realizada a análise no âmbito disciplinar; e

b) ressalta-se que o descumprimento dessa política poderá resultar em sanções administrativas, civis e criminais.

IV - esta norma deve ser revisada num período máximo de três anos.

ANEXO II

PORTARIA Nº /PRES/INSS, DE DE 2020

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF: _____, identidade _____, expedida pelo _____, em _____, e lotado no(a) _____ do Instituto Nacional do Seguro Social – INSS, DECLARO, sob pena das sanções cabíveis nos termos da Política de Segurança da Informação e Comunicações - POSIC do INSS que assumo a responsabilidade por:

I - tratar o(s) ativo(s) de informação como patrimônio do Instituto Nacional do Seguro Social;

II - utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do INSS;

III - contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, que Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;

IV - utilizar as credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do INSS;

V - responder, perante o INSS, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

_____, ____ de _____ de _____

Assinatura do usuário

Nome do usuário:	Unidade de Lotação:
Nome da Autoridade Responsável pela Autorização do Acesso:	

Assinatura e Carimbo do Responsável pela Autorização de Acesso



INSTITUTO NACIONAL DO SEGURO SOCIAL
MINUTA DE RESOLUÇÃO

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 4/CEGOV/INSS, DE
DE DE 2020

Institui a Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR do Instituto Nacional do Seguro Social.

O **COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS**, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída a Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR do INSS.

Art. 2º Os Anexos a esta Portaria serão publicados em Boletim de Serviço.

Art. 3º Esta Portaria complementa Política de Segurança da Informação e Comunicações POSIC-INSS vigente.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

MÁRCIA ELIZA DE SOUZA
Diretora de Benefícios

CLÓVIS DE CASTRO JÚNIOR
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

GUSTAVO PAULO LEITE DE SOUZA
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação

ANEXO I

RESOLUÇÃO Nº 4/CEGOV/INSS, DE DE DE 2020

EQUIPE DE TRATAMENTO DE INCIDENTES DE REDES COMPUTACIONAIS - ETIR

Art. 1º Para os efeitos desta norma ficam estabelecidos os seguintes conceitos e definições:

I - agente responsável: Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

II - artefato malicioso: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

III - comunidade ou Público Alvo: é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

IV - CTIR GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI;

V - equipe de tratamento e resposta a incidentes em redes computacionais – ETIR: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

VI - incidente de segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VII - serviço: é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

VIII - tratamento de Incidentes de Segurança em Redes Computacionais: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

IX - vulnerabilidade: é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados; e

X - usuário: pessoas que fazem uso de serviços de TI e sistemas de informação de propriedade do INSS, independente do cargo ocupado (contratados, consultores, conselheiros, servidores, temporários e etc).

Art. 2º Esta norma tem a missão de:

Parágrafo único. Agir proativamente, receber, analisar, monitorar, coordenar e propor respostas a notificações e atividades relacionadas a incidentes de segurança da informação e comunicações no âmbito do Instituto.

Art. 3º Esta norma tem como público alvo:

I - a abrangência das atividades pertinentes à ETIR-INSS inclui os usuários dos serviços de Tecnologia da Informação e Comunicações - TIC e os sistemas de informação do INSS;

II - as atividades pertinentes à ETIR-INSS serão realizadas com intercâmbio de informações e em cooperação com as seguintes instâncias:

a) o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR GOV;

b) a Comissão de Resposta e Tratamento de Incidentes em Redes Computacionais –CTIR, da Empresa de Tecnologia e Informações da Previdência Social - Dataprev;

c) equipes de tratamento de incidentes de redes computacionais dos demais órgãos, entidades e empresas, públicas ou privadas, que tenham contratos, acordos, convênios ou instrumentos congêneres com o INSS; e

d) o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República – GSI/PR.

Art. 4º a implementação e o funcionamento da ETIR-INSS seguirão a metodologia definida na Norma Complementar Nº 05 à luz da Instrução Normativa Nº 01 do Gabinete de Segurança Institucional da Presidência da República, de 04 de agosto de 2009, conforme definido a seguir:

I - o modelo de implementação no qual a ETIR-INSS se baseia é o “Modelo 1 – Utilizando a equipe de Tecnologia da Informação”, definido na Norma Complementar Nº 05;

II - a equipe será composta por profissionais da área de Tecnologia da Informação, lotados na Diretoria de Tecnologia da Informação e Inovação – DTI, sem prejuízo de suas atribuições típicas do cargo, com experiência e conhecimentos técnicos compatíveis com a importância da missão da ETIR-INSS;

III - a equipe será composta por servidores públicos efetivos;

IV - a ETIR-INSS ficará vinculada tecnicamente à Coordenação de Infraestrutura e Operações – CGIN, da Diretoria de Tecnologia da Informação e Inovação - DTI; e

V - o Coordenador da ETIR-INSS será o Gestor de Segurança da Informação e Comunicações, conforme definido na Política de Segurança da Informação e Comunicações – POSIC-INSS.

Art. 5º A ETIR-INSS será composta por membros:

I - permanentes: que efetivamente atuarão em todos os incidentes registrados; e

II - Colaboradores: que atuarão, de forma esporádica, no tratamento de incidentes relacionados às suas áreas de atuação.

III - sendo assim, a ETIR-INSS será formada pelos seguintes servidores:

Papel	Nome	Matrícula	Setor
Permanente	Roberto Rufino da Costa	1.057.683	Serviço de Segurança em TIC
Permanente	Nelson Antonio Pimentel Jacinto	1.095.044	Serviço de Segurança em TIC
Colaborador	Cristiano Santos de Souza	2.156.073	Divisão de Infraestrutura e Operações
Colaborador	Lourival de Sousa	2.262.639	Divisão de Infraestrutura e Operações
Colaborador	Jair Rodrigues Fernandes	2.276.407	Divisão de Infraestrutura e Operações
Colaborador	Rodrigo Gomes Rodrigues	2.135.059	Divisão de Arquitetura e Soluções

Art. 6º Quanto autonomia da ETIR-INSS:

I - terá autonomia limitada para o tratamento de incidentes de Segurança da Informação, devendo implementar ações que possam impactar outras áreas do Instituto somente com anuência do Diretor de Tecnologia da Informação e Inovação e do gestor responsável pela área/sistema afetada; e

II - poderá, ainda, gerar relatórios técnicos sugerindo a adoção de medidas para resolução de incidentes.

Art. 7º A ETIR-INSS fornecerá o serviço de Tratamento de Incidentes de Segurança em Redes Computacionais:

I - este serviço compreende basicamente as seguintes ações:

a) recepção: receber solicitações e alertas diversos. Para tanto o Instituto disponibilizará como canal de comunicação a caixa postal etir@inss.gov.br;

b) filtrar: todo conteúdo direcionado para a ETIR deve ser verificado, a partir desta análise deve ser tratado pela equipe ou, não se tratando de um incidente de segurança em redes computacionais, encaminhado para a área competente;

c) catalogar: os incidentes devem ser catalogados em ferramenta a ser indicada pela DTI, com nível de acesso restrito;

d) classificar: os incidentes devem ser classificados quanto ao nível de severidade e impacto;

e) tratar o incidente: indicar o tratamento do incidente com medidas corretivas e formas de se evitar que ocorra novamente;

f) responder: as solicitações e alertas encaminhados para a ETIR devem ser devidamente respondidos; e

g) monitorar: monitorar a aplicação do tratamento dos incidentes indicados.

II - a ETIR deve analisar os incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências; e

III - o detalhamento dos serviços prestados pela ETIR-INSS deve ser publicado em página específica da Intranet do Instituto no prazo de 30 dias a partir da publicação desta portaria.



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 5/CEGOV/INSS, DE DE DE 2020

Disciplina o uso da Internet no INSS, regulamenta e define o conjunto Internet, competências e conteúdo de acesso para cada perfil.

O **COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS**, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída, nos termos do Anexo I desta Portaria, norma que estabelece critérios para uso da Internet no âmbito do Instituto Nacional do Seguro Social - INSS.

Art. 2º Os Anexos a esta Portaria serão publicados em Boletim de Serviço.

Art. 3º Esta Portaria complementa a Política de Segurança da Informação e Comunicações POSIC-INSS vigente.

Art. 4º Revoga-se a Portaria MDS/DTP/INSS nº XXX/2005.

Art. 5º Esta Portaria entra em vigor na data de sua publicação.

ANEXO I

RESOLUÇÃO Nº 5/CEGOV/INSS, DE DE DE 2020

NORMA DE USO DA INTERNET

Art. 1º Esta norma se aplica a todos os servidores e colaboradores, vinculados direta ou indiretamente ao INSS, bem como a servidores e empregados de entidades e órgãos da Administração Pública ou privadas que necessitem ou estejam autorizados a acessar a Internet a partir da rede corporativa do Instituto.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União – AGU que atuarem na consultoria e no assessoramento jurídico, e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta norma, ficam estabelecidos os seguintes conceitos e definições:

I - internet: é a rede mundial que interliga computadores de diferentes tipos e dimensões e permite a comunicação entre pessoas e organizações, independentemente da localização geográfica;

II - intranet: é a rede de computadores administrada pelo INSS, que utiliza os mesmos serviços e tecnologias disponíveis na rede mundial, podendo ser definida como um tipo de Internet Local do Instituto;

III - sítio: um conjunto de informações ou serviços disponíveis na Internet ou na Intranet, organizados em páginas eletrônicas e acessíveis por meio de endereços que identificam, de forma padronizada, sua origem e conteúdo;

usuários;

IV - perfil de acesso: atributo que estabelece as categorias de sítios acessíveis e tipos de arquivos que podem ser recebidos ou transmitidos pelos

Internet;

V - usuário: Servidores, estagiários, terceirizados, contratados e colaboradores, que na execução de suas atividades necessitem de acesso à

de abrangência;

VI - autorizador: ocupantes de cargos que serão responsáveis pela autorização da concessão de perfis de acesso para usuários finais de sua área

válidos para acessos externos, cabe ao proxy enviar a solicitação do endereço local para o servidor, traduzindo e repassando-a para o seu computador;

VII - proxy: desempenha a função de conexão do computador (local) à rede externa (Internet). Como os endereços locais do computador não são

por meio de uma rede pública, como a Internet; e

VIII - VPN: Trata-se de uma rede privada construída sobre a infraestrutura de uma rede pública. Essa é uma forma de conectar dois computadores

Art. 3º Essa norma tem como diretrizes:

I - o acesso à Internet disponibilizado pelo Instituto Nacional do Seguro Social aos usuários deve ser utilizado exclusivamente em razão de trabalho, cumprindo os procedimentos dispostos nesta norma;

II - os recursos disponibilizados pelo Instituto, não poderão ser usados para quaisquer propósitos que sejam ilegais ou proibidos, de modo a danificar, desativar, sobrecarregar ou prejudicar qualquer área, serviço ou conteúdo, ou interferir no uso e execução das atividades laborais de outros usuários;

III - o volume de tráfego de Internet e os endereços *web* visitados poderão ser monitorados, visando assegurar o cumprimento desta norma; e

IV - o acesso à Internet para propósitos particulares ou estranhos às atividades do INSS poderá ser bloqueado, sem prévia comunicação ao usuário e sem prejuízo das demais sanções aplicáveis.

Art. 4º Quando aos Perfis de Acesso:

I - o acesso aos sítios da Internet para todos os usuários será realizado mediante a atribuição de perfis de acesso;

II - o processo de solicitação e autorização de perfil de acesso à Internet do INSS compreenderá os seguintes perfis:

a) Perfil 1 - Perfil Restrito, deve ser inicialmente atribuído para usuários com maior restrição de acesso à internet, permitido acessar somente sítios governamentais, instituições bancárias e sítios considerados de interesse do INSS;

b) Perfil 2 - Perfil Básico, deve ser inicialmente atribuído para estagiários, recepcionistas e usuários externos. O usuário poderá acessar todos os sítios permitidos pelo Perfil 1, sítios de provedores de e-mail pessoal e instituições de ensino;

c) Perfil 3 - Perfil Padrão, para os servidores do quadro do Instituto. O usuário poderá acessar a todos sítios da internet sem a veiculação de material em áudio e vídeo; e

d) Perfil 4 - Perfil Avançado, deve ser atribuído preferencialmente para servidores do quadro do Instituto e estagiários que desempenham funções relacionadas à Comunicação Social, Desenvolvimento de Pessoas e gestores, respeitado o princípio da necessidade de conhecer, designados pelos Autorizadores deste perfil. O usuário poderá acessar todos os sítios da Internet, incluindo sítios que veiculam material em áudio e vídeo (*streaming*), sítios de compartilhamento de vídeos, blogs e redes sociais.

III - o perfil concedido a agentes externos é de caráter temporário, com validade equivalente à vigência do trabalho a ser executado;

IV - o processo de alterações, bloqueios, liberações e categorizações de sítios, assim como a criação e/ou alterações de perfis de acesso descritos nesta norma, quando necessários, serão definidos pela Diretoria de Tecnologia da Informação e Inovação – DTI, e publicado no Portal do INSS na Intranet; e

V - os novos usuários que não tiverem um perfil de acesso atribuído, devem ser direcionados para uma página da intranet contendo orientações e normas relacionadas ao acesso à internet no INSS, entre outras informações definidas pela DTI.

Art. 5º Acesso de Usuários Externos:

I - quanto ao acesso de servidores ou funcionários públicos externos:

a) o acesso à Intranet e Internet a partir da rede de dados corporativa, nas dependências do INSS, aos demais órgãos da Administração Pública Direta e Indireta, de qualquer das esferas de governo, será concedido exclusivamente para servidores e empregados públicos, efetivos ou ocupantes de cargo em comissão;

b) os acessos dos usuários externos das entidades que compõem o Poder Público serão concedidos mediante o estabelecimento de acordos ou convênios específicos firmados com o INSS;

c) o gestor ou Coordenador-Geral da área responsável pelo convênio, contrato, ACT ou instrumento congênere, assumirá o papel de Autorizador do serviço de acesso à internet para usuários externos e deverá fundamentar as solicitações com base no instrumento; e

d) poderão ser concedidos acessos temporários para auditores de controle interno e externo, vinculados à Controladoria-Geral da União – CGU ou do Tribunal de Contas da União – TCU, no uso de suas atribuições.

II - quanto ao acesso de terceirizados:

a) o acesso à Internet por terceirizados deve ser provido pela empresa contratada;

b) em caráter de exceção, será concedido o acesso aos terceirizados a partir da infraestrutura de rede do INSS, desde que preenchidos os seguintes requisitos:

1. o contrato de prestação de serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

2. a empresa contratada deverá manter com seus funcionários Termo de Confidencialidade;

3. o contrato deve prever a necessidade de acesso à internet a partir das dependências do Instituto; e

4. o Autorizador, que para estes fins será o gestor do contrato ou o responsável pela área requisitante do serviço, deverá fundamentar as necessidades de acesso do contratado, definindo os recursos que devem ser disponibilizados, endereços da Intranet e Internet necessários para o desenvolvimento das atividades, bem como eventuais restrições a dias e horários para realização do acesso.

III - quanto ao acesso de visitantes:

a) a conexão de equipamentos pessoais à rede do Instituto, quando necessária e motivada pelo interesse da Administração, deve ser previamente autorizada pelo gestor da unidade onde o equipamento será utilizado;

b) só será permitida a utilização da rede local por equipamentos que atendam a todos os requisitos estabelecidos pela DTI; e

c) o acesso se dará, exclusivamente, à Internet, sendo vedado o acesso ao conteúdo disponibilizado na intranet.

Art. 6º A todos os perfis de acesso descritos nesta norma aplicam-se as restrições de acesso a sítios que:

I - contenham material pornográfico ou obsceno;

II - contenham material ilegal;

III - disponibilizem jogos, inclusive os da Internet (online);

IV - contenham material impróprio, ofensivo, preconceituoso ou discriminatório, que façam apologia à violência, ao terrorismo e às drogas; e

V - contenha e/ou divulgue conteúdo de violação de direito autoral (pirataria) e/ou execução de quaisquer tipos ou formas de fraudes.

Art. 7º Quanto ao processo de atribuição de acesso à Internet:

I - a atribuição dos perfis de acesso à Internet serão feitas pelos Autorizadores, de forma fundamentada respeitando o princípio da necessidade de conhecer, de acordo com a tabela abaixo:

Perfil	Autorizador
Perfil 1, 2 e 3	Gerente de APS, Gerente Executivo, Superintendentes Regionais, Procuradores Regionais, Coordenadores-Gerais, Superintendentes Regionais, Presidente do INSS, Auditor-Geral, Coordenadores-Gerais, Corregedoria-Geral, Procurador-Chefe da PFE-INSS, Diretores, Gestor ou chefe da área responsável pelo Contrato ou ato administrativo similar no âmbito do INSS.
Perfil 4	Chefes de Assessoria de Comunicação Social nas Superintendências Regionais, Assessor de Comunicação Social (Administração Central) e Presidente do INSS.

II - nos casos de novos usuários de rede (LDAP), criados por meio de registro de chamado técnico, quando o solicitante não indicar o perfil de acesso à internet, será atribuído o Perfil 1;

III - para proceder a alteração do perfil de acesso, os usuários deverão preencher “Formulário de Acesso à Internet” (Anexo II) e providenciar a assinatura pelo Autorizador do acesso; e

IV - ao registrar a solicitação, deve-se anexar o Formulário de Solicitação de Acesso à Internet devidamente preenchido e assinado (pelo solicitante e Autorizador), conforme documento nato digital ou digitalizado no formato PDF.

Art. 8º A solicitação para perfis de acesso em caráter temporário devem indicar no Formulário de Solicitação de Acesso à Internet, a motivação da necessidade e a data de expiração do acesso.

Art. 9º Responsabilidades:

I - o usuário deve:

- a) preencher os requisitos e termos estabelecidos nesta norma;
- b) estar devidamente autorizado a utilizar a Internet nas formas estabelecidas nesta norma;
- c) fazer uso da Internet de forma responsável e segura, utilizando o acesso exclusivamente em razão de trabalho, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal; e
- d) impedir a divulgação e compartilhamento das chaves de segurança atribuídas, que são pessoais e intransferíveis.

II - o autorizador deve:

- a) conceder os perfis de acesso à internet rigorosamente de acordo com as atribuições dos usuários de sua abrangência, observando os normativos do INSS;
- b) verificar periodicamente o uso dos acessos concedidos e, sempre que necessário, solicitar alteração dos perfis de acesso dos usuários de sua abrangência; e
- c) reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à equipe de tratamento de incidentes de rede do INSS.

III - a área responsável pela gestão de TIC no INSS deve:

- a) monitorar os acessos à internet e sua utilização de acordo com as diretrizes estabelecidas nesta norma; e
- b) identificar os casos de mau uso da Internet e adotar uma ou mais das seguintes providências:
 - 1. alertar ao usuário, responsável pelo acesso, e ao Autorizador, responsável pela concessão, acerca do uso indevido da internet;
 - 2. nos casos de reincidência, solicitar a revogação do acesso à internet concedido ao usuário; e
 - 3. encaminhar a documentação que comprova a má utilização do acesso concedido para Corregedoria do INSS, para análise e adoção das medidas cabíveis.

Art. 10º As seguintes práticas configuram-se como uso indevido da internet:

I - acessar a internet disponibilizada pelo Instituto sem estar devidamente autorizado, conforme estabelecido nesta norma;

II - não manifestar concordância com as regras estabelecidas nesta norma e nas demais aplicáveis;

III - fazer uso dos recursos de Internet disponibilizado pelo Instituto para fins alheios ao trabalho, em discordância com os procedimentos dispostos nesta norma, sem prejuízo de demais normatizações vigentes na Administração Pública Federal;

IV - utilizar os serviços extrapolando os privilégios do perfil de acesso que lhe foi designado;

V - divulgação e compartilhamento das chaves de segurança, que são pessoais e intransferíveis, permitindo a utilização por terceiros do perfil que lhe foi atribuído;

VI - praticar atos de comercialização de produtos e serviços, em proveito próprio ou de terceiros, que não atendam os interesses do INSS;

VII - utilizar recursos ou dispositivos para acesso a computadores ou redes externas ao Instituto, com o objetivo de obter informações não autorizadas ou provocar a interrupção de serviços de rede;

VIII - utilizar modem ou dispositivo de rede que interligue a rede interna do INSS a outras redes ou à Internet;

IX - a exposição, o armazenamento, a distribuição, a edição, a gravação e o compartilhamento, através do uso dos recursos computacionais e de comunicação do INSS, de arquivos estranhos às atividades do Instituto e não autorizados pela chefia imediata;

X - realizar qualquer atividade que apoie ou facilite os vazamentos de dados;

XI - baixar arquivos ou programas da Internet que contrariem as diretrizes da Política de Segurança da Informação e Comunicações – POSIC vigente; e

XII - utilizar *proxy* não disponibilizado pelo INSS.

Art. 11 O acesso à Internet é passível de registro e monitoração, incluindo quaisquer dados transmitidos pela rede do INSS.

Art. 12 Disposições Gerais:

I - em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a ETIR deverá ser imediatamente acionada, para tomar as providências necessárias a fim de sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação do INSS;

II - as ocorrências de mau uso do acesso à internet não previstas nesta norma, assim como os casos de dúvidas em relação à aplicação das disposições aqui estabelecidas, devem ser encaminhadas à DTI para registro, análise e avaliação da necessidade de alterações de acordo com o processo de governança em vigência no Instituto;

III - o descumprimento desta norma, poderá acarretar ao usuário as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei, responsabilidade administrativa, civil e criminal; e

IV - esta norma deve ser atualizada periodicamente, não excedendo o prazo máximo de 3 anos.



INSTITUTO NACIONAL DO SEGURO SOCIAL
COMITÊ ESTRATÉGICO DE GOVERNANÇA

REGISTRO DE REUNIÃO

ATA DE REUNIÃO

Reunião:	1ª Reunião Ordinária do Comitê Estratégico de Governança do INSS em 2020.
Data/hora:	17/02/2020, das 10h30 às 13h00
Local:	Sala de Reuniões da Presidência do INSS
Processo SEI:	35014.012037/2020-68

1. Informes

• **Estruturação do Sistema de Governança do INSS:**

Foi apresentada a estruturação do Sistema de Governança do INSS, sua composição, e as principais atribuições do CEGOV e dos comitês temáticos de apoio à Governança. Foi também apresentada a forma de funcionamento do CEGOV, qual seja:

- Reuniões mensais, a ser realizada sempre na última sexta-feira de cada mês, no período da manhã;
- Pautas, atas e resoluções dos comitês registradas no SEI;
- Pauta deliberativa e informativa, definida e divulgada 3 dias úteis antes das reuniões;
- Obrigatoriedade de que temas de deliberação sejam propostos antecipadamente e acompanhados de nota técnica que subsidie a tomada de decisão;
- Atas e resoluções assinadas digitalmente pelos membros do Comitê, e divulgadas no site do INSS.

Na oportunidade, o Presidente solicitou que se avalie a atribuição do CEGOV que trata do estabelecimento de diretrizes gerais para a integração das bases de dados, considerando o disposto no Decreto nº 10.047, de 9 de outubro de 2019.

2. Deliberações

DELIBERAÇÃO 1: Vídeo sobre Governança

Decisão

Foi aprovada a veiculação do vídeo informativo sobre o Sistema de Governança do INSS para todos os servidores do Instituto, após a substituição do termo "Resultados", no minuto 3:13, por frase que vincule os resultados ao cumprimento do plano de ações estratégicas.

Votos a favor

Decidido por unanimidade.

Votos contrários

Não houve.

DELIBERAÇÃO 2: Criação de seção no site do INSS para publicação de informações sobre as reuniões e deliberações do CEGOV

Decisão	
Foi aprovada a criação da seção "Governança" no site do INSS, no menu lateral esquerdo "Informação e Transparência". Comporão essa seção informações sobre: Sistema de Governança; Comitê Estratégico de Governança (Pautas e atas de reunião; Resoluções); Planejamento Estratégico; Planejamento de TI; Programa de Integridade Gestão de Riscos; Comissão de Ética. As subseções serão criadas progressivamente, a medida em que se tenha material relevante para publicação.	
Votos a favor	Votos contrários
Decidido por unanimidade.	Não houve.

DELIBERAÇÃO 3: Aprovação da Política de Segurança da Informação e Comunicações (POSIC)

Decisão	
Foi decido que a POSIC será revisada pelos membros do CEGOV e aprovada eletronicamente, por meio do SEI, após realização dos ajustes propostos na reunião, quais sejam: - Alterar o Anexo para que seja formatado em conformidade com o Manual de Redação da Presidência da República (Determinação do Art. 58 do Decreto nº 9.191/2017); - Verificar se é necessário manter o item 5.8.3. do Anexo e, se necessário, ajustar redação final com a AUDGER; - Revisar as definições referentes a dado, a informação e a ativos de informação, levando em consideração as definições trazidas pela nº Lei 13.709/2018 (LGPD), pela Lei nº 12.527/2011 (Lei de Acesso à Informação) e pelo Decreto nº 10.046/2019 (Decreto de Compartilhamento de Dados); - Incluir definições de termos que tratem da responsabilidade pela gestão das informações; - Incluir menção ao Comitê Temático de Gestão da Informação como responsável pela aprovação de procedimentos e de normas internas que orientem o compartilhamento de dados sob gestão do INSS e pela aprovação da categorização dos níveis de compartilhamento de dados com outras entidades públicas (federais ou de outras esferas e poderes) da sociedade civil (Vide atribuições do CTGI, no Art. 6º do Anexo da Portaria nº 3.213/PRES/INSS/2019). Os ajustes serão realizadas pela DTI, até o dia 19/02/2020, e enviados à Secretaria-Executiva do CEGOV para circularização com os membros do comitê. Os membros do CEGOV se pronunciarão até o dia 21/02/2020. O texto ajustado será enviada à PFE-INSS para análise, conforme preceitua a Resolução nº 708/PRES/INSS/2019.	
Votos a favor	Votos contrários
Decidido por unanimidade.	Não houve.

DELIBERAÇÃO 4: Aprovação da Política de Controle de Acesso Lógico

Decisão	
Foi decido que a Política de Controle de Acesso Lógico será revisada pelos membros do CEGOV e aprovada eletronicamente, por meio do SEI, após realização dos ajustes propostos na reunião, quais sejam: Alterar o Anexo para que seja formatado em conformidade com o Manual de Redação da Presidência da República (Determinação do Art. 58 do Decreto nº 9.191/2017) e com ato próprio do INSS que versa sobre a estrutura dos atos normativos, a saber: Resolução nº 708/PRES/INSS, de 6 de novembro de 2019;	

- Alterar o Art. 1º da minuta de resolução para "Fica instituída a Norma de Controle de Acesso Lógico do INSS";
- Compatibilizar conceitos e definições do Anexo, conforme alterações sugeridas na POSIC;
- Retirar itens 2.1.28, 2.1.29 e 2.1.30 do Anexo, por não se tratar de conceitos e definições;
- Alterar periodicidade prevista no item 4.1.2, que deve ser semanal;
- Mencionar a instituição de norma que definirá a transição dos acessos a sistemas do INSS por servidores que atuam na perícia médica e na PFE.

Os ajustes serão realizadas pela DTI, até o dia 19/02/2020, e enviados à Secretaria-Executiva do CEGOV para circularização com os membros do comitê. Os membros do CEGOV se pronunciarão até o dia 21/02/2020. O texto ajustado será enviada à PFE-INSS para análise, conforme preceitua a Resolução nº 708/PRES/INSS/2019.

Votos a favor	Votos contrários
Decidido por unanimidade.	Não houve.

DELIBERAÇÃO 5: Aprovação da norma de criação da Equipe de Tratamento de Incidentes de Redes – ETIR

Decisão

Foi decidido que a norma de criação da ETIR será revisada pelos membros do CEGOV e aprovada eletronicamente, por meio do SEI, após realização dos ajustes propostos na reunião, quais sejam:

- Alterar o Anexo para que seja formatado em conformidade com o Manual de Redação da Presidência da República (Determinação do Art. 58 do Decreto nº 9.191/2017) e com ato próprio do INSS que versa sobre a estrutura dos atos normativos, a saber: Resolução nº 708/PRES/INSS, de 6 de novembro de 2019;
- Verificar os itens 6.2 e 7.4 do Anexo, para evitar duplicidade.

Os ajustes serão realizadas pela DTI, até o dia 19/02/2020, e enviados à Secretaria-Executiva do CEGOV para circularização com os membros do comitê. Os membros do CEGOV se pronunciarão até o dia 21/02/2020. O texto ajustado será enviada à PFE-INSS para análise, conforme preceitua a Resolução nº 708/PRES/INSS/2019.

Votos a favor	Votos contrários
Decidido por unanimidade.	Não houve.

DELIBERAÇÃO 6: Aprovação da norma de acesso à Internet

Decisão

Foi decidido que a norma de será revisada pelos membros do CEGOV e aprovada eletronicamente, por meio do SEI, após realização dos ajustes propostos na reunião, quais sejam:

- Alterar o Anexo para que seja formatado em conformidade com o Manual de Redação da Presidência da República (Determinação do Art. 58 do Decreto nº 9.191/2017) e com ato próprio do INSS que versa sobre a estrutura dos atos normativos, a saber: Resolução nº 708/PRES/INSS, de 6 de novembro de 2019;
- Alterar item 4.2 - Perfil IV - do Anexo, para incluir os servidores das áreas de desenvolvimento de pessoas, tanto na administração central, quanto nas superintendências.

Os ajustes serão realizadas pela DTI, até o dia 19/02/2020, e enviados à Secretaria-Executiva do CEGOV para circularização com os membros do comitê. Os membros do CEGOV se pronunciarão até o dia 21/02/2020. O texto ajustado será enviada à PFE-INSS para análise, conforme preceitua a Resolução nº 708/PRES/INSS/2019.

Pontos de esclarecimento e debate

Foi ponderada a necessidade de realização de capacitações pelos servidores da casa, que muitas vezes são oferecidas por meio de vídeos no youtube. Como a norma indica que somente gestores, servidores da assessoria de comunicação e de desenvolvimento de pessoas poderão acessar sítios com material de áudio e vídeo, as capacitações poderão ser prejudicadas.

Para resolver a questão, a proposta foi que haja um espaço físico, um centro de treinamento, em que os servidores possam ter acesso aos cursos disponibilizados em plataformas que veiculem *streaming* de vídeo e áudio.

Votos a favor

Decidido por unanimidade.

Votos contrários

Não houve.

DELIBERAÇÃO 7: Seleção de processo de negócio para o piloto do mapeamento de riscos do INSS

Decisão

Foi selecionada a ação estratégica "Consolidar e monitorar os programas e centrais de análise", vinculada ao objetivo estratégico "Analisar com qualidade e tempestividade as demandas do cidadão" para o piloto do mapeamento de riscos do INSS.

Votos a favor

Decidido por unanimidade.

Votos contrários

Não houve.

3. Encaminhamentos

Encaminhamento	Responsável	Prazo
Solicitar revisão dos membros indicados para composição dos comitês temáticos, tendo em vista as mudanças recentes na alta gestão do INSS.	Secretaria-executiva do CEGOV	Fevereiro/2020

4. Registro de presença

Integrantes do Comitê

Unidade	Representante	Cargo
Presidência	Leonardo José Rolim Guimarães	Presidente
Diretoria de Benefícios	Alessandro Roosevelt da Silva Ribeiro	Diretor
Diretoria de Atendimento	Vítor Poubel da Silva	Diretor substituto
Diretoria de Gestão de Pessoas e Administração	Hélder Calado de Araújo	Diretor
Diretoria de Integridade, Governança e Gerenciamento de Riscos	Clóvis de Castro Júnior	Diretor
Diretoria de Tecnologia da Informação	Elávio Ferreira dos Santos	Diretor

Informação e Inovação	Flavio Ferreira dos Santos	Presidência
Auditoria Geral	William Guedes	Auditor Geral
Corregedoria Geral	Pedro Crisóstomo Rosário	Corregedor Geral
Procuradoria Federal Especializada junto ao INSS	Rodrigo Saito Barreto	Subprocurador
Demais participantes		
Unidade	Representante	Cargo
Gabinete da Presidência	Sidarta Costa de Azeredo Souza	Chefe de Gabinete
Coordenação-Geral de Governança/DIGOV Secretaria-executiva do CEGOV	Cibelle Cesar do Amaral Brasil	Coordenadora-Geral
Coordenação-Geral de Integridade e Gerenciamento de Riscos/DIGOV	Ziana Souza Santos	Coordenadora-Geral
Coordenação-Geral de Projetos Estratégicos e Inovação - CGPEI	Lorena Fonseca Ferreira Medeiros	Coordenadora-Geral
Assessoria de Comunicação Social - ACS	Bruno Leonardo de Almeida Dutra	Chefe da Assessoria
Coordenação-Geral de Projetos e Soluções Digitais/DTI	Kátia Macarini	Coordenadora-Geral
Coordenação Geral de Infraestrutura e Operações/DTI	Cláudio Ferraz	Coordenador-Geral
Diretoria de Tecnologia da Informação e Inovação	Renata C. O. Gomes	Coordenadora
Divisão de Segurança da Informação/DTI	Alexinaldo Cerqueira	Chefe de Divisão
Divisão de Segurança da Informação/DTI	Roberto Rufino da Costa	Técnico do Seguro Social
Divisão de Segurança da Informação/DTI	Nelson Antonio Pimentel Jacinto	Técnico do Seguro Social



Documento assinado eletronicamente por **FLAVIO FERREIRA DOS SANTOS, Diretor(a) de Tecnologia da Informação e Inovação**, em 26/02/2020, às 19:28, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **LEONARDO JOSE ROLIM GUIMARAES, Presidente**, em 27/02/2020, às 15:12, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site
[https://sei.inss.gov.br/sei/controlador_externo.php?
acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador
0368652 e o código CRC **59C88823**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 2/CEGOV/INSS, DE DE DE 2020

Atualiza a Política de Segurança da Informação e Comunicações do POSIC-INSS.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída no âmbito do INSS e nos termos do Anexo a esta Resolução, a Política de Segurança da Informação e Comunicações – POSIC-INSS.

Art. 2º Esta Resolução entra em vigor na data de sua publicação e seu Anexo será publicado em Boletim de Serviço.

Art. 3º Fica revogada a Resolução nº 672/PRES/INSS, de 27 de dezembro de 2018.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretora de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por FLAVIO FERREIRA DOS SANTOS, Diretor de Tecnologia da Informação e Inovação, em 02/03/2020, às 17:41, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador 0411821 e o código CRC 3CFC16ED.

ANEXO I

RESOLUÇÃO Nº 2/CEGOV/INSS, DE DE DE 2020

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO INSTITUTO NACIONAL DO SEGURO SOCIAL – POSIC-INSS

Art. 1º A Política de Segurança da Informação e Comunicações do Instituto Nacional do Seguro Social – POSIC-INSS, tem por objetivo estabelecer e difundir diretrizes e princípios de Segurança da Informação e Comunicações – SIC, com vistas à orientação para uso e proteção adequados das informações produzidas e custodiadas pelo Instituto, preservando sua disponibilidade, integridade, confidencialidade e autenticidade.

Parágrafo único. A Política de que trata o caput e suas normas complementares aplicam-se a todos os agentes públicos que têm vínculo direto e/ou indireto com o Instituto.

Art. 2º Para os efeitos da POSIC-INSS, entende-se:

I - agente público: todas as pessoas físicas que manifestam, por algum tipo de vínculo, a vontade do Estado, abrangendo servidores, ocupantes de cargo comissionado ou em comissão, prestadores de serviço e estagiários;

II - dado: é o registro do atributo de um ente objeto ou fenômeno onde registro indica o ato de registrar, ou seja, é a gravação ou a impressão de caracteres ou símbolos que tenham um significado em algum documento ou suporte físico;

III - Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

IV - ativos de informação: meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

V - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

VI - necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para que uma pessoa possuidora de credencial de segurança tenha acesso a dados ou informações sigilosas;

VII - riscos de segurança da informação e comunicações: potencial associado à exploração de uma ou mais vulnerabilidades nos ativos de informação, em razão de ameaças, com impacto negativo às atividades do Instituto;

VIII - segurança da informação e comunicações – SIC: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e autenticidades das informações;

IX - vínculo direto: agentes públicos contratados diretamente pelo INSS;

X - vínculo indireto: agentes privados ou públicos pertencentes a órgãos ou unidades da Administração Pública Federal, Estadual ou Municipal que mantenham contrato, convênio, acordo de cooperação técnica ou instrumento congênere com o INSS; e

XI - gestor de Segurança da Informação e Comunicações: é o responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF.

Art. 3º Esta POSIC-INSS foi elaborada com base nos seguintes documentos:

I - Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;

II - Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto na Constituição Federal;

III - Decreto nº 7.724, de 16 de maio de 2012, regulamenta a Lei nº 12.527, de 18 de novembro de 2011;

IV - Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

V - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

VI - Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

VII - Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008, que disciplina a gestão de segurança da informação e comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

VIII - Normas Complementares nº 01 a 21/IN01/DSIC/GSIPR;

IX - NBR ISO/IEC 27002:2013, que institui código de melhores práticas para a Gestão de Segurança da Informação;

X - Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais; e

XI - Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Art. 4º Esta POSIC-INSS foi elaborada com base nos seguintes princípios:

I - a preservação da imagem do Instituto e de seus agentes públicos;

II - a salvaguarda das informações do cidadão;

III - ações de segurança orientadas pela gestão de riscos;

IV - continuidade assegurada dos serviços ao cidadão;

V - o alinhamento com a missão institucional e seu planejamento estratégico; e

VI - respeito à natureza e finalidade de cada área do Instituto.

Art. 5º São diretrizes gerais da POSIC-INSS:

I - Tratamento da Informação:

a) toda informação produzida pelos agentes públicos, no exercício de suas atividades, é de propriedade do INSS e deve ser protegida;

b) informações produzidas, armazenadas e tratadas pelo Instituto, especialmente as informações pessoais e custodiadas, devem receber o devido tratamento para assegurar sua proteção durante todo o ciclo de vida; e

c) somente os canais de comunicação disponibilizados pelo INSS devem ser utilizados para trafegar informações institucionais.

II - Tratamento de Incidentes de Segurança da Informação (SIC):

a) todo incidente de segurança da informação deve ser imediatamente relatado à área responsável pela gestão de segurança da informação de TIC, observando-se a apropriada coleta de evidências.

III - Gestão de Riscos de Segurança:

a) os riscos de segurança da informação devem ser identificados e tratados; e

b) os critérios para a gestão de risco devem ser definidos e comunicados a toda instituição.

IV - Gestão de Continuidade:

a) os ativos de informação que suportam as atividades críticas do Instituto devem ser suportados por ambiente de alta disponibilidade e ter capacidade de recuperação em prazos e condições previamente definidos para situações de contingência, em conformidade com o processo de continuidade; e

b) a continuidade das operações e serviços de Tecnologia da Informação e Comunicações – TIC, deve estar prevista nos contratos, assim como os prazos e condições devem estar formalmente estabelecidos.

V - Controles de Acesso:

a) todo acesso à informação deve ser motivado pela necessidade de conhecer;

b) os sistemas de informação e as instalações físicas devem ter capacidade de controlar os acessos, com fins de responsabilização pelo seu uso; e

c) as autorizações de acesso às informações, sistemas e instalações físicas devem ter critérios de acesso definidos e divulgados a todos da instituição.

VI - Recursos Computacionais:

a) correio eletrônico:

1. o correio eletrônico, *e-mail*, é uma forma de comunicação oficial e deve ser utilizado exclusivamente no desempenho das atividades funcionais; e

2. ao produzir, responder ou encaminhar mensagem em caixa de correio eletrônico institucional, o servidor deverá se identificar, subscrevendo, ao menos, seu nome, cargo e telefone de contato institucional.

b) Acesso à Internet:

1. o acesso à Internet, por meio da rede de dados do INSS, é uma concessão e deve ter seu uso orientado para a execução das atividades do Instituto; e

2. os acessos serão liberados de acordo com perfis previamente definidos pelo órgão responsável pelos serviços de TIC.

c) Gestão de Mudanças de TIC:

1. toda mudança nos sistemas de informação do INSS deve ser previamente e formalmente autorizada; e

2. a gestão de mudanças deve prever, no mínimo, a guarda dos registros, realização de testes e a possibilidade de recuperação do ambiente.

VII - Educação e Conscientização:

a) esta Política e seus normativos complementares devem ser periodicamente divulgados a todos os agentes públicos do Instituto;

b) o Instituto deve manter programa contínuo de conscientização dos agentes públicos em Segurança da Informação e Comunicações – SIC; e

c) deve ser mantido plano de capacitação especializado aos profissionais que atuam na gestão de SIC.

VIII - Auditoria e Conformidade:

- a) o cumprimento desta Política e de suas normas complementares deve ser avaliado periodicamente, por meio de verificações de conformidade; e
- b) o uso dos recursos de TIC disponibilizados pelo Instituto é passível de monitoramento e auditoria.

IX - Responsabilidade da gestão das informações:

Parágrafo único. O Comitê Temático de Gestão da Informação é responsável pela aprovação de procedimentos e de normas internas que orientem o compartilhamento de dados sob gestão do INSS e pela aprovação da categorização dos níveis de compartilhamento de dados com outras entidades públicas (federais ou de outras esferas e poderes) da sociedade civil (Vide atribuições do CTGI, no Art. 6º do Anexo da Portaria nº 3.213/PRES/INSS/2019).

Art. 6º A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas, cíveis e penais, previstas na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), no Código Penal, no Código Civil, e, ainda, em legislação que regule ou venha regular a matéria.

Art. 7º Competências e Responsabilidades:

I - Cabe ao Gestor de Segurança da Informação e Comunicações:

- a) promover cultura de segurança da informação e comunicações;
- b) acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
- c) propor os recursos necessários à implementação das ações de SIC;
- d) coordenar o CSIC e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR do INSS; e
- e) propor o detalhamento das diretrizes desta Política, por meio de normas e procedimentos, e acompanhar sua implementação.

II - Cabe ao Presidente do Instituto nomear o Gestor de SIC;

Inovação; III - Caso o Gestor de SIC não seja nomeado, as atribuições relacionadas no item 7.1 serão desempenhadas pelo Diretor de Tecnologia da Informação e

IV - A ETIR-INSS deve analisar e propor respostas a notificações e atividades relacionadas a incidentes de SIC, no âmbito do Instituto; e

V - É responsabilidade de todos os agentes públicos, diretos e indiretos, conhecer e cumprir as diretrizes desta Política e demais normas e procedimentos complementares de SIC.

Art. 8º Esta Política deve ser revisada sempre que necessário, não excedendo o período máximo de três anos.



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 3/CEGOV/INSS, DE DE DE 2020

Define regras para a emissão de credenciais de acesso lógico no âmbito do INSS

O **COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS**, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída a Norma de Controle de Acesso Lógico - NCAL, do Instituto Nacional do Seguro Social – INSS.

Art. 2º Esta Resolução, bem como seus anexos, serão publicados em Boletim de Serviço, nos termos do Art. 15, § 2º, Inciso I da Resolução 70/INSS/PRES, de 06 de outubro de 2009.

Art. 3º Revogar a RESOLUÇÃO Nº 413/PRES/INSS, DE 20 DE MAIO DE 2014.

Art. 4º Esta Resolução entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretora de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **FLAVIO FERREIRA DOS SANTOS**, Diretor de Tecnologia da Informação e Inovação, em 02/03/2020, às 17:42, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0411838** e o código CRC **7A6B1766**.

ANEXO I

RESOLUÇÃO Nº 3/CEGOV/INSS, DE DE DE 2020

NORMA DE CONTROLE DE ACESSO LÓGICO – INSS

Art. 1º Os termos definidos nesta norma aplicam-se a todos os agentes públicos e privados com vínculo direto ou indireto, permanente ou temporário com o INSS.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União – AGU que atuarem na consultoria e no assessoramento jurídico, e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta Norma de Controle de Acesso Lógico são estabelecidos os seguintes conceitos e definições:

I - administrador de Domínio: Usuário responsável pela administração de um domínio por meio da aplicação de políticas globais, criação, edição e exclusão de usuários e grupos, e instalação de programas em um grande número de estações de trabalho;

II - administrador Local: Usuário responsável pela administração de partes de um domínio (geralmente restrito a um setor ou abrangência), por meio de políticas locais, edição de grupos e usuários locais, e instalação de programas em estações de trabalho limitadas a um setor ou abrangência;

III - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta;

IV - dado: é o registro do atributo de um ente objeto ou fenômeno onde registro indica o ato de registrar, ou seja, é a gravação ou a impressão de caracteres ou

símbolos que tenham um significado em algum documento ou suporte físico;

V - Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

VI - ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VII - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

VIII - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

IX - contas de serviço: contas de acesso à rede corporativa de computadores, necessárias para a execução de procedimentos automáticos (aplicação, script, etc) sem qualquer intervenção humana no seu uso;

X - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

XI - credenciamento: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer;

XII - credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física, como crachá, cartão e selo ou lógica como identificação usuário e senha;

XIII - domínio: agrupamento lógico de computadores em rede que compartilham recursos em um banco de dados de segurança, comum, onde a administração e autenticação são centralizadas. Desta forma um usuário precisa de uma conta para ter acesso ao domínio e aos recursos compartilhados;

XIV - endereço IP: sigla em inglês para *Internet Protocol*. Trata-se de endereço lógico que identifica a localização de determinado ativo na rede;

XV - entidade externa: Organização governamental, não governamental ou privada amparada por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica ou instrumento congênere com o INSS;

XVI - e-SIC: Sistema Eletrônico do Serviço de Informações ao Cidadão, aplicação disponibilizada na internet, que centraliza todos os pedidos de informações dirigidos ao Poder Executivo Federal;

XVII - estagiário: educando que esteja frequentando o ensino regular, em instituições de educação superior, de educação profissional, de ensino médio, de educação especial e dos anos finais do ensino fundamental, na modalidade profissional da educação de jovens e adultos, que desenvolve as atividades relacionadas à sua área de formação profissional junto as pessoas Jurídicas de Direito Privado, órgãos da Administração Pública e Instituições de Ensino, que tenham condições de proporcionar experiência prática na sua linha de formação;

XVIII - estágio Supervisionado: ato educativo escolar supervisionado, desenvolvido no ambiente de trabalho, que visa a preparação para o trabalho produtivo de educandos;

XIX - ferramenta de gestão de acessos: Software que possibilita a gestão integrada de papéis e permissões de acesso dos usuários nos sistemas corporativos;

XX - gestor da informação: usuário que gerou a informação, que responde pelo seu conteúdo ou que foi formalmente designado para definir, alterar a sua classificação nos graus de sigilo e perfil de acesso dos demais usuários e processos;

XXI - gestão de identidades: Combinação de sistemas técnicos, regras e procedimentos que definem a posse, utilização e segurança de uma identidade. Seu objetivo primário é estabelecer a confiança na associação de atributos a uma identidade digital e conectar esta identidade com uma entidade individual;

XXII - necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação;

XXIII - perfil de Acesso do Usuário: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

XIV - recursos de rede: Dispositivos (impressoras, scanners, multifuncionais, etc) ou serviços (sistemas, portais, etc) disponibilizados para os usuários por meio de uma rede de dados;

XXV - serviço de diretório: serviço que armazena e organiza informações relativas a recursos disponíveis e usuários de uma rede de dados. Permite que o administrador da rede gereencie o acesso de usuários e sistemas aos recursos disponíveis;

XXVI - sistemas corporativos: sistemas de operação, ou finalísticos, que se coadunam com os fins da Previdência Social. Assim, entende-se que este conceito comporta o conjunto de sistemas e subsistemas que garantem a operação dos regimes geral e próprio de previdência social, inclusive de previdência complementar;

XXVII - sistemas legados: compreendem o conjunto de aplicações desenvolvidas com tecnologias obsoletas que permanecem em operação no INSS;

XXVIII - usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal-APF, formalizada por meio da assinatura do Termo de Responsabilidade;

XXIX - usuário interno: servidor do quadro do INSS lotado em uma Unidade Orgânica – UO, que se utiliza dos sistemas corporativos do Instituto;

XXX - usuário externo: usuários vinculados a uma Entidade Externa, que se utiliza dos sistemas corporativos do Instituto por meio de um perfil de acesso concedido por um Gestor de Acesso Externo;

Art. 3º São diretrizes desta NCAL-INSS:

I - o acesso à rede e aos sistemas corporativos do INSS dar-se-á por meio de autenticação integrada de domínio baseado em serviço de diretório, administrado por meio de uma ferramenta de gestão de identidades;

II - as concessões de acesso à rede de dados e aos sistemas corporativos são distintas. Sendo assim, o usuário pode obter permissão de acesso apenas à rede de dados, ou apenas a determinado(s) sistema(s) corporativo(s);

III - as credenciais de acesso a rede de dados e aos sistemas corporativos do INSS são conferidas aos usuários com base na necessidade de conhecer, para viabilizar o exercício de suas atribuições funcionais e atividades a serem desenvolvidas no âmbito do INSS; e

IV - o uso indevido de informações dos sistemas corporativos do INSS sujeitará o agente às penalidades previstas na legislação.

Art. 4º Base Cadastral:

I - as bases de dados do Serviço de Diretórios (acesso à rede de dados), do Sistema de Gestão de Acessos (sistemas corporativos) e sistemas legados devem ser alimentadas por informações disponibilizadas pelo INSS;

II - para tanto, a área responsável pela gestão de pessoas do INSS disponibilizará periodicamente as informações extraídas do Sistema Integrado de Administração de Recursos Humanos – SIAPE para a área responsável pela gestão de TIC do INSS (não ultrapassando o prazo de sete dias), contendo, minimamente, os seguintes dados:

Tabela 1: Informações Usuários

Item	Informação	Campo	Descrição
1	GR-MATRICULA	N 0012	GRUPO NUMÉRICO COMPOSTO DE NÚMERO DO ÓRGÃO (N0005) E NÚMERO DE MATRÍCULA DO SERVIDOR (N0007)
2	IT-NU-IDEN-SERV-ORIGEM	A 0008	NÚMERO DE IDENTIFICAÇÃO DO SERVIDOR NA ORIGEM - NÚMERO VINCULADO AO CARGO EFETIVO OU EM COMISSÃO
3	IT-NO-SERVIDOR	A 0060	NOME
4	IT-DA-NASCIMENTO	N 0008	DATA DE NASCIMENTO
5	IT-NU-CPF	N 0011	NÚMERO DO CPF
6	IT-NU-PIS-PASEP	N 0011	NÚMERO DO PIS
7	IT-IN-SUPRESSAO-PAGAMENTO	A 0001	INDICATIVO DE SUPRESSÃO DE PAGAMENTO
8	IT-CO-SITUACAO-SERVIDOR	N 0002	CÓDIGO DE SITUAÇÃO FUNCIONAL DO SERVIDOR
9	IT-CO-GRUPO-OCOR-AFASTAMENTO	N 0002	CÓDIGO DE OCORRÊNCIA DE AFASTAMENTO
10	IT-DA-INICIO-OCOR-AFASTAMENTO	N 0008	DATA DO INÍCIO DA OCORRÊNCIA DE AFASTAMENTO
11	IT-DA-TERMINO-OCOR-AFASTAMENTO	N 0008	DATA DE TÉRMINO DA OCORRÊNCIA DE AFASTAMENTO
12	IT-CO-GRUPO-OCOR-EXCLUSAO	N 0002	CÓDIGO DE OCORRÊNCIA DE EXCLUSÃO
13	IT-CO-UORG-LOTACAO-SERVIDOR	N 0009	CÓDIGO DA UORG DE LOTAÇÃO DO SERVIDOR
14	IT-CO-ORGAO-REQUISITANTE	N 0005	CÓDIGO DO ÓRGÃO REQUISITANTE

III - a Diretoria de Tecnologia da Informação e Inovação procederá com a atualização dinâmica das bases cadastrais do serviço de diretórios e dos sistemas corporativos, bem como realizará a validação das informações disponibilizados pelo INSS por meio de outras bases, na periodicidade do envio das informações; e

IV - a área responsável pela gestão de pessoas do INSS poderá acordar, com a área responsável pela gestão de TIC do INSS, a inclusão de outras informações necessárias à administração de contas de usuários.

Art. 5º Credenciais e perfis de acesso:

I - a emissão de uma credencial permite ao usuário acessar a rede de dados corporativa do INSS. Para que o mesmo obtenha acesso aos sistemas corporativos a credencial deve ser associada a um perfil de acesso;

II - o processo de credenciamento de usuário aos ativos de informação deve ser feito observando os seguintes critérios:

- a) a credencial de acesso concedida para acesso à rede de dados e sistemas corporativos do INSS é de caráter pessoal e intransferível;
- b) as credenciais de acesso devem ser concedidas após a data de contratação ou entrada em exercício do usuário; e
- c) as mesmas credenciais de acesso devem ser utilizadas para o acesso à rede de dados e aos sistemas corporativos do INSS, mediante autenticação que permita ao usuário acessar vários sistemas, por meio de ferramenta de gestão de identidades e acessos.

III - os servidores lotados nas áreas responsáveis pela gestão de pessoas do INSS deverão utilizar os canais de atendimento disponibilizados pela Dataprev, ou outro canal informado pela DTI, para:

- a) solicitar, se necessário, o credenciamento de usuários, contratados ou requisitados, para compor o quadro de servidores do INSS, após o ato da posse, e de estagiários, após assinatura do contrato de prestação de serviço, para acesso à rede;
- b) solicitar a inativação imediata do perfil de acesso dos servidores cedidos a outros órgãos, inativos ou exonerados do quadro de servidores do INSS na data da publicação do ato;
- c) solicitar a suspensão imediata do perfil de acesso dos servidores afastados ou com licença programada de suas funções por mais de sessenta dias ininterruptos; e
- d) solicitar a exclusão do acesso de estagiários, cujo vínculo com o Instituto tenha sido encerrado, tão logo a rescisão do contrato seja efetivada.

IV - quanto ao processo de formação das credenciais de acesso fica estabelecido que:

a) o nome do usuário será composto de acordo com os padrões estabelecidos no Guia de Interoperabilidade do Governo Eletrônico – e-Ping, mais especificamente no documento “Caixas Individuais-Fundacionais no Governo Federal” (Rede do Governo, 2010) que define regras de formação de nomes para a composição de endereços eletrônicos;

b) quanto às senhas de acesso:

- 1. deverão ter no mínimo oito caracteres e conter, obrigatoriamente, caracteres alfanuméricos (combinação de letras e números). O usuário poderá acrescentar caracteres especiais (espaços em branco, símbolos, sinais de pontuação, etc);
- 2. é vedada a reutilização das últimas quatro senhas utilizadas pelo usuário;
- 3. podem ser alteradas sempre que preciso ou quando o usuário achar necessário;
- 4. o prazo de validade não deve ultrapassar noventa dias; e
- 5. o usuário receberá por meio de comunicado direto (via interface do sistema ou por mensagem no correio eletrônico) a informação do prazo próximo de vencimento da senha, quando esta estiver a 15 dias da sua data de expiração.

V - os perfis de acesso aos sistemas corporativos deverão contemplar um conjunto de permissões e ações vinculadas às atividades desenvolvidas pelo usuário;

VI- caberá à área responsável pela gestão de TIC do INSS estabelecer, em conjunto com as áreas responsáveis pela gestão dos sistemas corporativos, a política de criação dos perfis de acesso;

VII - as áreas responsáveis pela gestão dos sistemas corporativos, são responsáveis pelas permissões, transações e ações que devem compor cada perfil de acesso;

VIII - os perfis de acesso e perfis de gestão concedidos para usuários deverão ser objeto de revisão contínua pelos gestores responsáveis, não podendo ultrapassar o prazo máximo de 24 (vinte e quatro) meses;

IX - quanto à utilização das credenciais e perfis de acesso, o usuário:

- a) deve ter conhecimento prévio desta Política de Controle de Acesso Lógico e preencher os requisitos estabelecidos na mesma;
- b) deve estar devidamente autorizado a utilizar a rede corporativa e/ou os sistemas corporativos, de acordo com os requisitos estabelecidos nesta Política;
- c) deve utilizar os serviços e as informações obtidas, por meio do perfil de acesso, única e exclusivamente em razão do exercício da função pública e para os fins que lhe foi designado, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal;

d) não pode divulgar, nem mesmo compartilhar, os códigos de segurança que lhe forem atribuídos (credenciais de acesso), os quais são pessoais e intransferíveis;

e) não pode utilizar as credenciais para acessar os recursos disponíveis em mais de uma estação de trabalho simultaneamente;

f) não pode fazer uso das credenciais de acesso de outros usuários;

g) deve fornecer informações acessadas nos sistemas e na rede de dados corporativos do INSS somente mediante demanda formalizada de quem tenha competência para tal;

h) deve comunicar a chefia imediata ou responsável pela administração do sistema ou rede corporativa quaisquer violações ou incidentes referentes à proteção do equipamento utilizado, do software ou de outros ativos da informação; e

i) deve, sempre que for necessário afastar-se da estação de trabalho, certificar-se de que a sessão de rede ou acesso ao sistema corporativo esteja encerrado ou bloqueado.

X - a autenticação dos usuários será feita por meio de credenciais de acesso baseadas em nome de usuário e senha e, quando disponível, aliada ao uso de certificação digital padrão ICP-Brasil e/ou uso de dados biométricos;

XI - o usuário deverá, obrigatoriamente, efetuar processo de alteração da sua senha em seu primeiro acesso à rede de dados corporativa; e

XII - no ato do primeiro acesso, bem como após cada atualização desta Política, o usuário deverá manifestar concordância com os termos dispostos na mesma.

XIII - Credenciamento de Usuários Internos:

a) o cadastro de novos servidores ou ocupantes de cargo em comissão, no âmbito do Instituto, pode ser solicitado por servidor vinculado à área responsável pela gestão de pessoas ou pela chefia imediata do usuário; e

b) esse cadastro deve ser solicitado por meio dos canais de atendimento da Dataprev ou outro informado pela DTI.

XIV - credenciamento de estagiários:

a) a emissão de credencial de acesso se dará tendo como requisito as seguintes condições:

1. a empresa que atuar como agente de integração do estágio supervisionado deve manter contrato com o INSS; e

2. o contrato de estágio supervisionado deverá conter cláusula de confidencialidade e sigilo de informações preestabelecidos com a Administração Pública.

b) para viabilizar o acesso de estagiários aos sistemas corporativos, os gestores dos sistemas corporativos deverão criar perfis específicos e restritos às atividades do estagiário;

c) é vedada a concessão de perfis de acesso aos sistemas corporativos para estagiários com permissão de alteração das bases de dados institucionais;

d) o acesso será concedido mediante solicitação expressa de servidor do quadro do INSS, responsável pela supervisão do estágio, que deverá:

1. avaliar os riscos de utilização indevida de informações institucionais e as eventuais restrições referentes aos dias e horários para a realização dos acessos.

e) o acesso será precedido da assinatura do Termo de Confidencialidade e de Manutenção de Sigilo – TCMS, Anexo II, o qual deverá ser firmado pelo estagiário ou pelo estagiário e seu responsável legal, no caso de se tratar de estagiário menor de dezoito anos;

f) as solicitações de acesso à rede para estagiários devem ser procedidas por meio dos canais remotos de atendimento da Dataprev ou outro canal informado pela DTI, pela unidade de gestão de pessoas, pela chefia imediata do educando ou pelo responsável por sua supervisão;

g) os gestores de sistemas devem criar perfis diferenciados para estagiários de nível médio e nível superior;

h) o supervisor do estagiário deverá, periodicamente, orientá-lo quanto ao uso responsável e adequado do acesso aos sistemas corporativos; e

i) o acesso do estagiário limitar-se-á à data final do contrato ou imediatamente cessado na hipótese de rescisão antecipada do estágio, cabendo ao supervisor do estagiário, em quaisquer dos casos, adotar as providências necessárias ao bloqueio do acesso, tão logo finde a contratação.

XV - credenciamento de usuários externos:

a) as credenciais de acesso para usuários externos devem ser emitidas tendo em vista o interesse do INSS, devidamente justificadas e previstas no convênio, acordo de cooperação técnica ou instrumento congênere;

b) as solicitações de emissão de credenciais de acesso à rede corporativa para usuários amparados por força de legislação específica ou estabelecida em

convênio, acordo de cooperação técnica, contrato ou instrumento congênere devem:

1. ser feitas pelo gestor da unidade/área responsável pela gestão do instrumento legal; e

2. ser atendidas somente após validação das credenciais do gestor solicitante do Instituto, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700) ou outra base de dados indicada pela área responsável pela gestão de pessoas, a qual contenha informações referentes à estrutura organizacional do Instituto.

c) a emissão de credenciais de acesso à rede corporativa para prestadores de serviço terceirizados ou equiparados nas dependências do INSS, quando necessária, será provida unicamente pelo interesse do INSS. Para tanto, devem ser atendidos os seguintes requisitos:

1. a organização a qual o usuário é vinculado deve manter contrato, acordo de cooperação, convênio ou instrumento congênere vigente com o INSS;

2. instrumento deve conter cláusulas prevendo:

2.1. necessidade e justificativa para acesso à rede corporativa;

2.2. a confidencialidade e sigilo de informações preestabelecidas junto ao Instituto;

2.3. a obrigatoriedade da organização ou do ente contratado informar previamente ao representante legal do INSS, responsável pela gestão do contrato, quaisquer alterações em seu corpo de colaboradores que impacte na emissão/exclusão das contas de acesso;

2.4. a organização ou ente contratado também deverá manter com seus colaboradores Termo de Confidencialidade de Manutenção de Sigilo – TCMS; e

2.5. o gestor do contrato pelo INSS deve fundamentar a necessidade do acesso à rede para prestadores de serviço terceirizados ou equiparados, definindo os recursos que devem ser disponibilizados e eventuais restrições a dias e horas para realização do acesso à rede.

3. os TCMS deverão ser arquivados junto aos instrumentos assinados com o INSS e uma cópia ou link eletrônico deverá ser encaminhada ao Gestor do Contrato. O mesmo deve ocorrer para quaisquer alterações ocorridas na vigência dos contratos, acordos ou convênios;

3.1 caso os Termos sejam gerados de forma eletrônica, deverá ser disponibilizado o arquivo correspondente, atendendo aos requisitos necessários para garantia de integridade e disponibilidade de acesso, assim como os requisitos específicos previstos em contrato; e

4. a emissão de credenciais de acesso poderá ser feita pelo gestor do contrato, representante legal do INSS, ou pelo gestor da unidade responsável pela gestão do contrato, convênio, acordo de cooperação técnica ou instrumento congênere e serão atendidas somente após validação das credenciais do solicitante, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700) ou outra base de dados indicada pela área responsável pela gestão de pessoas, a qual contenha informações referentes à estrutura organizacional do Instituto.

d) o acesso aos prestadores de serviço vinculados à Central de Atendimento 135 se dará observando as seguintes condições:

1. a empresa deve manter contrato com o INSS;

2. o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

3. a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade - TCMS;

4. o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte do INSS, definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;

5. os acessos deverão ser realizados única e exclusivamente por necessidade de serviço; e

6. o INSS pode disponibilizar, de forma restrita, às centrais 135 uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

e) nos casos referentes a prestadores de serviço vinculados à Ouvidoria-Geral da Previdência Social – OUGPS, o acesso se dará observando-se as seguintes condições:

1. a empresa deve manter Contrato direto com a Ouvidoria-Geral da Previdência Social;

2. o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

3. a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade;

4. o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte da OUGPS, definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;

5. os acessos deverão ser realizados única e exclusivamente por necessidade de serviço; e

6. o INSS pode disponibilizar, de forma restrita, à OUGPS uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

f) o acesso à rede corporativa por servidores vinculados a órgãos de controle externo, envolvidos em ações de auditoria no âmbito do INSS, será concedido mediante apresentação da equipe de auditoria por meio de documento formal que conste:

1. dados necessários ao cadastro de usuários externos;
2. informações acerca dos objetivos dos trabalhos a serem executados;
3. os prazos envolvidos; e
4. informações complementares.

g) este tipo de acesso deverá observar as parcerias institucionalmente estabelecidas entre esses órgãos e o INSS no que tange à cobertura/previsão de acesso à rede corporativa do Instituto; e

h) o atendimento de pedido de solicitação de informações advindo de pessoas físicas ou jurídicas externas, respeitadas as restrições de acesso às informações previstas na Lei nº 12.527, de 18 de novembro de 2011, serão analisadas pela área designada para responder as demandas dos cidadãos por meio do e-SIC.

XVI - os procedimentos referentes às solicitações de inclusão, exclusão, inativação e suspensão de contas de acesso de usuários devem ser executados tendo como premissa a preservação dos registros para efeito de auditoria.

XVII - bloqueio administrativo:

a) o responsável pela Corregedoria-Geral do INSS, quando necessário, poderão solicitar a suspensão, bloqueio ou inativação imediata de contas de acesso de usuários que estiverem envolvidos em inquérito penal, em Processo Administrativo Disciplinar – PAD – ou em Sindicância, decorrente de infrações cometidas no exercício das atribuições do cargo;

b) estas solicitações deverão ser efetuadas mediante comunicação formal da Corregedoria-Geral para a Dataprev, ou outro canal informado pela DTI, a qual procederá a imediata implementação da mudança.

c) para disciplinar o disposto na "alínea a", é considerado possível de ter a senha bloqueada, o usuário que estiver na seguinte situação:

1. afastado temporariamente do cargo ou função pública em razão de ato que se encontra sob apuração;
2. indiciado em processo administrativo disciplinar, por incursão nos incisos IX, XI, XII, XV, XVI e XVII do art. 117 e arts. 130 e 132 da Lei nº 8.112, de 11 de dezembro de 1990, ou cuja proposta pela Comissão Processante, no relatório final, seja pela aplicação de penalidade a partir de suspensão de trinta dias; e
3. submetido à prisão em flagrante, temporária ou preventiva decorrente do cometimento de infração no exercício das atribuições do cargo, enquanto estiver em apuração de inquérito policial ou pelo Ministério Público Federal.

d) o bloqueio de acessos, tratados nas situações da "alínea c", será efetivado no âmbito da ferramenta de gestão de acessos nas seguintes situações:

1. usuário afastado temporariamente do cargo ou função, enquanto durar o afastamento; e
2. usuário indiciado nos termos do subitem "alínea c", desta Política, até o efetivo cumprimento da penalidade porventura aplicada ou, em caso de não aplicação de penalidade, enquanto durar o processo.

Art. 6º Rede de Dados Corporativa:

I - infraestrutura de rede:

a) a infraestrutura de rede do INSS é disponibilizada para uso Institucional. Sendo assim, apenas equipamentos de propriedade do Instituto são autorizados e devem ser conectados à rede corporativa;

1. em casos excepcionais, a conexão de equipamentos particulares à rede corporativa deve ser feita em razão do interesse do Instituto e sob prévia autorização do responsável pela gestão da unidade em que o equipamento estiver localizado.

b) o INSS poderá disponibilizar o acesso à rede de dados corporativa por meio de tecnologia *Wireless* (sem fio). Para tanto os seguintes critérios deverão ser adotados:

1. os projetos que envolvam a utilização de pontos de acesso sem fio à rede corporativa no âmbito do Instituto deverão ser devidamente registrados e aprovados pela área responsável pela gestão de TIC do INSS;

2. os pontos de acesso à rede de dados corporativa sem fio poderão ser objeto de testes periódicos de penetração e de auditoria a critério da área responsável pela gestão de TIC no INSS;

3. as conexões à rede sem fio serão avaliadas pela área responsável pela gestão de TIC do INSS em relação aos requisitos de segurança e deverão atender ao princípio do privilégio mínimo;

4. a área responsável pela gestão de TIC do INSS poderá disponibilizar rede sem fio com regras específicas de acesso para visitantes nas diversas unidades do Instituto;

5. os dispositivos conectados à rede do INSS por meio de conexão sem fio deverão suportar configurações de criptografia estabelecidas pela área responsável pela gestão de TIC no âmbito do INSS; e

6. qualquer tecnologia de acesso sem fio implementada no INSS deverá suportar autenticação forte, com possibilidade de efetuar checagens em bancos de dados externos.

c) a área responsável pela gestão de TIC do INSS deve dispor de mecanismos automáticos que possibilitem:

1. a detecção e bloqueio de equipamentos externos conectados à rede corporativa; e

2. a identificação e rastreamento dos endereços IP de origem e destino, bem como os serviços utilizados na rede corporativa inclusive nos acessos remotos.

II - administração da rede corporativa:

a) a administração da rede do INSS é realizada pela Empresa de Tecnologia e Informações da Previdência Social - Dataprev;

1. os ativos e serviços que compõem a rede de dados corporativa são providos, gerenciados e operacionalizados pela empresa; e

2. os acessos à rede de dados corporativa realizados pelos usuários do INSS são gerenciados e monitorados pela Dataprev, contudo seguem as regras desta política.

b) quanto ao processo de geração de contas de serviço fica estabelecido que:

1. os critérios para a emissão de contas de serviços serão vinculados a um processo formal estabelecido pela área responsável pela gestão de TIC do INSS;

2. a concessão de contas de serviços deve ser feita conforme a necessidade de uso de acordo com os critérios estabelecidos nesta Política de Controle de Acesso;

3. o direito de acesso privilegiado, por meio de contas de serviços, associado a sistemas ou processos, deve ser identificado;

4. deve ser viabilizada ferramenta que possibilite a gestão das contas de serviço de forma automatizada, possibilitando o registro e verificação de todos os privilégios concedidos;

5. as contas de serviço fornecidas devem ser utilizadas exclusivamente para os fins aos quais foram concedidas;

6. as contas de serviço emitidas devem ser revalidadas periodicamente com base na função exercida e na área de atuação do servidor; e

7. as contas de serviço com credenciais de acesso de uso compartilhado devem ter suas senhas alteradas periodicamente, conforme estabelecido nesta Política de Controle de Acesso Lógico, ou sempre que ocorrerem mudanças no grupo de usuários que utilizam as mesmas.

C) é vedado o uso da rede corporativa para:

1. acesso por meio de equipamento não homologado ou não autorizado pelo INSS;

2. fazer download, instalar e/ou utilizar sistemas ou aplicativos não homologados pela área responsável pela gestão de TIC do INSS nos equipamentos de propriedade do Instituto;

3. a utilização de softwares particulares em equipamentos do INSS sem autorização expressa;

4. a instalação e conexão de equipamentos particulares à rede corporativa do Instituto sem a prévia autorização do gestor responsável pela unidade ou da área responsável pela gestão de TIC do INSS;

5. o uso dos recursos de rede para fins particulares ou de terceiros alheios aos interesses do INSS, em especial quando tal procedimento prejudique o tráfego da rede de dados;

6. o uso para fins de divulgação ou distribuição de material que não possua vínculo com as atividades desenvolvidas pelo Instituto;

7. a instalação ou utilização de ferramentas de monitoramento de rede sem a anuência e autorização expressa da área responsável pela gestão de TIC no Instituto;

8. a instalação de dispositivos de comunicação ou de compartilhamento de dados sem fio, particulares, à rede corporativa do Instituto, sem autorização expressa da área responsável pela gestão de TIC do INSS; e

9. burlar as regras a internet configuradas em proxy ou ferramenta similar de gerenciamento de conteúdo web;

d) cabe a área responsável pela gestão de TIC no âmbito do INSS definir os aspectos relacionados à plataforma tecnológica, gestão operacional, forma de autenticação e sustentação do domínio de rede do INSS.

Art. 7º Gestão do Acesso aos Sistemas Corporativos:

I - sistemas legados:

a) as regras estabelecidas nesta norma devem ser aplicadas, guardando-se as devidas limitações tecnológicas, aos sistemas legados; e

b) o controle de acesso aos sistemas legados é efetuado por base própria.

II - sistemas de apoio à administração:

a) os ambientes de hospedagem desses sistemas são suportados por terceiros;

b) o ambiente deverá ser gerenciado e operacionalizado pela área de gestão de TIC do INSS;

c) o acesso pelos usuários a esses sistemas deverá ser autenticado pelo serviço de diretório utilizado pelo Instituto; e

d) as regras de hospedagem de sistemas serão definidas, em ato próprio, pela área de gestão de TIC do INSS.

III - armazenamento de registros logs:

a) as áreas responsáveis pela gestão de sistemas corporativos e demais aplicações devem definir, em conjunto com a área responsável pela gestão de TIC, a temporalidade de registro dos logs de acesso e transações, e quais registros devem ser armazenados por um período maior que o estipulado no item 8.1 desta Política; e

b) o INSS poderá alterar a temporalidade destes dados em norma específica.

IV - administração da ferramenta de gestão de acesso:

a) com o objetivo de operacionalizar a gestão dos acessos aos sistemas corporativos no âmbito do INSS, serão criados os seguintes papéis:

1. administrador de sistema INSS: Servidor do quadro, lotado na área responsável pela gestão de TIC, designado por meio de Portaria do Diretor de Tecnologia da Informação e Inovação, a ser publicada em Boletim de Serviço – BS, responsável pela administração da ferramenta de gestão de acesso aos sistemas corporativos no âmbito do INSS;

2. gestor de sistema: Servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em Boletim de Serviço, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedoria-Geral e Procuradoria Federal Especializada. É responsável pela implementação de sistemas corporativos no âmbito do INSS;

3. gestor de acesso central: Servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em Boletim de Serviço, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedoria-Geral e Procuradoria Federal Especializada. É responsável pela manutenção dos perfis de gestão dos usuários nas áreas que compõem a Administração Central e, quando necessário, dos gestores de acesso das Superintendências Regionais;

4. gestor de acesso interno: Servidor do quadro, lotado na Administração Central, Superintendência Regional, Gerência Executiva, Agência da Previdência Social, indicado pelo Gestor de Acesso Central ou por um Gestor de Acesso, responsável pela atribuição do perfil de acesso e de gestão dos usuários no INSS; e

5. gestor de acesso externo: Pessoa formalmente indicada, por documento previsto no instrumento legal que firmou a parceria ou por meio de Ofício de lavra do representante máximo de uma Entidade Externa, responsável pelo cadastro de usuários externos e a gestão dos acessos aos sistemas corporativos do Instituto.

b) a indicação e processo de substituição dos responsáveis pela gestão dos acessos aos sistemas corporativos no âmbito do INSS poderá ser procedida das seguintes formas:

1. a autoridade responsável pela indicação do gestor de acessos pode indicar opcionalmente o substituto;

2. o próprio gestor de acessos pode designar, a qualquer momento, por meio da ferramenta de gestão de acessos um substituto; ou

3. quando não houver um gestor responsável, ou substituto, por uma unidade devidamente designado, a gestão dos usuários será transferida, preferencialmente de forma automática, para o responsável pela área da abrangência daquela unidade e assim subsequentemente; e

4. o Gestor de Acesso é corresponsável com os perfis de gestão ou acesso que ele atribuir aos usuários.

c) ao usuário interno cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Política de Controle de Acesso Lógico e suas normas complementares;

2. solicitar, ao Gestor de Acesso responsável pela gestão da unidade de lotação a qual é vinculado, a suspensão do seu perfil de acesso nos períodos de afastamento do serviço por mais de trinta dias consecutivos;

3. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e

4. ter conhecimento e estar de acordo com o disposto nesta Política.

d) ao usuário externo cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Política de Controle de Acesso Lógico;

2. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e

3. ter conhecimento e estar de acordo com o disposto nesta Política.

e) ao administrador do sistema INSS cabe:

1. criar os sistemas e subsistemas, devidamente homologados pela área de negócio responsável, no ambiente de produção, por meio de ferramenta de gestão de acesso;

2. mediante apresentação de Portaria de designação para Gestores de Acesso Central, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores quanto à atribuição dos perfis de gestão; e

3. mediante apresentação de Portaria de designação para Gestores de Sistema, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores acerca do processo de implementação dos sistemas corporativos no âmbito do INSS.

f) ao gestor de sistema cabe:

1. efetuar os procedimentos de importação, inclusão, alteração e exclusão de papéis e permissões nos sistemas corporativos em ambiente de produção; e

2. atuar, em conjunto com o Administrador do Sistema INSS e a Dataprev, no planejamento e execução do processo de implementação dos sistemas corporativos dos quais for designado responsável.

g) ao gestor de acesso central cabe:

1. efetuar o credenciamento, suspensão ou exclusão de perfis de gestão dos sistemas corporativos aos Gestores de Acesso na Administração Central e, quando necessário, dos Gestores de Acesso da Superintendência Regional, Gerência Executiva, Agência da Previdência Social e demais usuários de sua abrangência; e

2. orientar os usuários de sua abrangência e os gestores da Administração Central e Superintendências Regionais, Gerências Executivas e Agências da Previdência Social acerca das regras para o acesso aos sistemas corporativos do INSS.

h) ao gestor de acesso interno cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários da Administração Central, Superintendência Regional, Gerência Executiva, Agência da Previdência Social;

2. atribuir, alterar ou excluir os perfis de acesso aos usuários da Administração Central, Superintendência Regional, Gerência Executiva, Agência da Previdência Social; e

3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS.

i) ao gestor de acesso externo cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários do seu Órgão/Entidade;

2. atribuir, alterar ou excluir os perfis de acesso aos usuários do seu Órgão/Entidade; e

3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS.

V - configura-se mau uso, sujeito a responsabilidade penal, civil e disciplinar:

a) a divulgação, sem autorização expressa da chefia imediata ou do gestor de acesso de sua abrangência, de informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS;

b) acessar sistemas corporativos sem autorização prévia, de acordo com os requisitos estabelecidos nesta Política;

c) utilizar-se das informações obtidas por meio de acesso concedido em desacordo com os procedimentos dispostos nesta Política e demais normas vigentes na Administração Pública Federal;

d) compartilhar ou fazer uso das credenciais de acesso, aos sistemas corporativos, de outros usuários;

e) a instalação de sistemas corporativos em equipamentos particulares; e

f) em casos excepcionais, a área responsável pela gestão de TIC do INSS, mediante ato formal, poderá autorizar o contido no Art.8º, III.

Art. 8º Disposições Gerais:

I - todo acesso à rede de dados e aos sistemas corporativos deve ser registrado e monitorado de modo que permita a rastreabilidade, a identificação e o bloqueio de usuários e equipamentos não autorizados. Estas informações devem ser armazenadas por um período de, no mínimo, 30 (trinta) meses;

II - as ocorrências de mau uso do acesso aos recursos disponíveis na rede e sistemas corporativos não previstas nesta norma e os casos omissos serão encaminhados para a área responsável pela gestão de TIC no âmbito do INSS para análise e pronunciamento;

III - identificada irregularidade de mau uso dos recursos de rede poderá ocorrer:

a) o bloqueio preventivo do acesso pela DTI, o encaminhamento de dossiê com as informações para a Corregedoria-Geral do INSS ou Corregedorias Regionais, nas suas áreas de abrangências, a fim de que seja realizada a análise no âmbito disciplinar; e

b) ressalta-se que o descumprimento dessa política poderá resultar em sanções administrativas, civis e criminais.

IV - esta norma deve ser revisada num período máximo de três anos.

ANEXO II

PORTARIA Nº ____/PRES/INSS, DE ____ DE 2020 TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF: _____, identidade _____, expedida pelo _____, em _____, e lotado no(a) _____ do Instituto Nacional do Seguro Social – INSS, DECLARO, sob pena das sanções cabíveis nos termos da Política de Segurança da Informação e Comunicações - POSIC do INSS que assumo a responsabilidade por:

I - tratar o(s) ativo(s) de informação como patrimônio do Instituto Nacional do Seguro Social;

II - utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do INSS;

III - contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, que Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;

IV - utilizar as credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do INSS;

V - responder, perante o INSS, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

_____, _____ de _____ de _____

Assinatura do usuário

Nome do usuário:	Unidade de Lotação:
Nome da Autoridade Responsável pela Autorização do Acesso:	

Assinatura e Carimbo do Responsável pela Autorização de Acesso



INSTITUTO NACIONAL DO SEGURO SOCIAL
MINUTA DE RESOLUÇÃO

MINUTA DE RESOLUÇÃO

**RESOLUÇÃO Nº 4/CEGOV/INSS, DE DE
DE 2020**

Institui a Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR do INSS.
Instituto Nacional do Seguro Social.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída a Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR do INSS.

Art. 2º Os Anexos a esta Portaria serão publicados em Boletim de Serviço.

Art. 3º Esta Portaria complementa Política de Segurança da Informação e Comunicações POSIC-INSS vigente.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretora de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **FLAVIO FERREIRA DOS SANTOS**, Diretor de Tecnologia da Informação e Inovação, em 02/03/2020, às 17:42, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0411846** e o código CRC **136BEE4**.

ANEXO I

RESOLUÇÃO Nº 4/CEGOV/INSS, DE DE DE 2020
EQUIPE DE TRATAMENTO DE INCIDENTES DE REDES COMPUTACIONAIS - ETIR

Art. 1º Para os efeitos desta norma ficam estabelecidos os seguintes conceitos e definições:

I - agente responsável: Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

II - artefato malicioso: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

III - comunidade ou Público Alvo: é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

IV - CTIR GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI;

V - equipe de tratamento e resposta a incidentes em redes computacionais – ETIR: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

VI - incidente de segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VII - serviço: é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

VIII - tratamento de Incidentes de Segurança em Redes Computacionais: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

IX - vulnerabilidade: é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados; e

X - usuário: pessoas que fazem uso de serviços de TI e sistemas de informação de propriedade do INSS, independente do cargo ocupado (contratados, consultores, conselheiros, servidores, temporários e etc).

Art. 2º Esta norma tem a missão de:

Parágrafo único. Agir proativamente, receber, analisar, monitorar, coordenar e propor respostas a notificações e atividades relacionadas a incidentes de segurança da informação e comunicações no âmbito do Instituto.

Art. 3º Esta norma tem como público alvo:

I - a abrangência das atividades pertinentes à ETIR-INSS inclui os usuários dos serviços de Tecnologia da Informação e Comunicações - TIC e os sistemas de informação do INSS;

II - as atividades pertinentes à ETIR-INSS serão realizadas com intercâmbio de informações e em cooperação com as seguintes instâncias:

a) o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR GOV;

b) a Comissão de Resposta e Tratamento de Incidentes em Redes Computacionais –CTIR, da Empresa de Tecnologia e Informações da Previdência Social - Dataprev;

c) equipes de tratamento de incidentes de redes computacionais dos demais órgãos, entidades e empresas, públicas ou privadas, que tenham contratos, acordos, convênios ou instrumentos congêneres com o INSS; e

d) o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República – GSI/PR.

Art. 4º a implementação e o funcionamento da ETIR-INSS seguirão a metodologia definida na Norma Complementar Nº 05 à luz da Instrução Normativa Nº 01 do Gabinete de Segurança Institucional da Presidência da República, de 04 de agosto de 2009, conforme definido a seguir:

I - o modelo de implementação no qual a ETIR-INSS se baseia é o “Modelo 1 – Utilizando a equipe de Tecnologia da Informação”, definido na Norma Complementar Nº 05;

II - a equipe será composta por profissionais da área de Tecnologia da Informação, lotados na Diretoria de Tecnologia da Informação e Inovação – DTI, sem prejuízo de suas atribuições típicas do cargo, com experiência e conhecimentos técnicos compatíveis com a importância da missão da ETIR-INSS;

III - a equipe será composta por servidores públicos efetivos;

IV - a ETIR-INSS ficará vinculada tecnicamente à Coordenação de Infraestrutura e Operações – CGIN, da Diretoria de Tecnologia da Informação e Inovação - DTI; e

V - o Coordenador da ETIR-INSS será o Gestor de Segurança da Informação e Comunicações, conforme definido na Política de Segurança da Informação e Comunicações – POSIC-INSS.

Art. 5º A ETIR-INSS será composta por membros:

I - permanentes: que efetivamente atuarão em todos os incidentes registrados; e

II - Colaboradores: que atuarão, de forma esporádica, no tratamento de incidentes relacionados às suas áreas de atuação.

III - sendo assim, a ETIR-INSS será formada pelos seguintes servidores:

Papel	Nome	Matrícula	Setor
Permanente	Roberto Rufino da Costa	1.057.683	Serviço de Segurança em TIC
Permanente	Nelson Antonio Pimentel Jacinto	1.095.044	Serviço de Segurança em TIC
Colaborador	Cristiano Santos de Souza	2.156.073	Divisão de Infraestrutura e Operações
Colaborador	Lourival de Sousa	2.262.639	Divisão de Infraestrutura e Operações
Colaborador	Jair Rodrigues Fernandes	2.276.407	Divisão de Infraestrutura e Operações
Colaborador	Rodrigo Gomes Rodrigues	2.135.059	Divisão de Arquitetura e Soluções

Art. 6º Quanto autonomia da ETIR-INSS:

I - terá autonomia limitada para o tratamento de incidentes de Segurança da Informação, devendo implementar ações que possam impactar outras áreas do Instituto somente com anuência do Diretor de Tecnologia da Informação e Inovação e do gestor responsável pela área/sistema afetada; e

II - poderá, ainda, gerar relatórios técnicos sugerindo a adoção de medidas para resolução de incidentes.

Art. 7º A ETIR-INSS fornecerá o serviço de Tratamento de Incidentes de Segurança em Redes Computacionais:

I - este serviço compreende basicamente as seguintes ações:

- a) recepção: receber solicitações e alertas diversos. Para tanto o Instituto disponibilizará como canal de comunicação a caixa postal etir@inss.gov.br;
- b) filtrar: todo conteúdo direcionado para a ETIR deve ser verificado, a partir desta análise deve ser tratado pela equipe ou, não se tratando de um incidente de segurança em redes computacionais, encaminhado para a área competente;
- c) catalogar: os incidentes devem ser catalogados em ferramenta a ser indicada pela DTI, com nível de acesso restrito;
- d) classificar: os incidentes devem ser classificados quanto ao nível de severidade e impacto;
- e) tratar o incidente: indicar o tratamento do incidente com medidas corretivas e formas de se evitar que ocorra novamente;
- f) responder: as solicitações e alertas encaminhados para a ETIR devem ser devidamente respondidos; e
- g) monitorar: monitorar a aplicação do tratamento dos incidentes indicados.

II - a ETIR deve analisar os incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências; e

III - o detalhamento dos serviços prestados pela ETIR-INSS deve ser publicado em página específica da Intranet do Instituto no prazo de 30 dias a partir da publicação desta portaria.



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 5/CEGOV/INSS, DE DE DE 2020

Disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis Internet, competências e conteúdo de acesso para cada perfil.

O **COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS**, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída, nos termos do Anexo I desta Portaria, norma que estabelece critérios para uso da Internet no âmbito do Instituto Nacional do Seguro Social - INSS.

Art. 2º Os Anexos a esta Portaria serão publicados em Boletim de Serviço.

Art. 3º Esta Portaria complementa a Política de Segurança da Informação e Comunicações POSIC-INSS vigente.

Art. 4º Revoga-se a Portaria Conjunta MDS/DTP/INSS nº 1/2005.

Art. 5º Esta Portaria entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretora de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **FLAVIO FERREIRA DOS SANTOS**, Diretor de Tecnologia da Informação e Inovação, em 02/03/2020, às 17:43, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0411856** e o código CRC **82CDCC8D**.

ANEXO I

RESOLUÇÃO Nº 5/CEGOV/INSS, DE DE DE 2020

NORMA DE USO DA INTERNET

Art. 1º Esta norma se aplica a todos os servidores e colaboradores, vinculados direta ou indiretamente ao INSS, bem como a servidores e empregados de entidades e órgãos da Administração Pública ou privadas que necessitem ou estejam autorizados a acessar a Internet a partir da rede corporativa do Instituto.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União – AGU que atuarem na consultoria e no assessoramento jurídico, e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta norma, ficam estabelecidos os seguintes conceitos e definições:

I - internet: é a rede mundial que interliga computadores de diferentes tipos e dimensões e permite a comunicação entre pessoas e organizações, independentemente da localização geográfica;

II - intranet: é a rede de computadores administrada pelo INSS, que utiliza os mesmos serviços e tecnologias disponíveis na rede mundial, podendo ser definida como um tipo de Internet Local do Instituto;

III - sítio: um conjunto de informações ou serviços disponíveis na Internet ou na Intranet, organizados em páginas eletrônicas e acessíveis por meio de endereços que identificam, de forma padronizada, sua origem e conteúdo;

IV - perfil de acesso: atributo que estabelece as categorias de sítios acessíveis e tipos de arquivos que podem ser recebidos ou transmitidos pelos usuários;

V - usuário: Servidores, estagiários, terceirizados, contratados e colaboradores, que na execução de suas atividades necessitem de acesso à Internet;

VI - autorizador: ocupantes de cargos que serão responsáveis pela autorização da concessão de perfis de acesso para usuários finais de sua área de abrangência;

VII - proxy: desempenha a função de conexão do computador (local) à rede externa (Internet). Como os endereços locais do computador não são válidos para acessos externos, cabe ao proxy enviar a solicitação do endereço local para o servidor, traduzindo e repassando-a para o seu computador;

VIII - VPN: Trata-se de uma rede privada construída sobre a infraestrutura de uma rede pública. Essa é uma forma de conectar dois computadores por meio de uma rede pública, como a Internet; e

Art. 3º Essa norma tem como diretrizes:

I - o acesso à Internet disponibilizado pelo Instituto Nacional do Seguro Social aos usuários deve ser utilizado exclusivamente em razão de trabalho, cumprindo os procedimentos dispostos nesta norma;

II - os recursos disponibilizados pelo Instituto, não poderão ser usados para quaisquer propósitos que sejam ilegais ou proibidos, de modo a danificar, desativar, sobrecarregar ou prejudicar qualquer área, serviço ou conteúdo, ou interferir no uso e execução das atividades laborais de outros usuários;

III - o volume de tráfego de Internet e os endereços *web* visitados poderão ser monitorados, visando assegurar o cumprimento desta norma; e

IV - o acesso à Internet para propósitos particulares ou estranhos às atividades do INSS poderá ser bloqueado, sem prévia comunicação ao usuário e sem prejuízo das demais sanções aplicáveis.

Art. 4º Quando aos Perfis de Acesso:

I - o acesso aos sítios da Internet para todos os usuários será realizado mediante a atribuição de perfis de acesso;

II - o processo de solicitação e autorização de perfil de acesso à Internet do INSS compreenderá os seguintes perfis:

a) Perfil 1 - Perfil Restrito, deve ser inicialmente atribuído para usuários com maior restrição de acesso à internet, permitido acessar somente sítios governamentais, instituições bancárias e sítios considerados de interesse do INSS;

b) Perfil 2 - Perfil Básico, deve ser inicialmente atribuído para estagiários, recepcionistas e usuários externos. O usuário poderá acessar todos os sítios permitidos pelo Perfil 1, sítios de provedores de e-mail pessoal e instituições de ensino;

c) Perfil 3 - Perfil Padrão, para os servidores do quadro do Instituto. O usuário poderá acessar a todos sítios da internet sem a veiculação de material em áudio e vídeo; e

d) Perfil 4 - Perfil Avançado, deve ser atribuído preferencialmente para servidores do quadro do Instituto e estagiários que desempenham funções relacionadas à Comunicação Social, Desenvolvimento de Pessoas e gestores, respeitado o princípio da necessidade de conhecer, designados pelos Autorizadores deste perfil. O usuário poderá acessar todos os sítios da Internet, incluindo sítios que veiculam material em áudio e vídeo (*streaming*), sítios de compartilhamento de vídeos, blogs e redes sociais.

III - o perfil concedido a agentes externos é de caráter temporário, com validade equivalente à vigência do trabalho a ser executado;

IV - o processo de alterações, bloqueios, liberações e categorizações de sítios, assim como a criação e/ou alterações de perfis de acesso descritos nesta norma, quando necessários, serão definidos pela Diretoria de Tecnologia da Informação e Inovação – DTI, e publicado no Portal do INSS na Intranet; e

V - os novos usuários que não tiverem um perfil de acesso atribuído, devem ser direcionados para uma página da intranet contendo orientações e normas relacionadas ao acesso à internet no INSS, entre outras informações definidas pela DTI.

Art. 5º Acesso de Usuários Externos:

I - quanto ao acesso de servidores ou funcionários públicos externos:

a) o acesso à Intranet e Internet a partir da rede de dados corporativa, nas dependências do INSS, aos demais órgãos da Administração Pública Direta e Indireta, de qualquer das esferas de governo, será concedido exclusivamente para servidores e empregados públicos, efetivos ou ocupantes de cargo em comissão;

b) os acessos dos usuários externos das entidades que compõem o Poder Público serão concedidos mediante o estabelecimento de acordos ou convênios específicos firmados com o INSS;

c) o gestor ou Coordenador-Geral da área responsável pelo convênio, contrato, ACT ou instrumento congênere, assumirá o papel de Autorizador do serviço de acesso à internet para usuários externos e deverá fundamentar as solicitações com base no instrumento; e

d) poderão ser concedidos acessos temporários para auditores de controle interno e externo, vinculados à Controladoria-Geral da União – CGU ou do Tribunal de Contas da União - TCU, no uso de suas atribuições.

II - quanto ao acesso de terceirizados:

a) o acesso à Internet por terceirizados deve ser provido pela empresa contratada;

b) em caráter de exceção, será concedido o acesso aos terceirizados a partir da infraestrutura de rede do INSS, desde que preenchidos os seguintes requisitos:

1. o contrato de prestação de serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

2. a empresa contratada deverá manter com seus funcionários Termo de Confidencialidade;

3. o contrato deve prever a necessidade de acesso à internet a partir das dependências do Instituto; e

4. o Autorizador, que para estes fins será o gestor do contrato ou o responsável pela área requisitante do serviço, deverá fundamentar as necessidades de acesso do contratado, definindo os recursos que devem ser disponibilizados, endereços da Intranet e Internet necessários para o desenvolvimento das atividades, bem como eventuais restrições a dias e horários para realização do acesso.

III - quanto ao acesso de visitantes:

a) a conexão de equipamentos pessoais à rede do Instituto, quando necessária e motivada pelo interesse da Administração, deve ser previamente autorizada pelo gestor da unidade onde o equipamento será utilizado;

b) só será permitida a utilização da rede local por equipamentos que atendam a todos os requisitos estabelecidos pela DTI; e

c) o acesso se dará, exclusivamente, à Internet, sendo vedado o acesso ao conteúdo disponibilizado na intranet.

Art. 6º A todos os perfis de acesso descritos nesta norma aplicam-se as restrições de acesso a sítios que:

I - contenham material pornográfico ou obsceno;

II - contenham material ilegal;

III - disponibilizem jogos, inclusive os da Internet (online);

IV - contenham material impróprio, ofensivo, preconceituoso ou discriminatório, que façam apologia à violência, ao terrorismo e às drogas; e

V - contenha e/ou divulgue conteúdo de violação de direito autoral (pirataria) e/ou execução de quaisquer tipos ou formas de fraudes.

Art. 7º Quanto ao processo de atribuição de acesso à Internet:

I - a atribuição dos perfis de acesso à Internet serão feitas pelos Autorizadores, de forma fundamentada respeitando o princípio da necessidade de conhecer, de acordo com a tabela abaixo:

Perfil	Autorizador
Perfil 1, 2 e 3	Gerente de APS, Gerente Executivo, Superintendentes Regionais, Procuradores Regionais, Coordenadores-Gerais, Superintendentes Regionais, Presidente do INSS, Auditor-Geral, Coordenadores-Gerais, Corregedoria-Geral, Procurador-Chefe da PFE-INSS, Diretores, Gestor ou chefe da área responsável pelo Contrato ou ato administrativo similar no âmbito do INSS.
Perfil 4	Chefes de Assessoria de Comunicação Social nas Superintendências Regionais, Assessor de Comunicação Social (Administração Central) e Presidente do INSS.

II - nos casos de novos usuários de rede (LDAP), criados por meio de registro de chamado técnico, quando o solicitante não indicar o perfil de acesso à internet, será atribuído o Perfil 1;

III - para proceder a alteração do perfil de acesso, os usuários deverão preencher “Formulário de Acesso à Internet” (Anexo II) e providenciar a assinatura pelo Autorizador do acesso; e

IV - ao registrar a solicitação, deve-se anexar o Formulário de Solicitação de Acesso à Internet devidamente preenchido e assinado (pelo solicitante e Autorizador), conforme documento nato digital ou digitalizado no formato PDF.

Art. 8º A solicitação para perfis de acesso em caráter temporário devem indicar no Formulário de Solicitação de Acesso à Internet, a motivação da necessidade e a data de expiração do acesso.

Art. 9º Responsabilidades:

I - o usuário deve:

- a) preencher os requisitos e termos estabelecidos nesta norma;
- b) estar devidamente autorizado a utilizar a Internet nas formas estabelecidas nesta norma;
- c) fazer uso da Internet de forma responsável e segura, utilizando o acesso exclusivamente em razão de trabalho, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal; e
- d) impedir a divulgação e compartilhamento das chaves de segurança atribuídas, que são pessoais e intransferíveis.

II - o autorizador deve:

- a) conceder os perfis de acesso à internet rigorosamente de acordo com as atribuições dos usuários de sua abrangência, observando os normativos do INSS;
- b) verificar periodicamente o uso dos acessos concedidos e, sempre que necessário, solicitar alteração dos perfis de acesso dos usuários de sua abrangência; e
- c) reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à equipe de tratamento de incidentes de rede do INSS.

III - a área responsável pela gestão de TIC no INSS deve:

- a) monitorar os acessos à internet e sua utilização de acordo com as diretrizes estabelecidas nesta norma; e
- b) identificar os casos de mau uso da Internet e adotar uma ou mais das seguintes providências:
 - 1. alertar ao usuário, responsável pelo acesso, e ao Autorizador, responsável pela concessão, acerca do uso indevido da internet;
 - 2. nos casos de reincidência, solicitar a revogação do acesso à internet concedido ao usuário; e
 - 3. encaminhar a documentação que comprova a má utilização do acesso concedido para Corregedoria do INSS, para análise e adoção das medidas cabíveis.

Art. 10º As seguintes práticas configuram-se como uso indevido da internet:

- I - acessar a internet disponibilizada pelo Instituto sem estar devidamente autorizado, conforme estabelecido nesta norma;
- II - não manifestar concordância com as regras estabelecidas nesta norma e nas demais aplicáveis;
- III - fazer uso dos recursos de Internet disponibilizado pelo Instituto para fins alheios ao trabalho, em discordância com os procedimentos dispostos nesta norma, sem prejuízo de demais normatizações vigentes na Administração Pública Federal;
- IV - utilizar os serviços extrapolando os privilégios do perfil de acesso que lhe foi designado;
- V - divulgação e compartilhamento das chaves de segurança, que são pessoais e intransferíveis, permitindo a utilização por terceiros do perfil que lhe foi atribuído;
- VI - praticar atos de comercialização de produtos e serviços, em proveito próprio ou de terceiros, que não atendam os interesses do INSS;
- VII - utilizar recursos ou dispositivos para acesso a computadores ou redes externas ao Instituto, com o objetivo de obter informações não autorizadas ou provocar a interrupção de serviços de rede;
- VIII - utilizar modem ou dispositivo de rede que interligue a rede interna do INSS a outras redes ou à Internet;
- IX - a exposição, o armazenamento, a distribuição, a edição, a gravação e o compartilhamento, através do uso dos recursos computacionais e de comunicação do INSS, de arquivos estranhos às atividades do Instituto e não autorizados pela chefia imediata;

X - realizar qualquer atividade que apoie ou facilite os vazamentos de dados;

XI - baixar arquivos ou programas da Internet que contrariem as diretrizes da Política de Segurança da Informação e Comunicações – POSIC vigente; e

XII - utilizar *proxy* não disponibilizado pelo INSS.

Art. 11 O acesso à Internet é passível de registro e monitoração, incluindo quaisquer dados transmitidos pela rede do INSS.

Art. 12 Disposições Gerais:

I - em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a ETIR deverá ser imediatamente acionada, para tomar as providências necessárias a fim de sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação do INSS;

II - as ocorrências de mau uso do acesso à internet não previstas nesta norma, assim como os casos de dúvidas em relação à aplicação das disposições aqui estabelecidas, devem ser encaminhadas à DTI para registro, análise e avaliação da necessidade de alterações de acordo com o processo de governança em vigência no Instituto;

III - o descumprimento desta norma, poderá acarretar ao usuário as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei, responsabilidade administrativa, civil e criminal; e

IV - esta norma deve ser atualizada periodicamente, não excedendo o prazo máximo de 3 anos.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência

Diretoria De Tecnologia da Informação e Inovação

Coordenação De Governança e Planejamento De Tecnologia da Informação e Comunicação

DESPACHO

Coordenação De Governança e Planejamento De Tecnologia da Informação e Comunicação, em 02/03/2020.

Ref.: Processo nº 35014.047735/2020-84

Int.: DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO

A s s . : Instrução de processo para proposição de resoluções do CEGOV para instituição de normas de segurança da informação e comunicação, em atendimento ao Decreto nº 9.637, de 26 de dezembro de 2018, que trata da Política Nacional de Segurança da Informação do Poder Executivo Federal.

1. Em atendimento ao despacho CEGOV 0409817, informa-se:

1.1. A nota técnica que justifica a necessidade de edição das normas em tela foi apresentada no Processo nº 35014.015095/2020-43 documento SEI 0427234. Esse processo trata da apresentação das normas no âmbito do Comitê Temático de Governança Digital - CTGD.

1.2. Sobre as eventuais demandas de ajustes solicitados pelas áreas, registra-se o email enviado pelo Auditor-Geral (SEI 0422403) e uma reunião presencial com o Sr. Corregedor-Geral. Esses foram os únicos ajustes demandados após a reunião do CEGOV.

1.2.3 Em relação ao email enviado pelo Sr. Auditor-Geral, informa-se que os itens "a" e "c" foram atendidos. Sobre o item "b", as automatizações citadas ainda estão em desenvolvimento pela Dataprev não sendo possível estabelecer em norma o alcance dessas mudanças. Dessa forma, achou-se razoável não haver previsão sobre o referido período de transição na referida norma.

1.2.4 Os ajustes relatados pelo Sr. Corregedor-Geral foram todos acatados.

2. Feitas as considerações, encaminhe-se à Secretaria-Executiva do CEGOV para prosseguimento.

FLÁVIO FERREIRA DOS SANTOS

Diretor de Tecnologia da Informação e Inovação

Coordenador do Comitê Temático de Governança Digital (CTGD)



Documento assinado eletronicamente por **FLAVIO FERREIRA DOS SANTOS**, **Diretor de Tecnologia da Informação e Inovação**, em 02/03/2020, às 17:49, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site

https://sei.inss.gov.br/sei/controlador_externo.php?

[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0421219** e o código CRC **1A4F1590**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 0421219



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência

Diretoria De Integridade, Governança e Gerenciamento De Riscos

Comitê Temático de Governança Digital

NOTA TÉCNICA Nº 1/2020/CTGD - CEGOV/DIGOV/PRES-INSS

PROCESSO Nº 35014.015095/2020-43

INTERESSADO: DTI, DGPA, DIRAT, DIRBEN, DIGOV

**Minutas de
normativos de
segurança da
informação e
comunicação**

1. Trata-se de nota técnica de apresentação de minutas de normativos de segurança da informação e comunicação.

2. A Portaria nº 3.213/2019 criou o Comitê Temático de Governança Digital definindo sua respectiva composição e atribuições.

3. A Portaria nº 59/2020 designou os membros dos comitês temáticos de apoio à governança que compõem o Sistema de Governança do INSS – SG-INSS. O art 2º detalhou a composição do Comitê Temático de Governança Digital (CTGD) da seguinte forma:

I - pela Diretoria de Tecnologia da Informação e Inovação: **Flávio Ferreira dos Santos**, que o coordenará;

II - pela Diretoria de Benefícios: **Roberto Dal Col Filho**;

III - pela Diretoria de Atendimento: **Ailton Nunes de Matos Júnior**;

IV - pela Diretoria de Gestão de Pessoas e Administração: **Gilvaneire Cavalcanti Beltrão**; e

V - pela Diretoria de Integridade, Governança e Gerenciamento de Riscos: **Cibelle Cesar do Amaral Brasil**.

4. São atribuições do CTGD:

I - propor políticas e diretrizes de tecnologia da informação e comunicação alinhadas à Política de Governança Digital, nos termos do Decreto nº 8.638, de 15 de janeiro de 2016, e do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP);

II - elaborar e propor ao CEGOV o plano diretor de tecnologia da informação e comunicação do INSS, nos termos do Decreto nº 8.638, de 2016;

III - monitorar a execução do plano diretor de tecnologia da informação e comunicação do INSS, e dar conhecimento ao CEGOV sobre a necessidade de revisões;

IV - identificar e propor a priorização de projetos e contratações de tecnologia da informação e comunicação, por meio da composição dos interesses das diferentes áreas demandantes, de modo a compatibilizar a alocação de recursos às diretrizes estratégicas estabelecidas

pelo CEGOV ou diretamente pela Presidência do INSS;

V - assessorar na implementação das ações de segurança da informação necessárias ao cumprimento da Política Nacional de Segurança da Informação, nos termos do Decreto nº 9.637, de 26 de dezembro de 2018;

VI - propor e monitorar a política e os planos de segurança da informação e comunicações do INSS, nos termos do Decreto nº 9.637, de 2018; e

VII - propor e acompanhar indicadores de desempenho, planos e normas internas relativas à gestão de tecnologia da informação e comunicação.

5. Para a realização da primeira reunião ordinária, esta Coordenação do CTGD apresenta como pauta os seguintes itens para discussão e validação prévia ao CEGOV:

- POSIC - Política de Segurança da Informação e Comunicações (0246296)

- PCAL - Política de Controle de Acesso Lógico (0246412)

- ETIR - Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais (0247354)

- Norma de uso da internet (0247495)

6. Sobre a POSIC, cabe esclarecer que o objetivo visa estabelecer e difundir diretrizes e princípios de Segurança da Informação e Comunicações – SIC, com vistas à orientação para uso e proteção adequados das informações produzidas e custodiadas pelo Instituto, preservando sua disponibilidade, integridade, confidencialidade e autenticidade, conforme Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008; e Norma Complementar nº 03/IN01/DSIC/GSIPR, de 3 de julho de 2009.

7. A PCAL define regras para a emissão de credenciais de acesso lógico no âmbito do INSS, conforme Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008 e Norma Complementar nº 7/IN01/DSIC/GSIPR de 6 de maio de 2010;

8. Sobre a ETIR, sua criação está disciplinada pela Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009 que estabelece as diretrizes de criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais e seu modelo de implementação. A ETIR tem por missão agir proativamente, receber, analisar, monitorar, coordenar e propor respostas a notificações e atividades relacionadas a incidentes de segurança da informação e comunicações no âmbito do Instituto.

9. A Norma de uso da Internet regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso permitido para cada perfil, conforme política definida pelo órgão, visando otimizar o tráfego de rede para as atividades finalísticas da instituição.

10. Portanto, cabe o CTGD avaliar as minutas de normativos de segurança da informação propostas pela equipe técnica da DTI visando um alinhamento com as áreas de negócio.

11. Diante do exposto, encaminham-se as minutas de resoluções e portarias constante deste processo para discussão e ajustes necessários com o intuito de apresentação ao CEGOV para aprovação final.

Brasília, 24 de janeiro de 2020.

FLÁVIO FERREIRA DOS SANTOS

Coordenador do Comitê Temático de Governança Digital (CTGD)



Documento assinado eletronicamente por **FLAVIO FERREIRA DOS SANTOS, Coordenador(a)**, em 24/01/2020, às 11:23, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site
https://sei.inss.gov.br/sei/controlador_externo.php?



[acao=documento_conferir&id_orgao_acesso_externo=0](#), informando o código verificador **0248219** e o código CRC **F278FEF4**.

Referência: Processo nº 35014.015095/2020-43

SEI nº 0248219



INSTITUTO NACIONAL DO SEGURO SOCIAL

Comitê Estratégico de Governança

DESPACHO

Comitê Estratégico de Governança, em 04/03/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass. Edição de Resoluções
do Comitê Estratégico de
Governança - CEGOV -
para instituição de normas
de segurança da
informação e comunicação
no âmbito do INSS.

1. Trata-se de processo para edição de resoluções destinadas à instituição de normas de segurança da informação e comunicação no âmbito do INSS, em atendimento ao Decreto nº 9.637, de 26 de dezembro de 2018, que cria a Política Nacional de Segurança da Informação do Poder Executivo Federal, quais sejam:

- 1.1. Política de Segurança da Informação e Comunicações (Minuta de Resolução nº 0411821);
- 1.2. Norma de Controle de Acesso Lógico (Minuta de Resolução nº 0411838);
- 1.3. Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR (Minuta de Resolução nº 0411846);
- 1.4. Norma de uso da Internet (Minuta de Resolução nº 0411856).

2. Primeiramente cabe informar que, com a criação do Sistema de Governança do INSS, por meio da Portaria nº 3.213/PRES/INSS/2019, o Comitê Estratégico de Governança do INSS - CEGOV - tem a competência de deliberar em última instância sobre os assuntos relativos à segurança da informação, previstas no Decreto nº 9.637/2018.

3. A Nota Técnica nº 0427234, anexada ao presente processo, emitida pela Diretoria de Tecnologia da Informação e Inovação - DTI, justifica tecnicamente o escopo e a necessidade e edição de cada norma de segurança aqui proposta.

4. As normas foram discutidas e aprovadas, primeiramente, no âmbito do Comitê Temático de Governança Digital (vide processo SEI nº 35014.015095/2020-43) e, posteriormente, no âmbito da CEGOV (vide processo SEI nº 35014.012037/2020-68).

5. Após a realização dos ajustes demandados pelos membros do CEGOV, e, em atendimento ao disposto na Resolução nº 708/PRES/INSS, de 6 de novembro de 2019, encaminham-se as minutas indicadas no primeiro parágrafo deste despacho para análise da PFE-INSS.

6. Registra-se que as deliberações do CEGOV são aqui propostas por meio de resoluções, em

consonância com o disposto no inciso II do art. 2º do Decreto nº 10.139, de 28 de novembro de 2019.

CIBELLE CESAR DO AMARAL BRASIL

Coordenadora-Geral de Governança
Secretária-Executiva do CEGOV



Documento assinado eletronicamente por **CIBELLE CESAR DO AMARAL BRASIL**,
Coordenador(a) Geral, em 04/03/2020, às 11:45, conforme horário oficial de Brasília, com fundamento
no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site
[https://sei.inss.gov.br/sei/controlador_externo.php?
acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0437711** e o
código CRC **B952CF39**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 0437711



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência

Diretoria De Integridade, Governança e Gerenciamento De Riscos

Comitê Temático de Governança Digital

NOTA TÉCNICA Nº 1/2020/CTGD - CEGOV/DIGOV/PRES-INSS**PROCESSO Nº 35014.015095/2020-43****INTERESSADO: DTI, DGPA, DIRAT, DIRBEN, DIGOV**

**Minutas de
normativos de
segurança da
informação e
comunicação**

1. Trata-se de nota técnica de apresentação de minutas de normativos de segurança da informação e comunicação.

2. A Portaria nº 3.213/2019 criou o Comitê Temático de Governança Digital definindo sua respectiva composição e atribuições.

3. A Portaria nº 59/2020 designou os membros dos comitês temáticos de apoio à governança que compõem o Sistema de Governança do INSS – SG-INSS. O art 2º detalhou a composição do Comitê Temático de Governança Digital (CTGD) da seguinte forma:

I - pela Diretoria de Tecnologia da Informação e Inovação: **Flávio Ferreira dos Santos**, que o coordenará;

II - pela Diretoria de Benefícios: **Roberto Dal Col Filho**;

III - pela Diretoria de Atendimento: **Ailton Nunes de Matos Júnior**;

IV - pela Diretoria de Gestão de Pessoas e Administração: **Gilvaneire Cavalcanti Beltrão**; e

V - pela Diretoria de Integridade, Governança e Gerenciamento de Riscos: **Cibelle Cesar do Amaral Brasil**.

4. São atribuições do CTGD:

I - propor políticas e diretrizes de tecnologia da informação e comunicação alinhadas à Política de Governança Digital, nos termos do Decreto nº 8.638, de 15 de janeiro de 2016, e do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP);

II - elaborar e propor ao CEGOV o plano diretor de tecnologia da informação e comunicação do INSS, nos termos do Decreto nº 8.638, de 2016;

III - monitorar a execução do plano diretor de tecnologia da informação e comunicação do INSS, e dar conhecimento ao CEGOV sobre a necessidade de revisões;

IV - identificar e propor a priorização de projetos e contratações de tecnologia da informação e comunicação, por meio da composição dos interesses das diferentes áreas demandantes, de modo a compatibilizar a alocação de recursos às diretrizes estratégicas estabelecidas

pelo CEGOV ou diretamente pela Presidência do INSS;

V - assessorar na implementação das ações de segurança da informação necessárias ao cumprimento da Política Nacional de Segurança da Informação, nos termos do Decreto nº 9.637, de 26 de dezembro de 2018;

VI - propor e monitorar a política e os planos de segurança da informação e comunicações do INSS, nos termos do Decreto nº 9.637, de 2018; e

VII - propor e acompanhar indicadores de desempenho, planos e normas internas relativas à gestão de tecnologia da informação e comunicações.

5. Para a realização da primeira reunião ordinária, esta Coordenação do CTGD apresenta como pauta os seguinte itens para discussão e validação prévia ao CEGOV:

- POSIC - Política de Segurança da Informação e Comunicações (0246296)

- PCAL - Política de Controle de Acesso Lógico (0246412)

- ETIR - Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais (0247354)

- Norma de uso da internet (0247495)

6. Sobre a POSIC, cabe esclarecer que o objetivo visa estabelecer e difundir diretrizes e princípios de Segurança da Informação e Comunicações – SIC, com vistas à orientação para uso e proteção adequados das informações produzidas e custodiadas pelo Instituto, preservando sua disponibilidade, integridade, confidencialidade e autenticidade, conforme Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008; e Norma Complementar nº 03/IN01/DSIC/GSIPR, de 3 de julho de 2009.

7. A PCAL define regras para a emissão de credenciais de acesso lógico no âmbito do INSS, conforme Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008 e Norma Complementar nº 7/IN01/DSIC/GSIPR de 6 de maio de 2010;

8. Sobre a ETIR, sua criação está disciplinada pela Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009 que estabelece as diretrizes de criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais e seu modelo de implementação. A ETIR tem por missão agir proativamente, receber, analisar, monitorar, coordenar e propor respostas a notificações e atividades relacionadas a incidentes de segurança da informação e comunicações no âmbito do Instituto.

9. A Norma de uso da Internet regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso permitido para cada perfil, conforme política definida pelo órgão, visando otimizar o tráfego de rede para as atividades finalísticas da instituição.

10. Portanto, cabe o CTGD avaliar as minutas de normativos de segurança da informação propostas pela equipe técnica da DTI visando um alinhamento com as áreas de negócio.

11. Diante do exposto, encaminham-se as minutas de resoluções e portarias constante deste processo para discussão e ajustes necessários com o intuito de apresentação ao CEGOV para aprovação final.

Brasília, 24 de janeiro de 2020.

FLÁVIO FERREIRA DOS SANTOS

Coordenador do Comitê Temático de Governança Digital (CTGD)



Documento assinado eletronicamente por **FLAVIO FERREIRA DOS SANTOS, Coordenador(a)**, em 24/01/2020, às 11:23, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site

https://sei.inss.gov.br/sei/controlador_externo.php?



[acao=documento_conferir&id_orgao_acesso_externo=0](#), informando o código verificador **0248219** e o código CRC **F278FEF4**.

Referência: Processo nº 35014.015095/2020-43

SEI nº 0248219



ADVOCACIA-GERAL DA UNIÃO
PROCURADORIA-GERAL FEDERAL
PROCURADORIA FEDERAL ESPECIALIZADA JUNTO AO INSTITUTO NACIONAL DO SEGURO SOCIAL -
PFE/INSS - SEDE
DIVISÃO DE ANÁLISE DE ATOS ADMINISTRATIVOS

PARECER n. 00012/2020/DAADM/PFE-INSS-SEDE/PGF/AGU

NUP: 35014.047735/2020-84

INTERESSADOS: DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO

ASSUNTOS: DIREITO ADMINISTRATIVO E OUTRAS MATÉRIAS DE DIREITO PÚBLICO

EMENTA: I. Direito Administrativo. Gestão Pública. Atos normativos para instituição de políticas e normas de segurança e comunicações do Instituto Nacional do Seguro Social - INSS. Política de Segurança da Informação e Comunicações - POSIC-INSS. Norma de Controle de Acesso Lógico - NCAL. Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR do INSS. Uso da Internet no âmbito do INSS.

II. Regularidade jurídico-formal. Aprovação, desde que atendidas as considerações e sugestões deste parecer.

Senhor Coordenador-Geral de Matéria Administrativa,

1. RELATÓRIO

1. Trata-se de análise jurídico-formal de minutas de Resoluções a serem expedidas pelo Comitê Estratégico de Governança que dispõem, respectivamente, sobre (i) Política de Segurança da Informação e Comunicações (Posic), (ii) Política de Controle de Acesso Lógico, (iii) a criação da Equipe de Tratamento de Incidentes de Redes (ETIR) e (iv) acesso à internet.

2. Os autos foram inaugurados com Despacho SEI/INSS - 0409817 (sequencial sapiens 01- outros 1), pelo qual a Coordenadora-Geral de Governança esclareceu que o processo se trata de proposição de atos normativos para instituição de políticas e normas de segurança e comunicações do Instituto Nacional do Seguro Social - INSS, de competência do Comitê Estratégico de Governança - CEGOV, conforme previsto no art. 5º da Portaria nº 3.213/PRES/INSS/2019.

3. Os autos foram instruídos com os seguintes documentos:

- Minuta de Resolução nº 2/CEGOV/INSS, que atualiza a política de Segurança da Informação e Comunicações - POSIC-INSS (sequencial sapiens 01- outros 3 e 8);
- Minuta de Resolução nº 3/CEGOV/INSS, que institui a Norma de Controle de Acesso Lógico - NCAL, no âmbito do INSS (sequencial sapiens 01- outros 4 e 9);
- Minuta de Resolução nº 4/CEGOV/INSS, que institui a equipe de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR do INSS (sequencial sapiens 01- outros 5 e 10);
- Minuta de Resolução nº 5/CEGOV/INSS, disciplina o uso da Internet no âmbito do INSS (sequencial sapiens 01- outros 6 e 11);
- Ata de Reunião da 1ª Reunião Ordinária do Comitê Estratégico de Governança do INSS em 2020, realizada em 17/02/2020 (sequencial sapiens 01- outros 7);
- Despacho SEI/INSS - 0421219, da Coordenação de Governança e Planejamento De Tecnologia da Informação e Comunicação, exarado pelo Diretor de tecnologia da Informação e Inovação (sequencial sapiens 01- outros 12);
- Cópia e e-mail encaminhado pelo Auditor-Geral, com as considerações realizadas nas minutas inicialmente propostas (sequencial sapiens 01- outros 13);

- o NOTA TÉCNICA Nº 1/2020/CTGD - CEGOV/DIGOV/PRES-INSS (SEI/INSS - 0248219), extraída do NUP: 35014.015095/2020-43 (sequencial sapiens 2 - outros 1).

4. Cabe registrar que o processo em epígrafe está sendo analisado prioritariamente, em detrimento da ordem cronológica de recebimento, haja vista o pedido de urgência formulado pelo Gabinete da Presidência.
5. Com efeito, o procedimento veio para análise desta Procuradoria por força do art. 10 da Lei nº 10.480/2002 c/c o art. 10 da Instrução Normativa Conjunta PGF/INSS nº 01/2010, do art. 15, §4º, da Resolução nº 708/INSS/PRES, de 2019.
6. É o relatório. Passe-se ao exame.

2. FUNDAMENTAÇÃO

7. De início, salienta-se que a presente manifestação toma por base, exclusivamente, os elementos constantes do Sistema Sapiens até a presente data (que conta até o sequencial sapiens - 2- Outros 1), e que, em face do que dispõe o art. 131 da Constituição Federal de 1988 e art. 11 da Lei Complementar nº 73/1993, incumbe, a este órgão de execução da Advocacia-Geral da União prestar assessoria sob o prisma estritamente jurídico, não lhe competindo adentrar na análise da conveniência e oportunidade dos atos praticados no âmbito do INSS, nem analisar aspectos de natureza eminentemente técnica ou administrativa.
8. Consoante se examina dos autos, tratam-se de quatro propostas normativas destinadas a regulamentar políticas e normas de segurança e comunicações do Instituto nacional do Seguro Social - INSS, especificamente a política de Segurança da Informação e Comunicações - POSIC-INSS, a Norma de Controle de Acesso Lógico - NCAL, a equipe de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR do INSS e o uso da Internet no âmbito do INSS.
9. Em vista disso, o presente processo veiculou 4 minutas de Resolução a serem analisadas por esta PFE. Assim, com vistas a facilitar a compreensão, esclarece-se que a análise será realizada de forma conjunta, uma vez que se tratam de normas relativas a políticas e normas de segurança e comunicações do Instituto nacional do Seguro Social - INSS, naquilo que for pertinente. E, em caso de anotações específicas para uma das determinadas proposições, será feito o devido destaque.
10. Quanto à **FORMA** do futuro ato – a Resolução n. 708/INSS/PRES, de 6 de novembro de 2019, que trata da elaboração, redação e alteração dos atos administrativos do INSS, assim estabelece:

Art. 17. Consideram-se atos normativos:

(...)

II - **Resolução**: ato administrativo de competência privativa do Presidente do INSS, utilizado para estabelecer procedimentos ou diretrizes gerais orientadoras da ação dos órgãos e unidades, para fiel aplicação da política e programação do Instituto.

(...)

Art. 20. Considera-se ato constitutivo:

I - Portaria: é o ato administrativo de autoridade competente, no âmbito de suas atribuições regimentais, que:

- a) contém recomendações de caráter técnico e específico;
- b) define, cria e institui normas de execução de serviço e procedimentais;
- c) constitui grupos de trabalho, comitês e comissão;
- d) aprova manuais, guias, cartilhas e minutas padrão;
- e) efetiva nomeações, exonerações, designações, dispensas, punições, delegação e subdelegação; ou
- f) dispõe sobre qualquer outra matéria relativa à gestão administrativa e ao funcionamento das unidades e Diretorias do INSS;

11. Contudo, cumpre destacar o disposto no Decreto nº 10.139, de 28 de novembro de 2019, em vigor desde o dia 03/02/2020, estabelece:

Objeto e âmbito de aplicação

Art. 1º Este Decreto dispõe sobre a revisão e a consolidação dos atos normativos inferiores a decreto editados por órgãos e entidades da administração pública federal direta, autárquica e fundacional.

§ 1º O disposto neste Decreto aplica-se a:

I - portarias;

II - resoluções;

III - instruções normativas;

IV - ofícios e avisos;

V - orientações normativas;

VI - diretrizes;

VII - recomendações;

VIII - despachos de aprovação; e

IX - qualquer outro ato inferior a decreto com conteúdo normativo.

§ 2º O disposto neste Decreto **não se aplica a:**

I - atos cujo destinatário, pessoa natural ou jurídica, esteja nominalmente identificado; e

II - recomendações ou diretrizes cujo não atendimento não implique aos destinatários consequências jurídicas, efetivas ou potenciais.

Espécies admitidas de atos normativos futuros

Art. 2º A partir da entrada em vigor deste Decreto os atos normativos inferiores a decreto serão editados sob a forma de:

I - portarias - atos normativos editados por uma ou mais autoridades singulares;

II - resoluções - atos normativos editados por colegiados; ou

III - instruções normativas - atos normativos que, sem inovar, orientem a execução das normas vigentes pelos agentes públicos.

Parágrafo único. O disposto no **caput** não afasta a possibilidade de:

I - uso excepcional de outras denominações de atos normativos por força de exigência legal; e

II - edição de portarias ou resoluções conjuntas.

12. Observa-se que a Resolução n. 708/INSS/PRES, de 2019, estabelece uma classificação material das normas, dispondo que a Resolução é ato administrativo de competência privativa do Presidente.

13. Nada obstante, o Decreto nº 10.139, de 2019, aplicável a atos normativos inferiores a Decreto, dispôs uma classificação dos atos de acordo com a pessoa que a edita, sem tecer uma classificação puramente material, tampouco uma distinção precisa de atos normativos e atos constitutivos, como o fez a Resolução n. 708/INSS/PRES, de 2019.

14. Nessa óptica, em razão da hierarquia, o Decreto nº 10.139, de 2019 revogou tacitamente a classificação material da Resolução n. 708/INSS/PRES, de 2019.

15. Assim, no presente caso, tratando-se de atos normativos inferiores a decretos e que não se enquadrem na situação descrita no §2º do art. 1º do Decreto nº 10.139, de 2019 ("*atos cujo destinatário, pessoa natural ou jurídica, esteja nominalmente identificado*", e "*recomendações ou diretrizes cujo não atendimento não implique aos destinatários consequências jurídicas, efetivas ou potenciais*"), a serem editados por colegiado (Comitê Estratégico de Governança - CEGOV), entende-se que os atos normativos devem ser editados por meio de Resolução.

16. No tocante à **competência**, vale destacar o disposto na Portaria nº 3.213/PRES/INSS, de 2019, que instituiu o sistema de governança do INSS, estabeleceu:

Art. 4º O Sistema de Governança do INSS é integrado por:

I - Comitê Estratégico de Governança (CEGOV);

II - Comitês temáticos de apoio à governança;

III - Auditoria-Geral; e

IV - Corregedoria-Geral.

§ 1º O CEGOV é órgão colegiado permanente, de caráter delibera|vo, vinculado diretamente à Presidência do INSS, responsável pela coordenação do SG-INSS, com o apoio técnico dos comitês temáticos.

§ 2º A secretaria-execu|tiva do CEGOV será exercida pela Diretoria de Integridade, Governança e Gerenciamento de Riscos - DIGOV.

Art. 5º Compete ao CEGOV:

- I - seguir as recomendações oriundas de manuais, guias e resoluções do Comitê Interministerial de Governança - CIG e encaminhar-lhe as propostas de aperfeiçoamento daqueles instrumentos;
 - II - incentivar, promover e monitorar a implementação de diretrizes e de melhores práticas organizacionais de governança;
 - III - estabelecer diretrizes estratégicas para a busca de melhores resultados para a sociedade, por meio da execução das políticas públicas previdenciária e assistencial;
 - IV - **estabelecer diretrizes para a gestão das políticas públicas executadas pelo INSS**, das contratações, de pessoal, **da tecnologia da informação e comunicação**, da integridade, **dos riscos e da transparência**, de modo a assegurar o alinhamento e a integração da atuação das diversas áreas à missão institucional da autarquia;
 - V - aprovar o planejamento estratégico do INSS e acompanhar os resultados alcançados, com vistas a estabelecer prioridades e determinar a implementação de ações para assegurar o cumprimento dos objetivos definidos;
 - VI - aprovar os planos anuais de ações estratégicas e prioritárias das diversas unidades do INSS, e monitorar sua execução;
 - VII - definir e monitorar os indicadores de resultados do INSS, visando a melhoria do seu desempenho institucional;
 - VIII - aprovar o plano diretor de tecnologia da informação e comunicação e o instrumento de planejamento de segurança da informação e comunicação, nos termos do Decreto nº 8.638, de 15 de janeiro de 2016;**
 - IX - aprovar a distribuição e priorização de recursos de tecnologia da informação e comunicação;**
 - X - acompanhar a execução do plano anual de contratações;
 - XI - deliberar sobre políticas, programas e planos de integridade e gestão de riscos;
 - XII - estabelecer diretrizes para o desenvolvimento dos membros da alta administração e dos servidores do INSS para assegurar que possuam as competências necessárias ao exercício de suas atribuições;
 - XIII - acompanhar a execução do plano de desenvolvimento de pessoas;
 - XIV - estabelecer diretrizes gerais para a integração das bases de dados necessárias ao cumprimento da missão institucional do INSS e promover o compartilhamento e a abertura de informações para o exercício do controle social;
 - XV - promover a transparência, a responsabilidade e a prestação de contas para fortalecer o acesso público à informação e a participação social;
 - XVI - deliberar sobre políticas, programas e ações estratégicas para o aperfeiçoamento da gestão de ativos do INSS;
 - XVII - aprovar o planejamento orçamentário do INSS, de modo a assegurar a distribuição adequada de recursos ao cumprimento da missão e dos objetivos estratégicos do Instituto;
 - XVIII - deliberar sobre propostas apresentadas pelos Comitês temáticos de apoio à governança;**
 - XIX - incentivar, promover e acompanhar a implementação de políticas institucionais de sustentabilidade; e
 - XX - registrar suas deliberações por meio de atas, publicadas em boletim de serviço e disponibilizadas no sítio eletrônico do INSS.
- Parágrafo único. Ao CEGOV cumpre deliberar em última instância, no âmbito do INSS, sobre os assuntos relativos à governança digital, de que trata o Decreto nº 8.638, de 15 de janeiro de 2016, e sobre os assuntos relativos à segurança da informação, de que trata o Decreto nº 9.637, de 26 de dezembro de 2018.**

17. Além disso, a Portaria nº 3.213/PRES/INSS, de 2019, em seu art. 8º, inciso II, criou o comitê temático de governança Digital (CTGD), com a finalidade de subsidiar as ações do CEGOV na área de governança digital, bem como propor políticas públicas, instrumentos e práticas organizacionais necessárias ao atendimento dos princípios e diretrizes de governança pública na área de referência. Nesse sentido, o art. 4º do anexo I da Portaria nº 3.213/PRES/INSS, de 2019, estabeleceu:

Art. 4º São atribuições do Comitê Temático de Governança Digital (CTGD):

- I - propor políticas e diretrizes de tecnologia da informação e comunicação alinhadas à política de Governança Digital, nos termos do Decreto nº 8.638, de 15 de janeiro de 2016, e do Sistema de

Administração dos Recursos de Tecnologia da Informação (SISP);

II - elaborar e propor ao CEGOV o plano diretor de tecnologia da informação e comunicação do INSS, nos termos do Decreto nº 8.638, de 2016;

III - monitorar a execução do plano diretor de tecnologia da informação e comunicação do INSS, e dar conhecimento ao CEGOV sobre a necessidade de revisões;

IV - identificar e propor a priorização de projetos e contratações de tecnologia da informação e comunicação, por meio da composição dos interesses das diferentes áreas demandantes, de modo a compatibilizar a alocação de recursos às diretrizes estratégicas estabelecidas pelo CEGOV ou diretamente pela Presidência do INSS;

V - assessorar na implementação das ações de segurança da informação necessárias ao cumprimento da política Nacional de Segurança da Informação, nos termos do Decreto nº 9.637, de 26 de dezembro de 2018;

VI - propor e monitorar a política e os planos de segurança da informação e comunicações do INSS, nos termos do Decreto nº 9.637, de 2018; e

VII - propor e acompanhar indicadores de desempenho, planos e normas internas relativas à gestão de tecnologia da informação e comunicação.

18. Dessa forma, nos termos da NOTA TÉCNICA Nº 1/2020/CTGD - CEGOV/DIGOV/PRES-INSS (SEI/INSS - 0248219), extraída do NUP: 35014.015095/2020-43 (sequencial sapiens 2 - outros 1), as normas de referência forma propostas pelo CTGD e submetidas à aprovação do CEGOV. Estando, pois as normas adequadas quanto a competência.

19. Quanto ao procedimento, deve-se destacar que, de acordo com o art. 14 da Resolução n. 708/INSS/PRES, de 6 de novembro de 2019, tratando-se de ato normativo, a ser assinado pelo Presidente do INSS, **a respectiva minuta deveria ter sido previamente submetida à apreciação da Coordenação de Suporte ao Gabinete - CSG - da Presidência do INSS.**

20. No caso, conforme anotado, a competência para firmar o ato será exercida pelo Comitê Estratégico de Governança, órgão colegiado permanente vinculado diretamente à Presidência do INSS, conforme art. 4º, §1º, da Portaria nº 3.213/PRES/INSS, de 2019.

21. **Em vista disso, entende-se que deve ser adotada parte da instrução pertinente prevista no art. 14, da Resolução n. 708/INSS/PRES, de 6 de novembro de 2019, inclusive quanto a submissão prévia à Coordenação de Suporte ao Gabinete, para revisão da minuta quanto aspectos redacionais, bem como processo devidamente carreado com a minuta do ato proposto, a documentação em que se fundamenta, e a Nota Técnica com a motivação e fundamento para a expedição do ato proposto.**

22. **Por se tratar de ato de comitê composto por todas as áreas da estrutura desta Autarquia** (vide art. 6º da Portaria nº 3.213/PRES/INSS, de 2019), entende-se que se dispensa a **manifestação das demais Diretorias afetadas, posto que suprimida pela sistemática de reunião do Comitê para aprovação das minutas e contribuições via comunicação digital.**

23. Assim, no ponto, sugere-se que os atos sejam devidamente avaliados pela Coordenação de Suporte ao Gabinete **com o fim de regularizar à devida instrução processual, nos termos apontados.**

24. No que se refere à **motivação e à finalidade**, a Nota Técnica nº 1/2020/CTGD - CEGOV/DIGOV/PRES-INSS (SEI/INSS - 0248219), extraída do NUP: 35014.015095/2020-43 (sequencial sapiens 2 - outros 1) exarou:

5. Para a realização da primeira reunião ordinária, esta Coordenação do CTGD apresenta como pauta os seguintes itens para discussão e validação prévia ao CEGOV:

- POSIC - Política de Segurança da Informação e Comunicações (0246296)

- PCAL - Política e Controle de Acesso Lógico (0246412)

- ETIR - Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais (0247354)

- Norma de uso da internet (0247495)

6. Sobre a POSIC, cabe esclarecer que o objetivos visa estabelecer e difundir diretrizes e princípios de Segurança da Informação e Comunicações – SIC, com vistas à orientação para uso e proteção adequados das informações produzidas e custodiadas pelo Instituto, preservando sua disponibilidade, integridade, confidencialidade e autenticidade, conforme Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008; e Norma Complementar nº 03/IN01/DSIC/GSIPR, de 3 de julho de 2009.

7. A PCAL define regras para a emissão de credenciais de acesso lógico no âmbito do INSS, conforme Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008 e Norma Complementar nº 7/IN01/DSIC/GSIPR de 6 de maio de 2010;

8. Sobre a ETIR, sua criação está disciplinada pela Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009 que estabelece as diretrizes de criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais e seu modelo de implementação. A ETIR tem por missão agir proativamente, receber, analisar, monitorar, coordenar e propor respostas a notificações e atividades relacionadas a incidentes de segurança da informação e comunicações no âmbito do Instituto.

9. A Norma de uso da Internet regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso permitido para cada perfil, conforme política definida pelo órgão, visando otimizar o tráfego de rede para as atividades finalísticas da instituição.

25. Conforme se examina da Ata de Reunião da 1ª Reunião Ordinária do Comitê Estratégico de Governança do INSS em 2020, realizada em 17/02/2020 (sequencial sapiens 01- outros 7), a deliberação para revisão de cada uma das normas referenciadas foi tomada por unanimidade pelos membros do CEGOV. Tendo sido consignada as seguintes razões para as pretendidas revisões:

POSIC - Política de Segurança da Informação e Comunicações:

Aprovação da Política de Segurança da Informação e Comunicações (POSIC)

Foi decidido que a POSIC será revisada pelos membros do CEGOV e aprovada eletronicamente, por meio do SEI, após realização dos ajustes propostos na reunião, quais sejam:

Alterar o Anexo para que seja formatado em conformidade com o Manual de Redação da Presidência da República (Determinação do Art. 58 do Decreto nº 9.191/2017); Verificar se é necessário manter o item 5.8.3. do Anexo e, se necessário, ajustar redação final com a AUDGER;

Revisar as definições referentes a dado, a informação e a ativos de informação, levando em consideração as definições trazidas pela nº Lei 13.709/2018 (LGPD), pela Lei nº 12.527/2011 (Lei de Acesso à Informação) e pelo Decreto nº 10.046/2019 (Decreto de Compartilhamento de Dados);

Incluir definições de termos que tratem da responsabilidade pela gestão das informações;

Incluir menção ao Comitê Temático de Gestão da Informação como responsável pela aprovação de procedimentos e de normas internas que orientem o compartilhamento de dados sob gestão do INSS e pela aprovação da categorização dos níveis de compartilhamento de dados com outras entidades públicas (federais ou de outras esferas e poderes) da sociedade civil (Vide atribuições do CTGI, no Art. 6º do Anexo da Portaria nº 3.213/PRES/INSS/2019).

PCAL - Política e Controle de Acesso Lógico:

Foi decidido que a Política de Controle de Acesso Lógico será revisada pelos membros do CEGOV e aprovada eletronicamente, por meio do SEI, após realização dos ajustes propostos na reunião, quais sejam:

Alterar o Anexo para que seja formatado em conformidade com o Manual de Redação da Presidência da República (Determinação do Art. 58 do Decreto nº 9.191/2017) e com ato próprio do INSS que versa sobre a estrutura dos atos normativos, a saber: Resolução nº 708/PRES/INSS, de 6 de novembro de 2019;

Alterar o Art. 1º da minuta de resolução para "Fica instituída a Norma de Controle de Acesso Lógico do INSS";

Compatibilizar conceitos e definições do Anexo, conforme alterações sugeridas na POSIC;

Retirar itens 2.1.28, 2.1.29 e 2.1.30 do Anexo, por não se tratar de conceitos e definições;

Alterar periodicidade prevista no item 4.1.2, que deve ser semanal;

Mencionar a instituição de norma que definirá a transição dos acessos a sistemas do INSS por servidores que atuam na perícia médica e na PFE.

ETIR - Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais

Foi decidido que a norma de criação da ETIR será revisada pelos membros do CEGOV e aprovada eletronicamente, por meio do SEI, após realização dos ajustes propostos na reunião, quais sejam:

Alterar o Anexo para que seja formatado em conformidade com o Manual de Redação da Presidência da República (Determinação do Art. 58 do Decreto nº 9.191/2017) e com ato próprio

do INSS que versa sobre a estrutura dos atos normativos, a saber: Resolução nº 708/PRES/INSS, de 6 de novembro de 2019;

Verificar os itens 6.2 e 7.4 do Anexo, para evitar duplicidade

Norma de uso da internet:

Foi decidido que a norma de será revisada pelos membros do CEGOV e aprovada eletronicamente, por meio do SEI, após realização dos ajustes propostos na reunião, quais sejam:

Alterar o Anexo para que seja formatado em conformidade com o Manual de Redação da Presidência da República (Determinação do Art. 58 do Decreto nº 9.191/2017) e com ato próprio do INSS que versa sobre a estrutura dos atos normativos, a saber: Resolução nº 708/PRES/INSS, de 6 de novembro de 2019;

Alterar item 4.2 - Perfil IV - do Anexo, para incluir os servidores das áreas de desenvolvimento de pessoas, tanto na administração central, quanto nas superintendências

26. Recomenda-se, nada obstante, que a Ata de Reunião da 1ª Reunião Ordinária do Comitê Estratégico de Governança do INSS em 2020, realizada em 17/02/2020 (sequencial sapiens 01- outros 7) seja devidamente firmada por todos os membros presentes, tendo em vista que no documento acostado ao Sapiens somente consta a assinatura eletrônica do Presidente e do Diretor de Tecnologia da Informação e Inovação.

27. Quanto ao objeto das normas, observa-se que estão relacionadas a política de segurança da informação.

28. No ponto, convém observar o disposto no art. 15 e 18 do Decreto nº 9.637, de 2018, que institui a política nacional de Segurança da Informação:

Art. 15. Aos órgãos e às entidades da administração pública federal, em seu âmbito de atuação, compete:

I - implementar a PNSI;

II - elaborar sua política de segurança da informação e as normas internas de segurança da informação, observadas as normas de segurança da informação editadas pelo Gabinete de Segurança Institucional da Presidência da República;

III - designar um gestor de segurança da informação interno, indicado pela alta administração do órgão ou da entidade;

IV - instituir comitê de segurança da informação ou estrutura equivalente, para deliberar sobre os assuntos relativos à PNSI;

V - destinar recursos orçamentários para ações de segurança da informação;

VI - promover ações de capacitação e profissionalização dos recursos humanos em temas relacionados à segurança da informação;

VII - instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais, que comporá a rede de equipes formada pelos órgãos e entidades da administração pública federal, coordenada pelo Centro de Tratamento de Incidentes de Redes do Governo do Gabinete de Segurança Institucional da Presidência da República;

VIII - coordenar e executar as ações de segurança da informação no âmbito de sua atuação;

IX - consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão de segurança da informação; e

X - aplicar as ações corretivas e disciplinares cabíveis nos casos de violação da segurança da informação.

(..)

Art. 18. Os órgãos e as entidades da administração pública federal direta, autárquica e fundacional, nos atos administrativos que envolvam ativos de tecnologia da informação, sem prejuízo dos demais dispositivos legais, **incorporarão as normas de segurança da informação estabelecidas pelo Gabinete de Segurança Institucional da Presidência da República e os normativos de gestão de tecnologia da informação e comunicação e de segurança da informação do Ministério do Planejamento, Desenvolvimento e Gestão.**

29. Assim, depreende-se que as minuta de resolução remetidas à análise encontram o devido amparo jurídico, sob o aspecto material.

30. No tocante ao conteúdo das normas em si, verifica-se que elas se revestem de matéria afeta à discricionariedade administrativa e de cunho eminentemente técnico, a qual não cabe ao órgão jurídico imiscuir-se, senão para consignar a inexistência de ilegalidade.

31. Avalia-se, contudo, que o Decreto nº 9.637, de 2018 claramente destacou a necessidade de observar as normas de segurança da informação estabelecidas pelo Gabinete de Segurança Institucional da Presidência da República e os normativos de gestão de tecnologia da informação e comunicação e de segurança da informação do Ministério do Planejamento, Desenvolvimento e Gestão (atualmente incorporado à estrutura do ministério da economia). Assim, recomenda-se, desde já, que a área proponente certifique expressamente a compatibilidade dos atos.

32. Recomenda-se ainda, que a área proponente certifique nos autos que as proposições em tela abordam o tema de forma exaustiva, considerando a necessidade de consolidação dos atos normativos almejada pelo Decreto nº 10.139, de 28 de novembro de 2019.

33. Além disso, recomenda-se desde já, as seguintes adequações na minuta proposta:

- a. Em cada uma delas, no item referente a vigência da publicação, deve-se observar o disposto no Decreto 10.139, de 2019, de modo que é necessário estabelecer uma data certa para a entrada em vigor do ato, data esta que deverá estar, simultaneamente, no mínimo, uma semana após a data de sua publicação e sempre no primeiro dia do mês ou em seu primeiro dia útil. Tal regramento não se aplicará nas hipóteses de urgência justificada da Administração, que deverão estar expressa e devidamente demonstradas no processo administrativo - o que não se verificou no presente caso.
- b. **Realizar, em cada uma das normas, revisão redacional, a fim de corrigir erros na utilização de parágrafos, incisos e etc, bem para realizar a devida remissão dos atos normativos.** Em vista disso, recomenda-se revisão textual para a devida adequação redacional nos termos da Lei Complementar nº 1995, de 1998, e do Decreto 9.191, de 2017.
- c. Na minuta de Resolução nº 2/CEGOV/INSS, que institui a política de Segurança da Informação e Comunicações - POSIC-INSS (sequencial sapiens 01- outros 8), sugere-se: no art. 3º de seu anexo, sugere-se que se arrole os documentos legais em ordem hierárquica, de modo que as Leis nº 12.965, de 23 de abril de 2014, e nº 13.709, de 14 de agosto de 2018, sejam arroladas antes de decretos e demais normas inferiores;
- d. Na Minuta de Resolução nº 3/CEGOV/INSS, que institui a Norma de Controle de Acesso Lógico - NCAL, no âmbito do INSS (sequencial sapiens 01- outros 9), sugere-se: (1) no art. 2º, excluir a remissão à Resolução 70/INSS/PRES, de 06 de outubro de 2009, ou substituí-la pela atual Resolução n. 708/INSS/PRES, de 6 de novembro de 2019; (2) no anexo II, fazer referência a Minuta de Resolução nº 3/CEGOV/INSS, ao invés de Portaria.
- e. Na Minuta de Resolução nº 4/CEGOV/INSS, que institui a equipe de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR do INSS (sequencial sapiens 01- outros 10), sugere-se: no art. 4º, recomenda-se que a remissão aos atos normativos sejam feitas de acordo com o disposto no art. 14, inciso II, alínea "k", itens 1 e 2, o Decreto 9.191, de 2017. De modo que, na primeira remissão no corpo da norma sob análise se grafie o ato normativo da seguinte forma: "Norma Complementar Nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009; e nas demais remissões se grafie o ato normativo da seguinte forma: " 05/IN01/DSIC/GSIPR, de 2009. Recomenda-se que tal revisão albergue todas as remissões a atos normativos feitas no texto da norma sob análise.
- f. Na Minuta de Resolução nº 5/CEGOV/INSS, disciplina o uso da Internet no âmbito do INSS (sequencial sapiens 01- outros 11), sugere-se: no art. 4º, sugere-se a exclusão, posto que o INSS estará revogando em ato próprio, e de forma isolada, ato normativo conjunto, emitido pelo então Ministério da Previdência Social, por este Instituto e pela Empresa de Tecnologia e Informações da Previdência Social - DATAPREV. No caso, recomenda-se que a revogação seja feita de forma conjunta em ato próprio, em atenção ao paralelismo das formas. Ou, ainda, que este INSS justifique que detém atualmente a competência plena para tratar toda a matéria disciplinada pela Portaria Conjunta MDS/DTP/INSS nº 1/2005. Situação que merece reparos.

3. CONCLUSÃO

34. Com base nos fundamentos anteriormente expostos, opina-se pela regularidade jurídico-formal das minutas apresentadas (sequencial sapiens 1 - outros 8, 9, 10, 11), considerando-a apta a produzir seus efeitos jurídicos e legais, observando-se, previamente, as considerações e sugestões deste parecer, em especial as contidas nos parágrafos 21/23, 26, 31, 32 e 33.

35. É o parecer, elaborada através do Sistema AGU de Inteligência Jurídica – SAPIENS.

36. Face o exposto, recomenda-se o envio dos autos, ao Comitê Temático de Governança Digital, para ciência e providências pertinentes ao prosseguimento do feito.

À consideração superior.

Brasília, 12 de março de 2020.

(assinado eletronicamente)
ANA VALESKA ESTEVÃO VALENTIM
PROCURADORA FEDERAL

De acordo com a manifestação jurídica supra, por seus próprios e jurídicos fundamentos.

Tratando-se de análise de ato a ser subscrito pelo Sr. Presidente do INSS, remetam-se à consideração do Exmo. Sr. Procurador-Geral da Procuradoria Federal Especializada junto ao INSS, para apreciação nos termos do art. 7º da Portaria AGU nº 1.399, de 5 de outubro de 2009 combinado com art. 13 da Portaria PGF nº 526, de 26 de agosto de 2013.

(assinado eletronicamente)
LUCAS HAYNE DANTAS BARRETO
PROCURADOR FEDERAL
COORDENADOR-GERAL DE MATÉRIA ADMINISTRATIVA
PROCURADORIA FEDERAL ESPECIALIZADA JUNTO AO INSS - SEDE NACIONAL

Aprovo, nos termos do art. 7º da Portaria AGU nº 1.399, de 5 de outubro de 2009 combinado com art. 13 da Portaria PGF nº 526, de 26 de agosto de 2013, a manifestação jurídica supra, por seus próprios e jurídicos fundamentos.

Encaminhe-se conforme sugerido.

(assinado eletronicamente)
ADLER ANAXIMANDRO DE CRUZ E ALVES
Procurador-Geral do INSS

Atenção, a consulta ao processo eletrônico está disponível em <http://sapiens.agu.gov.br> mediante o fornecimento do Número Único de Protocolo (NUP) 35014047735202084 e da chave de acesso bd3f7ef1

Documento assinado eletronicamente por ADLER ANAXIMANDRO DE CRUZ E ALVES, de acordo com os normativos legais aplicáveis. A conferência da autenticidade do documento está disponível com o código 390835656 no endereço eletrônico <http://sapiens.agu.gov.br>. Informações adicionais: Signatário (a): ADLER ANAXIMANDRO DE CRUZ E ALVES. Data e Hora: 13-03-2020 16:34. Número de Série: 13920089. Emissor: Autoridade Certificadora SERPRORFBv4.

Documento assinado eletronicamente por LUCAS HAYNE DANTAS BARRETO, de acordo com os normativos legais aplicáveis. A conferência da autenticidade do documento está disponível com o código 390835656 no endereço eletrônico <http://sapiens.agu.gov.br>. Informações adicionais: Signatário (a): LUCAS HAYNE DANTAS BARRETO. Data e Hora: 13-03-2020 14:58. Número de Série: 17137116. Emissor: Autoridade Certificadora SERPRORFBv5.

Documento assinado eletronicamente por ANA VALESKA ESTEVAO VALENTIM, de acordo com os normativos legais aplicáveis. A conferência da autenticidade do documento está disponível com o código 390835656 no endereço eletrônico <http://sapiens.agu.gov.br>. Informações adicionais: Signatário (a): ANA VALESKA ESTEVAO VALENTIM. Data e Hora: 13-03-2020 10:58. Número de Série: 17350535. Emissor: Autoridade Certificadora SERPRORFBv5.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Diretoria De Integridade, Governança e Gerenciamento De Riscos
Comitê Estratégico de Governança

DESPACHO

Comitê Estratégico de Governança, em 05/05/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Solicita ajustes nas
normas de segurança da
informação aprovadas pelo
CEGOV, após análise da
PFE

1. Trata-se de processo para proposição de atos normativos para instituição de políticas e normas de segurança da informação e comunicações do Instituto Nacional do Seguro Social - INSS, de competência do Comitê Estratégico de Governança - CEGOV, conforme previsto no Art. 5 da Portaria nº 3.213/PRES/INSS/2019 (inciso VIII e parágrafo único), quais sejam:

- 1.1. Política de Segurança da Informação e Comunicações (Minuta de Resolução nº 0411821);
- 1.2. Norma de Controle de Acesso Lógico (Minuta de Resolução nº 0411838);
- 1.3. Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR (Minuta de Resolução nº 0411846);
- 1.4. Norma de uso da Internet (Minuta de Resolução nº 0411856).

2. Tendo em vista a aprovação das referidas normas na Reunião Ordinária nº 1/CEGOV/2020, realizada em 17/02/2020, e o retorno da análise das normas por parte da Procuradoria-Federal Especializada junto ao INSS (PFE-INSS), registrada no documento SEI nº 0500778, vem-se solicitar providências da Diretoria de Tecnologia da Informação e Inovação (DTI), quais sejam:

- 2.1. Adequação das normas propostas, como consta do item 33, subitens a) a f) do documento SEI nº 0500778, para ajustes formais solicitados pela PFE-INSS;
- 2.2. Anexar ao presente processo nota técnica ou nota informativa que certifique que:
 - 2.2.1. As normas aplicáveis estabelecidas pelo Gabinete de Segurança Institucional - PR e os normativos de gestão de TIC e SIC do Ministério do Planejamento, Desenvolvimento e Gestão (atualmente incorporado à estrutura do ministério da economia) foram observadas na proposição dos atos normativos em tela (Vide item 31 do documento SEI nº 0500778).
 - 2.2.2. As resoluções aqui propostas abordam o tema de forma exaustiva, considerando a necessidade de consolidação dos atos normativos almejada pelo Decreto nº 10.139, de 28 de novembro de 2019 (Vide item 32 do documento SEI nº 0500778).

3. Ressalta-se, na oportunidade, que a indicação do item 26 do documento SEI nº 0500778 já se encontra cumprida, uma vez que os membros votantes integrantes do CEGOV assinaram a Ata de Reunião da 1ª Reunião Ordinária do Comitê Estratégico de Governança do INSS em 2020, como consta do documento SEI nº 0368652. As últimas assinaturas eletrônicas foram registradas no dia 28/02/2020.
4. Diante do exposto, encaminha-se o processo à DTI, para proceder aos ajustes demandados pela PFE.
5. Em seguida, retornem-se os autos à Secretaria-Executiva do CEGOV, para encaminhamento do normativo para a Coordenação de Suporte ao Gabinete - CSG, em consonância com o disposto no art. 14, da Resolução n. 708/INSS/PRES, de 6 de novembro de 2019.

CIBELLE CESAR DO AMARAL BRASIL

Coordenadora-Geral de Governança



Documento assinado eletronicamente por **CIBELLE CESAR DO AMARAL BRASIL**, **Coordenador(a) Geral**, em 05/05/2020, às 17:32, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0758185** e o código CRC **8FCC72D6**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 0758185



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Diretoria De Tecnologia da Informação e Inovação

DESPACHO

Diretoria De Tecnologia da Informação e Inovação, em 05/05/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Solicita ajustes nas
normas de segurança da
informação aprovadas pelo
CEGOV, após análise da
PFE

Dada ciência do Diretor desta DTI, encaminhe-se ao Serviço de Segurança em TIC, com trâmite pela Coordenação-Geral de Infraestrutura e Operações, para as tratativas solicitadas no despacho CEGOV 0758185.

RENATA CESÁRIO DE OLIVEIRA GOMES

Analista em Tecnologia da Informação



Documento assinado eletronicamente por **RENATA CESARIO DE OLIVEIRA GOMES, Analista em Tecnologia da Informação**, em 05/05/2020, às 21:01, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site
https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0759325** e o código CRC **95A0A5B1**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 0759325



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações

DESPACHO

Coordenação-Geral De Infraestrutura e Operações, em 07/05/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

A s s . : Solicitação de
ajustes nas normas de
segurança da informação
aprovadas pelo CEGOV,
após análise da PFE

1. Trata-se de ajustes nas normas de segurança da informação aprovadas pelo CEGOV, após análise da PFE.
2. Encaminhe-se ao Serviço de Segurança em TIC, para as tratativas solicitadas no despacho CEGOV 0758185.

CLAUDIO AUGUSTO NOVAIS FERRAZ

Coordenador-Geral de Infraestrutura e Operações



Documento assinado eletronicamente por **Claudio Augusto Novais Ferraz, Coordenador(a) Geral**, em 07/05/2020, às 17:19, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site
https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0774524** e o código CRC **0EBE69CD**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência

Diretoria De Tecnologia da Informação e Inovação

Coordenação-Geral De Infraestrutura e Operações

Coordenação De Suporte e Infraestrutura De Tecnologia da Informação e Comunicação

Serviço De Segurança em Tecnologia da Informação e Comunicação

NOTA TÉCNICA Nº 3/2020/SSEG/CGIN/DTI/INSS

PROCESSO Nº 35014.047735/2020-84

INTERESSADO: DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO

**Minuta s de
Normativos de
Segurança da
Informação e
Comunicações.**

1. Esta nota técnica trata da publicação de minutas de normativos de Segurança da Informação e Comunicações.
2. As propostas de minutas foram submetidas e aprovadas pelo Comitê Temático de Governança Digital - CTGD (0427234) e pelo Comitê Estratégico de Governança - CEGOV (0437711).
3. Após análise da Procuradoria Federal Especializada - PFE-INSS, por meio do PARECER n. 00012/2020/DAADM/PFE-INSS-SEDE/PGF/AGU (0500778), retornam os autos para o Serviço de Segurança em Tecnologia da Informação e Comunicações, para os devidos ajustes, conforme Despacho CEGOV (0758185).
4. No entanto, durante o período necessário para proceder as intervenções sugeridas pela PFE-INSS, este Serviço de Segurança da Tecnologia da Informação e Comunicação - SSEG, foi acionado para tratar de ação de auditoria da Controladoria Geral da União - CGU, Processo nº 35000.003409/2019-81, em fase de relatório (1049291), com recomendações que fazem referência à necessidade de ajustes nas normas sob análise.
5. Neste íterim, o Gabinete de Segurança Institucional da Presidência da República - GSI-PR, publicou a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal. As definições e demais disposições contidas no normativo recém publicado têm impacto nas normas propostas pela DTI.
6. Sendo assim, após verificação à luz dos apontes da PFE-INSS, do Relatório de Auditoria da CGU e da IN 01/2020 publicada pelo GSI-PR, foram procedidas as alterações necessárias para atendimento dos itens 25 e 33 do documento SEI nº 0500778:
 - 6.1. Revisão dos conceitos de "dado", "informação" e "ativos de informação", levando em consideração as definições trazidas pela nº Lei 13.709/2018 (LGPD), pela Lei nº 12.527/2011 (Lei de Acesso à Informação) e pelo Decreto nº 10.046/2019 (Decreto de Compartilhamento de Dados);
 - 6.2. A inclusão das definições relativas ao item "Responsabilidade pela gestão das informações" das diretrizes da minuta da Política de Segurança da Informação - POSIN-INSS;

6.3. Alterações necessárias nos itens que se referem ao processo de concessão do Perfil 4 de acesso à internet para incluir os servidores das áreas de desenvolvimento de pessoas, tanto na administração central, quanto nas superintendências, na proposta de Norma de Acesso à Internet;

6.4. Em referência ao que preconiza o Decreto nº 10.139, de 28 de novembro de 2019, as normas propostas devem entrar em vigor a partir de suas respectivas datas de publicação. A urgência para a imediata validade dos normativos sob análise, se justifica tendo em vista que:

6.4.1. A POSIC INSS apresenta atualizações necessárias a partir de mudanças de estrutura e regimentais do Instituto procedidas no ano de 2019;

6.4.2. A Norma de Controle de Acesso Lógico - NCAL, substitui a Política de Controle de Acesso Lógico - PCAL-INSS, que foi publicada em 2014. Sendo assim, é imperativo que tal ato seja publicado e entre em vigência com urgência;

6.4.3. A implementação da Equipe de Tratamento de Incidentes em Redes Computacionais - ETIR, no âmbito do Instituto é alvo de constantes cobranças de órgãos de controle internos/externos, e a sua imediata vigência é necessária;

6.4.4. A adoção dos termos definidos na norma de controle de acesso à internet é uma necessidade urgente do INSS, tendo em vista que trata-se de atualização de norma emitida em 2005. A implementação da norma proposta possibilitará a adoção de medidas para conter a má utilização dos *links* de internet disponibilizados pelo Instituto e a consequente melhora no processo de atendimento prestado aos cidadãos e cidadãs.

6.5. É válido lembrar que a pronta entrada em vigência dos atos ora propostos, não terá impacto ou afetará de forma imediata os usuários dos serviços de Tecnologia da Informação - TI do Instituto.

6.6. Na minuta proposta da política de Segurança da Informação, os documentos legais foram ajustados em ordem hierárquica, de modo que as Leis nº 12.965, de 23 de abril de 2014, e nº 13.709, de 14 de agosto de 2018, passaram a ser arroladas antes de decretos e demais normas inferiores;

6.7. Na minuta da Norma de Controle de Acesso Lógico -NCAL-INSS, foi procedida a substituição da remissão à Resolução 70/INSS/PRES, de 06 de outubro de 2009, pela Resolução nº 708/INSS/PRES, de 6 de novembro de 2019. E o anexo II, foi editado, passando a fazer referência à Minuta de Resolução nº 3/CEGOV/INSS;

6.8. Adequações no texto da proposta de minuta que institui a Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR do INSS no que se refere a remissão de atos normativos, de acordo com o disposto no art. 14, inciso II, alínea "k", itens 1 e 2, o Decreto 9.191, de 2017.

6.9. Na Minuta de Resolução nº 5/CEGOV/INSS, que disciplina o uso da Internet no âmbito do INSS (0411856), foi procedida a exclusão do *Art. 4º*, tendo em vista que com a extinção do Ministério da Previdência Social - MPS e do Comitê de Segurança e Tecnologia da Informação e Comunicações da Previdência Social - CSTIC-PS, o Instituto tem autonomia para regulamentar a matéria em tela;

6.10. Adesão às normas estabelecidas pelo Gabinete de Segurança Institucional - GSI-PR e os normativos de gestão de TIC e SIC do Ministério do Planejamento, Desenvolvimento e Gestão (atualmente incorporado à estrutura do Ministério da Economia) foram observadas na proposição dos atos normativos em tela (Vide item 31 do documento SEI nº 0500778).

7. A partir das recomendações contidas no Relatório (preliminar) de Auditoria, resultado de ação executada pela Controladoria Geral da União - CGU, com várias referências à necessidade de alterações na POSIC e na PCAL-INSS (em vigência), este SSEG procedeu os seguintes ajustes nas minutas de atualização ora propostas:

7.1. Inclusão, na alínea "b", Inciso IX do Art. 4º da proposta de minuta para a Política de Segurança da Informação, de referência ao princípio da segregação de funções (conforme Recomendação nº 12 do Relatório de Auditoria da CGU).

7.2. Alteração Inciso II do Art. 4º, especificando os prazos envolvidos para disponibilização das informações enviadas pelo INSS para atualização da base de dados do LDAP (Recomendação CGU nº 3) na minuta de Norma de Controle de Acesso;

- 7.3. Inclusão de referência, no Inciso VIII, do Art. 5º na minuta da NCAL, ao prazo para revisão dos acessos concedidos para usuários externos (Recomendação CGU nº 2);
- 7.4. A possibilidade do acesso aos sistemas corporativos por meio de certificação digital e/ou fator duplo de autenticação (Recomendação nº 5 do relatório CGU) já constava no texto da NCAL (Artigo 5º, inciso X)
- 7.5. A obrigatoriedade das organizações ou entes que mantiverem contrato ou instrumento congênere com o Instituto informar previamente ao INSS quaisquer alterações em seu corpo de colaboradores que impacte na emissão/exclusão de acessos (Recomendação nº 6 do Relatório da CGU) é descrita no artigo 5º, Inciso XV, alínea "c", subitem 2.3, da proposta de minuta da NCAL;
- 7.6. Foram procedidas alterações no texto do item 6 da alínea "d", do Inciso XV do Artigo 5º da proposta de minuta da NCAL, para atendimento da Recomendação nº 7 do relatório da CGU;
- 7.7. A definição dos logs de registro dos sistemas corporativos (objeto da Recomendação nº 4 do relatório da CGU) são definidos no Artigo 7º, inciso III, alínea "c" e no anexo III da minuta proposta da NCAL;
- 7.8. Inclusão de item, alínea "b" do inciso IV do artigo 7º da NCAL, que trata da distribuição dos perfis de acesso conforme o fluxo operacional dos sistemas corporativos, objeto da recomendação nº 1 do relatório da CGU;
- 7.9. Adequação do inciso I do art. 8º da minuta proposta da NCAL para contemplar a recomendação nº 19 do relatório da CGU.
8. Para adequação das normas propostas às diretrizes emanadas pela recém publicada IN GSI-PR Nº 01/2020, foram precedidas as seguintes alterações:
- 8.1. Alterações dos termos "Política de Segurança da Informação e Comunicações - POSIC" e "Segurança da Informação e Comunicações - SIC" e seus respectivos acrônimos para "Política de Segurança da Informação - POSIN" e "Segurança da Informação - SI";
- 8.2. Revisão de todos os conceitos e definições contidas nas normas propostas de acordo com os termos da Portaria do GSI-PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação;
- 8.3. Inclusão de itens que abordam os seguintes temas: Computação em Nuvem (art. 5º, inciso VI, alínea "d"); Segurança Física e do Ambiente (art. 5º, inciso X); e Gestão de Ativos (art. 5º, inciso XI) nas diretrizes gerais da POSIN;
- 8.4. Foram procedidas alterações e inclusões nas atribuições do Gestor de Segurança da Informação do INSS (art. 7º, inciso I) da POSIN, e as adequações necessárias para que as atribuições do Comitê de Segurança da Informação sejam desempenhadas pelo Comitê Temático de Gestão da Informação (art. 7º, inciso VI);
9. A Diretoria de Gestão de Pessoas e Administração - DGPA, encaminhou na data de 04/06/2020, por meio de mensagem do correio eletrônico corporativo (1077008), documento (1077060) contendo sugestões de alterações na Norma de Controle de Acesso Lógico - NCAL.
- 9.1. Este SSEG fez uma análise prévia das propostas e procedeu a inserção das alterações propostas na minuta do documento, no entanto consideramos que para efetivar tais mudanças será necessário submeter o conteúdo para aprovação do CEGOV.
10. Encaminhe-se, em devolução, à Coordenação-Geral de Infraestrutura e Suporte da Diretoria de Tecnologia da Informação e Inovação.

Brasília, 03 de julho de 2020.

ROBERTO RUFINO DA COSTA

Chefe do Serviço de Segurança em Tecnologia da Informação e Comunicações Substituto



Documento assinado eletronicamente por **ROBERTO RUFINO DA COSTA, Chefe de Serviço Substituto(a)**, em 03/07/2020, às 17:00, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0829620** e o código CRC **3DC78C25**.

Referência: Processo nº 35014.047735/2020-84

SEI nº 0829620



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 2/CEGOV/INSS, DE DE DE 2020

Atualiza a Política de Segurança da Informação e Comunicações do POSIC POSIN-INSS. (IN 01/2020) e PORTARIA Nº 93

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída no âmbito do INSS e nos termos do Anexo a esta Resolução, a Política de Segurança da Informação e Comunicações do POSIC POSIN-INSS (01/2020) e PORTARIA Nº 93.

Art. 2º Esta Resolução entra em vigor na data de sua publicação e seu Anexo será publicado em Boletim de Serviço.

Art. 3º Fica revogada a Resolução nº 672/PRES/INSS, de 27 de dezembro de 2018.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretora de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **ROBERTO RUFINO DA COSTA**, **Chefe de Serviço Substituto(a)**, em 03/07/2020, às 17:01, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1075215** e o código CRC **9574DCD1**.

ANEXO I

RESOLUÇÃO Nº 2/CEGOV/INSS, DE DE DE 2020

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO INSTITUTO NACIONAL DO SEGURO SOCIAL – POSIC POSIN-INSS (IN 01/2020) E PORTARIA Nº 93.

Art. 1º A Política de Segurança da Informação e Comunicações do Instituto Nacional do Seguro Social POSIC POSIN-INSS, tem por objetivo estabelecer e difundir diretrizes e princípios de Segurança da Informação e Comunicações – SI, com vistas à orientação para uso e proteção adequados das informações produzidas e custodiadas pelo Instituto, preservando sua disponibilidade, integridade, confidencialidade e autenticidade. (IN 01/2020) e PORTARIA Nº 93.

Parágrafo único. A Política de que trata o **caput** e suas normas complementares aplicam-se a todos os agentes públicos que têm vínculo direto e/ou indireto com o Instituto.

Art. 2º Para os efeitos da POSIC POSIN-INSS, entende-se: (IN 01/2020) e PORTARIA Nº 93.

I - agente público: Todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da APF, direta e indireta; (IN 1/2020)

II - atividade crítica - atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo; (IN 01/2020) Incluído

III - ativos de informação: meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV - dados processados: dados submetidos a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação; (IN 01/2020) e PORTARIA Nº 93.

V - gestor de Segurança da Informação e Comunicações: é o responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF. (IN 01/2020) e PORTARIA Nº 93.

VI - Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

VII - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

VIII - necessidade de conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais; (IN 01/2020) e PORTARIA Nº 93.

IX - riscos de segurança da informação e comunicações: potencial associado à exploração de uma ou mais vulnerabilidades nos ativos de informação, em razão de ameaças, com impacto negativo às atividades do Instituto; (IN 01/2020) e PORTARIA Nº 93.

X - segurança da informação e comunicações – SI: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e autenticidades das informações; (IN 01/2020) e PORTARIA Nº 93.

XI - vínculo direto: agentes públicos contratados diretamente pelo INSS;

XII - vínculo indireto: agentes privados ou públicos pertencentes a órgãos ou unidades da Administração Pública Federal, Estadual ou Municipal que mantenham contrato, convênio, acordo de cooperação técnica ou instrumento congênere com o INSS; e

Art. 3º Esta POSIC POSIN-INSS foi elaborada com base nos seguintes documentos: (IN 01/2020) e PORTARIA Nº 93.

I - Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;

II - Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto na Constituição Federal;

III - Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

IV - Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais;

V - Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

VI - Decreto nº 7.724, de 16 de maio de 2012, regulamenta a Lei nº 12.527, de 18 de novembro de 2011;

VII - Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

VIII - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

IX - Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

X - Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que disciplina a gestão de segurança da informação e comunicações na Administração Pública Federal, direta e indireta, e dá outras providências; (IN 01/2020) e PORTARIA Nº 93.

XI - Instruções normativas relacionadas à segurança da informação, publicadas pelo Gabinete de Segurança Institucional da Presidência da República;

XII - Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação, (incluído)

XIII - NBR ISO/IEC 27002:2013, que institui código de melhores práticas para a Gestão de Segurança da Informação;

Art. 4º Esta POSIC POSIN-INSS foi elaborada com base nos seguintes princípios: (IN 01/2020) e PORTARIA Nº 93.

I - a preservação da imagem do Instituto e de seus agentes públicos;

II - a salvaguarda das informações do cidadão;

III - ações de segurança orientadas pela gestão de riscos;

IV - continuidade assegurada dos serviços ao cidadão;

V - o alinhamento com a missão institucional e seu planejamento estratégico; e

VI - respeito à natureza e finalidade de cada área do Instituto.

Art. 5º São diretrizes gerais da **POSI** POSIN-INSS: **(IN 01/2020)** e PORTARIA Nº 93.

I - Tratamento da Informação:

- a) toda informação produzida pelos agentes públicos, no exercício de suas atividades, é de propriedade do INSS e deve ser protegida;
- b) informações produzidas, armazenadas e tratadas pelo Instituto, especialmente as informações pessoais e custodiadas, devem receber o devido tratamento para assegurar sua proteção durante todo o ciclo de vida; e
- c) somente os canais de comunicação disponibilizados pelo INSS devem ser utilizados para trafegar informações institucionais.

II - Tratamento de Incidentes de Segurança da Informação (SI): **(IN 01/2020)** e PORTARIA Nº 93.

- a) todo incidente de segurança da informação deve ser imediatamente relatado à área responsável pela gestão de segurança da informação de TI, observando-se a apropriada coleta de evidências. **(IN 01/2020)** e PORTARIA Nº 93.

III - Gestão de Riscos de Segurança:

- a) os riscos de segurança da informação devem ser identificados e tratados; e
- b) os critérios para a gestão de risco devem ser definidos e comunicados a toda instituição.

IV - Gestão de Continuidade:

- a) os ativos de informação que suportam as atividades críticas do Instituto devem ser suportados por ambiente de alta disponibilidade e ter capacidade de recuperação em prazos e condições previamente definidos para situações de contingência, em conformidade com o processo de continuidade; e
- b) a continuidade das operações e serviços de Tecnologia da Informação e Comunicações – TIC, deve estar prevista nos contratos, assim como os prazos e condições devem estar formalmente estabelecidos. **(IN 01/2020)** e PORTARIA Nº 93.

V - Controles de Acesso:

- a) todo acesso à informação deve ser motivado pela necessidade de conhecer;
- b) os sistemas de informação e as instalações físicas devem ter capacidade de controlar os acessos, com fins de responsabilização pelo seu uso; e
- c) as autorizações de acesso às informações, sistemas e instalações físicas devem ter critérios de acesso definidos e divulgados a todos da instituição.

VI - Recursos Computacionais:

a) correio eletrônico:

- 1. o correio eletrônico, *e-mail*, é uma forma de comunicação oficial e deve ser utilizado exclusivamente no desempenho das atividades funcionais; e
- 2. ao produzir, responder ou encaminhar mensagem em caixa de correio eletrônico institucional, o servidor deverá se identificar, subscrevendo, ao menos, seu nome, cargo e telefone de contato institucional.

b) Acesso à Internet:

- 1. o acesso à Internet, por meio da rede de dados do INSS, é uma concessão e deve ter seu uso orientado para a execução das atividades do Instituto; e
- 2. os acessos serão liberados de acordo com perfis previamente definidos pelo órgão responsável pelos serviços de TI. **(IN 01/2020)**

c) Gestão de Mudanças de TI: **(IN 01/2020)** e PORTARIA Nº 93.

- 1. toda mudança nos sistemas de informação do INSS deve ser previamente e formalmente autorizada; e
- 2. a gestão de mudanças deve prever, no mínimo, a guarda dos registros, realização de testes e a possibilidade de recuperação do ambiente.

d) Computação em Nuvem **(IN 01/2020)** (incluído)

1. o ambiente de computação em nuvem, sua infraestrutura e canal de comunicação devem estar aderentes às diretrizes e normas de SI estabelecidas pelo instituto, e às legislações vigentes;(incluído)

2. o contrato de prestação de serviço, quando for o caso, deverá conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço;(incluído)

VII - Educação e Conscientização:

a) esta Política e seus normativos complementares devem ser periodicamente divulgados a todos os agentes públicos do Instituto;

b) o Instituto deve manter programa contínuo de conscientização dos agentes públicos em Segurança da Informação ~~e Comunicações~~ – SI; e (IN 01/2020) e PORTARIA Nº 93;

c) deve ser mantido plano de capacitação especializado aos profissionais que atuam na gestão de SI;(IN 01/2020) e PORTARIA Nº 93.

VIII - Auditoria e Conformidade:

a) o cumprimento desta Política e de suas normas complementares deve ser avaliado periodicamente, por meio de verificações de conformidade; e

b) o uso dos recursos de TI disponibilizados pelo Instituto é passível de monitoramento e auditoria.(IN 01/2020) e PORTARIA Nº 93.

IX - Responsabilidade pela gestão das informações:

a) Os responsáveis pela gestão dos ativos da informação e sistemas corporativos devem descrever os requisitos de segurança;

b) Os sistemas de informação devem ser concebidos possibilitando a segregação de funções. (o parecer da PFE indicou que este item estava incompleto. Adicionamos sugestão de texto que aborda o princípio da segregação de funções (tema citado na Recomendação nº 12 do Relatório de Auditoria da CGU. Na minuta da PCAL será incluso o conceito de proprietário da informação e as responsabilidades do mesmo.)

X - Segurança física e do ambiente;(IN 01/2020)

a) As instalações em que as informações críticas ou sensíveis serão processadas deverão ser mantidas em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção física;(incluído)

b) Os ativos da organização devem ser protegidos contra acesso físico não autorizado, danos, perdas, furto e interferência. As proteções devem estar alinhadas aos riscos identificados;(incluído)

XI - Gestão de ativos da informação;(IN 01/2020)

a) os ativos de informação devem;(incluído)

I

1. ser inventariados e protegidos;(incluído)

2. ter identificados os seus proprietários e custodiantes;(incluído)

3. ter a sua entrada e saída nas dependências do Instituto autorizadas e registradas por autoridade competente;(incluído)

4. ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins;(incluído)

Parágrafo único. O Comitê Temático de Gestão da Informação é responsável pela aprovação de procedimentos e de normas internas que orientem o compartilhamento de dados sob gestão do INSS e pela aprovação da categorização dos níveis de compartilhamento de dados com outras entidades públicas (federais ou de outras esferas e poderes) da sociedade civil (Vide atribuições do CTGI, no Art. 6º do Anexo da Portaria nº 3.213/PRES/INSS/2019). (Reposicionado para o artigo 7º)

Art. 6º A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas, cíveis e penais, previstas na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), no Código Penal, no Código Civil, e, ainda, em legislação que regule ou venha regular a matéria.

Art. 7º Competências e Responsabilidades:

I - Cabe ao Gestor de Segurança da Informação ~~e Comunicações~~;(IN 01/2020) e PORTARIA Nº 93.

a) promover cultura de segurança da informação ~~e comunicações~~;(IN 01/2020) e PORTARIA Nº 93.

b) acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

c) propor os recursos necessários à implementação das ações de SI;(IN 01/2020)

d) coordenar o CSIE ou estrutura equivalente ; e (IN 01/2020) e PORTARIA Nº 93.

e) acompanhar os trabalhos e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR do INSS (IN 01/2020)

f) propor o detalhamento das diretrizes desta Política, por meio de normas e procedimentos, e acompanhar sua implementação.

g) assessorar a alta administração na implementação da Política de Segurança da Informação; (IN 01/2020)

h) estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação; (IN 01/2020)

i) promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no INSS; (IN 01/2020)

j) incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação; (IN 01/2020)

k) verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação; (IN 01/2020)

l) acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e (IN 01/2020)

m) manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação. (IN 01/2020)

II - Cabe ao Presidente do Instituto nomear o Gestor de SI; (IN 01/2020) e PORTARIA Nº 93.

III - Caso o Gestor de SI não seja nomeado, as atribuições relacionadas no art. 7º inciso I serão desempenhadas pelo Diretor de Tecnologia da Informação e Inovação; (IN 01/2020) e PORTARIA Nº 93.

IV - A ETIR-INSS deve analisar e propor respostas a notificações e atividades relacionadas a incidentes de SI, no âmbito do Instituto; e (IN 01/2020) e PORTARIA Nº 93.

V - É responsabilidade de todos os agentes públicos, diretos e indiretos, conhecer e cumprir as diretrizes desta Política e demais normas e procedimentos complementares de SI. (IN 01/2020) e PORTARIA Nº 93.

VI - Tendo em vista a Política de Governança do INSS as atribuições contidas no Art. 20 da Instrução Normativa Nº 1, DE 27 DE MAIO DE 2020, no âmbito do Instituto serão desempenhadas pelo Comitê Temático de Gestão da Informação. (IN 01/2020)

Parágrafo único. O Comitê Temático de Gestão da Informação é responsável pela aprovação de procedimentos e de normas internas que orientem o compartilhamento de dados sob gestão do INSS e pela aprovação da categorização dos níveis de compartilhamento de dados com outras entidades públicas (federais ou de outras esferas e poderes) da sociedade civil (Vide atribuições do CTGI, no Art. 6º do Anexo da Portaria nº 3.213/PRES/INSS/2019). (remanejado do artigo 6º)

Art. 8º Esta Política e seus normativos ~~devem~~ ~~deve ser revisada~~ ~~revisados~~ sempre que necessário, não excedendo o período máximo de três anos. (incluído)



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 3/CEGOV/INSS, DE DE DE 2020

Define regras para a emissão de credenciais de acesso lógico no âmbito do INSS

O **COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS**, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída a Norma de Controle de Acesso Lógico - NCAL, do Instituto Nacional do Seguro Social – INSS.

Art. 2º Esta Resolução, bem como seus anexos, serão publicados em Boletim de Serviço, nos termos do Inciso I do Art. 16, da Resolução n.708/INSS/PRES, de 6 de novembro de 2019.

Art. 3º Revogar a RESOLUÇÃO Nº 413/PRES/INSS, DE 20 DE MAIO DE 2014.

Art. 4º Esta Resolução entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretora de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **ROBERTO RUFINO DA COSTA**, **Chefe de Serviço Substituto(a)**, em 03/07/2020, às 17:01, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1075264** e o código CRC **6402B92B**.

ANEXO I

RESOLUÇÃO Nº 3/CEGOV/INSS, DE DE DE 2020

NORMA DE CONTROLE DE ACESSO LÓGICO – INSS

Art. 1º Os termos definidos nesta norma aplicam-se a todos os agentes públicos e privados com vínculo direto ou indireto, permanente ou temporário com o INSS.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União – AGU que atuarem na consultoria e no assessoramento jurídico, e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta Norma de Controle de Acesso Lógico são estabelecidos os seguintes conceitos e definições:

I - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

II - administrador de Domínio: Usuário responsável pela administração de um domínio por meio da aplicação de políticas globais, criação, edição e exclusão de usuários e grupos, e instalação de programas em um grande número de estações de trabalho;

III - administrador Local: Usuário responsável pela administração de partes de um domínio (geralmente restrito a um setor ou abrangência), por meio de políticas locais, edição de grupos e usuários locais, e instalação de programas em estações de trabalho limitadas a um setor ou abrangência;

IV - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta;

V - ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VI - contas de serviço: contas de acesso à rede corporativa de computadores, necessárias para a execução de procedimentos automáticos (aplicação, script, etc) sem qualquer intervenção humana no seu uso;

VII - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso **ao uso de recursos físicos ou computacionais**; **(IN 01/2020) e PORTARIA Nº 93 (incluído)**

VIII - credenciamento: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer;

IX - credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física, como crachá, cartão e selo ou lógica como identificação usuário e senha;

X - dado: Sugestão de Alteração "O dado é um elemento informativo concreto e sua forma plural expressa uma informação" é o registro do atributo de um ente objeto ou fenômeno onde registro indica o ato de registrar, ou seja, é a gravação ou a impressão de caracteres ou símbolos que tenham um significado em algum documento ou suporte físico;

XI - domínio: agrupamento lógico de computadores em rede que compartilham recursos em um banco de dados de segurança, comum, onde a administração e autenticação são centralizadas. Desta forma um usuário precisa de uma conta para ter acesso ao domínio e aos recursos compartilhados;

XII - endereço IP: **sigla em inglês para Internet Protocol. Trata-se de endereço lógico que identifica a localização de determinado ativo na rede; conjunto de elementos numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores. Sequência de números associada a cada computador conectado à Internet. No caso de IPv4, o endereço IP é dividido em quatro grupos, separados por "." e compostos por números entre 0 e 255. No caso de IPv6, o endereço IP é dividido em até oito grupos, separados por ":" e compostos por números hexadecimais (números e letras de "A" a "F") entre 0 e FFFF; (IN 01/2020) e PORTARIA Nº 93. Substituir**

XIII - entidade externa: Organização governamental, não governamental ou privada amparada por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica ou instrumento congênere com o INSS;

XIV - e-SIC: Sistema Eletrônico do Serviço de Informações ao Cidadão, aplicação disponibilizada na internet, que centraliza todos os pedidos de informações dirigidos ao Poder Executivo Federal;

XV - estagiário: educando que esteja frequentando o ensino regular, em instituições de educação superior, de educação profissional, de ensino médio, de educação especial e dos anos finais do ensino fundamental, na modalidade profissional da educação de jovens e adultos, que desenvolve as atividades relacionadas à sua área de formação profissional junto as pessoas Jurídicas de Direito Privado, órgãos da Administração Pública e Instituições de Ensino, que tenham condições de proporcionar experiência prática na sua linha de formação;

XVI - estágio Supervisionado: ato educativo escolar supervisionado, desenvolvido no ambiente de trabalho, que visa a preparação para o trabalho produtivo de educandos;

XVII - ferramenta de gestão de acessos: Software que possibilita a gestão integrada de papéis e permissões de acesso dos usuários nos sistemas corporativos;

XVIII - gestor da informação: usuário que gerou a informação, que responde pelo seu conteúdo ou que foi formalmente designado para definir, alterar a sua classificação nos graus de sigilo e perfil de acesso dos demais usuários e processos;

XIX - gestão de identidades: Combinação de sistemas técnicos, regras e procedimentos que definem a posse, utilização e segurança de uma identidade. Seu objetivo primário é estabelecer a confiança na associação de atributos a uma identidade digital e conectar esta identidade com uma entidade individual;

XX - Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXI - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

XXII - Log ou Registro de Auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional; (IN 01/2020) e PORTARIA Nº 93. (incluído)

XXIII - necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação; condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais; (IN 01/2020) e PORTARIA Nº 93

XXIV - perfil de Acesso do Usuário: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

XXV - recursos de rede: Dispositivos (impressoras, scanners, multifuncionais, etc) ou serviços (sistemas, portais, etc) disponibilizados para os usuários por

meio de uma rede de dados;

XXVI - serviço de diretório: serviço que armazena e organiza informações relativas a recursos disponíveis e usuários de uma rede de dados. Permite que o administrador da rede gerencie o acesso de usuários e sistemas aos recursos disponíveis;

XXVII - sistemas corporativos: sistemas de operação, ou finalísticos, que se coadunam com os fins da Previdência Social. Assim, entende-se que este conceito comporta o conjunto de sistemas e subsistemas que garantem a operação dos regimes geral e próprio de previdência social, inclusive de previdência complementar;

XXVIII - sistemas legados: compreendem o conjunto de aplicações desenvolvidas com tecnologias obsoletas que permanecem em operação no INSS;

XXIX - usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal-APF, formalizada por meio da assinatura do Termo de Responsabilidade;

XXX - usuário interno: servidor do quadro do INSS lotado em uma Unidade Orgânica – UO, que se utiliza dos sistemas corporativos do Instituto;

XXXI - usuário externo: usuários vinculados a uma Entidade Externa, que se utiliza dos sistemas corporativos do Instituto por meio de um perfil de acesso concedido por um Gestor de Acesso Externo;

Art. 3º São diretrizes desta NCAL-INSS:

I - o acesso à rede e aos sistemas corporativos do INSS dar-se-á por meio de autenticação integrada de domínio baseado em serviço de diretório, administrado por meio de uma ferramenta de gestão de identidades;

II - as concessões de acesso à rede de dados e aos sistemas corporativos são distintas. Sendo assim, o usuário pode obter permissão de acesso apenas à rede de dados, ou apenas a determinado(s) sistema(s) corporativo(s);

III - as credenciais de acesso a rede de dados e aos sistemas corporativos do INSS são conferidas aos usuários com base na necessidade de conhecer, para viabilizar o exercício de suas atribuições funcionais e atividades a serem desenvolvidas no âmbito do INSS; e

IV - o uso indevido de informações dos sistemas corporativos do INSS sujeitará o agente às penalidades previstas na legislação.

Art. 4º Base Cadastral:

I - as bases de dados do Serviço de Diretórios (acesso à rede de dados), do Sistema de Gestão de Acessos (sistemas corporativos) e sistemas legados devem ser alimentadas por informações disponibilizadas pelo INSS;

II - para tanto, a área responsável pela gestão de pessoas do INSS disponibilizará semanalmente as informações extraídas do Sistema Integrado de Administração de Recursos Humanos – SIAPE para a empresa prestadora de serviços tecnológicos contratada pelo Instituto, com a supervisão da área de gestão de TIE do INSS, contendo, minimamente, os seguintes dados: Recomendação 3

Tabela 1: Informações Usuários

Item	Informação	Campo	Descrição
1	GR-MATRICULA	N 0012	GRUPO NUMÉRICO COMPOSTO DE NÚMERO DO ÓRGÃO (N0005) E NÚMERO DE MATRÍCULA DO SERVIDOR (N0007)
2	IT-NU-IDEN-SERV-ORIGEM	A 0008	NÚMERO DE IDENTIFICAÇÃO DO SERVIDOR NA ORIGEM - NÚMERO VINCULADO AO CARGO EFETIVO OU EM COMISSÃO
3	IT-NO-SERVIDOR	A 0060	NOME
4	IT-DA-NASCIMENTO	N 0008	DATA DE NASCIMENTO
5	IT-NU-CPF	N 0011	NÚMERO DO CPF
6	IT-NU-PIS-PASEP	N 0011	NÚMERO DO PIS
7	IT-IN-SUPRESSAO-PAGAMENTO	A 0001	INDICATIVO DE SUPRESSÃO DE PAGAMENTO
8	IT-CO-SITUACAO-SERVIDOR	N 0002	CÓDIGO DE SITUAÇÃO FUNCIONAL DO SERVIDOR
9	IT-CO-GRUPO-OCOR-AFASTAMENTO	N 0002	CÓDIGO DE OCORRÊNCIA DE AFASTAMENTO
10	IT-DA-INICIO-OCOR-AFASTAMENTO	N 0008	DATA DO INÍCIO DA OCORRÊNCIA DE AFASTAMENTO
11	IT-DA-TERMINO-OCOR-AFASTAMENTO	N 0008	DATA DE TÉRMINO DA OCORRÊNCIA DE AFASTAMENTO

12	IT-CO-GRUPO-OCOR-EXCLUSAO	N 0002	CÓDIGO DE OCORRÊNCIA DE EXCLUSÃO
13	IT-CO-UORG-LOTACAO-SERVIDOR	N 0009	CÓDIGO DA UORG DE LOTAÇÃO DO SERVIDOR
14	IT-CO-ORGAO-REQUISITANTE	N 0005	CÓDIGO DO ÓRGÃO REQUISITANTE

III - a Diretoria de Tecnologia da Informação e Inovação procederá com a atualização das bases cadastrais do serviço de diretórios e dos sistemas corporativos, bem como realizará a validação das informações disponibilizados pelo INSS por meio de outras bases, na periodicidade do envio das informações; e

IV - a área responsável pela gestão de pessoas do INSS poderá acordar, com a área responsável pela gestão de TI do INSS, a revisão das informações necessárias à administração de contas de usuários. (IN 01/2020) e PORTARIA N° 93.

Art. 5º Credenciais e perfis de acesso:

I - a emissão de uma credencial permite ao usuário acessar a rede de dados corporativa do INSS. Para que o mesmo obtenha acesso aos sistemas corporativos a credencial deve ser associada a um perfil de acesso;

II - o processo de credenciamento de usuário aos ativos de informação deve ser feito observando os seguintes critérios:

a) a credencial de acesso concedida para acesso à rede de dados e sistemas corporativos do INSS é de caráter pessoal e intransferível;

b) as credenciais de acesso devem ser concedidas após a data de contratação ou entrada em exercício do usuário; e

c) as mesmas credenciais de acesso devem ser utilizadas para o acesso à rede de dados e aos sistemas corporativos do INSS, mediante autenticação que permita ao usuário acessar vários sistemas, por meio de ferramenta de gestão de identidades e acessos.

III - a área responsável pela gestão de pessoas do INSS deverá (sugestão de texto da DGPA) os servidores lotados nas áreas responsáveis pela gestão de pessoas do INSS deverão utilizar os canais de atendimento disponibilizados pela Dataprev, ou outro canal informado pela DTI, para:

a) solicitar o credenciamento de usuários do quadro de pessoal do INSS na data do ato administrativo de retorno ou ingresso no órgão, para acesso à rede (sugestão de redação da DGPA) solicitar, se necessário, o credenciamento de usuários, contratados ou requisitados, para compor o quadro de servidores do INSS, após o ato da posse; e de estagiários, após assinatura do contrato de prestação de serviço, para acesso à rede;

b) solicitar a revogação de credenciais de acesso de servidores do quadro de pessoal do INSS cedidos a outros órgãos (sugestão de redação da DGPA); solicitar a inativação imediata do perfil de acesso dos servidores cedidos a outros órgãos, inativos ou exonerados do quadro de servidores do INSS na data da publicação do ato;

c) solicitar a desativação de usuários do quadro de pessoal do INSS na data do ato administrativo ou de ocorrências que ensejem desligamento para fins de acesso lógico (sugestão de redação da DGPA); solicitar a suspensão imediata do perfil de acesso dos servidores afastados ou com licença programada de suas funções por mais de sessenta dias ininterruptos; e

d) solicitar a exclusão do acesso de usuários do quadro de pessoal em atividade do INSS afastados ou com licença programada de suas funções por mais de sessenta dias ininterruptos (sugestão de redação da DGPA); estagiários, cujo vínculo com o Instituto tenha sido encerrado, tão logo a rescisão do contrato seja efetivada;

IV - quanto ao processo de formação das credenciais de acesso fica estabelecido que:

a) o nome do usuário será composto de acordo com os padrões estabelecidos no Guia de Interoperabilidade do Governo Eletrônico – e-Ping, mais especificamente no documento “Caixas Individuais-Fundacionais no Governo Federal” (Rede do Governo, 2010) que define regras de formação de nomes para a composição de endereços eletrônicos;

b) quanto às senhas de acesso:

1. deverão ter no mínimo oito caracteres e conter, obrigatoriamente, caracteres alfanuméricos (combinação de letras e números). O usuário poderá acrescentar caracteres especiais (espaços em branco, símbolos, sinais de pontuação, etc);

2. é vedada a reutilização das últimas quatro senhas utilizadas pelo usuário;

3. podem ser alteradas sempre que preciso ou quando o usuário achar necessário;

4. o prazo de validade não deve ultrapassar noventa dias; e

5. o usuário receberá por meio de comunicado direto (via interface do sistema ou por mensagem no correio eletrônico) a informação do prazo próximo de vencimento da senha, quando esta estiver a 15 dias da sua data de expiração.

V - os perfis de acesso aos sistemas corporativos deverão contemplar um conjunto de permissões e ações vinculadas às atividades desenvolvidas pelo usuário;

VI- caberá à área responsável pela gestão de TI do INSS estabelecer, em conjunto com as áreas responsáveis pela gestão dos sistemas corporativos, a norma de criação dos perfis de acesso; (IN 01/2020) e PORTARIA Nº 93.

VII - as áreas responsáveis pela gestão dos sistemas corporativos, são responsáveis pelas permissões, transações e ações que devem compor cada perfil de acesso;

VIII - os perfis de acesso e perfis de gestão concedidos para usuários interno e externos deverão ser objeto de revisão contínua pelos gestores responsáveis, não podendo ultrapassar o prazo máximo de 30 (trinta) meses; Recomendação 2

IX - quanto à utilização das credenciais e perfis de acesso, o usuário:

- a) deve ter conhecimento prévio desta Norma de Controle de Acesso Lógico e preencher os requisitos estabelecidos na mesma;
- b) deve estar devidamente autorizado a utilizar a rede corporativa e/ou os sistemas corporativos, de acordo com os requisitos estabelecidos nesta Norma;
- c) deve utilizar os serviços e as informações obtidas, por meio do perfil de acesso, única e exclusivamente em razão do exercício da função pública e para os fins que lhe foi designado, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal;
- d) não pode divulgar, nem mesmo compartilhar, os códigos de segurança que lhe forem atribuídos (credenciais de acesso), os quais são pessoais e intransferíveis;
- e) não pode utilizar as credenciais para acessar os recursos disponíveis em mais de uma estação de trabalho simultaneamente;
- f) não pode fazer uso das credenciais de acesso de outros usuários;
- g) deve fornecer informações acessadas nos sistemas e na rede de dados corporativos do INSS somente mediante demanda formalizada de quem tenha competência para tal;
- h) deve comunicar a chefia imediata ou responsável pela administração do sistema ou rede corporativa quaisquer violações ou incidentes referentes à proteção do equipamento utilizado, do software ou de outros ativos da informação; e
- i) deve, sempre que for necessário afastar-se da estação de trabalho, certificar-se de que a sessão de rede ou acesso ao sistema corporativo esteja encerrado ou bloqueado.

X - a autenticação dos usuários será feita por meio de credenciais de acesso baseadas em nome de usuário e senha e, quando disponível, aliada ao uso de certificação digital padrão ICP-Brasil e/ou uso de dados biométricos; Recomendação 5

XI - o usuário deverá, obrigatoriamente, efetuar processo de alteração da sua senha em seu primeiro acesso à rede de dados corporativa; e

XII - no ato do primeiro acesso, bem como após cada atualização desta Norma, o usuário deverá manifestar concordância com os termos dispostos na mesma.

XIII - Credenciamento de Usuários Internos:

a) o cadastro de novos servidores ou ocupantes de cargo em comissão, no âmbito do Instituto, pode ser solicitado por servidor vinculado à área responsável pela gestão de pessoas ou pela chefia imediata do usuário; e

b) esse cadastro deve ser solicitado por meio dos canais de atendimento da Dataprev ou outro informado pela DTI.

XIV - credenciamento de estagiários:

a) a emissão de credencial de acesso se dará tendo como requisito as seguintes condições:

1. a empresa que atuar como agente de integração do estágio supervisionado deve manter contrato com o INSS; e
2. o contrato de estágio supervisionado deverá conter cláusula de confidencialidade e sigilo de informações preestabelecidos com a Administração Pública.

b) para viabilizar o acesso de estagiários aos sistemas corporativos, os gestores dos sistemas corporativos deverão criar perfis específicos e restritos às atividades do estagiário;

c) é vedada a concessão de perfis de acesso aos sistemas corporativos para estagiários com permissão de alteração das bases de dados institucionais;

d) o acesso será concedido mediante solicitação expressa de servidor do quadro do INSS, responsável pela supervisão do estágio, que deverá:

1. avaliar os riscos de utilização indevida de informações institucionais e as eventuais restrições referentes aos dias e horários para a realização dos acessos.

e) o acesso será precedido da assinatura do Termo de Confidencialidade e de Manutenção de Sigilo – TCMS, Anexo II, o qual deverá ser firmado pelo

estagiário ou pelo estagiário e seu responsável legal, no caso de se tratar de estagiário menor de dezoito anos;

f) as solicitações de acesso à rede para estagiários devem ser procedidas por meio dos canais remotos de atendimento da Dataprev ou outro canal informado pela DTI, pela unidade de gestão de pessoas, pela chefia imediata do educando ou pelo responsável por sua supervisão;

g) os gestores de sistemas devem criar perfis diferenciados para estagiários de nível médio e nível superior;

h) o supervisor do estagiário deverá, periodicamente, orientá-lo quanto ao uso responsável e adequado do acesso aos sistemas corporativos; e

i) o acesso do estagiário limitar-se-á à data final do contrato ou imediatamente cessado na hipótese de rescisão antecipada do estágio, cabendo ao supervisor do estagiário, em quaisquer dos casos, adotar as providências necessárias ao bloqueio do acesso, tão logo finde a contratação.

XV - credenciamento de usuários externos:

a) as credenciais de acesso para usuários externos devem ser emitidas tendo em vista o interesse do INSS, devidamente justificadas e previstas no convênio, acordo de cooperação técnica ou instrumento congênere;

b) as solicitações de emissão de credenciais de acesso à rede corporativa para usuários amparados por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica, contrato ou instrumento congênere devem:

1. ser feitas pelo gestor da unidade/área responsável pela gestão do instrumento legal; e

2. ser atendidas somente após validação das credenciais do gestor solicitante do Instituto, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700) ou outra base de dados indicada pela área responsável pela gestão de pessoas, a qual contenha informações referentes à estrutura organizacional do Instituto (sugestão de redação feita pela DGPA).

c) a emissão de credenciais de acesso à rede corporativa para prestadores de serviço terceirizados ou equiparados nas dependências do INSS, quando necessária, será provida unicamente pelo interesse do INSS. Para tanto, devem ser atendidos os seguintes requisitos:

1. a organização a qual o usuário é vinculado deve manter contrato, acordo de cooperação, convênio ou instrumento congênere vigente com o INSS;

2. instrumento deve conter cláusulas prevendo:

2.1. necessidade e justificativa para acesso à rede corporativa;

2.2. a confidencialidade e sigilo de informações preestabelecidas junto ao Instituto;

2.3. a obrigatoriedade da organização ou do ente contratado informar previamente ao representante legal do INSS, responsável pela gestão do contrato, quaisquer alterações em seu corpo de colaboradores que impacte na emissão/exclusão das contas de acesso; (atendendo a recomendação nº 6 da CGU)

2.4. a organização ou ente contratado também deverá manter com seus colaboradores Termo de Confidencialidade de Manutenção de Sigilo – TCMS; e

2.5. o gestor do contrato pelo INSS deve fundamentar a necessidade do acesso à rede para prestadores de serviço terceirizados ou equiparados, definindo os recursos que devem ser disponibilizados e eventuais restrições a dias e horas para realização do acesso à rede.

3. os TCMS deverão ser arquivados junto aos instrumentos assinados com o INSS e uma cópia ou link eletrônico deverá ser encaminhada ao Gestor do Contrato. O mesmo deve ocorrer para quaisquer alterações ocorridas na vigência dos contratos, acordos ou convênios;

3.1 caso os Termos sejam gerados de forma eletrônica, deverá ser disponibilizado o arquivo correspondente, atendendo aos requisitos necessários para garantia de integridade e disponibilidade de acesso, assim como os requisitos específicos previstos em contrato; e

4. a emissão de credenciais de acesso poderá ser feita pelo gestor do contrato, representante legal do INSS, ou pelo gestor da unidade responsável pela gestão do contrato, convênio, acordo de cooperação técnica ou instrumento congênere e serão atendidas somente após validação das credenciais do solicitante, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700) ou outra base de dados indicada pela área responsável pela gestão de pessoas, a qual contenha informações referentes à estrutura organizacional do Instituto (sugestão de texto feita pela DPGA).

d) o acesso aos prestadores de serviço vinculados à Central de Atendimento 135 se dará observando as seguintes condições:

1. a empresa deve manter contrato com o INSS;

2. o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

3. a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade - TCMS;

4. o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte do INSS, definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;

5. os acessos deverão ser realizados única e exclusivamente por necessidade de serviço; e

6. Os contratos de prestação de serviços de teleatendimento devem conter documento a ser utilizado para formalização das indicações de gestores de acesso aos sistemas corporativos do Instituto; (sugestão de texto para atendimento da recomendação nº 7 do Relatório da CGU)

7. o INSS pode disponibilizar, de forma restrita, às centrais 135 uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

e) nos casos referentes a prestadores de serviço vinculados à Ouvidoria-Geral da Previdência Social – OUGPS, o acesso se dará observando-se as seguintes condições:

1. a empresa deve manter Contrato direto com a Ouvidoria-Geral da Previdência Social;
2. o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;
3. a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade;
4. o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte da OUGPS, definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;

5. os acessos deverão ser realizados única e exclusivamente por necessidade de serviço; e

6. o INSS pode disponibilizar, de forma restrita, à OUGPS uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

f) o acesso à rede corporativa por servidores vinculados a órgãos de controle externo, envolvidos em ações de auditoria no âmbito do INSS, será concedido mediante apresentação da equipe de auditoria por meio de documento formal que conste:

1. dados necessários ao cadastro de usuários externos;
2. informações acerca dos objetivos dos trabalhos a serem executados;
3. os prazos envolvidos; e
4. informações complementares.

g) este tipo de acesso deverá observar as parcerias institucionalmente estabelecidas entre esses órgãos e o INSS no que tange à cobertura/previsão de acesso à rede corporativa do Instituto; e

h) o atendimento de pedido de solicitação de informações advindo de pessoas físicas ou jurídicas externas, respeitadas as restrições de acesso às informações previstas na Lei nº 12.527, de 18 de novembro de 2011, serão analisadas pela área designada para responder as demandas dos cidadãos por meio do e-SIC.

XVI - os procedimentos referentes às solicitações de inclusão, exclusão, inativação e suspensão de contas de acesso de usuários devem ser executados tendo como premissa a preservação dos registros para efeito de auditoria.

XVII - bloqueio administrativo:

a) o responsável pela Corregedoria-Geral do INSS, quando necessário, poderão solicitar a suspensão, bloqueio ou inativação imediata de contas de acesso de usuários que estiverem envolvidos em inquérito penal, em Processo Administrativo Disciplinar – PAD – ou em Sindicância, decorrente de infrações cometidas no exercício das atribuições do cargo;

b) estas solicitações deverão ser efetuadas mediante comunicação formal da Corregedoria-Geral para a Dataprev, ou outro canal informado pela DTI, a qual procederá a imediata implementação da mudança.

c) para disciplinar o disposto na "alínea a", é considerado possível de ter a senha bloqueada, o usuário que estiver na seguinte situação:

1. afastado temporariamente do cargo ou função pública em razão de ato que se encontra sob apuração;
2. indiciado em processo administrativo disciplinar, por incursão nos incisos IX, XI, XII, XV, XVI e XVII do art. 117 e arts. 130 e 132 da Lei nº 8.112, de 11 de dezembro de 1990, ou cuja proposta pela Comissão Processante, no relatório final, seja pela aplicação de penalidade a partir de suspensão de trinta dias; e
3. submetido à prisão em flagrante, temporária ou preventiva decorrente do cometimento de infração no exercício das atribuições do cargo, enquanto estiver em apuração de inquérito policial ou pelo Ministério Público Federal.

d) o bloqueio de acessos, tratados nas situações da "alínea c", será efetivado no âmbito da ferramenta de gestão de acessos nas seguintes situações:

1. usuário afastado temporariamente do cargo ou função, enquanto durar o afastamento; e

2. usuário indiciado nos termos do subitem "alínea c", desta Norma, até o efetivo cumprimento da penalidade porventura aplicada ou, em caso de não aplicação de penalidade, enquanto durar o processo.

Art. 6º Rede de Dados Corporativa:

I - infraestrutura de rede:

a) a infraestrutura de rede do INSS é disponibilizada para uso Institucional. Sendo assim, apenas equipamentos de propriedade do Instituto são autorizados e devem ser conectados à rede corporativa;

1. em casos excepcionais, a conexão de equipamentos particulares à rede corporativa deve ser feita em razão do interesse do Instituto e sob prévia autorização do responsável pela gestão da unidade em que o equipamento estiver localizado.

b) o INSS poderá disponibilizar o acesso à rede de dados corporativa por meio de tecnologia *Wireless* (sem fio). Para tanto os seguintes critérios deverão ser adotados:

1. os projetos que envolvam a utilização de pontos de acesso sem fio à rede corporativa no âmbito do Instituto deverão ser devidamente registrados e aprovados pela área responsável pela gestão de TI do INSS; (IN 01/2020) e PORTARIA Nº 93.

2. os pontos de acesso à rede de dados corporativa sem fio poderão ser objeto de testes periódicos de penetração e de auditoria a critério da área responsável pela gestão de TI no INSS; (IN 01/2020) e PORTARIA Nº 93.

3. as conexões à rede sem fio serão avaliadas pela área responsável pela gestão de TI do INSS em relação aos requisitos de segurança e deverão atender ao princípio do privilégio mínimo; (IN 01/2020) e PORTARIA Nº 93.

4. a área responsável pela gestão de TI do INSS poderá disponibilizar rede sem fio com regras específicas de acesso para visitantes nas diversas unidades do Instituto; (IN 01/2020) e PORTARIA Nº 93.

5. os dispositivos conectados à rede do INSS por meio de conexão sem fio deverão suportar configurações de criptografia estabelecidas pela área responsável pela gestão de TI no âmbito do INSS; e (IN 01/2020) e PORTARIA Nº 93.

6. qualquer tecnologia de acesso sem fio implementada no INSS deverá suportar autenticação forte, com possibilidade de efetuar checagens em bancos de dados externos.

c) a área responsável pela gestão de TI do INSS deve dispor de mecanismos automáticos que possibilitem: (IN 01/2020) e PORTARIA Nº 93.

1. a detecção e bloqueio de equipamentos externos conectados à rede corporativa; e

2. a identificação e rastreamento dos endereços IP de origem e destino, bem como os serviços utilizados na rede corporativa inclusive nos acessos remotos.

II - administração da rede corporativa:

a) a administração da rede do INSS é realizada pela Empresa de Tecnologia e Informações da Previdência Social - Dataprev;

1. os ativos e serviços que compõem a rede de dados corporativa são providos, gerenciados e operacionalizados pela empresa; e

2. os acessos à rede de dados corporativa realizados pelos usuários do INSS são gerenciados e monitorados pela Dataprev, contudo seguem as regras desta Norma.

b) quanto ao processo de geração de contas de serviço fica estabelecido que:

1. os critérios para a emissão de contas de serviços serão vinculados a um processo formal estabelecido pela área responsável pela gestão de TI do INSS; (IN 01/2020) e PORTARIA Nº 93.

2. a concessão de contas de serviços deve ser feita conforme a necessidade de uso de acordo com os critérios estabelecidos nesta Norma de Controle de Acesso;

3. o direito de acesso privilegiado, por meio de contas de serviços, associado a sistemas ou processos, deve ser identificado;

4. deve ser viabilizada ferramenta que possibilite a gestão das contas de serviço de forma automatizada, possibilitando o registro e verificação de todos os privilégios concedidos;

5. as contas de serviço fornecidas devem ser utilizadas exclusivamente para os fins aos quais foram concedidas;

6. as contas de serviço emitidas devem ser revalidadas periodicamente com base na função exercida e na área de atuação do servidor; e

7. as contas de serviço com credenciais de acesso de uso compartilhado devem ter suas senhas alteradas periodicamente, conforme estabelecido nesta Norma de Controle de Acesso Lógico, ou sempre que ocorrerem mudanças no grupo de usuários que utilizam as mesmas.

C) é vedado o uso da rede corporativa para:

1. acesso por meio de equipamento não homologado ou não autorizado pelo INSS;

2. fazer download, instalar e/ou utilizar sistemas ou aplicativos não homologados pela área responsável pela gestão de TI do INSS nos equipamentos de propriedade do Instituto; (IN 01/2020) e PORTARIA Nº 93.

3. a utilização de softwares particulares em equipamentos do INSS sem autorização expressa;

4. a instalação e conexão de equipamentos particulares à rede corporativa do Instituto sem a prévia autorização do gestor responsável pela unidade ou da área responsável pela gestão de TI do INSS; (IN 01/2020) e PORTARIA Nº 93.

5. o uso dos recursos de rede para fins particulares ou de terceiros alheios aos interesses do INSS, em especial quando tal procedimento prejudique o tráfego da rede de dados;

6. o uso para fins de divulgação ou distribuição de material que não possua vínculo com as atividades desenvolvidas pelo Instituto;

7. a instalação ou utilização de ferramentas de monitoramento de rede sem a anuência e autorização expressa da área responsável pela gestão de TI no Instituto; (IN 01/2020) e PORTARIA Nº 93.

8. a instalação de dispositivos de comunicação ou de compartilhamento de dados sem fio, particulares, à rede corporativa do Instituto, sem autorização expressa da área responsável pela gestão de TI do INSS; e (IN 01/2020) e PORTARIA Nº 93.

9. burlar as regras de acesso a internet configuradas em proxy ou ferramenta similar de gerenciamento de conteúdo web; (incluído)

d) cabe à área responsável pela gestão de TI no âmbito do INSS definir os aspectos relacionados à plataforma tecnológica, gestão operacional, forma de autenticação e sustentação do domínio de rede do INSS. (IN 01/2020) e PORTARIA Nº 93.

Art. 7º Gestão do Acesso aos Sistemas Corporativos:

I - sistemas legados:

a) as regras estabelecidas nesta norma devem ser aplicadas, guardando-se as devidas limitações tecnológicas, aos sistemas legados; e

b) o controle de acesso aos sistemas legados é efetuado por base própria.

II - sistemas de apoio à administração:

a) os ambientes de hospedagem desses sistemas são suportados por terceiros;

b) o ambiente deverá ser gerenciado e operacionalizado pela área de gestão de TI do INSS; (IN 01/2020) e PORTARIA Nº 93.

c) o acesso pelos usuários a esses sistemas deverá ser autenticado pelo serviço de diretório utilizado pelo Instituto; e

d) as regras de hospedagem de sistemas serão definidas, em ato próprio, pela área de gestão de TI do INSS. (IN 01/2020) e PORTARIA Nº 93.

III - armazenamento de registros logs:

a) as áreas responsáveis pela gestão de sistemas corporativos e demais aplicações devem definir, em conjunto com a área responsável pela gestão de TI, a temporalidade de registro dos logs de acesso e transações, e quais registros devem ser armazenados por um período maior que o estipulado no Art. 8º, I desta Norma; e (IN 01/2020) e PORTARIA Nº 93.

b) o INSS poderá alterar a temporalidade destes dados em norma específica;

c) Os logs de acesso devem contemplar minimamente os registros relacionados no ANEXO III desta norma. Recomendação 4.

IV - administração da ferramenta de gestão de acesso:

a) com o objetivo de operacionalizar a gestão dos acessos aos sistemas corporativos no âmbito do INSS, serão criados os seguintes papéis:

1. administrador de sistema INSS: Servidor do quadro, lotado na área responsável pela gestão de TI, designado por meio de Portaria do Diretor de

2. gestor de sistema: Servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em Boletim de Serviço, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedoria-Geral e Procuradoria Federal Especializada. É responsável pela implementação de sistemas corporativos no âmbito do INSS;

3. gestor de acesso central: Servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em Boletim de Serviço, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedoria-Geral e Procuradoria Federal Especializada. É responsável pela manutenção dos perfis de gestão dos usuários nas áreas que compõem a Administração Central e, quando necessário, dos gestores de acesso das Superintendências Regionais;

4. gestor de acesso interno: Servidor do quadro, lotado na Administração Central, Superintendência Regional, Gerência Executiva, Agência da Previdência Social, indicado pelo Gestor de Acesso Central ou por um Gestor de Acesso, responsável pela atribuição do perfil de acesso e de gestão dos usuários no INSS; e

5. gestor de acesso externo: Pessoa formalmente indicada, por documento previsto no instrumento legal que firmou a parceria ou por meio de Ofício de lavra do representante máximo de uma Entidade Externa, responsável pelo cadastro de usuários externos e a gestão dos acessos aos sistemas corporativos do Instituto.

b) Os perfis de acesso serão atribuídos de acordo com a necessidade do fluxo de operação definido para cada sistema corporativo. (Recomendação 1)

c) a indicação e processo de substituição dos responsáveis pela gestão dos acessos aos sistemas corporativos no âmbito do INSS poderá ser procedida das seguintes formas:

1. a autoridade responsável pela indicação do gestor de acessos pode indicar opcionalmente o substituto;
2. o próprio gestor de acessos pode designar, a qualquer momento, por meio da ferramenta de gestão de acessos um substituto; ou
3. quando não houver um gestor responsável, ou substituto, por uma unidade devidamente designado, a gestão dos usuários será transferida, preferencialmente de forma automática, para o responsável pela área da abrangência daquela unidade e assim subsequentemente; e
4. o Gestor de Acesso é corresponsável com os perfis de gestão ou acesso que ele atribuir aos usuários.

c) ao usuário interno cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Norma de Controle de Acesso Lógico e suas normas complementares;
2. solicitar, ao Gestor de Acesso responsável pela gestão da unidade de lotação a qual é vinculado, a suspensão do seu perfil de acesso nos períodos de afastamento do serviço por mais de trinta dias consecutivos;
3. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e
4. ter conhecimento e estar de acordo com o disposto nesta Norma.

d) ao usuário externo cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Norma de Controle de Acesso Lógico;
2. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e
3. ter conhecimento e estar de acordo com o disposto nesta Norma.

e) ao administrador do sistema INSS cabe:

1. criar os sistemas e subsistemas, devidamente homologados pela área de negócio responsável, no ambiente de produção, por meio de ferramenta de gestão de acesso;
2. mediante apresentação de Portaria de designação para Gestores de Acesso Central, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores quanto à atribuição dos perfis de gestão; e
3. mediante apresentação de Portaria de designação para Gestores de Sistema, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores acerca do processo de implementação dos sistemas corporativos no âmbito do INSS.

f) ao gestor de sistema cabe:

1. efetuar os procedimentos de importação, inclusão, alteração e exclusão de papéis e permissões nos sistemas corporativos em ambiente de

produção; e

2. atuar, em conjunto com o Administrador do Sistema INSS e a Dataprev, no planejamento e execução do processo de implementação dos sistemas corporativos dos quais for designado responsável.

g) ao gestor de acesso central cabe:

1. efetuar o credenciamento, suspensão ou exclusão de perfis de gestão dos sistemas corporativos aos Gestores de Acesso na Administração Central e, quando necessário, dos Gestores de Acesso da Superintendência Regional, Gerência Executiva, Agência da Previdência Social e demais usuários de sua abrangência; e

2. orientar os usuários de sua abrangência e os gestores da Administração Central e Superintendências Regionais, Gerências Executivas e Agências da Previdência Social acerca das regras para o acesso aos sistemas corporativos do INSS.

h) ao gestor de acesso interno cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários da Administração Central, Superintendência Regional, Gerência Executiva, Agência da Previdência Social;

2. atribuir, alterar ou excluir os perfis de acesso aos usuários da Administração Central, Superintendência Regional, Gerência Executiva, Agência da Previdência Social; e

3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS.

i) ao gestor de acesso externo cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários do seu Órgão/Entidade;

2. atribuir, alterar ou excluir os perfis de acesso aos usuários do seu Órgão/Entidade; e

3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS.

V - configura-se mau uso, sujeito a responsabilidade penal, civil e disciplinar:

a) a divulgação, sem autorização expressa da chefia imediata ou do gestor de acesso de sua abrangência, de informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS;

b) acessar sistemas corporativos sem autorização prévia, de acordo com os requisitos estabelecidos nesta Norma;

c) utilizar-se das informações obtidas por meio de acesso concedido em desacordo com os procedimentos dispostos nesta Norma e demais normas vigentes na Administração Pública Federal;

d) compartilhar ou fazer uso das credenciais de acesso, aos sistemas corporativos, de outros usuários;

e) a instalação de sistemas corporativos em equipamentos particulares; e

f) em casos excepcionais, a área responsável pela gestão de TI do INSS, mediante ato formal, poderá autorizar o contido no Art.8º, III. (IN 01/2020) e PORTARIA Nº 93.

Art. 8º Disposições Gerais:

I - todo acesso à rede de dados e aos sistemas corporativos deve ser registrado e monitorado de modo que permita a rastreabilidade, a identificação e o bloqueio de usuários e equipamentos não autorizados. Estas informações devem ser armazenadas por um período de, no mínimo, 30 (trinta) meses; (atendimento da recomendação nº 19 da CGU)

II - as ocorrências de mau uso do acesso aos recursos disponíveis na rede e sistemas corporativos não previstas nesta norma e os casos omissos serão encaminhados para a área responsável pela gestão de TI no âmbito do INSS para análise e pronunciamento; (IN 01/2020) e PORTARIA Nº 93.

III - identificada irregularidade de mau uso dos recursos de rede poderá ocorrer:

a) o bloqueio preventivo do acesso pela DTI, o encaminhamento de dossiê com as informações para a Corregedoria-Geral do INSS ou Corregedorias Regionais, nas suas áreas de abrangências, a fim de que seja realizada a análise no âmbito disciplinar; e

b) ressalta-se que o descumprimento dessa Norma poderá resultar em sanções administrativas, civis e criminais.

IV - esta norma deve ser revisada num período máximo de três anos.

ANEXO II

RESOLUÇÃO Nº 3/CEGOV/INSS, DE DE DE 2020

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF: _____, identidade _____, expedida pelo _____, em _____, e lotado no(a) _____ do Instituto Nacional do Seguro Social – INSS, DECLARO, sob pena das sanções cabíveis nos termos da Política de Segurança da Informação e Comunicações - POSIC POSIN do INSS que assumo a responsabilidade por: (IN 01/2020)

I - tratar o(s) ativo(s) de informação como patrimônio do Instituto Nacional do Seguro Social;

II - utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do INSS;

III - contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, que Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta; Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que disciplina a gestão de segurança da informação na Administração Pública Federal, direta e indireta, e dá outras providências; (IN 01/2020) Substituir

IV - utilizar as credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do INSS;

V - responder, perante o INSS, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

_____, _____ de _____ de _____

Assinatura do usuário

Nome do usuário:	Unidade de Lotação:
Nome da Autoridade Responsável pela Autorização do Acesso:	

Assinatura e Carimbo do Responsável pela Autorização de Acesso

ANEXO III

RESOLUÇÃO Nº 3/CEGOV/INSS, DE DE DE 2020

REGISTROS DE LOGS

1. Relação dos campos de registros de logs do GERID
 - 1.1. Dados Gerais
 - 1.1.1. Data
 - 1.1.2. Sistema
 - 1.1.3. Ambiente
 - 1.1.4. IP destino
 - 1.1.5. IP origem
 - 1.1.6. CPF usuário
 - 1.1.7. URL de origem
 2. Ações:
 - 2.1. CAS (autenticação): Central Authentication Service - Serviço Central de Autenticação
 - 2.1.1. Criação de service ticket (ST)
 - 2.1.2. Criação de ticket granting ticket (TGT)
 - 2.1.3. validação de ST
 - 2.1.4. Exclusão de ticket TGT
 - 2.1.5. Autenticação com sucesso (login+password)
 - 2.1.6. Autenticação com sucesso (certificado digital)
 - 2.1.7. Autenticação com falha
 - 2.2. GPA: Gerenciamento de Permissão de Acesso
 - 2.2.1. Início de sessão

- 2.2.2. Dados do usuário em sessão (CPF, NOME, PAPEL)
- 2.2.3. Requisição de logout
- 2.2.4. Dados de credenciais
- 2.2.5. Concessão de credenciais
- 2.2.6. Alteração de Credenciais
- 2.2.7. Dados de receptor (CPF, NOME, Lotação)
- 2.2.8. Inserção de credencial no usuário
- 2.2.9. Revogação de Credenciais
- 2.2.10. Pesquisa de credenciais
- 2.2.11. Pesquisa de usuários
- 2.2.12. Substituição de gestor



INSTITUTO NACIONAL DO SEGURO SOCIAL
MINUTA DE RESOLUÇÃO

MINUTA DE RESOLUÇÃO

**RESOLUÇÃO Nº 4/CEGOV/INSS, DE DE
DE 2020**

Institui a Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR do INSS.
Instituto Nacional do Seguro Social.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída a Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR do INSS.

Art. 2º Os Anexos a esta Portaria serão publicados em Boletim de Serviço.

Art. 3º Esta Portaria complementa Política de Segurança da Informação e Comunicações – POSIC POSIN-INSS vigente.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretora de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **ROBERTO RUFINO DA COSTA**, **Chefe de Serviço Substituto(a)**, em 03/07/2020, às 17:02, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1075281** e o código CRC **D0D856D4**.

ANEXO I

RESOLUÇÃO Nº 4/CEGOV/INSS, DE DE DE 2020
EQUIPE DE TRATAMENTO DE INCIDENTES DE REDES COMPUTACIONAIS - ETIR

Art. 1º Para os efeitos desta norma ficam estabelecidos os seguintes conceitos e definições:

I - agente responsável: Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

II - artefato malicioso: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

III - comunidade ou Público Alvo: é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

IV - CTIR GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI;

V - equipe de tratamento e resposta a incidentes em redes computacionais – ETIR: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

VI - incidente de segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VII - serviço: é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

VIII - tratamento de Incidentes de Segurança em Redes Computacionais: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

XI - usuário: pessoas que fazem uso de serviços de TI e sistemas de informação de propriedade do INSS, independente do cargo ocupado (contratados, consultores, conselheiros, servidores, temporários e etc); e

X - vulnerabilidade: ~~é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados;~~ conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou por uma organização, os quais podem ser evitados por uma ação interna de segurança da informação. **(IN 01/2020) e PORTARIA Nº 93.(alterado)**

Art. 2º Esta norma tem a missão de:

Parágrafo único. Agir proativamente, receber, analisar, monitorar, coordenar e propor respostas a notificações e atividades relacionadas a incidentes de segurança da informação e comunicações no âmbito do Instituto.

Art. 3º Esta norma tem como público alvo:

I - a abrangência das atividades pertinentes à ETIR-INSS inclui os usuários dos serviços de Tecnologia da Informação ~~e Comunicações - TI~~ e os sistemas de informação do INSS; **(IN 01/2020) e PORTARIA Nº 93**

II - as atividades pertinentes à ETIR-INSS serão realizadas com intercâmbio de informações e em cooperação com as seguintes instâncias:

a) o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR GOV;

b) a Comissão de Resposta e Tratamento de Incidentes em Redes Computacionais – CTIR, da Empresa de Tecnologia e Informações da Previdência Social - Dataprev;

c) equipes de tratamento de incidentes de redes computacionais dos demais órgãos, entidades e empresas, públicas ou privadas, que tenham contratos, acordos, convênios ou instrumentos congêneres com o INSS; e

d) o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República – GSI/PR.

Art. 4º a implementação e o funcionamento da ETIR-INSS seguirão a metodologia definida pelo Gabinete de Segurança Institucional da Presidência da República, conforme definido a seguir:

I - o modelo de implementação no qual a ETIR-INSS se baseia é o “Modelo 1 – Utilizando a equipe de Tecnologia da Informação”, conforme definido pelo GSI/PR;

II - a equipe será composta por profissionais da área de Tecnologia da Informação, lotados na Diretoria de Tecnologia da Informação e Inovação – DTI, sem prejuízo de suas atribuições típicas do cargo, com experiência e conhecimentos técnicos compatíveis com a importância da missão da ETIR-INSS;

III - a equipe será composta por servidores públicos efetivos;

IV - a ETIR-INSS ficará vinculada tecnicamente à Coordenação de Infraestrutura e Operações – CGIN, da Diretoria de Tecnologia da Informação e Inovação - DTI; e

~~V - o Coordenador da ETIR-INSS será o Gestor de Segurança da Informação e Comunicações o Diretor de Tecnologia da Informação e Inovação, conforme definido na Política de Segurança da Informação e Comunicações – POSIC POSIN-INSS.~~ **(IN 01/2020) (alterado)**

Art. 5º A ETIR-INSS será composta por membros:

I - permanentes: que efetivamente atuarão em todos os incidentes registrados;

II - colaboradores: que atuarão, de forma esporádica, no tratamento de incidentes relacionados às suas áreas de atuação; e

III - Opcionais: servidores das unidades descentralizadas sob supervisão da DTI.

IV - sendo assim, a ETIR-INSS será formada pelos seguintes servidores: por servidores lotados na área de TI, de acordo com os papéis abaixo:(incluído)

Papel	Nome	Matrícula	Setor
Permanente	Roberto Rufino da Costa	1.057.683	Serviço de Segurança em TIC
Permanente	Nelson Antonio Pimentel Jacinto	1.095.044	Serviço de Segurança em TIC
Colaborador	Cristiano Santos de Souza	2.156.073	Divisão de Infraestrutura e Operações
Colaborador	Lourival de Sousa	2.262.639	Divisão de Infraestrutura e Operações
Colaborador	Jair Rodrigues Fernandes	2.276.407	Divisão de Infraestrutura e Operações
Colaborador	Rodrigo Gomes Rodrigues	2.135.059	Divisão de Arquitetura e Soluções

Quantidade	Papel	Setor
2	Permanente	Serviço de Segurança de TIC
2	Colaborador	Coordenação-Geral de Infraestrutura e Operações
2	Colaborador	Coordenação-Geral de Projetos e Soluções Digitais
2	Opcional	Unidades descentralizadas

V - Os membros da ETIR-INSS serão designados por meio de ato do Diretor de Tecnologia da Informação e Inovação.

Art. 6º Quanto autonomia da ETIR-INSS:

I - terá autonomia limitada para o tratamento de incidentes de Segurança da Informação, devendo implementar ações que possam impactar outras áreas do Instituto somente com anuência do Diretor de Tecnologia da Informação e Inovação e do gestor responsável pela área/sistema afetada; e

II - poderá, ainda, gerar relatórios técnicos sugerindo a adoção de medidas para resolução de incidentes.

Art. 7º A ETIR-INSS fornecerá o serviço de Tratamento de Incidentes de Segurança em Redes Computacionais:

I - este serviço compreende basicamente as seguintes ações:

- recepção: receber solicitações e alertas diversos. Para tanto o Instituto disponibilizará como canal de comunicação a caixa postal etir@inss.gov.br;
- filtrar: todo conteúdo direcionado para a ETIR deve ser verificado, a partir desta análise deve ser tratado pela equipe ou, não se tratando de um incidente de segurança em redes computacionais, encaminhado para a área competente;
- catalogar: os incidentes devem ser catalogados em ferramenta a ser indicada pela DTI, com nível de acesso restrito;
- classificar: os incidentes devem ser classificados quanto ao nível de severidade e impacto;
- tratar o incidente: indicar o tratamento do incidente com medidas corretivas e formas de se evitar que ocorra novamente;
- responder: as solicitações e alertas encaminhados para a ETIR devem ser devidamente respondidos; e
- monitorar: monitorar a aplicação do tratamento dos incidentes indicados.

II - a ETIR deve analisar os incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências; e

III - o detalhamento dos serviços prestados pela ETIR-INSS deve ser publicado em página específica da Intranet do Instituto no prazo de 30 dias a partir da publicação desta portaria.



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 5/CEGOV/INSS, DE DE DE 2020

Disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis Internet, competências e conteúdo de acesso para cada perfil.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída, nos termos do Anexo I desta Portaria, norma que estabelece critérios para uso da Internet no âmbito do Instituto Nacional do Seguro Social - INSS.

Art. 2º Os Anexos a esta Portaria serão publicados em Boletim de Serviço.

Art. 3º Esta Portaria complementa a Política de Segurança da Informação e Comunicações POSIC POSIN-INSS vigente. (IN 01/2020)

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretora de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **ROBERTO RUFINO DA COSTA**, **Chefe de Serviço Substituto(a)**, em 03/07/2020, às 17:02, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1075292** e o código CRC **66F4E9E1**.

ANEXO I

RESOLUÇÃO Nº 5/CEGOV/INSS, DE DE DE 2020

NORMA DE USO DA INTERNET

Art. 1º Esta norma se aplica a todos os servidores e colaboradores, vinculados direta ou indiretamente ao INSS, bem como a servidores e empregados de entidades e órgãos da Administração Pública ou privadas que necessitem ou estejam autorizados a acessar a Internet a partir da rede corporativa do Instituto.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União – AGU que atuem na consultoria e no assessoramento jurídico, e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta norma, ficam estabelecidos os seguintes conceitos e definições:

I - autorizador: ocupantes de cargos que serão responsáveis pela autorização da concessão de perfis de acesso para usuários finais de sua área de abrangência;

II - internet: é a rede mundial que interliga computadores de diferentes tipos e dimensões e permite a comunicação entre pessoas e organizações, independentemente da localização geográfica;

III - intranet: é a rede de computadores administrada pelo INSS, que utiliza os mesmos serviços e tecnologias disponíveis na rede mundial, podendo ser definida como um tipo de Internet Local do Instituto;

IV - perfil de acesso: atributo que estabelece as categorias de sítios acessíveis e tipos de arquivos que podem ser recebidos ou transmitidos pelos usuários;

V - proxy: desempenha a função de conexão do computador (local) à rede externa (Internet). Como os endereços locais do computador não são válidos para acessos externos, cabe ao proxy enviar a solicitação do endereço local para o servidor, traduzindo e repassando-a para o seu computador;

VI - sítio: um conjunto de informações ou serviços disponíveis na Internet ou na Intranet, organizados em páginas eletrônicas e acessíveis por meio de endereços que identificam, de forma padronizada, sua origem e conteúdo;

VII - usuário: Servidores, estagiários, terceirizados, contratados e colaboradores, que na execução de suas atividades necessitem de acesso à internet; servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal-APF, formalizada por meio da assinatura do Termo de Responsabilidade; e Substituir

VIII - VPN: Trata-se de uma Rede Privada Virtual (Virtual Private Network) construída sobre a infraestrutura de uma rede pública. Essa é uma forma de conectar dois computadores por meio de uma rede pública, como a Internet;

Art. 3º Essa norma tem como diretrizes:

I - o acesso à Internet disponibilizado pelo Instituto Nacional do Seguro Social aos usuários deve ser utilizado exclusivamente em razão de trabalho, cumprindo os procedimentos dispostos nesta norma;

II - os recursos disponibilizados pelo Instituto, não poderão ser usados para quaisquer propósitos que sejam ilegais ou proibidos, de modo a danificar, desativar, sobrecarregar ou prejudicar qualquer área, serviço ou conteúdo, ou interferir no uso e execução das atividades laborais de outros usuários;

III - o volume de tráfego de Internet e os endereços *web* visitados poderão ser monitorados, visando assegurar o cumprimento desta norma; e

IV - o acesso à Internet para propósitos particulares ou estranhos às atividades do INSS poderá ser bloqueado, sem prévia comunicação ao usuário e sem prejuízo das demais sanções aplicáveis.

Art. 4º Quando aos Perfis de Acesso:

I - o acesso aos sítios da Internet para todos os usuários será realizado mediante a atribuição de perfis de acesso;

II - o processo de solicitação e autorização de perfil de acesso à Internet do INSS compreenderá os seguintes perfis:

a) Perfil 1 - Perfil Restrito, deve ser inicialmente atribuído para usuários com maior restrição de acesso à internet, permitido acessar somente sítios governamentais, instituições bancárias e sítios considerados de interesse do INSS;

b) Perfil 2 - Perfil Básico, deve ser inicialmente atribuído para estagiários, recepcionistas e usuários externos. O usuário poderá acessar todos os sítios permitidos pelo Perfil 1, sítios de provedores de e-mail pessoal e instituições de ensino;

c) Perfil 3 - Perfil Padrão, para os servidores do quadro do Instituto. O usuário poderá acessar a todos sítios da internet sem a veiculação de material em áudio e vídeo; e

d) Perfil 4 - Perfil Avançado, deve ser atribuído preferencialmente para servidores do quadro do Instituto e estagiários que desempenham funções relacionadas à Comunicação Social, Desenvolvimento de Pessoas e gestores, respeitado o princípio da necessidade de conhecer, designados pelos Autorizadores deste perfil. O usuário poderá acessar todos os sítios da Internet, incluindo sítios que veiculam material em áudio e vídeo (*streaming*), sítios de compartilhamento de vídeos, blogs e redes sociais.

III - o perfil concedido a agentes externos é de caráter temporário, com validade equivalente à vigência do trabalho a ser executado;

IV - o processo de alterações, bloqueios, liberações e categorizações de sítios, assim como a criação e/ou alterações de perfis de acesso descritos nesta norma, quando necessários, serão definidos pela Diretoria de Tecnologia da Informação e Inovação – DTI, e publicado no Portal do INSS na Intranet; e

V - os novos usuários que não tiverem um perfil de acesso atribuído, devem ser direcionados para uma página da intranet contendo orientações e normas relacionadas ao acesso à internet no INSS, entre outras informações definidas pela DTI.

Art. 5º Acesso de Usuários Externos:

I - quanto ao acesso de servidores ou funcionários públicos externos:

a) o acesso à Intranet e Internet a partir da rede de dados corporativa, nas dependências do INSS, aos demais órgãos da Administração Pública Direta e Indireta, de qualquer das esferas de governo, será concedido exclusivamente para servidores e empregados públicos, efetivos ou ocupantes de cargo em comissão;

b) os acessos dos usuários externos das entidades que compõem o Poder Público serão concedidos mediante o estabelecimento de acordos ou convênios específicos firmados com o INSS;

c) o gestor ou Coordenador-Geral da área responsável pelo convênio, contrato, ACT ou instrumento congênere, assumirá o papel de Autorizador do serviço de acesso à internet para usuários externos e deverá fundamentar as solicitações com base no instrumento; e

d) poderão ser concedidos acessos temporários para auditores de controle interno e externo, vinculados à Controladoria-Geral da União – CGU ou do Tribunal de Contas da União - TCU, no uso de suas atribuições.

II - quanto ao acesso de terceirizados:

a) o acesso à Internet por terceirizados deve ser provido pela empresa contratada;

b) em caráter de exceção, será concedido o acesso aos terceirizados a partir da infraestrutura de rede do INSS, desde que preenchidos os seguintes requisitos:

1. o contrato de prestação de serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

2. a empresa contratada deverá manter com seus funcionários Termo de Confidencialidade;

3. o contrato deve prever a necessidade de acesso à internet a partir das dependências do Instituto; e

4. o Autorizador, que para estes fins será o gestor do contrato ou o responsável pela área requisitante do serviço, deverá fundamentar as necessidades de acesso do contratado, definindo os recursos que devem ser disponibilizados, endereços da Intranet e Internet necessários para o desenvolvimento das atividades, bem como eventuais restrições a dias e horários para realização do acesso.

III - quanto ao acesso de visitantes:

a) a conexão de equipamentos pessoais à rede do Instituto, quando necessária e motivada pelo interesse da Administração, deve ser previamente autorizada pelo gestor da unidade onde o equipamento será utilizado;

b) só será permitida a utilização da rede local por equipamentos que atendam a todos os requisitos estabelecidos pela DTI; e

c) o acesso se dará, exclusivamente, à Internet, sendo vedado o acesso ao conteúdo disponibilizado na intranet.

Art. 6º A todos os perfis de acesso descritos nesta norma aplicam-se as restrições de acesso a sítios que:

I - contenham material pornográfico ou obsceno;

II - contenham material ilegal;

III - disponibilizem jogos, inclusive os da Internet (online);

IV - contenham material impróprio, ofensivo, preconceituoso ou discriminatório, que façam apologia à violência, ao terrorismo e às drogas; e

V - contenha e/ou divulgue conteúdo de violação de direito autoral (pirataria) e/ou execução de quaisquer tipos ou formas de fraudes.

Art. 7º Quanto ao processo de atribuição de acesso à Internet:

I - a atribuição dos perfis de acesso à Internet serão feitas pelos Autorizadores, de forma fundamentada respeitando o princípio da necessidade de conhecer, de acordo com a tabela abaixo:

Perfil	Autorizador
Perfil 1, 2 e 3	Gerente de APS, Gerente Executivo, Superintendentes Regionais, Procuradores Regionais, Coordenadores-Gerais, Superintendentes Regionais, Presidente do INSS, Auditor-Geral, Coordenadores-Gerais, Corregedoria-Geral, Procurador-Chefe da PFE-INSS, Diretores, Gestor ou chefe da área responsável pelo Contrato ou ato administrativo similar no âmbito do INSS.
Perfil 4	Chefes de Assessoria de Comunicação Social nas Superintendências Regionais, Assessor de Comunicação Social (Administração Central), Diretor de Tecnologia da Informação e Inovação, Diretor de Gestão de Pessoas e Administração e Presidente do INSS.

II - nos casos de novos usuários de rede (LDAP), criados por meio de registro de chamado técnico, quando o solicitante não indicar o perfil de acesso à internet, será atribuído o Perfil 1;

III - para proceder a alteração do perfil de acesso, os usuários deverão preencher “Formulário de Acesso à Internet” (Anexo II) e providenciar a assinatura pelo Autorizador do acesso; e

IV - ao registrar a solicitação, deve-se anexar o Formulário de Solicitação de Acesso à Internet devidamente preenchido e assinado (pelo solicitante e Autorizador), conforme documento nato digital ou digitalizado no formato PDF.

Art. 8º A solicitação para perfis de acesso em caráter temporário devem indicar no Formulário de Solicitação de Acesso à Internet, a motivação da necessidade e a data de expiração do acesso.

Art. 9º Responsabilidades:

I - o usuário deve:

- a) preencher os requisitos e termos estabelecidos nesta norma;
- b) estar devidamente autorizado a utilizar a Internet nas formas estabelecidas nesta norma;
- c) fazer uso da Internet de forma responsável e segura, utilizando o acesso exclusivamente em razão de trabalho, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal; e
- d) impedir a divulgação e compartilhamento das chaves de segurança atribuídas, que são pessoais e intransferíveis.

II - o autorizador deve:

- a) conceder os perfis de acesso à internet rigorosamente de acordo com as atribuições dos usuários de sua abrangência, observando os normativos do INSS;
- b) verificar periodicamente o uso dos acessos concedidos e, sempre que necessário, solicitar alteração dos perfis de acesso dos usuários de sua abrangência; e
- c) reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à equipe de tratamento de incidentes de rede do INSS.

III - a área responsável pela gestão de TI no INSS deve: (IN 01/2020) e PORTARIA Nº 93.

- a) monitorar os acessos à internet e sua utilização de acordo com as diretrizes estabelecidas nesta norma; e
- b) identificar os casos de mau uso da Internet e adotar uma ou mais das seguintes providências:
 - 1. alertar ao usuário, responsável pelo acesso, e ao Autorizador, responsável pela concessão, acerca do uso indevido da internet;
 - 2. nos casos de reincidência, solicitar a revogação do acesso à internet concedido ao usuário; e
 - 3. encaminhar a documentação que comprova a má utilização do acesso concedido para Corregedoria do INSS, para análise e adoção das medidas cabíveis.

Art. 10º As seguintes práticas configuram-se como uso indevido da internet:

- I - acessar a internet disponibilizada pelo Instituto sem estar devidamente autorizado, conforme estabelecido nesta norma;
- II - não manifestar concordância com as regras estabelecidas nesta norma e nas demais aplicáveis;
- III - fazer uso dos recursos de Internet disponibilizado pelo Instituto para fins alheios ao trabalho, em discordância com os procedimentos dispostos nesta norma, sem prejuízo de demais normatizações vigentes na Administração Pública Federal;
- IV - utilizar os serviços extrapolando os privilégios do perfil de acesso que lhe foi designado;
- V - divulgação e compartilhamento das chaves de segurança, que são pessoais e intransferíveis, permitindo a utilização por terceiros do perfil que lhe foi atribuído;
- VI - praticar atos de comercialização de produtos e serviços, em proveito próprio ou de terceiros, que não atendam os interesses do INSS;
- VII - utilizar recursos ou dispositivos para acesso a computadores ou redes externas ao Instituto, com o objetivo de obter informações não autorizadas ou provocar a interrupção de serviços de rede;
- VIII - utilizar modem ou dispositivo de rede que interligue a rede interna do INSS a outras redes ou à Internet;
- IX - a exposição, o armazenamento, a distribuição, a edição, a gravação e o compartilhamento, através do uso dos recursos computacionais e de comunicação do INSS, de arquivos estranhos às atividades do Instituto e não autorizados pela chefia imediata;

X - realizar qualquer atividade que apoie ou facilite os vazamentos de dados;

XI - baixar arquivos ou programas da Internet que contrariem as diretrizes da Política de Segurança da Informação e Comunicações - POSIC POSIN vigente;
e (IN 01/2020)

XII - utilizar *proxy* não disponibilizado pelo INSS.

Art. 11 O acesso à Internet é passível de registro e monitoração, incluindo quaisquer dados transmitidos pela rede do INSS.

Art. 12 Disposições Gerais:

I - em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a ETIR deverá ser imediatamente acionada, para tomar as providências necessárias a fim de sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação do INSS;

II - as ocorrências de mau uso do acesso à internet não previstas nesta norma, assim como os casos de dúvidas em relação à aplicação das disposições aqui estabelecidas, devem ser encaminhadas à DTI para registro, análise e avaliação da necessidade de alterações de acordo com o processo de governança em vigência no Instituto;

III - o descumprimento desta norma, poderá acarretar ao usuário as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei, responsabilidade administrativa, civil e criminal; e

IV - esta norma deve ser atualizada periodicamente, não excedendo o prazo máximo de 3 anos.

SUGESTÃO DE ADEQUAÇÕES PARA A NCAL NO QUE COMPETE À GESTÃO DE PESSOAS E PROPOSTA DE NOVOS FLUXOS

Texto original na minuta da Norma de Controle de Acesso Lógico - NCAL no que compete a ações da Gestão de Pessoas:

"Art. 4º Base Cadastral:

(...) II - para tanto, a área responsável pela gestão de pessoas do INSS disponibilizará periodicamente as informações extraídas do Sistema Integrado de Administração de Recursos Humanos - SIAPE para a área responsável pela gestão de TIC do INSS (não ultrapassando o prazo de sete dias), contendo, minimamente, os seguintes dados: (...)

Art. 5º Credenciais e perfis de acesso:

(...) III - os servidores lotados nas áreas responsáveis pela gestão de pessoas do INSS deverão utilizar os canais de atendimento disponibilizados pela Dataprev, ou outro canal informado pela DTI, para:

- a) solicitar, se necessário, o credenciamento de usuários, contratados ou requisitados, para compor o quadro de servidores do INSS, após o ato da posse, e de estagiários, após assinatura do contrato de prestação de serviço, para acesso à rede;*
- b) solicitar a inativação imediata do perfil de acesso dos servidores cedidos a outros órgãos, inativos ou exonerados do quadro de servidores do INSS na data da publicação do ato;*
- c) solicitar suspensão imediata do perfil de acesso dos servidores afastados ou com licença programada de suas funções por mais de sessenta dias ininterruptos; e*
- d) solicitar a exclusão do acesso de estagiários cujo vínculo com o Instituto tenha sido encerrado, tão logo a rescisão do contrato tenha sido efetivada.*

(...) XV - Credenciamento de usuários externos:

b) (...) 2. ser atendidas somente após validação das credenciais do gestor solicitante do Instituto, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700) ou outra base de dados indicada pela área responsável pela gestão de pessoas, a qual contenha informações referentes à estrutura organizacional do Instituto.

(...)4. A emissão de credenciais de acesso poderá ser feita pelo gestor do contrato, representante legal do INSS, ou pelo gestor da unidade responsável pela gestão do contrato, convênio, acordo de cooperação técnica ou instrumento congênere e serão atendidas somente após validação das credenciais pelo solicitante, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700) ou outra base de dados indicada pela área responsável pela gestão de pessoas, a qual contenha informações referentes à estrutura organizacional do Instituto."

Sugestão de adequações de texto para a NCAL:

"Art. 4º Base Cadastral:

(...) II - para tanto, a área responsável pela gestão de pessoas do INSS disponibilizará periodicamente as informações extraídas do Sistema Integrado de Administração de Recursos Humanos - SIAPE para a Dataprev e a área responsável pela gestão de TIC do INSS (não ultrapassando o prazo de sete dias), contendo, minimamente, os seguintes dados: (...)

Art. 5º Credenciais e perfis de acesso:

(...) III - a área responsável pela gestão de pessoas do INSS deverá utilizar os canais de atendimento disponibilizados pela Dataprev, ou outro canal informado pela DTI, para:

- a) solicitar o credenciamento de usuários do quadro de pessoal do INSS na data do ato administrativo de retorno ou ingresso no órgão, para acesso à rede;*

b) *solicitar a revogação de credenciais de acesso de servidores do quadro de pessoal do INSS cedidos a outros órgãos;*

c) *solicitar a desativação de usuários do quadro de pessoal do INSS na data do ato administrativo ou de ocorrências que ensejem desligamento para fins de acesso lógico; e*

d) *solicitar suspensão imediata do perfil de acesso de usuários do quadro de pessoal em atividade do INSS afastados ou com licença programada de suas funções por mais de sessenta dias ininterruptos.*

(...) XV - Credenciamento de usuários externos:

c) *(...) 2. ser atendidas somente após validação das credenciais do gestor solicitante do Instituto, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700). (RETIRAR O TEXTO POSTERIOR)*

(...)4. A emissão de credenciais de acesso poderá ser feita pelo gestor do contrato, representante legal do INSS, ou pelo gestor da unidade responsável pela gestão do contrato, convênio, acordo de cooperação técnica ou instrumento congênere e serão atendidas somente após validação das credenciais pelo solicitante, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700).” (RETIRAR O TEXTO POSTERIOR)

Justificativa da sugestão de adequações de texto:

Relativamente ao **artigo 5º, inciso III**, quanto ao uso do termo mais genérico, a sugestão se dá por ser inviável o cumprimento nos termos atuais, devido principalmente à falta de pessoal nas unidades descentralizadas de gestão de pessoas para o registro tempestivo no SIAPE de atos administrativos que ensejam desligamento para fins de acesso lógico (rede e sistemas corporativos), portanto não também não há pessoal suficiente para a rotina de solicitações de credenciamento e desligamento de usuários junto à Dataprev.

Ainda, com a centralização das solicitações de credenciamento e credenciamento/revogação de usuários do quadro de pessoal do INSS conforme fluxo proposto a seguir, e com o povoamento das aplicações de gestão de acessos com as extrações semanais de dados de pessoal no SIAPE para atender ao art. 4º da minuta da NCAL, será imediatamente mitigada a validação de usuários que não mais possuem status de pessoal em atividade.

Relativamente ao texto sugerido para o **artigo 5º, inciso XV**, haja vista ser competência da Diretoria de Atendimento a atribuição de codificação numérica (OL) aos órgãos que compõem estrutura organizacional do INSS, a TB 0700 é a fonte de dados mais adequada, e ainda, por estarem registradas no SIAPE apenas os códigos de UORG dessas unidades, o controle relativo à estrutura extrapola a governança da Gestão de Pessoas.

Proposta de novo fluxo para informação de desligamentos para fins de acesso lógico:

Até saneamento da falta de pessoal nas unidades descentralizadas de gestão de pessoas para registro tempestivo no SIAPE dos atos administrativos e ocorrências que ensejam desligamento para fins de acesso lógico, e até a identificação de fluxo mais adequado, as unidades descentralizadas de gestão de pessoas encaminharão à Divisão de Gerenciamento e Produção de Informações - DGPI/CGGP/DGPA, na data do ato administrativo, o nome, a matrícula e tipo de ato administrativo do usuário a ser desligado.

Atos administrativos ou ocorrências que ensejam desligamento para fins de acesso lógico:

- Aposentadoria de servidor do quadro de pessoal do INSS;
- Exoneração ou demissão de servidor do quadro de pessoal do INSS;
- Exoneração de nomeado para cargo em comissão sem vínculo com o serviço público;

- Vacância por posse em cargo inacumulável;
- Retorno de servidor em exercício descentralizado de carreiras ao órgão de origem.
- Fim de contrato temporário;
- Retorno de servidor requisitado ao órgão de origem;
- Desligamento de estagiário;
- Cessão de servidor do quadro de pessoal do INSS - o desligamento para fins de acesso lógico só pode ser efetivado quando do início do exercício do servidor cedido no órgão de destino, que pode ter um prazo de até 30 dias. Não é viável revogar credencial de servidor cedido na data de publicação do ato administrativo para que o mesmo não fique impossibilitado de acessar a rede e sistemas corporativos para desempenhar as suas atividades no INSS enquanto não se apresentar no órgão de destino;
- Ocorrência de óbito - a ocorrência de óbito pode demorar mais de um dia para ser informada à unidade descentralizada de gestão de pessoas, porém a validação de usuários com sistema de registro de óbitos por ação da DTI junto à Dataprev irá sanar essa lacuna.

Procedimento junto à Dataprev:

A DGPI irá compilar as informações de desligamentos para fins de acesso lógico encaminhadas pelas unidades descentralizadas de gestão de pessoas e complementar os dados para apresentar diariamente, em layout pré-acordado, à Dataprev, por meio de upload em repositório GIS.

O upload do arquivo com a relação desses usuários irá gerar protocolo a ser encaminhado à DTI por email.

A relação de usuários para descredenciamento/revogação será informada diária e cumulativamente até o fechamento da folha de pagamento, para que a rotina de saneamento não prejudique as exclusões, já que as unidades descentralizadas de gestão de pessoas têm uma janela de aproximadamente 20 dias para registro das alterações funcionais no SIAPE, conforme cronograma mensal de fechamento da folha de pagamento.

Proposta de novo fluxo para solicitação de credenciamento de acesso de novos usuários:

As unidades descentralizadas de gestão de pessoas encaminharão à DGPI, na data do ato administrativo de ingresso no órgão, o nome e a matrícula do usuário a ser credenciado para fins de acesso lógico.

Relativamente aos estagiários, nos termos da minuta da NCAL, art. 5º, inciso XIV, alínea d, *"o acesso será concedido mediante solicitação expressa de servidor do quadro do INSS, responsável pela supervisão do estágio (...)"*, portanto, além da informação da data de início do contrato pela unidade descentralizada de gestão de pessoas, será necessária a ratificação pelo supervisor de estágio.

A DGPI irá compilar as informações para credenciamentos encaminhadas pelas unidades descentralizadas de gestão de pessoas e complementar os dados para informar diariamente à Dataprev por meio de ??? (upload em repositório GIS ou abertura de chamado via SDM/Dataprev - a definir).



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações

DESPACHO

Coordenação-Geral De Infraestrutura e Operações, em 06/07/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

A s s . : Minutas de
Normativos de Segurança
da Informação e
Comunicações.

1. Trata-se de processo para proposição de atos normativos para instituição de políticas e normas de segurança da informação e comunicações do Instituto Nacional do Seguro Social - INSS, de competência do Comitê Estratégico de Governança - CEGOV, conforme previsto no Art. 5 da Portaria nº 3.213/PRES/INSS/2019 (inciso VIII e parágrafo único).
2. Em atendimento as tratativas solicitadas no despacho CEGOV 0758185, o Serviço de Segurança em Tecnologia da Informação (SSEG) emitiu a Nota Técnica 3 (SEI 0829620) acerca das sugestões de alterações das normas e as novas minutas para aprovação pelo Comitê Estratégico de Governança - CEGOV (SEI 1075215, 1075264, 1075281 e 1075292).
3. Feitas as considerações, encaminhe-se ao Comitê Estratégico de Governança - CEGOV.

CLAUDIO AUGUSTO NOVAIS FERRAZ

Coordenador-Geral de Infraestrutura e Operações



Documento assinado eletronicamente por **Claudio Augusto Novais Ferraz, Coordenador(a) Geral**, em 06/07/2020, às 18:08, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1209308** e o código CRC **FFEAC188**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1209308



INSTITUTO NACIONAL DO SEGURO SOCIAL

Comitê Estratégico de Governança

DESPACHO

Comitê Estratégico de Governança, em 07/07/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Revisão de normas
de segurança da
informação.

1. Em resposta ao Despacho CGIN nº 1209308, diante da quantidade e do teor das mudanças realizadas nas normas de segurança da informação, após a sua apresentação inicial no âmbito do CEGOV (Reunião Ordinária nº 1/CEGOV/2020), solicita-se que os documentos sejam novamente discutidos e aprovados no Comitê Temático de Governança Digital (CTGD), para posterior encaminhamento ao CEGOV.

2. Ademais, informa-se que as "adequações necessárias para que as atribuições do Comitê de Segurança da Informação sejam desempenhadas pelo Comitê Temático de Gestão da Informação", propostas no item 8.4 da Nota Técnica nº 3 (0829620), não são compatíveis com as atribuições do Comitê Temático de Gestão da Informação do INSS (CTGI), conforme estabelecido na Portaria nº 3.213/PRES/INSS/2019.

3. A referida Portaria atribui ao CTGI, em linhas gerais, a discussão de assuntos relativos à transparência pública, à publicação de dados abertos e à categorização de dados das bases de negócio do INSS que podem ser compartilhadas com a sociedade e/ou com outros órgãos ou entidades da administração pública. A Portaria nº 3.213/PRES/INSS/2019 atribui expressamente ao CTGD a discussão de temas relativos à proposição de normas e planejamento de segurança da informação (vide Art. 4º do Anexo).

4. Cabe ainda destacar que o Comitê Estratégico de Governança (CEGOV) é a estrutura colegiada formalmente instituída para deliberar sobre temas afetos à governança digital e à segurança da informação, como transcrito abaixo:

Art.. 5º. Compete ao CEGOV:

....

Parágrafo único. Ao CEGOV cumpre deliberar em última instância, no âmbito do INSS, sobre os assuntos relativos à governança digital, de que trata o Decreto nº 8.638, de 15 de janeiro de 2016, e sobre os assuntos relativos à segurança da informação, de que trata o Decreto nº 9.637, de 26 de dezembro de 2018.

5. Ressalta-se que tanto o Decreto nº 8.638, de 15 de janeiro de 2016, quanto o Decreto nº 9.637, de 26 de dezembro de 2018, exigem que os integrantes dos comitês deliberativos sobre governança digital e segurança da informação sejam ocupantes do, no mínimo, cargo ou função comissionada de nível 5 ou superior. Por essa razão, cabe ao CEGOV deliberação sobre os temas. Os comitês temáticos de apoio

à governança são compostos por ocupantes de cargo ou função comissionada de nível 3 ou superior.

6. Na oportunidade, informa-se que a 6ª Reunião Ordinária do CEGOV está agendada para o dia 22/07/2020, das 15h às 17h, para deliberação sobre as normas de segurança da informação constantes deste processo.

7. Diante do exposto, restituam-se os autos à CGIN, e encaminhem-se também à DTI e ao CTGD, para conhecimento e providências.

CIBELLE CESAR DO AMARAL BRASIL

Secretária-Executiva do CEGOV
Coordenadora-Geral de Governança



Documento assinado eletronicamente por **CIBELLE CESAR DO AMARAL BRASIL**, **Coordenador(a) Geral**, em 07/07/2020, às 12:27, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1214131** e o código CRC **48FF7ED9**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1214131



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações

DESPACHO

Coordenação-Geral De Infraestrutura e Operações, em 08/07/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Revisão de normas
de segurança da
informação..

1. Trata-se da Despacho CEGOV (SEI 1222878) que refere-se as mudanças realizadas nas normas de segurança da informação.
2. Encaminha-se à SSEG para proceder com os ajustes necessários e retorna à esta CGIN.

CLAUDIO AUGUSTO NOVAIS FERRAZ

Coordenador-Geral de Infraestrutura e Operações



Documento assinado eletronicamente por **Claudio Augusto Novais Ferraz, Coordenador(a) Geral**, em 08/07/2020, às 11:42, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site
https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1222878** e o código CRC **118B829E**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1222878



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações
Coordenação De Suporte e Infraestrutura De Tecnologia da Informação e Comunicação
Serviço De Segurança em Tecnologia da Informação e Comunicação

DESPACHO

Serviço De Segurança em Tecnologia da Informação e Comunicação, em 08/07/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Revisão de normas
de segurança da
informação.

1. Trata-se de processo para proposição de atos normativos para instituição de políticas e normas de segurança da informação e comunicações do Instituto Nacional do Seguro Social - INSS, de competência do Comitê Estratégico de Governança - CEGOV, conforme previsto no Art. 5 da Portaria nº 3.213/PRES/INSS/2019 (inciso VIII e parágrafo único)
2. Retornam os autos para este Serviço de Segurança em Tecnologia da Informação e Comunicações - SSEG, para conhecimento e considerações referentes ao item 2 do Despacho exarado pelo CEGOV-INSS, em 07 de julho de 2020 (Documento SEI 1222878).
3. O Despacho emitido pelo CEGOV, aponta a incompatibilidade das atribuições do Comitê Temático de Gestão da Informação do INSS (CTGI), conforme estabelecido na Portaria nº 3.213/PRES/INSS/2019, com as definições contidas no item 8.4 da Nota Técnica nº 3 (0829620), de lavra deste SSEG, e informa que a Portaria nº 3.213/PRES/INSS/2019 atribui ao Comitê Temático de Governança Digital - CTGD, a discussão de temas relativos à proposição de normas e planejamento de segurança da informação.
4. Informo que este SSEG está de acordo com o posicionamento do CEGOV, e que a menção ao Comitê Temático de Gestão da Informação nas adequações indicadas na Nota Técnica SSEG Nº 3, foi feita equivocadamente. Sendo assim, onde se lê, no item 8.4, "*que as atribuições do Comitê de Segurança da Informação sejam desempenhadas pelo Comitê Temático de Gestão da Informação*", leia-se "*que as atribuições do Comitê de Segurança da Informação sejam desempenhadas pelo Comitê Temático de Governança Digital - CTGD*".
5. É válido lembrar que tal equívoco se refletiu na minuta de proposta da Política de Segurança da Informação - POSIN (1075215) do INSS. Sendo assim, as alterações necessárias foram procedidas no documento em tela e uma nova versão foi acostada aos autos (SEI 1227904).
6. Encaminhe-se, em devolução, à Coordenação-Geral de Infraestrutura e Suporte (CGIN), para conhecimento e encaminhamentos posteriores.

ROBERTO RUFINO DA COSTA

Chefe do Serviço de Segurança em Tecnologia da Informação e Comunicações Substituto



Documento assinado eletronicamente por **ROBERTO RUFINO DA COSTA, Chefe de Serviço Substituto(a)**, em 08/07/2020, às 18:41, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site

[https://sei.inss.gov.br/sei/controlador_externo.php?](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)

[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **1225291** e o código CRC **672C2737**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1225291



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 2/CEGOV/INSS, DE DE DE 2020

Atualiza a Política de Segurança da Informação e Comunicações do POSIC POSIN-INSS. (IN 01/2020) e PORTARIA Nº 93

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída no âmbito do INSS e nos termos do Anexo a esta Resolução, a Política de Segurança da Informação e Comunicações do POSIC POSIN-INSS (01/2020) e PORTARIA Nº 93.

Art. 2º Esta Resolução entra em vigor na data de sua publicação e seu Anexo será publicado em Boletim de Serviço.

Art. 3º Fica revogada a Resolução nº 672/PRES/INSS, de 27 de dezembro de 2018.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretora de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **ROBERTO RUFINO DA COSTA**, **Chefe de Serviço Substituto(a)**, em 08/07/2020, às 18:42, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1227904** e o código CRC **9D0C0611**.

ANEXO I

RESOLUÇÃO Nº 2/CEGOV/INSS, DE DE DE 2020

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO INSTITUTO NACIONAL DO SEGURO SOCIAL – POSIC POSIN-INSS (IN 01/2020) E PORTARIA Nº 93.

Art. 1º A Política de Segurança da Informação e Comunicações do Instituto Nacional do Seguro Social POSIC POSIN-INSS, tem por objetivo estabelecer e difundir diretrizes e princípios de Segurança da Informação e Comunicações – SI, com vistas à orientação para uso e proteção adequados das informações produzidas e custodiadas pelo Instituto, preservando sua disponibilidade, integridade, confidencialidade e autenticidade. (IN 01/2020) e PORTARIA Nº 93.

Parágrafo único. A Política de que trata o caput e suas normas complementares aplicam-se a todos os agentes públicos que têm vínculo direto e/ou indireto com o Instituto.

Art. 2º Para os efeitos da POSIC POSIN-INSS, entende-se: (IN 01/2020) e PORTARIA Nº 93.

I - agente público: Todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da APF, direta e indireta; (IN 1/2020)

II - atividade crítica - atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo; (IN 01/2020) Incluído

III - ativos de informação: meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV - dados processados: dados submetidos a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação; (IN 01/2020) e PORTARIA Nº 93.

V - gestor de Segurança da Informação e Comunicações: é o responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF. (IN 01/2020) e PORTARIA Nº 93.

VI - Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

VII - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

VIII - necessidade de conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais; (IN 01/2020) e PORTARIA Nº 93.

IX - riscos de segurança da informação e comunicações: potencial associado à exploração de uma ou mais vulnerabilidades nos ativos de informação, em razão de ameaças, com impacto negativo às atividades do Instituto; (IN 01/2020) e PORTARIA Nº 93.

X - segurança da informação e comunicações – SI: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e autenticidades das informações; (IN 01/2020) e PORTARIA Nº 93.

XI - vínculo direto: agentes públicos contratados diretamente pelo INSS;

XII - vínculo indireto: agentes privados ou públicos pertencentes a órgãos ou unidades da Administração Pública Federal, Estadual ou Municipal que mantenham contrato, convênio, acordo de cooperação técnica ou instrumento congênere com o INSS; e

Art. 3º Esta POSIC POSIN-INSS foi elaborada com base nos seguintes documentos: (IN 01/2020) e PORTARIA Nº 93.

I - Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;

II - Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto na Constituição Federal;

III - Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

IV - Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais;

V - Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

VI - Decreto nº 7.724, de 16 de maio de 2012, regulamenta a Lei nº 12.527, de 18 de novembro de 2011;

VII - Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

VIII - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

IX - Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

X - Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que disciplina a gestão de segurança da informação e comunicações na Administração Pública Federal, direta e indireta, e dá outras providências; (IN 01/2020) e PORTARIA Nº 93.

XI - Instruções normativas relacionadas à segurança da informação, publicadas pelo Gabinete de Segurança Institucional da Presidência da República;

XII - Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação; (incluído)

XIII - NBR ISO/IEC 27002:2013, que institui código de melhores práticas para a Gestão de Segurança da Informação;

Art. 4º Esta POSIC POSIN-INSS foi elaborada com base nos seguintes princípios: (IN 01/2020) e PORTARIA Nº 93.

I - a preservação da imagem do Instituto e de seus agentes públicos;

II - a salvaguarda das informações do cidadão;

III - ações de segurança orientadas pela gestão de riscos;

IV - continuidade assegurada dos serviços ao cidadão;

V - o alinhamento com a missão institucional e seu planejamento estratégico; e

VI - respeito à natureza e finalidade de cada área do Instituto.

Art. 5º São diretrizes gerais da **POSI** POSIN-INSS: **(IN 01/2020)** e PORTARIA Nº 93.

I - Tratamento da Informação:

- a) toda informação produzida pelos agentes públicos, no exercício de suas atividades, é de propriedade do INSS e deve ser protegida;
- b) informações produzidas, armazenadas e tratadas pelo Instituto, especialmente as informações pessoais e custodiadas, devem receber o devido tratamento para assegurar sua proteção durante todo o ciclo de vida; e
- c) somente os canais de comunicação disponibilizados pelo INSS devem ser utilizados para trafegar informações institucionais.

II - Tratamento de Incidentes de Segurança da Informação (SI): **(IN 01/2020)** e PORTARIA Nº 93.

- a) todo incidente de segurança da informação deve ser imediatamente relatado à área responsável pela gestão de segurança da informação de TI, observando-se a apropriada coleta de evidências. **(IN 01/2020)** e PORTARIA Nº 93.

III - Gestão de Riscos de Segurança:

- a) os riscos de segurança da informação devem ser identificados e tratados; e
- b) os critérios para a gestão de risco devem ser definidos e comunicados a toda instituição.

IV - Gestão de Continuidade:

- a) os ativos de informação que suportam as atividades críticas do Instituto devem ser suportados por ambiente de alta disponibilidade e ter capacidade de recuperação em prazos e condições previamente definidos para situações de contingência, em conformidade com o processo de continuidade; e
- b) a continuidade das operações e serviços de Tecnologia da Informação e Comunicações – TIC, deve estar prevista nos contratos, assim como os prazos e condições devem estar formalmente estabelecidos. **(IN 01/2020)** e PORTARIA Nº 93.

V - Controles de Acesso:

- a) todo acesso à informação deve ser motivado pela necessidade de conhecer;
- b) os sistemas de informação e as instalações físicas devem ter capacidade de controlar os acessos, com fins de responsabilização pelo seu uso; e
- c) as autorizações de acesso às informações, sistemas e instalações físicas devem ter critérios de acesso definidos e divulgados a todos da instituição.

VI - Recursos Computacionais:

a) correio eletrônico:

- 1. o correio eletrônico, *e-mail*, é uma forma de comunicação oficial e deve ser utilizado exclusivamente no desempenho das atividades funcionais; e
- 2. ao produzir, responder ou encaminhar mensagem em caixa de correio eletrônico institucional, o servidor deverá se identificar, subscrevendo, ao menos, seu nome, cargo e telefone de contato institucional.

b) Acesso à Internet:

- 1. o acesso à Internet, por meio da rede de dados do INSS, é uma concessão e deve ter seu uso orientado para a execução das atividades do Instituto; e
- 2. os acessos serão liberados de acordo com perfis previamente definidos pelo órgão responsável pelos serviços de TI. **(IN 01/2020)**

c) Gestão de Mudanças de TI: **(IN 01/2020)** e PORTARIA Nº 93.

- 1. toda mudança nos sistemas de informação do INSS deve ser previamente e formalmente autorizada; e
- 2. a gestão de mudanças deve prever, no mínimo, a guarda dos registros, realização de testes e a possibilidade de recuperação do ambiente.

d) Computação em Nuvem **(IN 01/2020)** (incluído)

1. o ambiente de computação em nuvem, sua infraestrutura e canal de comunicação devem estar aderentes às diretrizes e normas de SI estabelecidas pelo instituto, e às legislações vigentes;(incluído)

2. o contrato de prestação de serviço, quando for o caso, deverá conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço;(incluído)

VII - Educação e Conscientização:

a) esta Política e seus normativos complementares devem ser periodicamente divulgados a todos os agentes públicos do Instituto;

b) o Instituto deve manter programa contínuo de conscientização dos agentes públicos em Segurança da Informação ~~e Comunicações~~ – SI; e (IN 01/2020) e PORTARIA Nº 93;

c) deve ser mantido plano de capacitação especializado aos profissionais que atuam na gestão de SI;(IN 01/2020) e PORTARIA Nº 93.

VIII - Auditoria e Conformidade:

a) o cumprimento desta Política e de suas normas complementares deve ser avaliado periodicamente, por meio de verificações de conformidade; e

b) o uso dos recursos de TI disponibilizados pelo Instituto é passível de monitoramento e auditoria.(IN 01/2020) e PORTARIA Nº 93.

IX - Responsabilidade pela gestão das informações:

a) Os responsáveis pela gestão dos ativos da informação e sistemas corporativos devem descrever os requisitos de segurança;

b) Os sistemas de informação devem ser concebidos possibilitando a segregação de funções. (o parecer da PFE indicou que este item estava incompleto. Adicionamos sugestão de texto que aborda o princípio da segregação de funções (tema citado na Recomendação nº 12 do Relatório de Auditoria da CGU. Na minuta da PCAL será incluso o conceito de proprietário da informação e as responsabilidades do mesmo.)

X - Segurança física e do ambiente;(IN 01/2020)

a) As instalações em que as informações críticas ou sensíveis serão processadas deverão ser mantidas em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção física;(incluído)

b) Os ativos da organização devem ser protegidos contra acesso físico não autorizado, danos, perdas, furto e interferência. As proteções devem estar alinhadas aos riscos identificados;(incluído)

XI - Gestão de ativos da informação;(IN 01/2020)

a) os ativos de informação devem;(incluído)

I

1. ser inventariados e protegidos;(incluído)

2. ter identificados os seus proprietários e custodiantes;(incluído)

3. ter a sua entrada e saída nas dependências do Instituto autorizadas e registradas por autoridade competente;(incluído)

4. ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins;(incluído)

Parágrafo único. O Comitê Temático de Gestão da Informação é responsável pela aprovação de procedimentos e de normas internas que orientem o compartilhamento de dados sob gestão do INSS e pela aprovação da categorização dos níveis de compartilhamento de dados com outras entidades públicas (federais ou de outras esferas e poderes) da sociedade civil (Vide atribuições do CTGI, no Art. 6º do Anexo da Portaria nº 3.213/PRES/INSS/2019). (Reposicionado para o artigo 7º)

Art. 6º A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas, cíveis e penais, previstas na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), no Código Penal, no Código Civil, e, ainda, em legislação que regule ou venha regular a matéria.

Art. 7º Competências e Responsabilidades:

I - Cabe ao Gestor de Segurança da Informação ~~e Comunicações~~;(IN 01/2020) e PORTARIA Nº 93.

a) promover cultura de segurança da informação ~~e comunicações~~;(IN 01/2020) e PORTARIA Nº 93.

b) acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

c) propor os recursos necessários à implementação das ações de SI;(IN 01/2020)

d) coordenar o CSIE ou estrutura equivalente ; e (IN 01/2020) e PORTARIA Nº 93.

e) acompanhar os trabalhos e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR do INSS (IN 01/2020)

f) propor o detalhamento das diretrizes desta Política, por meio de normas e procedimentos, e acompanhar sua implementação.

g) assessorar a alta administração na implementação da Política de Segurança da Informação; (IN 01/2020)

h) estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação; (IN 01/2020)

i) promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no INSS; (IN 01/2020)

j) incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação; (IN 01/2020)

k) verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação; (IN 01/2020)

l) acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e (IN 01/2020)

m) manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação. (IN 01/2020)

II - Cabe ao Presidente do Instituto nomear o Gestor de SI; (IN 01/2020) e PORTARIA Nº 93.

III - Caso o Gestor de SI não seja nomeado, as atribuições relacionadas no art. 7º inciso I serão desempenhadas pelo Diretor de Tecnologia da Informação e Inovação; (IN 01/2020) e PORTARIA Nº 93.

IV - A ETIR-INSS deve analisar e propor respostas a notificações e atividades relacionadas a incidentes de SI, no âmbito do Instituto; e (IN 01/2020) e PORTARIA Nº 93.

V - É responsabilidade de todos os agentes públicos, diretos e indiretos, conhecer e cumprir as diretrizes desta Política e demais normas e procedimentos complementares de SI. (IN 01/2020) e PORTARIA Nº 93.

VI - Tendo em vista a Política de Governança do INSS as atribuições contidas no Art. 20 da Instrução Normativa Nº 1, DE 27 DE MAIO DE 2020, no âmbito do Instituto serão desempenhadas pelo Comitê Temático de Governança Digital. (IN 01/2020)

Parágrafo único. O Comitê Temático de Gestão da Informação é responsável pela aprovação de procedimentos e de normas internas que orientem o compartilhamento de dados sob gestão do INSS e pela aprovação da categorização dos níveis de compartilhamento de dados com outras entidades públicas (federais ou de outras esferas e poderes) da sociedade civil (Vide atribuições do CTGI, no Art. 6º do Anexo da Portaria nº 3.213/PRES/INSS/2019). (remanejado do artigo 6º)

Art. 8º Esta Política e seus normativos devem ~~deve ser revisada~~ ser revisados sempre que necessário, não excedendo o período máximo de três anos. (incluído)



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações

DESPACHO

Coordenação-Geral De Infraestrutura e Operações, em 08/07/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Revisão de normas
de segurança da
informação.

1. Trata-se da Despacho CEGOV (SEI 1222878) que refere-se as mudanças realizadas nas normas de segurança da informação.
2. Os ajustes apontados no referido Despacho foram considerados no texto da Minuta de Resolução SSEG (SEI 1227904) e na Nota Técnica conforme o Despacho SSEG (SEI 1225291).
3. Feitas as considerações, encaminhe-se ao Comitê Temático de Governança Digital - CTGD para análise das mudanças propostas nos normativos.

CLAUDIO AUGUSTO NOVAIS FERRAZ

Coordenador-Geral de Infraestrutura e Operações



Documento assinado eletronicamente por **Claudio Augusto Novais Ferraz, Coordenador(a) Geral**, em 08/07/2020, às 19:00, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1228286** e o código CRC **29D7B965**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

DESPACHO

Diretoria De Tecnologia da Informação e Inovação, em 10/07/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Revisão de normas
de segurança da
informação.

1. Trata-se de processo sobre tratativas em relação à revisão de normas de segurança da informação.
2. Após a reunião do CTGD para tratar do tema, ocorrida na data de hoje, encaminhe-se ao Serviço de Segurança em TIC, com trâmite pela CGIN, para adequação das minutas e encaminhamento ao Comitê Temático.

FLÁVIO FERREIRA DOS SANTOS

Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **FLAVIO FERREIRA DOS SANTOS, Diretor(a) de Tecnologia da Informação e Inovação**, em 10/07/2020, às 17:20, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1244356** e o código CRC **A26CD8D0**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1244356



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações
Coordenação De Suporte e Infraestrutura De Tecnologia da Informação e Comunicação
Serviço De Segurança em Tecnologia da Informação e Comunicação

DESPACHO

Serviço De Segurança em Tecnologia da Informação e Comunicação, em 16/07/2020.

Ref.: Processo nº 35014.047735/2020-84

Int.: DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO

A s s . : Revisão e proposição de normas de segurança da informação.

1. Trata-se de processo sobre tratativas em relação à revisão e proposição de normas de segurança da informação.
2. Retornam os autos para este Serviço de Segurança em Tecnologia da Informação e Comunicações - SSEG, após análise das alterações efetuadas nas minutas dos normativos, conforme relatado na Nota Técnica nº 3 (documento SEI 0829620), pelo Comitê Temático de Governança Digital - CTGD, para adequação das minutas.
3. Sendo assim, foram procedidas as seguintes alterações na documentação sob análise:
 - a) redação do Inciso VI do Art. 7º da minuta da Política de Segurança da Informação - POSIN-INSS;
 - b) substituição do termo "exclusão" por "desativação" na alínea "d", inciso III do Art. 5º da minuta de proposta da Norma de Controle de Acesso - NCAL;
 - c) atualização da nomenclatura da Ouvidoria Geral da Previdência Social - OUGPS, que passa a constar como Ouvidoria do Ministério da Economia na alínea "e", inciso XV do Art. 7º da NCAL;
 - d) exclusão de menção à "Dataprev" do texto contido na alínea "f", inciso XIV do Art. 5º da NCAL;
 - e) redação dos incisos V e VI do Art. 4º, da proposta de minuta que institui a Equipe de Tratamento de Incidentes de Redes Computacionais - ETIR-INSS, acerca do processo de nomeação do coordenador da equipe;
 - f) formatação de destaque nos textos dos tópicos que sofreram alterações na minuta proposta de norma que disciplina o uso da Internet (alínea "d", inciso II do Art. 4º e inciso I do Art. 4º)
4. Feitas as considerações necessárias, encaminhe-se, em devolução ao Comitê Temático de Governança Digital - CTGD, com trâmite pela Coordenação-Geral de Infraestrutura e Suporte - CGIN,

para conhecimento.

ALEXINALDO MESSIAS CERQUEIRA

Chefe do Serviço de Segurança em Tecnologia da Informação e Comunicação



Documento assinado eletronicamente por **ALEXINALDO MESSIAS CERQUEIRA, Chefe de Serviço**, em 16/07/2020, às 10:48, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1249313** e o código CRC **09ABD8EB**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1249313



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 2/CEGOV/INSS, DE DE DE 2020

Atualiza a Política de Segurança da Informação e Comunicações do POSIC POSIN-INSS. (IN 01/2020) e PORTARIA Nº 93

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída no âmbito do INSS e nos termos do Anexo a esta Resolução, a Política de Segurança da Informação e Comunicações do POSIC POSIN-INSS (01/2020) e PORTARIA Nº 93.

Art. 2º Esta Resolução entra em vigor na data de sua publicação e seu Anexo será publicado em Boletim de Serviço.

Art. 3º Fica revogada a Resolução nº 672/PRES/INSS, de 27 de dezembro de 2018.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretora de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por ALEXINALDO MESSIAS CERQUEIRA, Chefe de Serviço, em 16/07/2020, às 10:49, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador 1249859 e o código CRC E40DB47D.

ANEXO I

RESOLUÇÃO Nº 2/CEGOV/INSS, DE DE DE 2020

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO INSTITUTO NACIONAL DO SEGURO SOCIAL – POSIC POSIN-INSS (IN 01/2020) E PORTARIA Nº 93.

Art. 1º A Política de Segurança da Informação e Comunicações do Instituto Nacional do Seguro Social POSIC POSIN-INSS, tem por objetivo estabelecer e difundir diretrizes e princípios de Segurança da Informação e Comunicações – SI, com vistas à orientação para uso e proteção adequados das informações produzidas e custodiadas pelo Instituto, preservando sua disponibilidade, integridade, confidencialidade e autenticidade. (IN 01/2020) e PORTARIA Nº 93.

Parágrafo único. A Política de que trata o caput e suas normas complementares aplicam-se a todos os agentes públicos que têm vínculo direto e/ou indireto com o Instituto.

Art. 2º Para os efeitos da POSIC POSIN-INSS, entende-se: (IN 01/2020) e PORTARIA Nº 93.

I - agente público: Todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da APF, direta e indireta; (IN 1/2020)

II - atividade crítica - atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo; (IN 01/2020) Incluído

III - ativos de informação: meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV - dados processados: dados submetidos a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação; (IN 01/2020) e PORTARIA Nº 93.

V - gestor de Segurança da Informação e Comunicações: é o responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF. (IN 01/2020) e PORTARIA Nº 93.

VI - Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

VII - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

VIII - necessidade de conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais; (IN 01/2020) e PORTARIA Nº 93.

IX - riscos de segurança da informação e comunicações: potencial associado à exploração de uma ou mais vulnerabilidades nos ativos de informação, em razão de ameaças, com impacto negativo às atividades do Instituto; (IN 01/2020) e PORTARIA Nº 93.

X - segurança da informação e comunicações – SI: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e autenticidades das informações; (IN 01/2020) e PORTARIA Nº 93.

XI - vínculo direto: agentes públicos contratados diretamente pelo INSS;

XII - vínculo indireto: agentes privados ou públicos pertencentes a órgãos ou unidades da Administração Pública Federal, Estadual ou Municipal que mantenham contrato, convênio, acordo de cooperação técnica ou instrumento congênere com o INSS; e

Art. 3º Esta POSIC POSIN-INSS foi elaborada com base nos seguintes documentos: (IN 01/2020) e PORTARIA Nº 93.

I - Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;

II - Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto na Constituição Federal;

III - Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

IV - Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais;

V - Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

VI - Decreto nº 7.724, de 16 de maio de 2012, regulamenta a Lei nº 12.527, de 18 de novembro de 2011;

VII - Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

VIII - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

IX - Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

X - Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que disciplina a gestão de segurança da informação e comunicações na Administração Pública Federal, direta e indireta, e dá outras providências; (IN 01/2020) e PORTARIA Nº 93.

XI - Instruções normativas relacionadas à segurança da informação, publicadas pelo Gabinete de Segurança Institucional da Presidência da República;

XII - Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação; (incluído)

XIII - NBR ISO/IEC 27002:2013, que institui código de melhores práticas para a Gestão de Segurança da Informação;

Art. 4º Esta POSIC POSIN-INSS foi elaborada com base nos seguintes princípios: (IN 01/2020) e PORTARIA Nº 93.

I - a preservação da imagem do Instituto e de seus agentes públicos;

II - a salvaguarda das informações do cidadão;

III - ações de segurança orientadas pela gestão de riscos;

IV - continuidade assegurada dos serviços ao cidadão;

V - o alinhamento com a missão institucional e seu planejamento estratégico; e

VI - respeito à natureza e finalidade de cada área do Instituto.

Art. 5º São diretrizes gerais da **POSI** POSIN-INSS: **(IN 01/2020)** e PORTARIA Nº 93.

I - Tratamento da Informação:

- a) toda informação produzida pelos agentes públicos, no exercício de suas atividades, é de propriedade do INSS e deve ser protegida;
- b) informações produzidas, armazenadas e tratadas pelo Instituto, especialmente as informações pessoais e custodiadas, devem receber o devido tratamento para assegurar sua proteção durante todo o ciclo de vida; e
- c) somente os canais de comunicação disponibilizados pelo INSS devem ser utilizados para trafegar informações institucionais.

II - Tratamento de Incidentes de Segurança da Informação (SI): **(IN 01/2020)** e PORTARIA Nº 93.

- a) todo incidente de segurança da informação deve ser imediatamente relatado à área responsável pela gestão de segurança da informação de TI, observando-se a apropriada coleta de evidências. **(IN 01/2020)** e PORTARIA Nº 93.

III - Gestão de Riscos de Segurança:

- a) os riscos de segurança da informação devem ser identificados e tratados; e
- b) os critérios para a gestão de risco devem ser definidos e comunicados a toda instituição.

IV - Gestão de Continuidade:

- a) os ativos de informação que suportam as atividades críticas do Instituto devem ser suportados por ambiente de alta disponibilidade e ter capacidade de recuperação em prazos e condições previamente definidos para situações de contingência, em conformidade com o processo de continuidade; e
- b) a continuidade das operações e serviços de Tecnologia da Informação e Comunicações – TIC, deve estar prevista nos contratos, assim como os prazos e condições devem estar formalmente estabelecidos. **(IN 01/2020)** e PORTARIA Nº 93.

V - Controles de Acesso:

- a) todo acesso à informação deve ser motivado pela necessidade de conhecer;
- b) os sistemas de informação e as instalações físicas devem ter capacidade de controlar os acessos, com fins de responsabilização pelo seu uso; e
- c) as autorizações de acesso às informações, sistemas e instalações físicas devem ter critérios de acesso definidos e divulgados a todos da instituição.

VI - Recursos Computacionais:

a) correio eletrônico:

- 1. o correio eletrônico, *e-mail*, é uma forma de comunicação oficial e deve ser utilizado exclusivamente no desempenho das atividades funcionais; e
- 2. ao produzir, responder ou encaminhar mensagem em caixa de correio eletrônico institucional, o servidor deverá se identificar, subscrevendo, ao menos, seu nome, cargo e telefone de contato institucional.

b) Acesso à Internet:

- 1. o acesso à Internet, por meio da rede de dados do INSS, é uma concessão e deve ter seu uso orientado para a execução das atividades do Instituto; e
- 2. os acessos serão liberados de acordo com perfis previamente definidos pelo órgão responsável pelos serviços de TI. **(IN 01/2020)**

c) Gestão de Mudanças de TI: **(IN 01/2020)** e PORTARIA Nº 93.

- 1. toda mudança nos sistemas de informação do INSS deve ser previamente e formalmente autorizada; e
- 2. a gestão de mudanças deve prever, no mínimo, a guarda dos registros, realização de testes e a possibilidade de recuperação do ambiente.

d) Computação em Nuvem **(IN 01/2020)** (incluído)

1. o ambiente de computação em nuvem, sua infraestrutura e canal de comunicação devem estar aderentes às diretrizes e normas de SI estabelecidas pelo instituto, e às legislações vigentes;(incluído)

2. o contrato de prestação de serviço, quando for o caso, deverá conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço;(incluído)

VII - Educação e Conscientização:

a) esta Política e seus normativos complementares devem ser periodicamente divulgados a todos os agentes públicos do Instituto;

b) o Instituto deve manter programa contínuo de conscientização dos agentes públicos em Segurança da Informação ~~e Comunicações~~ – SI; e (IN 01/2020) e PORTARIA Nº 93;

c) deve ser mantido plano de capacitação especializado aos profissionais que atuam na gestão de SI;(IN 01/2020) e PORTARIA Nº 93.

VIII - Auditoria e Conformidade:

a) o cumprimento desta Política e de suas normas complementares deve ser avaliado periodicamente, por meio de verificações de conformidade; e

b) o uso dos recursos de TI disponibilizados pelo Instituto é passível de monitoramento e auditoria.(IN 01/2020) e PORTARIA Nº 93.

IX - Responsabilidade pela gestão das informações:

a) Os responsáveis pela gestão dos ativos da informação e sistemas corporativos devem descrever os requisitos de segurança;

b) Os sistemas de informação devem ser concebidos possibilitando a segregação de funções. (o parecer da PFE indicou que este item estava incompleto. Adicionamos sugestão de texto que aborda o princípio da segregação de funções (tema citado na Recomendação nº 12 do Relatório de Auditoria da CGU. Na minuta da PCAL será incluso o conceito de proprietário da informação e as responsabilidades do mesmo.)

X - Segurança física e do ambiente;(IN 01/2020)

a) As instalações em que as informações críticas ou sensíveis serão processadas deverão ser mantidas em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção física;(incluído)

b) Os ativos da organização devem ser protegidos contra acesso físico não autorizado, danos, perdas, furto e interferência. As proteções devem estar alinhadas aos riscos identificados;(incluído)

XI - Gestão de ativos da informação;(IN 01/2020)

a) os ativos de informação devem;(incluído)

I

1. ser inventariados e protegidos;(incluído)

2. ter identificados os seus proprietários e custodiantes;(incluído)

3. ter a sua entrada e saída nas dependências do Instituto autorizadas e registradas por autoridade competente;(incluído)

4. ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins;(incluído)

Parágrafo único. O Comitê Temático de Gestão da Informação é responsável pela aprovação de procedimentos e de normas internas que orientem o compartilhamento de dados sob gestão do INSS e pela aprovação da categorização dos níveis de compartilhamento de dados com outras entidades públicas (federais ou de outras esferas e poderes) da sociedade civil (Vide atribuições do CTGI, no Art. 6º do Anexo da Portaria nº 3.213/PRES/INSS/2019). (Reposicionado para o artigo 7º)

Art. 6º A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas, cíveis e penais, previstas na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), no Código Penal, no Código Civil, e, ainda, em legislação que regule ou venha regular a matéria.

Art. 7º Competências e Responsabilidades:

I - Cabe ao Gestor de Segurança da Informação ~~e Comunicações~~;(IN 01/2020) e PORTARIA Nº 93.

a) promover cultura de segurança da informação ~~e comunicações~~;(IN 01/2020) e PORTARIA Nº 93.

b) acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

c) propor os recursos necessários à implementação das ações de SI;(IN 01/2020)

d) coordenar o CSIE ou estrutura equivalente ; e (IN 01/2020) e PORTARIA Nº 93.

e) acompanhar os trabalhos e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR do INSS (IN 01/2020)

f) propor o detalhamento das diretrizes desta Política, por meio de normas e procedimentos, e acompanhar sua implementação.

g) assessorar a alta administração na implementação da Política de Segurança da Informação; (IN 01/2020)

h) estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação; (IN 01/2020)

i) promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no INSS; (IN 01/2020)

j) incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação; (IN 01/2020)

k) verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação; (IN 01/2020)

l) acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e (IN 01/2020)

m) manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação. (IN 01/2020)

II - Cabe ao Presidente do Instituto nomear o Gestor de SI; (IN 01/2020) e PORTARIA Nº 93.

III - Caso o Gestor de SI não seja nomeado, as atribuições relacionadas no art. 7º inciso I serão desempenhadas pelo Diretor de Tecnologia da Informação e Inovação; (IN 01/2020) e PORTARIA Nº 93.

IV - A ETIR-INSS deve analisar e propor respostas a notificações e atividades relacionadas a incidentes de SI, no âmbito do Instituto; e (IN 01/2020) e PORTARIA Nº 93.

V - É responsabilidade de todos os agentes públicos, diretos e indiretos, conhecer e cumprir as diretrizes desta Política e demais normas e procedimentos complementares de SI. (IN 01/2020) e PORTARIA Nº 93.

VI - Tendo em vista o Sistema de Governança do INSS, instituído pela Portaria nº 3.213/PRES/INSS/2019, compete ao Comitê Estratégico de Governança - CEGOV - deliberar sobre políticas e normas de segurança da informação, assessorado pelo Comitê Temático de Governança Digital. (Redação sugerida pela Diretoria de Governança, conforme reunião CTDG de 10/07/2020)

Parágrafo único. O Comitê Temático de Gestão da Informação é responsável pela aprovação de procedimentos e de normas internas que orientem o compartilhamento de dados sob gestão do INSS e pela aprovação da categorização dos níveis de compartilhamento de dados com outras entidades públicas (federais ou de outras esferas e poderes) da sociedade civil (Vide atribuições do CTGI, no Art. 6º do Anexo da Portaria nº 3.213/PRES/INSS/2019). (remanejado do artigo 6º)

Art. 8º Esta Política e seus normativos ~~devem-deve ser revisada-revisados~~ sempre que necessário, não excedendo o período máximo de três anos. (incluído)



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 3/CEGOV/INSS, DE DE DE 2020

Define regras para a emissão de credenciais de acesso lógico no âmbito do INSS

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída a Norma de Controle de Acesso Lógico - NCAL, do Instituto Nacional do Seguro Social – INSS.

Art. 2º Esta Resolução, bem como seus anexos, serão publicados em Boletim de Serviço, nos termos do Inciso I do Art. 16, da Resolução n.708/INSS/PRES, de 6 de novembro de 2019.

Art. 3º Revogar a RESOLUÇÃO Nº 413/PRES/INSS, DE 20 DE MAIO DE 2014.

Art. 4º Esta Resolução entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretora de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por ALEXINALDO MESSIAS CERQUEIRA, Chefe de Serviço, em 16/07/2020, às 10:50, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador 1249899 e o código CRC A51EC5EB.

ANEXO I

RESOLUÇÃO Nº 3/CEGOV/INSS, DE DE DE 2020

NORMA DE CONTROLE DE ACESSO LÓGICO – INSS

Art. 1º Os termos definidos nesta norma aplicam-se a todos os agentes públicos e privados com vínculo direto ou indireto, permanente ou temporário com o INSS.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União – AGU que atuarem na consultoria e no assessoramento jurídico, e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta Norma de Controle de Acesso Lógico são estabelecidos os seguintes conceitos e definições:

I - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

II - administrador de Domínio: Usuário responsável pela administração de um domínio por meio da aplicação de políticas globais, criação, edição e exclusão de usuários e grupos, e instalação de programas em um grande número de estações de trabalho;

III - administrador Local: Usuário responsável pela administração de partes de um domínio (geralmente restrito a um setor ou abrangência), por meio de políticas locais, edição de grupos e usuários locais, e instalação de programas em estações de trabalho limitadas a um setor ou abrangência;

IV - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta; (conceito ajustado de

V - ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VI - contas de serviço: contas de acesso à rede corporativa de computadores, necessárias para a execução de procedimentos automáticos (aplicação, script, etc) sem qualquer intervenção humana no seu uso;

VII - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso **ao uso de recursos físicos ou computacionais**; **(IN 01/2020) e PORTARIA Nº 93 (incluído)**

VIII - credenciamento: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer;

IX - credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física, como crachá, cartão e selo ou lógica como identificação usuário e senha;

X - dado: Sugestão de Alteração "O dado é um elemento informativo concreto e sua forma plural expressa uma informação" é o registro do atributo de um ente objeto ou fenômeno onde registro indica o ato de registrar, ou seja, é a gravação ou a impressão de caracteres ou símbolos que tenham um significado em algum documento ou suporte físico;

XI - domínio: agrupamento lógico de computadores em rede que compartilham recursos em um banco de dados de segurança, comum, onde a administração e autenticação são centralizadas. Desta forma um usuário precisa de uma conta para ter acesso ao domínio e aos recursos compartilhados;

XII - endereço IP: **sigla em inglês para Internet Protocol. Trata-se de endereço lógico que identifica a localização de determinado ativo na rede; conjunto de elementos numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores. Sequência de números associada a cada computador conectado à Internet. No caso de IPv4, o endereço IP é dividido em quatro grupos, separados por "." e compostos por números entre 0 e 255. No caso de IPv6, o endereço IP é dividido em até oito grupos, separados por ":" e compostos por números hexadecimais (números e letras de "A" a "F") entre 0 e FFFF; (IN 01/2020) e PORTARIA Nº 93. Substituir**

XIII - entidade externa: Organização governamental, não governamental ou privada amparada por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica ou instrumento congênere com o INSS;

XIV - e-SIC: Sistema Eletrônico do Serviço de Informações ao Cidadão, aplicação disponibilizada na internet, que centraliza todos os pedidos de informações dirigidos ao Poder Executivo Federal;

XV - estagiário: educando que esteja frequentando o ensino regular, em instituições de educação superior, de educação profissional, de ensino médio, de educação especial e dos anos finais do ensino fundamental, na modalidade profissional da educação de jovens e adultos, que desenvolve as atividades relacionadas à sua área de formação profissional junto as pessoas Jurídicas de Direito Privado, órgãos da Administração Pública e Instituições de Ensino, que tenham condições de proporcionar experiência prática na sua linha de formação;

XVI - estágio Supervisionado: ato educativo escolar supervisionado, desenvolvido no ambiente de trabalho, que visa a preparação para o trabalho produtivo de educandos;

XVII - ferramenta de gestão de acessos: Software que possibilita a gestão integrada de papéis e permissões de acesso dos usuários nos sistemas corporativos;

XVIII - gestor da informação: usuário que gerou a informação, que responde pelo seu conteúdo ou que foi formalmente designado para definir, alterar a sua classificação nos graus de sigilo e perfil de acesso dos demais usuários e processos;

XIX - gestão de identidades: Combinação de sistemas técnicos, regras e procedimentos que definem a posse, utilização e segurança de uma identidade. Seu objetivo primário é estabelecer a confiança na associação de atributos a uma identidade digital e conectar esta identidade com uma entidade individual;

XX - Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXI - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

XXII - Log ou Registro de Auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional; (IN 01/2020) e PORTARIA Nº 93. (incluído)

XXIII - necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação; condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais; (IN 01/2020) e PORTARIA Nº 93

XXIV - perfil de Acesso do Usuário: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

XXV - recursos de rede: Dispositivos (impressoras, scanners, multifuncionais, etc) ou serviços (sistemas, portais, etc) disponibilizados para os usuários por meio de uma rede de dados;

XXVI - serviço de diretório: serviço que armazena e organiza informações relativas a recursos disponíveis e usuários de uma rede de dados. Permite que o administrador da rede gerencie o acesso de usuários e sistemas aos recursos disponíveis;

XXVII - sistemas corporativos: sistemas de operação, ou finalísticos, que se coadunam com os fins da Previdência Social. Assim, entende-se que este conceito comporta o conjunto de sistemas e subsistemas que garantem a operação dos regimes geral e próprio de previdência social, inclusive de previdência complementar;

XXVIII - sistemas legados: compreendem o conjunto de aplicações desenvolvidas com tecnologias obsoletas que permanecem em operação no INSS;

XXIX - usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal-APF, formalizada por meio da assinatura do Termo de Responsabilidade;

XXX - usuário interno: servidor do quadro do INSS lotado em uma Unidade Orgânica – UO, que se utiliza dos sistemas corporativos do Instituto;

XXXI - usuário externo: usuários vinculados a uma Entidade Externa, que se utiliza dos sistemas corporativos do Instituto por meio de um perfil de acesso concedido por um Gestor de Acesso Externo;

Art. 3º São diretrizes desta NCAL-INSS:

I - o acesso à rede e aos sistemas corporativos do INSS dar-se-á por meio de autenticação integrada de domínio baseado em serviço de diretório, administrado por meio de uma ferramenta de gestão de identidades;

II - as concessões de acesso à rede de dados e aos sistemas corporativos são distintas. Sendo assim, o usuário pode obter permissão de acesso apenas à rede de dados, ou apenas a determinado(s) sistema(s) corporativo(s);

III - as credenciais de acesso a rede de dados e aos sistemas corporativos do INSS são conferidas aos usuários com base na necessidade de conhecer, para viabilizar o exercício de suas atribuições funcionais e atividades a serem desenvolvidas no âmbito do INSS; e

IV - o uso indevido de informações dos sistemas corporativos do INSS sujeitará o agente às penalidades previstas na legislação.

Art. 4º Base Cadastral:

I - as bases de dados do Serviço de Diretórios (acesso à rede de dados), do Sistema de Gestão de Acessos (sistemas corporativos) e sistemas legados devem ser alimentadas por informações disponibilizadas pelo INSS;

II - para tanto, a área responsável pela gestão de pessoas do INSS disponibilizará semanalmente as informações extraídas do Sistema Integrado de Administração de Recursos Humanos – SIAPE para a empresa prestadora de serviços tecnológicos contratada pelo Instituto, com a supervisão da área de gestão de TI e do INSS, contendo, minimamente, os seguintes dados: **Recomendação 3**

Tabela 1: Informações Usuários

Item	Informação	Campo	Descrição
1	GR-MATRICULA	N 0012	GRUPO NUMÉRICO COMPOSTO DE NÚMERO DO ÓRGÃO (N0005) E NÚMERO DE MATRÍCULA DO SERVIDOR (N0007)
2	IT-NU-IDEN-SERV-ORIGEM	A 0008	NÚMERO DE IDENTIFICAÇÃO DO SERVIDOR NA ORIGEM - NÚMERO VINCULADO AO CARGO EFETIVO OU EM COMISSÃO
3	IT-NO-SERVIDOR	A 0060	NOME
4	IT-DA-NASCIMENTO	N 0008	DATA DE NASCIMENTO
5	IT-NU-CPF	N 0011	NÚMERO DO CPF
6	IT-NU-PIS-PASEP	N 0011	NÚMERO DO PIS
7	IT-IN-SUPRESSAO-PAGAMENTO	A 0001	INDICATIVO DE SUPRESSÃO DE PAGAMENTO
8	IT-CO-SITUACAO-SERVIDOR	N 0002	CÓDIGO DE SITUAÇÃO FUNCIONAL DO SERVIDOR
9	IT-CO-GRUPO-OCOR-AFASTAMENTO	N 0002	CÓDIGO DE OCORRÊNCIA DE AFASTAMENTO
10	IT-DA-INICIO-OCOR-AFASTAMENTO	N 0008	DATA DO INÍCIO DA OCORRÊNCIA DE AFASTAMENTO
11	IT-DA-TERMINO-OCOR-AFASTAMENTO	N 0008	DATA DE TÉRMINO DA OCORRÊNCIA DE AFASTAMENTO

12	IT-CO-GRUPO-OCOR-EXCLUSAO	N 0002	CÓDIGO DE OCORRÊNCIA DE EXCLUSÃO
13	IT-CO-UORG-LOTACAO-SERVIDOR	N 0009	CÓDIGO DA UORG DE LOTAÇÃO DO SERVIDOR
14	IT-CO-ORGAO-REQUISITANTE	N 0005	CÓDIGO DO ÓRGÃO REQUISITANTE

III - a Diretoria de Tecnologia da Informação e Inovação procederá com a atualização das bases cadastrais do serviço de diretórios e dos sistemas corporativos, bem como realizará a validação das informações disponibilizados pelo INSS por meio de outras bases, na periodicidade do envio das informações; e

IV - a área responsável pela gestão de pessoas do INSS poderá acordar, com a área responsável pela gestão de TI do INSS, a revisão das informações necessárias à administração de contas de usuários. (IN 01/2020) e PORTARIA Nº 93.

Art. 5º Credenciais e perfis de acesso:

I - a emissão de uma credencial permite ao usuário acessar a rede de dados corporativa do INSS. Para que o mesmo obtenha acesso aos sistemas corporativos a credencial deve ser associada a um perfil de acesso;

II - o processo de credenciamento de usuário aos ativos de informação deve ser feito observando os seguintes critérios:

- a) a credencial de acesso concedida para acesso à rede de dados e sistemas corporativos do INSS é de caráter pessoal e intransferível;
- b) as credenciais de acesso devem ser concedidas após a data de contratação ou entrada em exercício do usuário; e
- c) as mesmas credenciais de acesso devem ser utilizadas para o acesso à rede de dados e aos sistemas corporativos do INSS, mediante autenticação que permita ao usuário acessar vários sistemas, por meio de ferramenta de gestão de identidades e acessos.

III - a área responsável pela gestão de pessoas do INSS deverá (sugestão de texto da DGPA) os servidores lotados nas áreas responsáveis pela gestão de pessoas do INSS deverão utilizar os canais de atendimento disponibilizados pela Dataprev, ou outro canal informado pela DTI, para:

- a) solicitar o credenciamento de usuários do quadro de pessoal do INSS na data do ato administrativo de retorno ou ingresso no órgão, para acesso à rede (sugestão de redação da DGPA) solicitar, se necessário, o credenciamento de usuários, contratados ou requisitados, para compor o quadro de servidores do INSS, após o ato da posse; e de estagiários, após assinatura do contrato de prestação de serviço, para acesso à rede;
- b) solicitar a revogação de credenciais de acesso de servidores do quadro de pessoal do INSS cedidos a outros órgãos (sugestão de redação da DGPA); solicitar a inativação imediata do perfil de acesso dos servidores cedidos a outros órgãos, inativos ou exonerados do quadro de servidores do INSS na data da publicação do ato;
- c) solicitar a desativação de usuários do quadro de pessoal do INSS na data do ato administrativo ou de ocorrências que ensejem desligamento para fins de acesso lógico (sugestão de redação da DGPA); -solicitar a suspensão imediata do perfil de acesso dos servidores afastados ou com licença programada de suas funções por mais de sessenta dias ininterruptos; e
- d) solicitar a exclusão desativação (alteração proposta pelo CTGD em 10/07/2020) do acesso de usuários do quadro de pessoal em atividade do INSS afastados ou com licença programada de suas funções por mais de sessenta dias ininterruptos (sugestão de redação da DGPA). -estagiários, cujo vínculo com o Instituto tenha sido encerrado, tão logo a rescisão do contrato seja efetivada.

IV - quanto ao processo de formação das credenciais de acesso fica estabelecido que:

a) o nome do usuário será composto de acordo com os padrões estabelecidos no Guia de Interoperabilidade do Governo Eletrônico – e-Ping, mais especificamente no documento “Caixas Individuais-Fundacionais no Governo Federal” (Rede do Governo, 2010) que define regras de formação de nomes para a composição de endereços eletrônicos;

b) quanto às senhas de acesso:

1. deverão ter no mínimo oito caracteres e conter, obrigatoriamente, caracteres alfanuméricos (combinação de letras e números). O usuário poderá acrescentar caracteres especiais (espaços em branco, símbolos, sinais de pontuação, etc);
2. é vedada a reutilização das últimas quatro senhas utilizadas pelo usuário;
3. podem ser alteradas sempre que preciso ou quando o usuário achar necessário;
4. o prazo de validade não deve ultrapassar noventa dias; e
5. o usuário receberá por meio de comunicado direto (via interface do sistema ou por mensagem no correio eletrônico) a informação do prazo próximo de vencimento da senha, quando esta estiver a 15 dias da sua data de expiração.

V - os perfis de acesso aos sistemas corporativos deverão contemplar um conjunto de permissões e ações vinculadas às atividades desenvolvidas pelo usuário;

VI- caberá à área responsável pela gestão de TI do INSS estabelecer, em conjunto com as áreas responsáveis pela gestão dos sistemas corporativos, a norma de criação dos perfis de acesso; (IN 01/2020) e PORTARIA Nº 93.

VII - as áreas responsáveis pela gestão dos sistemas corporativos, são responsáveis pelas permissões, transações e ações que devem compor cada perfil de acesso;

VIII - os perfis de acesso e perfis de gestão concedidos para usuários interno e externos deverão ser objeto de revisão contínua pelos gestores responsáveis não podendo ultrapassar o prazo máximo de 30 (trinta) meses; Recomendação 2

IX - quanto à utilização das credenciais e perfis de acesso, o usuário:

- a) deve ter conhecimento prévio desta Norma de Controle de Acesso Lógico e preencher os requisitos estabelecidos na mesma;
- b) deve estar devidamente autorizado a utilizar a rede corporativa e/ou os sistemas corporativos, de acordo com os requisitos estabelecidos nesta Norma;
- c) deve utilizar os serviços e as informações obtidas, por meio do perfil de acesso, única e exclusivamente em razão do exercício da função pública e para os fins que lhe foi designado, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal;
- d) não pode divulgar, nem mesmo compartilhar, os códigos de segurança que lhe forem atribuídos (credenciais de acesso), os quais são pessoais e intransferíveis;
- e) não pode utilizar as credenciais para acessar os recursos disponíveis em mais de uma estação de trabalho simultaneamente;
- f) não pode fazer uso das credenciais de acesso de outros usuários;
- g) deve fornecer informações acessadas nos sistemas e na rede de dados corporativos do INSS somente mediante demanda formalizada de quem tenha competência para tal;
- h) deve comunicar a chefia imediata ou responsável pela administração do sistema ou rede corporativa quaisquer violações ou incidentes referentes à proteção do equipamento utilizado, do software ou de outros ativos da informação; e
- i) deve, sempre que for necessário afastar-se da estação de trabalho, certificar-se de que a sessão de rede ou acesso ao sistema corporativo esteja encerrado ou bloqueado.

X - a autenticação dos usuários será feita por meio de credenciais de acesso baseadas em nome de usuário e senha e, quando disponível, aliada ao uso de certificação digital padrão ICP-Brasil e/ou uso de dados biométricos; Recomendação 5

XI - o usuário deverá, obrigatoriamente, efetuar processo de alteração da sua senha em seu primeiro acesso à rede de dados corporativa; e

XII - no ato do primeiro acesso, bem como após cada atualização desta Norma, o usuário deverá manifestar concordância com os termos dispostos na mesma.

XIII - Credenciamento de Usuários Internos:

- a) o cadastro de novos servidores ou ocupantes de cargo em comissão, no âmbito do Instituto, pode ser solicitado por servidor vinculado à área responsável pela gestão de pessoas ou pela chefia imediata do usuário; e
- b) esse cadastro deve ser solicitado por meio dos canais de atendimento da Dataprev ou outro informado pela DTI.

XIV - credenciamento de estagiários:

- a) a emissão de credencial de acesso se dará tendo como requisito as seguintes condições:
 - 1. a empresa que atuar como agente de integração do estágio supervisionado deve manter contrato com o INSS; e
 - 2. o contrato de estágio supervisionado deverá conter cláusula de confidencialidade e sigilo de informações preestabelecidos com a Administração Pública.
- b) para viabilizar o acesso de estagiários aos sistemas corporativos, os gestores dos sistemas corporativos deverão criar perfis específicos e restritos às atividades do estagiário;
- c) é vedada a concessão de perfis de acesso aos sistemas corporativos para estagiários com permissão de alteração das bases de dados institucionais;
- d) o acesso será concedido mediante solicitação expressa de servidor do quadro do INSS, responsável pela supervisão do estágio, que deverá:
 - 1. avaliar os riscos de utilização indevida de informações institucionais e as eventuais restrições referentes aos dias e horários para a realização dos acessos.

e) o acesso será precedido da assinatura do Termo de Confidencialidade e de Manutenção de Sigilo – TCMS, Anexo II, o qual deverá ser firmado pelo estagiário ou pelo estagiário e seu responsável legal, no caso de se tratar de estagiário menor de dezoito anos;

f) as solicitações de acesso à rede para estagiários devem ser procedidas por meio dos canais remotos de atendimento disponibilizados pela empresa prestadora de serviços tecnológicos contratada pelo Instituto (alteração solicitada conforme reunião do CTGD em 10/07/2020) ou outro canal informado pela DTI, pela unidade de gestão de pessoas, pela chefia imediata do educando ou pelo responsável por sua supervisão;

g) os gestores de sistemas devem criar perfis diferenciados para estagiários de nível médio e nível superior;

h) o supervisor do estagiário deverá, periodicamente, orientá-lo quanto ao uso responsável e adequado do acesso aos sistemas corporativos; e

i) o acesso do estagiário limitar-se-á à data final do contrato ou imediatamente cessado na hipótese de rescisão antecipada do estágio, cabendo ao supervisor do estagiário, em quaisquer dos casos, adotar as providências necessárias ao bloqueio do acesso, tão logo finde a contratação.

XV - credenciamento de usuários externos:

a) as credenciais de acesso para usuários externos devem ser emitidas tendo em vista o interesse do INSS, devidamente justificadas e previstas no convênio, acordo de cooperação técnica ou instrumento congênere;

b) as solicitações de emissão de credenciais de acesso à rede corporativa para usuários amparados por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica, contrato ou instrumento congênere devem:

1. ser feitas pelo gestor da unidade/área responsável pela gestão do instrumento legal; e

2. ser atendidas somente após validação das credenciais do gestor solicitante do Instituto, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700) ou outra base de dados indicada pela área responsável pela gestão de pessoas, a qual contenha informações referentes à estrutura organizacional do Instituto (sugestão de redação feita pela DGPA).

c) a emissão de credenciais de acesso à rede corporativa para prestadores de serviço terceirizados ou equiparados nas dependências do INSS, quando necessária, será provida unicamente pelo interesse do INSS. Para tanto, devem ser atendidos os seguintes requisitos:

1. a organização a qual o usuário é vinculado deve manter contrato, acordo de cooperação, convênio ou instrumento congênere vigente com o INSS;

2. instrumento deve conter cláusulas prevendo:

2.1. necessidade e justificativa para acesso à rede corporativa;

2.2. a confidencialidade e sigilo de informações preestabelecidas junto ao Instituto;

2.3. a obrigatoriedade da organização ou do ente contratado informar previamente ao representante legal do INSS, responsável pela gestão do contrato, quaisquer alterações em seu corpo de colaboradores que impacte na emissão/exclusão das contas de acesso; (atendendo a recomendação nº 6 da CGU)

2.4. a organização ou ente contratado também deverá manter com seus colaboradores Termo de Confidencialidade de Manutenção de Sigilo – TCMS; e

2.5. o gestor do contrato pelo INSS deve fundamentar a necessidade do acesso à rede para prestadores de serviço terceirizados ou equiparados, definindo os recursos que devem ser disponibilizados e eventuais restrições a dias e horas para realização do acesso à rede.

3. os TCMS deverão ser arquivados junto aos instrumentos assinados com o INSS e uma cópia ou link eletrônico deverá ser encaminhada ao Gestor do Contrato. O mesmo deve ocorrer para quaisquer alterações ocorridas na vigência dos contratos, acordos ou convênios;

3.1 caso os Termos sejam gerados de forma eletrônica, deverá ser disponibilizado o arquivo correspondente, atendendo aos requisitos necessários para garantia de integridade e disponibilidade de acesso, assim como os requisitos específicos previstos em contrato; e

4. a emissão de credenciais de acesso poderá ser feita pelo gestor do contrato, representante legal do INSS, ou pelo gestor da unidade responsável pela gestão do contrato, convênio, acordo de cooperação técnica ou instrumento congênere e serão atendidas somente após validação das credenciais do solicitante, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700) ou outra base de dados indicada pela área responsável pela gestão de pessoas, a qual contenha informações referentes à estrutura organizacional do Instituto (sugestão de texto feita pela DPGA).

d) o acesso aos prestadores de serviço vinculados à Central de Atendimento 135 se dará observando as seguintes condições:

1. a empresa deve manter contrato com o INSS;

2. o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

3. a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade - TCMS;

4. o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte do INSS, definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;

5. os acessos deverão ser realizados única e exclusivamente por necessidade de serviço; e

6. Os contratos de prestação de serviços de teleatendimento devem conter documento a ser utilizado para formalização das indicações de gestores de acesso aos sistemas corporativos do Instituto; (sugestão de texto para atendimento da recomendação nº 7 do Relatório da CGU)

7. o INSS pode disponibilizar, de forma restrita, às centrais 135 uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

e) nos casos referentes a prestadores de serviço vinculados à Ouvidoria-Geral da Previdência Social — OUGPS — Ouvidoria do Ministério da Economia (alteração proposta pelo CTGD em 10/07/2020), o acesso se dará observando-se as seguintes condições:

1. a empresa deve manter Contrato direto com a Ouvidoria-Geral da Previdência Social — Ouvidoria do Ministério da Economia (alteração proposta pelo CTGD em 10/07/2020);

2. o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

3. a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade;

4. o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte da OUGPS — Ouvidoria do Ministério da Economia (alteração proposta pelo CTGD em 10/07/2020), definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;

5. os acessos deverão ser realizados única e exclusivamente por necessidade de serviço; e

6. o INSS pode disponibilizar, de forma restrita, à OUGPS — Ouvidoria do Ministério da Economia (alteração proposta pelo CTGD em 10/07/2020) uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

f) o acesso à rede corporativa por servidores vinculados a órgãos de controle externo, envolvidos em ações de auditoria no âmbito do INSS, será concedido mediante apresentação da equipe de auditoria por meio de documento formal que conste:

1. dados necessários ao cadastro de usuários externos;

2. informações acerca dos objetivos dos trabalhos a serem executados;

3. os prazos envolvidos; e

4. informações complementares.

g) este tipo de acesso deverá observar as parcerias institucionalmente estabelecidas entre esses órgãos e o INSS no que tange à cobertura/previsão de acesso à rede corporativa do Instituto; e

h) o atendimento de pedido de solicitação de informações advindo de pessoas físicas ou jurídicas externas, respeitadas as restrições de acesso às informações previstas na Lei nº 12.527, de 18 de novembro de 2011, serão analisadas pela área designada para responder as demandas dos cidadãos por meio do e-SIC.

XVI - os procedimentos referentes às solicitações de inclusão, exclusão, inativação e suspensão de contas de acesso de usuários devem ser executados tendo como premissa a preservação dos registros para efeito de auditoria.

XVII - bloqueio administrativo:

a) o responsável pela Corregedoria-Geral do INSS, quando necessário, poderão solicitar a suspensão, bloqueio ou inativação imediata de contas de acesso de usuários que estiverem envolvidos em inquérito penal, em Processo Administrativo Disciplinar – PAD – ou em Sindicância, decorrente de infrações cometidas no exercício das atribuições do cargo;

b) estas solicitações deverão ser efetuadas mediante comunicação formal da Corregedoria-Geral para a Dataprev, ou outro canal informado pela DTI, a qual procederá a imediata implementação da mudança.

c) para disciplinar o disposto na "alínea a", é considerado possível de ter a senha bloqueada, o usuário que estiver na seguinte situação:

1. afastado temporariamente do cargo ou função pública em razão de ato que se encontra sob apuração;

2. iniciado em processo administrativo disciplinar, por incursão nos incisos IX, XI, XII, XV, XVI e XVII do art. 117 e arts. 130 e 132 da Lei nº 8.112, de 11 de dezembro de 1990, ou cuja proposta pela Comissão Processante, no relatório final, seja pela aplicação de penalidade a partir de suspensão de trinta dias; e

3. submetido à prisão em flagrante, temporária ou preventiva decorrente do cometimento de infração no exercício das atribuições do cargo, enquanto estiver em apuração de inquérito policial ou pelo Ministério Público Federal.

d) o bloqueio de acessos, tratados nas situações da "alínea c", será efetivado no âmbito da ferramenta de gestão de acessos nas seguintes situações:

1. usuário afastado temporariamente do cargo ou função, enquanto durar o afastamento; e
2. usuário indiciado nos termos do subitem "alínea c", desta Norma, até o efetivo cumprimento da penalidade porventura aplicada ou, em caso de não aplicação de penalidade, enquanto durar o processo.

Art. 6º Rede de Dados Corporativa:

I - infraestrutura de rede:

a) a infraestrutura de rede do INSS é disponibilizada para uso Institucional. Sendo assim, apenas equipamentos de propriedade do Instituto são autorizados e devem ser conectados à rede corporativa;

1. em casos excepcionais, a conexão de equipamentos particulares à rede corporativa deve ser feita em razão do interesse do Instituto e sob prévia autorização do responsável pela gestão da unidade em que o equipamento estiver localizado.

b) o INSS poderá disponibilizar o acesso à rede de dados corporativa por meio de tecnologia *Wireless* (sem fio). Para tanto os seguintes critérios deverão ser adotados:

1. os projetos que envolvam a utilização de pontos de acesso sem fio à rede corporativa no âmbito do Instituto deverão ser devidamente registrados e aprovados pela área responsável pela gestão de TI do INSS; (IN 01/2020) e PORTARIA Nº 93.

2. os pontos de acesso à rede de dados corporativa sem fio poderão ser objeto de testes periódicos de penetração e de auditoria a critério da área responsável pela gestão de TI no INSS; (IN 01/2020) e PORTARIA Nº 93.

3. as conexões à rede sem fio serão avaliadas pela área responsável pela gestão de TI do INSS em relação aos requisitos de segurança e deverão atender ao princípio do privilégio mínimo; (IN 01/2020) e PORTARIA Nº 93.

4. a área responsável pela gestão de TI do INSS poderá disponibilizar rede sem fio com regras específicas de acesso para visitantes nas diversas unidades do Instituto; (IN 01/2020) e PORTARIA Nº 93.

5. os dispositivos conectados à rede do INSS por meio de conexão sem fio deverão suportar configurações de criptografia estabelecidas pela área responsável pela gestão de TI no âmbito do INSS; e (IN 01/2020) e PORTARIA Nº 93.

6. qualquer tecnologia de acesso sem fio implementada no INSS deverá suportar autenticação forte, com possibilidade de efetuar checagens em bancos de dados externos.

c) a área responsável pela gestão de TI do INSS deve dispor de mecanismos automáticos que possibilitem: (IN 01/2020) e PORTARIA Nº 93.

1. a detecção e bloqueio de equipamentos externos conectados à rede corporativa; e
2. a identificação e rastreamento dos endereços IP de origem e destino, bem como os serviços utilizados na rede corporativa inclusive nos acessos remotos.

II - administração da rede corporativa:

a) a administração da rede do INSS é realizada pela Empresa de Tecnologia e Informações da Previdência Social - Dataprev;

1. os ativos e serviços que compõem a rede de dados corporativa são providos, gerenciados e operacionalizados pela empresa; e
2. os acessos à rede de dados corporativa realizados pelos usuários do INSS são gerenciados e monitorados pela Dataprev, contudo seguem as regras desta Norma.

b) quanto ao processo de geração de contas de serviço fica estabelecido que:

1. os critérios para a emissão de contas de serviços serão vinculados a um processo formal estabelecido pela área responsável pela gestão de TI do INSS; (IN 01/2020) e PORTARIA Nº 93.

2. a concessão de contas de serviços deve ser feita conforme a necessidade de uso de acordo com os critérios estabelecidos nesta Norma de Controle de Acesso;

3. o direito de acesso privilegiado, por meio de contas de serviços, associado a sistemas ou processos, deve ser identificado;

4. deve ser viabilizada ferramenta que possibilite a gestão das contas de serviço de forma automatizada, possibilitando o registro e verificação de

todos os privilégios concedidos;

5. as contas de serviço fornecidas devem ser utilizadas exclusivamente para os fins aos quais foram concedidas;

6. as contas de serviço emitidas devem ser revalidadas periodicamente com base na função exercida e na área de atuação do servidor; e

7. as contas de serviço com credenciais de acesso de uso compartilhado devem ter suas senhas alteradas periodicamente, conforme estabelecido nesta Norma de Controle de Acesso Lógico, ou sempre que ocorrerem mudanças no grupo de usuários que utilizam as mesmas.

C) é vedado o uso da rede corporativa para:

1. acesso por meio de equipamento não homologado ou não autorizado pelo INSS;

2. fazer download, instalar e/ou utilizar sistemas ou aplicativos não homologados pela área responsável pela gestão de TI do INSS nos equipamentos de propriedade do Instituto; (IN 01/2020) e PORTARIA Nº 93.

3. a utilização de softwares particulares em equipamentos do INSS sem autorização expressa;

4. a instalação e conexão de equipamentos particulares à rede corporativa do Instituto sem a prévia autorização do gestor responsável pela unidade ou da área responsável pela gestão de TI do INSS; (IN 01/2020) e PORTARIA Nº 93.

5. o uso dos recursos de rede para fins particulares ou de terceiros alheios aos interesses do INSS, em especial quando tal procedimento prejudique o tráfego da rede de dados;

6. o uso para fins de divulgação ou distribuição de material que não possua vínculo com as atividades desenvolvidas pelo Instituto;

7. a instalação ou utilização de ferramentas de monitoramento de rede sem a anuência e autorização expressa da área responsável pela gestão de TI no Instituto; (IN 01/2020) e PORTARIA Nº 93.

8. a instalação de dispositivos de comunicação ou de compartilhamento de dados sem fio, particulares, à rede corporativa do Instituto, sem autorização expressa da área responsável pela gestão de TI do INSS; e (IN 01/2020) e PORTARIA Nº 93.

9. burlar as regras de acesso a internet configuradas em proxy ou ferramenta similar de gerenciamento de conteúdo web; (incluído)

d) cabe a área responsável pela gestão de TI no âmbito do INSS definir os aspectos relacionados à plataforma tecnológica, gestão operacional, forma de autenticação e sustentação do domínio de rede do INSS. (IN 01/2020) e PORTARIA Nº 93.

Art. 7º Gestão do Acesso aos Sistemas Corporativos:

I - sistemas legados:

a) as regras estabelecidas nesta norma devem ser aplicadas, guardando-se as devidas limitações tecnológicas, aos sistemas legados; e

b) o controle de acesso aos sistemas legados é efetuado por base própria.

II - sistemas de apoio à administração:

a) os ambientes de hospedagem desses sistemas são suportados por terceiros;

b) o ambiente deverá ser gerenciado e operacionalizado pela área de gestão de TI do INSS; (IN 01/2020) e PORTARIA Nº 93.

c) o acesso pelos usuários a esses sistemas deverá ser autenticado pelo serviço de diretório utilizado pelo Instituto; e

d) as regras de hospedagem de sistemas serão definidas, em ato próprio, pela área de gestão de TI do INSS. (IN 01/2020) e PORTARIA Nº 93.

III - armazenamento de registros logs:

a) as áreas responsáveis pela gestão de sistemas corporativos e demais aplicações devem definir, em conjunto com a área responsável pela gestão de TI, a temporalidade de registro dos logs de acesso e transações, e quais registros devem ser armazenados por um período maior que o estipulado no Art. 8º, I desta Norma; e (IN 01/2020) e PORTARIA Nº 93.

b) o INSS poderá alterar a temporalidade destes dados em norma específica;

c) Os logs de acesso devem contemplar minimamente os registros relacionados no ANEXO III desta norma. Recomendação 4.

IV - administração da ferramenta de gestão de acesso:

a) com o objetivo de operacionalizar a gestão dos acessos aos sistemas corporativos no âmbito do INSS, serão criados os seguintes papéis:

1. administrador de sistema INSS: Servidor do quadro, lotado na área responsável pela gestão de TI, designado por meio de Portaria do Diretor de Tecnologia da Informação e Inovação, a ser publicada em Boletim de Serviço – BS, responsável pela administração da ferramenta de gestão de acesso aos sistemas corporativos no âmbito do INSS; **(IN 01/2020) e PORTARIA Nº 93.**

2. gestor de sistema: Servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em Boletim de Serviço, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedoria-Geral e Procuradoria Federal Especializada. É responsável pela implementação de sistemas corporativos no âmbito do INSS;

3. gestor de acesso central: Servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em Boletim de Serviço, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedoria-Geral e Procuradoria Federal Especializada. É responsável pela manutenção dos perfis de gestão dos usuários nas áreas que compõem a Administração Central e, quando necessário, dos gestores de acesso das Superintendências Regionais;

4. gestor de acesso interno: Servidor do quadro, lotado na Administração Central, Superintendência Regional, Gerência Executiva, Agência da Previdência Social, indicado pelo Gestor de Acesso Central ou por um Gestor de Acesso, responsável pela atribuição do perfil de acesso e de gestão dos usuários no INSS; e

5. gestor de acesso externo: Pessoa formalmente indicada, por documento previsto no instrumento legal que firmou a parceria ou por meio de Ofício de lavra do representante máximo de uma Entidade Externa, responsável pelo cadastro de usuários externos e a gestão dos acessos aos sistemas corporativos do Instituto.

b) Os perfis de acesso serão atribuídos de acordo com a necessidade do fluxo de operação definido para cada sistema corporativo. (Recomendação 1)

c) a indicação e processo de substituição dos responsáveis pela gestão dos acessos aos sistemas corporativos no âmbito do INSS poderá ser procedida das seguintes formas:

1. a autoridade responsável pela indicação do gestor de acessos pode indicar opcionalmente o substituto;
2. o próprio gestor de acessos pode designar, a qualquer momento, por meio da ferramenta de gestão de acessos um substituto; ou
3. quando não houver um gestor responsável, ou substituto, por uma unidade devidamente designado, a gestão dos usuários será transferida, preferencialmente de forma automática, para o responsável pela área da abrangência daquela unidade e assim subsequentemente; e
4. o Gestor de Acesso é corresponsável com os perfis de gestão ou acesso que ele atribuir aos usuários.

c) ao usuário interno cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Norma de Controle de Acesso Lógico e suas normas complementares;
2. solicitar, ao Gestor de Acesso responsável pela gestão da unidade de lotação a qual é vinculado, a suspensão do seu perfil de acesso nos períodos de afastamento do serviço por mais de trinta dias consecutivos;
3. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e
4. ter conhecimento e estar de acordo com o disposto nesta Norma.

d) ao usuário externo cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Norma de Controle de Acesso Lógico;
2. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e
3. ter conhecimento e estar de acordo com o disposto nesta Norma.

e) ao administrador do sistema INSS cabe:

1. criar os sistemas e subsistemas, devidamente homologados pela área de negócio responsável, no ambiente de produção, por meio de ferramenta de gestão de acesso;
2. mediante apresentação de Portaria de designação para Gestores de Acesso Central, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores quanto à atribuição dos perfis de gestão; e
3. mediante apresentação de Portaria de designação para Gestores de Sistema, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores acerca do processo de implementação dos sistemas corporativos no âmbito do INSS.

f) ao gestor de sistema cabe:

1. efetuar os procedimentos de importação, inclusão, alteração e exclusão de papéis e permissões nos sistemas corporativos em ambiente de produção; e
2. atuar, em conjunto com o Administrador do Sistema INSS e a Dataprev, no planejamento e execução do processo de implementação dos sistemas corporativos dos quais for designado responsável.

g) ao gestor de acesso central cabe:

1. efetuar o credenciamento, suspensão ou exclusão de perfis de gestão dos sistemas corporativos aos Gestores de Acesso na Administração Central e, quando necessário, dos Gestores de Acesso da Superintendência Regional, Gerência Executiva, Agência da Previdência Social e demais usuários de sua abrangência; e
2. orientar os usuários de sua abrangência e os gestores da Administração Central e Superintendências Regionais, Gerências Executivas e Agências da Previdência Social acerca das regras para o acesso aos sistemas corporativos do INSS.

h) ao gestor de acesso interno cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários da Administração Central, Superintendência Regional, Gerência Executiva, Agência da Previdência Social;
2. atribuir, alterar ou excluir os perfis de acesso aos usuários da Administração Central, Superintendência Regional, Gerência Executiva, Agência da Previdência Social; e
3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS.

i) ao gestor de acesso externo cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários do seu Órgão/Entidade;
2. atribuir, alterar ou excluir os perfis de acesso aos usuários do seu Órgão/Entidade; e
3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS.

V - configura-se mau uso, sujeito a responsabilidade penal, civil e disciplinar:

- a) a divulgação, sem autorização expressa da chefia imediata ou do gestor de acesso de sua abrangência, de informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS;
- b) acessar sistemas corporativos sem autorização prévia, de acordo com os requisitos estabelecidos nesta Norma;
- c) utilizar-se das informações obtidas por meio de acesso concedido em desacordo com os procedimentos dispostos nesta Norma e demais normas vigentes na Administração Pública Federal;
- d) compartilhar ou fazer uso das credenciais de acesso, aos sistemas corporativos, de outros usuários;
- e) a instalação de sistemas corporativos em equipamentos particulares; e
- f) em casos excepcionais, a área responsável pela gestão de TI do INSS, mediante ato formal, poderá autorizar o contido no Art.8º, III. (IN 01/2020) e PORTARIA Nº 93.

Art. 8º Disposições Gerais:

I - todo acesso à rede de dados e aos sistemas corporativos deve ser registrado e monitorado de modo que permita a rastreabilidade, a identificação e o bloqueio de usuários e equipamentos não autorizados. Estas informações devem ser armazenadas por um período de, no mínimo, 30 (trinta) meses; (atendimento da recomendação nº 19 da CGU)

II - as ocorrências de mau uso do acesso aos recursos disponíveis na rede e sistemas corporativos não previstas nesta norma e os casos omissos serão encaminhados para a área responsável pela gestão de TI no âmbito do INSS para análise e pronunciamento; (IN 01/2020) e PORTARIA Nº 93.

III - identificada irregularidade de mau uso dos recursos de rede poderá ocorrer:

- a) o bloqueio preventivo do acesso pela DTI, o encaminhamento de dossiê com as informações para a Corregedoria-Geral do INSS ou Corregedorias Regionais, nas suas áreas de abrangências, a fim de que seja realizada a análise no âmbito disciplinar; e
- b) ressalta-se que o descumprimento dessa Norma poderá resultar em sanções administrativas, civis e criminais.

IV - esta norma deve ser revisada num período máximo de três anos.

ANEXO II

RESOLUÇÃO Nº 3/CEGOV/INSS, DE DE DE 2020

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF: _____, identidade _____, expedida pelo _____, em _____, e lotado no(a) _____ do Instituto Nacional do Seguro Social – INSS, DECLARO, sob pena das sanções cabíveis nos termos da Política de Segurança da Informação e Comunicações - POSIC POSIN do INSS que assumo a responsabilidade por: **(IN 01/2020)**

I - tratar o(s) ativo(s) de informação como patrimônio do Instituto Nacional do Seguro Social;

II - utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do INSS;

III - contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, que Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta; Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que disciplina a gestão de segurança da informação na Administração Pública Federal, direta e indireta, e dá outras providências; **(IN 01/2020) Substituir**

IV - utilizar as credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do INSS;

V - responder, perante o INSS, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

_____, _____ de _____ de _____

Assinatura do usuário

Nome do usuário:	Unidade de Lotação:
Nome da Autoridade Responsável pela Autorização do Acesso:	

Assinatura e Carimbo do Responsável pela Autorização de Acesso

ANEXO III

RESOLUÇÃO Nº 3/CEGOV/INSS, DE DE DE 2020

REGISTROS DE LOGS

1. Relação dos campos de registros de logs do GERID
 - 1.1. Dados Gerais
 - 1.1.1. Data
 - 1.1.2. Sistema
 - 1.1.3. Ambiente
 - 1.1.4. IP destino
 - 1.1.5. IP origem
 - 1.1.6. CPF usuário
 - 1.1.7. URL de origem
 2. Ações:
 - 2.1. CAS (autenticação): Central Authentication Service - Serviço Central de Autenticação
 - 2.1.1. Criação de service ticket (ST)
 - 2.1.2. Criação de ticket granting ticket (TGT)
 - 2.1.3. validação de ST
 - 2.1.4. Exclusão de ticket TGT
 - 2.1.5. Autenticação com sucesso (login+password)

- 2.1.6. Autenticação com sucesso (certificado digital)
- 2.1.7. Autenticação com falha
- 2.2. GPA: Gerenciamento de Permissão de Acesso
 - 2.2.1. Início de sessão
 - 2.2.2. Dados do usuário em sessão (CPF, NOME, PAPEL)
 - 2.2.3. Requisição de logout
 - 2.2.4. Dados de credenciais
 - 2.2.5. Concessão de credenciais
 - 2.2.6. Alteração de Credenciais
 - 2.2.7. Dados de receptor (CPF, NOME, Lotação)
 - 2.2.8. Inserção de credencial no usuário
 - 2.2.9. Revogação de Credenciais
 - 2.2.10. Pesquisa de credenciais
 - 2.2.11. Pesquisa de usuários
 - 2.2.12. Substituição de gestor



INSTITUTO NACIONAL DO SEGURO SOCIAL
MINUTA DE RESOLUÇÃO

MINUTA DE RESOLUÇÃO

**RESOLUÇÃO Nº 4/CEGOV/INSS, DE DE
DE 2020**

Institui a Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR do INSS.
Instituto Nacional do Seguro Social.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída a Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR do INSS.

Art. 2º Os Anexos a esta Portaria serão publicados em Boletim de Serviço.

Art. 3º Esta Portaria complementa Política de Segurança da Informação e Comunicações – POSIC POSIN-INSS vigente.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretora de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **ALEXINALDO MESSIAS CERQUEIRA**, **Chefe de Serviço**, em 16/07/2020, às 10:50, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1250265** e o código CRC **6EDF1478**.

ANEXO I

RESOLUÇÃO Nº 4/CEGOV/INSS, DE DE DE 2020
EQUIPE DE TRATAMENTO DE INCIDENTES DE REDES COMPUTACIONAIS - ETIR

Art. 1º Para os efeitos desta norma ficam estabelecidos os seguintes conceitos e definições:

I - agente responsável: Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

II - artefato malicioso: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

III - comunidade ou Público Alvo: é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

IV - CTIR GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI;

V - equipe de tratamento e resposta a incidentes em redes computacionais – ETIR: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

VI - incidente de segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VII - serviço: é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

VIII - tratamento de Incidentes de Segurança em Redes Computacionais: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

XI - usuário: pessoas que fazem uso de serviços de TI e sistemas de informação de propriedade do INSS, independente do cargo ocupado (contratados, consultores, conselheiros, servidores, temporários e etc); e

X - vulnerabilidade: ~~é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados;~~ conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou por uma organização, os quais podem ser evitados por uma ação interna de segurança da informação. **(IN 01/2020) e PORTARIA Nº 93.(alterado)**

Art. 2º Esta norma tem a missão de:

Parágrafo único. Agir proativamente, receber, analisar, monitorar, coordenar e propor respostas a notificações e atividades relacionadas a incidentes de segurança da informação e comunicações no âmbito do Instituto.

Art. 3º Esta norma tem como público alvo:

I - a abrangência das atividades pertinentes à ETIR-INSS inclui os usuários dos serviços de Tecnologia da Informação ~~e Comunicações - TI~~ e os sistemas de informação do INSS; **(IN 01/2020) e PORTARIA Nº 93**

II - as atividades pertinentes à ETIR-INSS serão realizadas com intercâmbio de informações e em cooperação com as seguintes instâncias:

a) o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR GOV;

b) a Comissão de Resposta e Tratamento de Incidentes em Redes Computacionais – CTIR, da Empresa de Tecnologia e Informações da Previdência Social - Dataprev;

c) equipes de tratamento de incidentes de redes computacionais dos demais órgãos, entidades e empresas, públicas ou privadas, que tenham contratos, acordos, convênios ou instrumentos congêneres com o INSS; e

d) o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República – GSI/PR.

Art. 4º a implementação e o funcionamento da ETIR-INSS seguirão a metodologia definida pelo Gabinete de Segurança Institucional da Presidência da República, conforme definido a seguir:

I - o modelo de implementação no qual a ETIR-INSS se baseia é o “Modelo 1 – Utilizando a equipe de Tecnologia da Informação”, conforme definido pelo GSI/PR;

II - a equipe será composta por profissionais da área de Tecnologia da Informação, lotados na Diretoria de Tecnologia da Informação e Inovação – DTI, sem prejuízo de suas atribuições típicas do cargo, com experiência e conhecimentos técnicos compatíveis com a importância da missão da ETIR-INSS;

III - a equipe será composta por servidores públicos efetivos;

IV - a ETIR-INSS ficará vinculada tecnicamente à Coordenação de Infraestrutura e Operações – CGIN, da Diretoria de Tecnologia da Informação e Inovação - DTI; e

~~V - o Coordenador da ETIR-INSS será nomeado por meio de ato do Diretor de Tecnologia da Informação e Inovação - DTI;(conforme solicitação reunião do CTGD em 10/07/2020)~~

~~VI - o Gestor de Segurança da Informação e Comunicações Caso o Coordenador da ETIR-INSS não seja formalmente nomeado, as atribuições relacionadas a coordenação da equipe serão desempenhadas pelo Coordenador-Geral de Infraestrutura e Suporte (conforme solicitação reunião do CTGD em 10/07/2020); (IN 01/2020) e PORTARIA Nº 9~~

Art. 5º A ETIR-INSS será composta por membros:

I - permanentes: que efetivamente atuarão em todos os incidentes registrados;

II - colaboradores: que atuarão, de forma esporádica, no tratamento de incidentes relacionados às suas áreas de atuação; e

III - Opcionais: servidores das unidades descentralizadas sob supervisão da DTI.

IV - sendo assim, a ETIR-INSS será formada pelos seguintes servidores: por servidores lotados na área de TI, de acordo com os papéis abaixo:(incluído)

Papel	Nome	Matrícula	Setor
Permanente	Roberto Rufino da Costa	1.057.683	Serviço de Segurança em TIC
Permanente	Nelson Antonio Pimentel Jacinto	1.095.044	Serviço de Segurança em TIC
Colaborador	Cristiano Santos de Souza	2.156.072	Divisão de Infraestrutura e Operações
Colaborador	Lourival de Sousa	2.262.639	Divisão de Infraestrutura e Operações
Colaborador	Jair Rodrigues Fernandes	2.276.407	Divisão de Infraestrutura e Operações
Colaborador	Rodrigo Gomes Rodrigues	2.135.059	Divisão de Arquitetura e Soluções

Quantidade	Papel	Setor
2	Permanente	Serviço de Segurança de TIC
2	Colaborador	Coordenação-Geral de Infraestrutura e Operações
2	Colaborador	Coordenação-Geral de Projetos e Soluções Digitais
2	Opcional	Unidades descentralizadas

V - Os membros da ETIR-INSS serão designados por meio de ato do Diretor de Tecnologia da Informação e Inovação.

Art. 6º Quanto autonomia da ETIR-INSS:

I - terá autonomia limitada para o tratamento de incidentes de Segurança da Informação, devendo implementar ações que possam impactar outras áreas do Instituto somente com anuência do Diretor de Tecnologia da Informação e Inovação e do gestor responsável pela área/sistema afetada; e

II - poderá, ainda, gerar relatórios técnicos sugerindo a adoção de medidas para resolução de incidentes.

Art. 7º A ETIR-INSS fornecerá o serviço de Tratamento de Incidentes de Segurança em Redes Computacionais:

I - este serviço compreende basicamente as seguintes ações:

- a) recepção: receber solicitações e alertas diversos. Para tanto o Instituto disponibilizará como canal de comunicação a caixa postal etir@inss.gov.br;
- b) filtrar: todo conteúdo direcionado para a ETIR deve ser verificado, a partir desta análise deve ser tratado pela equipe ou, não se tratando de um incidente de segurança em redes computacionais, encaminhado para a área competente;
- c) catalogar: os incidentes devem ser catalogados em ferramenta a ser indicada pela DTI, com nível de acesso restrito;
- d) classificar: os incidentes devem ser classificados quanto ao nível de severidade e impacto;
- e) tratar o incidente: indicar o tratamento do incidente com medidas corretivas e formas de se evitar que ocorra novamente;
- f) responder: as solicitações e alertas encaminhados para a ETIR devem ser devidamente respondidos; e
- g) monitorar: monitorar a aplicação do tratamento dos incidentes indicados.

II - a ETIR deve analisar os incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências; e

III - o detalhamento dos serviços prestados pela ETIR-INSS deve ser publicado em página específica da Intranet do Instituto no prazo de 30 dias a partir da publicação desta portaria.



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 5/CEGOV/INSS, DE DE DE 2020

Disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis Internet, competências e conteúdo de acesso para cada perfil.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída, nos termos do Anexo I desta Portaria, norma que estabelece critérios para uso da Internet no âmbito do Instituto Nacional do Seguro Social - INSS.

Art. 2º Os Anexos a esta Portaria serão publicados em Boletim de Serviço.

Art. 3º Esta Portaria complementa a Política de Segurança da Informação e Comunicações POSIC POSIN-INSS vigente. (IN 01/2020)

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretora de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por ALEXINALDO MESSIAS CERQUEIRA, Chefe de Serviço, em 16/07/2020, às 10:52, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador 1253280 e o código CRC A358A740.

ANEXO I

RESOLUÇÃO Nº 5/CEGOV/INSS, DE DE DE 2020

NORMA DE USO DA INTERNET

Art. 1º Esta norma se aplica a todos os servidores e colaboradores, vinculados direta ou indiretamente ao INSS, bem como a servidores e empregados de entidades e órgãos da Administração Pública ou privadas que necessitem ou estejam autorizados a acessar a Internet a partir da rede corporativa do Instituto.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União – AGU que atuarem na consultoria e no assessoramento jurídico, e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta norma, ficam estabelecidos os seguintes conceitos e definições:

I - autorizador: ocupantes de cargos que serão responsáveis pela autorização da concessão de perfis de acesso para usuários finais de sua área de abrangência;

II - internet: é a rede mundial que interliga computadores de diferentes tipos e dimensões e permite a comunicação entre pessoas e organizações, independentemente da localização geográfica;

III - intranet: é a rede de computadores administrada pelo INSS, que utiliza os mesmos serviços e tecnologias disponíveis na rede mundial, podendo ser definida como um tipo de Internet Local do Instituto;

IV - perfil de acesso: atributo que estabelece as categorias de sítios acessíveis e tipos de arquivos que podem ser recebidos ou transmitidos pelos usuários;

V - proxy: desempenha a função de conexão do computador (local) à rede externa (Internet). Como os endereços locais do computador não são válidos para acessos externos, cabe ao proxy enviar a solicitação do endereço local para o servidor, traduzindo e repassando-a para o seu computador;

VI - sítio: um conjunto de informações ou serviços disponíveis na Internet ou na Intranet, organizados em páginas eletrônicas e acessíveis por meio de endereços que identificam, de forma padronizada, sua origem e conteúdo;

VII - usuário: ~~Servidores, estagiários, terceirizados, contratados e colaboradores, que na execução de suas atividades necessitem de acesso à internet; servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal-APF, formalizada por meio da assinatura do Termo de Responsabilidade; e Substituir~~

VIII - VPN: Trata-se de uma Rede Privada Virtual (Virtual Private Network) construída sobre a infraestrutura de uma rede pública. Essa é uma forma de conectar dois computadores por meio de uma rede pública, como a Internet;

Art. 3º Essa norma tem como diretrizes:

I - o acesso à Internet disponibilizado pelo Instituto Nacional do Seguro Social aos usuários deve ser utilizado exclusivamente em razão de trabalho, cumprindo os procedimentos dispostos nesta norma;

II - os recursos disponibilizados pelo Instituto, não poderão ser usados para quaisquer propósitos que sejam ilegais ou proibidos, de modo a danificar, desativar, sobrecarregar ou prejudicar qualquer área, serviço ou conteúdo, ou interferir no uso e execução das atividades laborais de outros usuários;

III - o volume de tráfego de Internet e os endereços *web* visitados poderão ser monitorados, visando assegurar o cumprimento desta norma; e

IV - o acesso à Internet para propósitos particulares ou estranhos às atividades do INSS poderá ser bloqueado, sem prévia comunicação ao usuário e sem prejuízo das demais sanções aplicáveis.

Art. 4º Quando aos Perfis de Acesso:

I - o acesso aos sítios da Internet para todos os usuários será realizado mediante a atribuição de perfis de acesso;

II - o processo de solicitação e autorização de perfil de acesso à Internet do INSS compreenderá os seguintes perfis:

a) Perfil 1 - Perfil Restrito, deve ser inicialmente atribuído para usuários com maior restrição de acesso à internet, permitido acessar somente sítios governamentais, instituições bancárias e sítios considerados de interesse do INSS;

b) Perfil 2 - Perfil Básico, deve ser inicialmente atribuído para estagiários, recepcionistas e usuários externos. O usuário poderá acessar todos os sítios permitidos pelo Perfil 1, sítios de provedores de e-mail pessoal e instituições de ensino;

c) Perfil 3 - Perfil Padrão, para os servidores do quadro do Instituto. O usuário poderá acessar a todos sítios da internet sem a veiculação de material em áudio e vídeo; e

d) Perfil 4 - Perfil Avançado, deve ser atribuído preferencialmente para servidores do quadro do Instituto e estagiários que desempenham funções relacionadas à Comunicação Social, **Desenvolvimento de Pessoas (conforme parecer PFE-INSS)** e gestores, respeitado o princípio da necessidade de conhecer, designados pelos Autorizadores deste perfil. O usuário poderá acessar todos os sítios da Internet, incluindo sítios que veiculam material em áudio e vídeo (*streaming*), sítios de compartilhamento de vídeos, blogs e redes sociais.

III - o perfil concedido a agentes externos é de caráter temporário, com validade equivalente à vigência do trabalho a ser executado;

IV - o processo de alterações, bloqueios, liberações e categorizações de sítios, assim como a criação e/ou alterações de perfis de acesso descritos nesta norma, quando necessários, serão definidos pela Diretoria de Tecnologia da Informação e Inovação – DTI, e publicado no Portal do INSS na Intranet; e

V - os novos usuários que não tiverem um perfil de acesso atribuído, devem ser direcionados para uma página da intranet contendo orientações e normas relacionadas ao acesso à internet no INSS, entre outras informações definidas pela DTI.

Art. 5º Acesso de Usuários Externos:

I - quanto ao acesso de servidores ou funcionários públicos externos:

a) o acesso à Intranet e Internet a partir da rede de dados corporativa, nas dependências do INSS, aos demais órgãos da Administração Pública Direta e Indireta, de qualquer das esferas de governo, será concedido exclusivamente para servidores e empregados públicos, efetivos ou ocupantes de cargo em comissão;

b) os acessos dos usuários externos das entidades que compõem o Poder Público serão concedidos mediante o estabelecimento de acordos ou convênios específicos firmados com o INSS;

c) o gestor ou Coordenador-Geral da área responsável pelo convênio, contrato, ACT ou instrumento congênere, assumirá o papel de Autorizador do serviço de acesso à internet para usuários externos e deverá fundamentar as solicitações com base no instrumento; e

d) poderão ser concedidos acessos temporários para auditores de controle interno e externo, vinculados à Controladoria-Geral da União – CGU ou do Tribunal de Contas da União - TCU, no uso de suas atribuições.

II - quanto ao acesso de terceirizados:

a) o acesso à Internet por terceirizados deve ser provido pela empresa contratada;

b) em caráter de exceção, será concedido o acesso aos terceirizados a partir da infraestrutura de rede do INSS, desde que preenchidos os seguintes requisitos:

1. o contrato de prestação de serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

2. a empresa contratada deverá manter com seus funcionários Termo de Confidencialidade;

3. o contrato deve prever a necessidade de acesso à internet a partir das dependências do Instituto; e

4. o Autorizador, que para estes fins será o gestor do contrato ou o responsável pela área requisitante do serviço, deverá fundamentar as necessidades de acesso do contratado, definindo os recursos que devem ser disponibilizados, endereços da Intranet e Internet necessários para o desenvolvimento das atividades, bem como eventuais restrições a dias e horários para realização do acesso.

III - quanto ao acesso de visitantes:

a) a conexão de equipamentos pessoais à rede do Instituto, quando necessária e motivada pelo interesse da Administração, deve ser previamente autorizada pelo gestor da unidade onde o equipamento será utilizado;

b) só será permitida a utilização da rede local por equipamentos que atendam a todos os requisitos estabelecidos pela DTI; e

c) o acesso se dará, exclusivamente, à Internet, sendo vedado o acesso ao conteúdo disponibilizado na intranet.

Art. 6º A todos os perfis de acesso descritos nesta norma aplicam-se as restrições de acesso a sítios que:

I - contenham material pornográfico ou obsceno;

II - contenham material ilegal;

III - disponibilizem jogos, inclusive os da Internet (online);

IV - contenham material impróprio, ofensivo, preconceituoso ou discriminatório, que façam apologia à violência, ao terrorismo e às drogas; e

V - contenha e/ou divulgue conteúdo de violação de direito autoral (pirataria) e/ou execução de quaisquer tipos ou formas de fraudes.

Art. 7º Quanto ao processo de atribuição de acesso à Internet:

I - a atribuição dos perfis de acesso à Internet serão feitas pelos Autorizadores, de forma fundamentada respeitando o princípio da necessidade de conhecer, de acordo com a tabela abaixo:

Perfil	Autorizador
Perfil 1, 2 e 3	Gerente de APS, Gerente Executivo, Superintendentes Regionais, Procuradores Regionais, Coordenadores-Gerais, Superintendentes Regionais, Presidente do INSS, Auditor-Geral, Coordenadores-Gerais, Corregedoria-Geral, Procurador-Chefe da PFE-INSS, Diretores, Gestor ou chefe da área responsável pelo Contrato ou ato administrativo similar no âmbito do INSS.
Perfil 4	Chefes de Assessoria de Comunicação Social nas Superintendências Regionais, Assessor de Comunicação Social (Administração Central), Diretor de Tecnologia da Informação e Inovação, Diretor de Gestão de Pessoas e Administração (conforme parecer PFE) e Presidente do INSS.

II - nos casos de novos usuários de rede (LDAP), criados por meio de registro de chamado técnico, quando o solicitante não indicar o perfil de acesso à internet, será atribuído o Perfil 1;

III - para proceder a alteração do perfil de acesso, os usuários deverão preencher “Formulário de Acesso à Internet” (Anexo II) e providenciar a assinatura pelo Autorizador do acesso; e

IV - ao registrar a solicitação, deve-se anexar o Formulário de Solicitação de Acesso à Internet devidamente preenchido e assinado (pelo solicitante e Autorizador), conforme documento nato digital ou digitalizado no formato PDF.

Art. 8º A solicitação para perfis de acesso em caráter temporário devem indicar no Formulário de Solicitação de Acesso à Internet, a motivação da necessidade e a data de expiração do acesso.

Art. 9º Responsabilidades:

I - o usuário deve:

- a) preencher os requisitos e termos estabelecidos nesta norma;
- b) estar devidamente autorizado a utilizar a Internet nas formas estabelecidas nesta norma;
- c) fazer uso da Internet de forma responsável e segura, utilizando o acesso exclusivamente em razão de trabalho, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal; e
- d) impedir a divulgação e compartilhamento das chaves de segurança atribuídas, que são pessoais e intransferíveis.

II - o autorizador deve:

- a) conceder os perfis de acesso à internet rigorosamente de acordo com as atribuições dos usuários de sua abrangência, observando os normativos do INSS;
- b) verificar periodicamente o uso dos acessos concedidos e, sempre que necessário, solicitar alteração dos perfis de acesso dos usuários de sua abrangência; e
- c) reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à equipe de tratamento de incidentes de rede do INSS.

III - a área responsável pela gestão de TI no INSS deve: **(IN 01/2020) e PORTARIA Nº 93.**

- a) monitorar os acessos à internet e sua utilização de acordo com as diretrizes estabelecidas nesta norma; e
- b) identificar os casos de mau uso da Internet e adotar uma ou mais das seguintes providências:
 - 1. alertar ao usuário, responsável pelo acesso, e ao Autorizador, responsável pela concessão, acerca do uso indevido da internet;
 - 2. nos casos de reincidência, solicitar a revogação do acesso à internet concedido ao usuário; e
 - 3. encaminhar a documentação que comprova a má utilização do acesso concedido para Corregedoria do INSS, para análise e adoção das medidas cabíveis.

Art. 10º As seguintes práticas configuram-se como uso indevido da internet:

- I - acessar a internet disponibilizada pelo Instituto sem estar devidamente autorizado, conforme estabelecido nesta norma;
- II - não manifestar concordância com as regras estabelecidas nesta norma e nas demais aplicáveis;
- III - fazer uso dos recursos de Internet disponibilizado pelo Instituto para fins alheios ao trabalho, em discordância com os procedimentos dispostos nesta norma, sem prejuízo de demais normatizações vigentes na Administração Pública Federal;
- IV - utilizar os serviços extrapolando os privilégios do perfil de acesso que lhe foi designado;
- V - divulgação e compartilhamento das chaves de segurança, que são pessoais e intransferíveis, permitindo a utilização por terceiros do perfil que lhe foi atribuído;
- VI - praticar atos de comercialização de produtos e serviços, em proveito próprio ou de terceiros, que não atendam os interesses do INSS;
- VII - utilizar recursos ou dispositivos para acesso a computadores ou redes externas ao Instituto, com o objetivo de obter informações não autorizadas ou provocar a interrupção de serviços de rede;
- VIII - utilizar modem ou dispositivo de rede que interligue a rede interna do INSS a outras redes ou à Internet;
- IX - a exposição, o armazenamento, a distribuição, a edição, a gravação e o compartilhamento, através do uso dos recursos computacionais e de comunicação do INSS, de arquivos estranhos às atividades do Instituto e não autorizados pela chefia imediata;

X - realizar qualquer atividade que apoie ou facilite os vazamentos de dados;

XI - baixar arquivos ou programas da Internet que contrariem as diretrizes da Política de Segurança da Informação e Comunicações - POSIC POSIN vigente;
e (IN 01/2020)

XII - utilizar *proxy* não disponibilizado pelo INSS.

Art. 11 O acesso à Internet é passível de registro e monitoração, incluindo quaisquer dados transmitidos pela rede do INSS.

Art. 12 Disposições Gerais:

I - em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a ETIR deverá ser imediatamente acionada, para tomar as providências necessárias a fim de sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação do INSS;

II - as ocorrências de mau uso do acesso à internet não previstas nesta norma, assim como os casos de dúvidas em relação à aplicação das disposições aqui estabelecidas, devem ser encaminhadas à DTI para registro, análise e avaliação da necessidade de alterações de acordo com o processo de governança em vigência no Instituto;

III - o descumprimento desta norma, poderá acarretar ao usuário as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei, responsabilidade administrativa, civil e criminal; e

IV - esta norma deve ser atualizada periodicamente, não excedendo o prazo máximo de 3 anos.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações

DESPACHO

Coordenação-Geral De Infraestrutura e Operações, em 17/07/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Revisão de normas
de segurança da
informação.

1. Trata-se da Despacho DTI (SEI 1244356) que refere-se as mudanças realizadas nas normas de segurança da informação após análise do CTGD.
2. As adequações propostas pelo CTGD foram realizadas conforme o Despacho SSEG (SEI 1249313).
3. Feitas as considerações, encaminhe-se ao Comitê Temático de Governança Digital - CTGD para aprovação e encaminhamento das minutas dos normativos.

CLAUDIO AUGUSTO NOVAIS FERRAZ

Coordenador-Geral de Infraestrutura e Operações



Documento assinado eletronicamente por **Claudio Augusto Novais Ferraz, Coordenador(a) Geral**, em 17/07/2020, às 11:58, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1284437** e o código CRC **F8BAD720**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

CEGOV

Comitê Temático de Governança Digital

REGISTRO DE REUNIÃO

1. PAUTA: APRESENTAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (POSIN) E DA NORMA DE CONTROLE DE ACESSO LÓGICO (NCAL) COM OS DEMAIS NORMATIVOS

- **Área Responsável pela Reunião:** CTGD/DTI / Coordenação-Geral de Infraestrutura e Operações

Data	Horário de Início	Horário de Término	Local
10/07/2020	14h00min	15h45min	Reunião realizada através de videoconferência

2. PARTICIPANTES**2.1. Internos:**

Nome	Unidade	E-mail
Flávio Ferreira	DTI	flaviof.santos@inss.gov.br
Cláudio Novais	DTI	claudio.ferraz@inss.gov.br
Renata Cesário	DTI	renata.cgomes@inss.gov.br
Nelson Jacinto	DTI	nelson.jacinto@inss.gov.br
Rodolfo Costa	DTI	rodolfo.couy@inss.gov.br
Roberto Rufino	DTI	roberto.rufino@inss.gov.br
Ailton Nunes	DIRAT	ailtonnunes.junior@inss.gov.br
Roberto Dal Col Filho	DIRBEN	roberto.dalfilho@inss.gov.br
Renato Alves	DIGOV	renato.alves@inss.gov.br

3. PAUTA

Item	Descrição
1	Apresentação da Política de Segurança da Informação (POSIN) e da Norma de Controle de Acesso Lógico (NCAL)

4. RELATO DA REUNIÃO

Item	Descrição
1	Discussão sobre o processo nº 35014.047735/2020-84 que trata da validação das normas de SIC.
2	O Coordenador-Geral de Infraestrutura e Operações realizou a apresentação da Minuta da Nota Técnica (SEI 0829620) e da Minuta (SEI SSEG 1227904) contendo as orientações para implementação da Política de Segurança da Informação.
3	Proposta pelo Coordenador-Geral de Infraestrutura e Operações a avaliação da Minuta (SEI 1075264) que aborda as regras gerais da Norma de Controle de Acesso Lógico - NCAL.

Item	Descrição
4	Discussão e avaliação da Minuta (SEI 1075281) apresentada pelo Coordenador-Geral de Infraestrutura e Operações que trata da instituição da Equipe de Tratamento de Incidentes de Redes - ETIR.
5	Apresentação da Minuta (SEI 1075293) pelo Coordenador-Geral de Infraestrutura e Operações que trata da Norma de Controle de Acesso à Internet. Não foi atingido o quórum mínimo necessário de participantes para essa norma específica e o CTGD fará a validação via email/processo SEI para posterior apresentação ao CEGOV.

5. DELIBERAÇÕES

Item	Descrição	Responsável
1	Validação da minuta da Política de Segurança da Informação (0411821)	Comitê Temático de Governança Digital
2	Validação da minuta da PCAL para apresentação ao CEGOV (0411838)	Comitê Temático de Governança Digital
3	Validação da minuta de criação da ETIR (0411846)	Comitê Temático de Governança Digital
4	A validação da minuta de Norma de uso da internet pelo CTGD será feita via email/processo SEI (0411856)	Comitê Temático de Governança Digital

6. APROVAÇÃO

6.1. Segue o presente Registro de Reunião assinado eletronicamente pelos participantes acima identificados.



Documento assinado eletronicamente por **FLAVIO FERREIRA DOS SANTOS, Diretor(a)**, em 15/07/2020, às 18:12, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **Claudio Augusto Novais Ferraz, Coordenador(a) Geral**, em 17/07/2020, às 16:20, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **ROBERTO RUFINO DA COSTA, Chefe de Serviço Substituto(a)**, em 20/07/2020, às 15:06, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **AILTON NUNES DE MATOS JUNIOR, Coordenador(a) Geral**, em 20/07/2020, às 15:12, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **RENATO DO CARMO DAS NEVES ALVES, Técnico do Seguro Social**, em 20/07/2020, às 15:24, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **ROBERTO DAL COL FILHO, Coordenador(a) Geral**, em 20/07/2020, às 17:43, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **NELSON ANTONIO PIMENTEL JACINTO, Servidor(a)**, em 20/07/2020, às 17:54, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site
https://sei.inss.gov.br/sei/controlador_externo.php?



[acao=documento_conferir&id_orgao_acesso_externo=0](#), informando o código verificador **1264651** e o código CRC **108B4C06**.

Referência: Processo nº 35014.171888/2020-41

SEI nº 1264651



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria De Integridade, Governança e Gerenciamento De Riscos
Comitê Temático de Governança Digital

DESPACHO

Comitê Temático de Governança Digital, em 20/07/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Revisão de normas
de segurança da
informação.

1. Trata-se do processo de mudanças realizadas nas normas de segurança da informação.
2. Informa-se que conforme o e-mail (SEI 1297554) enviado aos membros do Comitê Temático de Governança Digital - CTGD, foi acordado na reunião do dia 10/07 (SEI 1297542) a validação final nas normas de SIC e que a única norma não revalidada na reunião foi a de Acesso à Internet. Foi solicitado na resposta deste e-mail os eventuais ajustes e sugestões com resposta até o dia 20/07, onde somente a DGPA manifestou-se (SEI 1297768) concordando com as alterações. Após esta data, as propostas serão encaminhadas ao CEGOV.
3. Feitas as considerações, encaminhe-se ao SSEG - Serviço de Segurança em Tecnologia da Informação, com ciência da Coordenação-Geral de Infraestrutura e Operação - CGIN, para resumo das modificações sugeridas nos normativos, com retorno a esta CTGD para posterior encaminhamento ao CEGOV.

CLAUDIO AUGUSTO NOVAIS FERRAZ

Diretor de Tecnologia da Informação e Inovação - Substituto



Documento assinado eletronicamente por **Claudio Augusto Novais Ferraz, Diretor(a) de Tecnologia da Informação e Inovação Substituto(a)**, em 20/07/2020, às 19:00, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1297557** e o código CRC **0358C694**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1297557



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações
Coordenação De Suporte e Infraestrutura De Tecnologia da Informação e Comunicação
Serviço De Segurança em Tecnologia da Informação e Comunicação

DESPACHO

Serviço De Segurança em Tecnologia da Informação e Comunicação, em 20/07/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

A s s . : Revisão e
proposição de normas de
segurança da informação.

1. Trata-se do Despacho CTGD - CEGOV (documento SEI nº 1297557) que refere-se as mudanças realizadas nas normas de segurança da informação.
2. Após as alterações nas minutas dos normativos para instituição de políticas e normas de segurança da informação e comunicações do Instituto Nacional do Seguro Social - INSS (documentos SEI nº 1249859, 1249899, 1250265 e 1253280), efetuadas pelo Serviço de Segurança em Tecnologia da Informação e Comunicações – SSEG, conforme relatos na Nota Técnica nº 3 (documento SEI nº 0829620) e Despachos SSEG (documentos SEI nº 1225291 e 1249313), para adequação das minutas, aprovadas pelo Comitê Temático de Governança Digital - CTGD.
3. Solicitamos que sejam encaminhadas ao Comitê Estratégico de Governança – CEGOV, para conhecimento e aprovação.
4. Feitas as considerações necessárias, encaminhe-se a Coordenação-Geral de Infraestrutura e Operações - CGIN, para conhecimento e providências.

ALEXINALDO MESSIAS CERQUEIRA

Chefe do Serviço de Segurança em Tecnologia da Informação e Comunicação



Documento assinado eletronicamente por **ALEXINALDO MESSIAS CERQUEIRA, Chefe de Serviço**, em 20/07/2020, às 20:10, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1297938** e o código CRC **DD090C1F**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1297938



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações

DESPACHO

Coordenação-Geral De Infraestrutura e Operações, em 20/07/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Revisão de normas
de segurança da
informação.

1. Trata-se do Despacho SSEG (SEI 1297938) que refere-se as mudanças realizadas nas normas de segurança da informação após análise do CTGD.
2. Feitas as considerações n referido Despacho, encaminhe-se ao Comitê Temático de Governança Digital - CTGD.

CLAUDIO AUGUSTO NOVAIS FERRAZ

Coordenador-Geral de Infraestrutura e Operações



Documento assinado eletronicamente por **Claudio Augusto Novais Ferraz, Coordenador(a) Geral**, em 20/07/2020, às 20:21, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site
https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1298109** e o código CRC **544F85E1**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1298109



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria De Integridade, Governança e Gerenciamento De Riscos
Comitê Temático de Governança Digital

DESPACHO

Comitê Temático de Governança Digital, em 20/07/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Revisão de normas
de segurança da
informação.

1. Trata-se de processo sobre tratativas em relação à revisão de normas de segurança da informação.
2. Após reunião deste Comitê Temático de Governança Digital - CTGD - realizada em 10/07/2020 (SEI 1297542), consulta aos membros deste CTGD (SEI 1297554) e revisão pelo Serviço de Segurança em Tecnologia da Informação - SSEG, as normas de Segurança da Informação foram validadas por este Comitê.
3. Feitas as considerações, encaminhe-se ao Comitê Estratégico de Governança - CEGOV - para análise das mudanças propostas.

CLAUDIO AUGUSTO NOVAIS FERRAZ

Diretor de Tecnologia da Informação e Inovação - Substituto



Documento assinado eletronicamente por **Claudio Augusto Novais Ferraz, Diretor(a) de Tecnologia da Informação e Inovação Substituto(a)**, em 20/07/2020, às 20:33, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site
https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1298125** e o código CRC **6A59ABA8**.



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria De Integridade, Governança e Gerenciamento De Riscos
Comitê Estratégico de Governança

DESPACHO

Comitê Estratégico de Governança, em 23/07/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Solicita ajuste nas
normas de segurança da
informação apresentadas
na Reunião Ordinárias
CEGOV nº 6/2020.

1. Os normativos para instituição de políticas e normas de segurança da informação do Instituto Nacional do Seguro Social - INSS (documentos SEI nº 1249859, 1249899, 1250265 e 1253280) foram discutidos na 6ª Reunião Ordinária do Comitê Estratégico de Governança - CEGOV, realizada no dia 22/07/2020 (Processo SEI nº 35014.164930/2020-78).
2. Os membros do CEGOV solicitaram alguns ajustes nas normas, conforme registrado na Minuta da Ata da Reunião, constante do documento SEI nº 1322155. Tal minuta foi submetida aos integrantes do comitê para revisão antes da assinatura.
3. No entanto, tendo em vista o acordado na 6ª Reunião Ordinária do CEGOV, retornam-se os autos à DTI e ao CTGD, para que procedam às mudanças já registradas no documento SEI nº 1322155.
4. Ressalta-se que as 4 minutas de resolução serão novamente submetidas à apreciação dos membros do CEGOV, por e-mail.
5. Após ajustes, solicita-se que os autos sejam retornados ao CEGOV para demais providências.

CIBELLE CESAR DO AMARAL BRASIL
Coordenadora-Geral de Governança
Secretaria-Executiva do Comitê Estratégico de Governança



Documento assinado eletronicamente por **CIBELLE CESAR DO AMARAL BRASIL**,
Coordenador(a) Geral, em 23/07/2020, às 16:57, conforme horário oficial de Brasília, com fundamento
no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1322316** e o código CRC **51C9692A**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1322316



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria De Integridade, Governança e Gerenciamento De Riscos
Comitê Temático de Governança Digital

DESPACHO

Comitê Temático de Governança Digital, em 23/07/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Solicita ajuste nas
normas de segurança da
informação apresentadas
na Reunião Ordinárias
CEGOV nº 6/2020.

1. Em atenção ao Despacho CEGOV (SEI 1322316), encaminha-se à DTI e SSEG com ciência da Coordenação-Geral de Infraestrutura e Operações - CGIN, para proceder com os ajustes nas minutas das Normas.

CLAUDIO AUGUSTO NOVAIS FERRAZ

Diretor de Tecnologia da Informação e Inovação - Substituto



Documento assinado eletronicamente por **Claudio Augusto Novais Ferraz, Diretor(a) de Tecnologia da Informação e Inovação Substituto(a)**, em 23/07/2020, às 23:55, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site
https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1323985** e o código CRC **3A08BAB6**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1323985



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

DESPACHO

Diretoria De Tecnologia da Informação e Inovação, em 23/07/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Solicita ajuste nas
normas de segurança da
informação apresentadas
na Reunião Ordinárias
CEGOV nº 6/2020.

1. Em atenção ao Despacho (SEI 1323985) encaminha-se ao Serviço de Segurança em Tecnologia da Informação - SSEG, com ciência da Coordenação-Geral de Infraestrutura e Operações - CGIN. para proceder com os ajustes nas normas.
2. Solicita-se devolução à esta Diretoria em 24/07/2020 para posterior encaminhamento ao CTGD - CEGOV.

CLAUDIO AUGUSTO NOVAIS FERRAZ

Diretor de Tecnologia da Informação - Substituto



Documento assinado eletronicamente por **Claudio Augusto Novais Ferraz, Diretor(a) de Tecnologia da Informação e Inovação Substituto(a)**, em 24/07/2020, às 00:01, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site

[https://sei.inss.gov.br/sei/controlador_externo.php?](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)

[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **1323991** e o código CRC **19E544D0**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1323991



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações
Coordenação De Suporte e Infraestrutura De Tecnologia da Informação e Comunicação
Serviço De Segurança em Tecnologia da Informação e Comunicação

DESPACHO

Serviço De Segurança em Tecnologia da Informação e Comunicação, em 24/07/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Solicita ajuste nas
normas de segurança da
informação apresentadas
na Reunião Ordinárias
CEGOV nº 6/2020

1. Trata o presente de minutas de normativos para instituição de políticas e normas de segurança da informação do Instituto Nacional do Seguro Social - INSS (documentos SEI nº 1249859, 1249899, 1250265 e 1253280). Os documentos foram discutidos na 6ª Reunião Ordinária do Comitê Estratégico de Governança - CEGOV, realizada no dia 22/07/2020 (Processo SEI nº 35014.164930/2020-78).
2. Retornam os autos para o Serviço de Segurança em Tecnologia da Informação e Comunicação - SSEG, para que sejam procedidas às mudanças registradas no documento SEI nº 1322155.
3. Após a edição dos documentos sob análise, novas versões foram acostadas aos autos com as seguintes modificações (em referência ao Documento SEI nº 1322155):
 - 3.1. Minuta de proposta da POSIN-INSS (documento SEI nº 1326575):
 - a) procedida a substituição das referências à Dataprev; e
 - b) ajustes de formatação do documento.
 - 3.2. Minuta de proposta de Norma de Controle de Acesso Lógico - NCAL-INSS (documento SEI nº 1327478):
 - a) procedida a substituição das referências à Dataprev;
 - b) edição do inciso X do Art. 5º acerca do processo de autenticação de usuários;
 - c) alteração do prazo para manutenção dos registros de acesso a sistemas indicados no inciso I do Art. 8º para 12 meses e inserção de referência, no item em tela, ao inciso III, do Art. 7º da norma, que indica a possibilidade de adequação desse prazo caso seja necessário;
 - d) ajustes de formatação do documento.

- 3.3. Minuta de proposta de Norma que Institui a ETIR-INSS (documento SEI nº 1328742):
- a) procedida a substituição das referências à Dataprev;
 - b) correção do nome da Coordenação-Geral de Infraestrutura e Operações no inciso IV do art. 4º da norma proposta;
 - c) ajustes de formatação do documento.
- 3.4. Minuta de proposta de Norma de Controle de Acesso à Internet (documento SEI nº 1329042):
- a) procedida a substituição das referências à Dataprev;
 - b) Tratando especificamente da proposta de inclusão, na norma sob análise, de item definindo "a liberação de acesso por IP, para organização das salas de treinamento com acesso a sites de streaming de áudio e vídeo", a Diretoria de Tecnologia da Informação e Inovação - DTI, não dispõe de elementos técnicos suficientes para deliberar se a proposição em tela é possível de ser implementada. Sendo assim, tal proposta deve ser avaliada tecnicamente para então ser compor uma futura versão da norma proposta;
 - c) ajustes de formatação do documento.
4. Feitas as considerações, encaminhe-se, em devolução, para a Diretoria de Tecnologia da Informação e Inovação - DTI, para conhecimento e prosseguimento.

ALEXINALDO MESSIAS CERQUEIRA

CHEFE DO SERVIÇO DE SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO E
COMUNICAÇÃO



Documento assinado eletronicamente por **ALEXINALDO MESSIAS CERQUEIRA, Chefe de Serviço**, em 24/07/2020, às 18:33, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1326078** e o código CRC **29272996**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1326078



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 2/CEGOV/INSS, DE DE DE 2020

Atualiza a Política de Segurança da Informação do Instituto Nacional

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída no âmbito do INSS e nos termos do Anexo a esta Resolução, a Política de Segurança da Informação POSIN-INSS.

Art. 2º Esta Resolução entra em vigor na data de sua publicação e seu Anexo será publicado em Boletim de Serviço.

Art. 3º Fica revogada a Resolução nº 672/PRES/INSS, de 27 de dezembro de 2018.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretora de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por ALEXINALDO MESSIAS CERQUEIRA, **Chefe de Serviço**, em 24/07/2020, às 18:34, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1326575** e o código CRC **F577757D**.

ANEXO I

RESOLUÇÃO Nº 2/CEGOV/INSS, DE DE DE 2020

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO INSTITUTO NACIONAL DO SEGURO SOCIAL – POSIN-INSS .

Art. 1º A Política de Segurança da Informação do Instituto Nacional do Seguro Social – POSIN-INSS, tem por objetivo estabelecer e difundir diretrizes e princípios de Segurança da Informação – SI, com vistas à orientação para uso e proteção adequados das informações produzidas e custodiadas pelo Instituto, preservando sua disponibilidade, integridade, confidencialidade e autenticidade.

Parágrafo único. A Política de que trata o **caput** e suas normas complementares aplicam-se a todos os agentes públicos que têm vínculo direto e/ou indireto com o Instituto.

Art. 2º Para os efeitos da POSIN-INSS, entende-se:

I - agente público: Todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da APF, direta e indireta;

II - atividade crítica - atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo;

III - ativos de informação: meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV - dados processados: dados submetidos a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação;

V - gestor de Segurança da Informação: é o responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da APF;

formato; VI - Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou

VII - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

VIII - necessidade de conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

IX - riscos de segurança da informação: potencial associado à exploração de uma ou mais vulnerabilidades nos ativos de informação, em razão de ameaças, com impacto negativo às atividades do Instituto;

X - segurança da informação – SI: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e autenticidades das informações;

XI - vínculo direto: agentes públicos contratados diretamente pelo INSS;

XII - vínculo indireto: agentes privados ou públicos pertencentes a órgãos ou unidades da Administração Pública Federal, Estadual ou Municipal que mantenham contrato, convênio, acordo de cooperação técnica ou instrumento congênere com o INSS; e

Art. 3º Esta POSIN-INSS foi elaborada com base nos seguintes documentos:

I - Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;

II - Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto na Constituição Federal;

III - Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

IV - Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais;

V - Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

VI - Decreto nº 7.724, de 16 de maio de 2012, regulamenta a Lei nº 12.527, de 18 de novembro de 2011;

VII - Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

VIII - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

IX - Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

X - Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que disciplina a gestão de segurança da informação na Administração Pública Federal, direta e indireta, e dá outras providências;

XI - Instruções normativas relacionadas à segurança da informação, publicadas pelo Gabinete de Segurança Institucional da Presidência da República;

XII - Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação;

XIII - NBR ISO/IEC 27002:2013, que institui código de melhores práticas para a Gestão de Segurança da Informação;

Art. 4º Esta POSIN-INSS foi elaborada com base nos seguintes princípios:

I - a preservação da imagem do Instituto e de seus agentes públicos;

II - a salvaguarda das informações do cidadão;

III - ações de segurança orientadas pela gestão de riscos;

IV - continuidade assegurada dos serviços ao cidadão;

V - o alinhamento com a missão institucional e seu planejamento estratégico; e

VI - respeito à natureza e finalidade de cada área do Instituto.

Art. 5º São diretrizes gerais da POSIN-INSS:

I - Tratamento da Informação:

- a) toda informação produzida pelos agentes públicos, no exercício de suas atividades, é de propriedade do INSS e deve ser protegida;
- b) informações produzidas, armazenadas e tratadas pelo Instituto, especialmente as informações pessoais e custodiadas, devem receber o devido tratamento para assegurar sua proteção durante todo o ciclo de vida; e
- c) somente os canais de comunicação disponibilizados pelo INSS devem ser utilizados para trafegar informações institucionais.

II - Tratamento de Incidentes de Segurança da Informação (SI):

- a) todo incidente de segurança da informação deve ser imediatamente relatado à área responsável pela gestão de segurança da informação de TI, observando-se a apropriada coleta de evidências.

III - Gestão de Riscos de Segurança:

- a) os riscos de segurança da informação devem ser identificados e tratados; e
- b) os critérios para a gestão de risco devem ser definidos e comunicados a toda instituição.

IV - Gestão de Continuidade:

- a) os ativos de informação que suportam as atividades críticas do Instituto devem ser suportados por ambiente de alta disponibilidade e ter capacidade de recuperação em prazos e condições previamente definidos para situações de contingência, em conformidade com o processo de continuidade; e
- b) a continuidade das operações e serviços de Tecnologia da Informação – TI, deve estar prevista nos contratos, assim como os prazos e condições devem estar formalmente estabelecidos.

V - Controles de Acesso:

- a) todo acesso à informação deve ser motivado pela necessidade de conhecer;
- b) os sistemas de informação e as instalações físicas devem ter capacidade de controlar os acessos, com fins de responsabilização pelo seu uso; e
- c) as autorizações de acesso às informações, sistemas e instalações físicas devem ter critérios de acesso definidos e divulgados a todos da instituição.

VI - Recursos Computacionais:

a) correio eletrônico:

- 1. o correio eletrônico, *e-mail*, é uma forma de comunicação oficial e deve ser utilizado exclusivamente no desempenho das atividades funcionais; e
- 2. ao produzir, responder ou encaminhar mensagem em caixa de correio eletrônico institucional, o servidor deverá se identificar, subscrevendo, ao menos, seu nome, cargo e telefone de contato institucional.

b) Acesso à Internet:

- 1. o acesso à Internet, por meio da rede de dados do INSS, é uma concessão e deve ter seu uso orientado para a execução das atividades do Instituto; e
- 2. os acessos serão liberados de acordo com perfis previamente definidos pelo órgão responsável pelos serviços de TI.

c) Gestão de Mudanças de TI:

- 1. toda mudança nos sistemas de informação do INSS deve ser previamente e formalmente autorizada; e
- 2. a gestão de mudanças deve prever, no mínimo, a guarda dos registros, realização de testes e a possibilidade de recuperação do ambiente.

d) Computação em Nuvem:

- 1. o ambiente de computação em nuvem, sua infraestrutura e canal de comunicação devem estar aderentes às diretrizes e normas de SI, estabelecidas pelo instituto, e às legislações vigentes.

2. o contrato de prestação de serviço, quando for o caso, deverá conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço.

VII - Educação e Conscientização:

- a) esta Política e seus normativos complementares devem ser periodicamente divulgados a todos os agentes públicos do Instituto;
- b) o Instituto deve manter programa contínuo de conscientização dos agentes públicos em Segurança da Informação— SI; e
- c) deve ser mantido plano de capacitação especializado aos profissionais que atuam na gestão de SI.

VIII - Auditoria e Conformidade:

- a) o cumprimento desta Política e de suas normas complementares deve ser avaliado periodicamente, por meio de verificações de conformidade; e
- b) o uso dos recursos de TI disponibilizados pelo Instituto é passível de monitoramento e auditoria.

IX - Responsabilidade pela gestão das informações:

- a) Os responsáveis pela gestão dos ativos da informação e sistemas corporativos devem descrever os requisitos de segurança;
- b) Os sistemas de informação devem ser concebidos possibilitando a segregação de funções.

X - Segurança física e do ambiente:

- a) As instalações em que as informações críticas ou sensíveis serão processadas deverão ser mantidas em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção física;
- b) Os ativos da organização devem ser protegidos contra acesso físico não autorizado, danos, perdas, furto e interferência. As proteções devem estar alinhadas aos riscos identificados.

XI - Gestão de ativos da informação

- a) os ativos de informação devem:

- 1. ser inventariados e protegidos;
- 2. ter identificados os seus proprietários e custodiantes;
- 3. ter a sua entrada e saída nas dependências do Instituto autorizadas e registradas por autoridade competente;
- 4. ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 6º A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas, cíveis e penais, previstas na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), no Código Penal, no Código Civil, e, ainda, em legislação que regule ou venha regular a matéria.

Art. 7º Competências e Responsabilidades:

I - Cabe ao Gestor de Segurança da Informação:

- a) promover cultura de segurança da informação;
- b) acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
- c) propor os recursos necessários à implementação das ações de SI;
- d) coordenar o CSI ou estrutura equivalente;
- e) acompanhar os trabalhos e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR-INSS;
- f) propor o detalhamento das diretrizes desta Política, por meio de normas e procedimentos, e acompanhar sua implementação;

- g) assessorar a alta administração na implementação da Política de Segurança da Informação;
- h) estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;
- i) promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no INSS;
- j) incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;
- k) verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;
- l) acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e
- m) manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

II - Cabe ao Presidente do Instituto nomear o Gestor de SI;

III - Caso o Gestor de SI não seja nomeado, as atribuições relacionadas no art. 7º inciso I serão desempenhadas pelo Diretor de Tecnologia da Informação e Inovação;

IV - A ETIR-INSS deve analisar e propor respostas a notificações e atividades relacionadas a incidentes de SI, no âmbito do Instituto; e

V - É responsabilidade de todos os agentes públicos, diretos e indiretos, conhecer e cumprir as diretrizes desta Política e demais normas e procedimentos complementares de SI;

VI - Tendo em vista o Sistema de Governança do INSS, instituído pela Portaria nº 3.213/PRES/INSS/2019, compete ao Comitê Estratégico de Governança - CEGOV - deliberar sobre políticas e normas de segurança da informação, assessorado pelo Comitê Temático de Governança Digital.

Parágrafo único. O Comitê Temático de Gestão da Informação é responsável pela aprovação de procedimentos e de normas internas que orientem o compartilhamento de dados sob gestão do INSS e pela aprovação da categorização dos níveis de compartilhamento de dados com outras entidades públicas (federais ou de outras esferas e poderes) da sociedade civil (Vide atribuições do CTGI, no Art. 6º do Anexo da Portaria nº 3.213/PRES/INSS/2019).

Art. 8º Esta Política e seus normativos devem ser revisados sempre que necessário, não excedendo o período máximo de três anos.



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 3/CEGOV/INSS, DE DE DE 2020

Define regras para a emissão de credenciais de acesso lógico no âmbito do INSS

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída a Norma de Controle de Acesso Lógico - NCAL, do Instituto Nacional do Seguro Social – INSS.

Art. 2º Esta Resolução, bem como seus anexos, serão publicados em Boletim de Serviço, nos termos do Inciso I do Art. 16, da Resolução n.708/INSS/PRES, de 6 de novembro de 2019.

Art. 3º Revogar a RESOLUÇÃO Nº 413/PRES/INSS, DE 20 DE MAIO DE 2014.

Art. 4º Esta Resolução entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretora de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por ALEXINALDO MESSIAS CERQUEIRA, Chefe de Serviço, em 24/07/2020, às 18:35, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador 1327478 e o código CRC 1594D5BA.

ANEXO I

RESOLUÇÃO Nº 3/CEGOV/INSS, DE DE DE 2020

NORMA DE CONTROLE DE ACESSO LÓGICO – INSS

Art. 1º Os termos definidos nesta norma aplicam-se a todos os agentes públicos e privados com vínculo direto ou indireto, permanente ou temporário com o INSS.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União – AGU que atuarem na consultoria e no assessoramento jurídico, e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta Norma de Controle de Acesso Lógico são estabelecidos os seguintes conceitos e definições:

I - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

II - administrador de Domínio: Usuário responsável pela administração de um domínio por meio da aplicação de políticas globais, criação, edição e exclusão de usuários e grupos, e instalação de programas em um grande número de estações de trabalho;

III - administrador Local: Usuário responsável pela administração de partes de um domínio (geralmente restrito a um setor ou abrangência), por meio de políticas locais, edição de grupos e usuários locais, e instalação de programas em estações de trabalho limitadas a um setor ou abrangência;

IV - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta;

V - ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VI - contas de serviço: contas de acesso à rede corporativa de computadores, necessárias para a execução de procedimentos automáticos (aplicação, script, etc) sem qualquer intervenção humana no seu uso;

VII - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais;

VIII - credenciamento: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer;

IX - credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física, como crachá, cartão e selo ou lógica como identificação usuário e senha;

X - dado: Sugestão de Alteração "O dado é um elemento informativo concreto e sua forma plural expressa uma informação" é o registro do atributo de um ente objeto ou fenômeno onde registro indica o ato de registrar, ou seja, é a gravação ou a impressão de caracteres ou símbolos que tenham um significado em algum documento ou suporte físico;

XI - domínio: agrupamento lógico de computadores em rede que compartilham recursos em um banco de dados de segurança, comum, onde a administração e autenticação são centralizadas. Desta forma um usuário precisa de uma conta para ter acesso ao domínio e aos recursos compartilhados;

XII - endereço IP: conjunto de elementos numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores. Sequência de números associada a cada computador conectado à Internet. No caso de IPv4, o endereço IP é dividido em quatro grupos, separados por "." e compostos por números entre 0 e 255. No caso de IPv6, o endereço IP é dividido em até oito grupos, separados por ":" e compostos por números hexadecimais (números e letras de "A" a "F") entre 0 e FFFF;

XIII - entidade externa: Organização governamental, não governamental ou privada amparada por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica ou instrumento congênera com o INSS;

XIV - e-SIC: Sistema Eletrônico do Serviço de Informações ao Cidadão, aplicação disponibilizada na internet, que centraliza todos os pedidos de informações dirigidos ao Poder Executivo Federal;

XV - estagiário: educando que esteja frequentando o ensino regular, em instituições de educação superior, de educação profissional, de ensino médio, de educação especial e dos anos finais do ensino fundamental, na modalidade profissional da educação de jovens e adultos, que desenvolve as atividades relacionadas à sua área de formação profissional junto as pessoas Jurídicas de Direito Privado, órgãos da Administração Pública e Instituições de Ensino, que tenham condições de proporcionar experiência prática na sua linha de formação;

XVI - estágio Supervisionado: ato educativo escolar supervisionado, desenvolvido no ambiente de trabalho, que visa a preparação para o trabalho produtivo de educandos;

XVII - ferramenta de gestão de acessos: Software que possibilita a gestão integrada de papéis e permissões de acesso dos usuários nos sistemas corporativos;

XVIII - gestor da informação: usuário que gerou a informação, que responde pelo seu conteúdo ou que foi formalmente designado para definir, alterar a sua classificação nos graus de sigilo e perfil de acesso dos demais usuários e processos;

XIX - gestão de identidades: Combinação de sistemas técnicos, regras e procedimentos que definem a posse, utilização e segurança de uma identidade. Seu objetivo primário é estabelecer a confiança na associação de atributos a uma identidade digital e conectar esta identidade com uma entidade individual;

XX - Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXI - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

XXII - Log ou Registro de Auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional;

XXIII - necessidade de conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

XXIV - perfil de Acesso do Usuário: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

XXV - recursos de rede: Dispositivos (impressoras, scanners, multifuncionais, etc) ou serviços (sistemas, portais, etc) disponibilizados para os usuários por meio de uma rede de dados;

XXVI - serviço de diretório: serviço que armazena e organiza informações relativas a recursos disponíveis e usuários de uma rede de dados. Permite que o

administrador da rede gerencie o acesso de usuários e sistemas aos recursos disponíveis;

XXVII - sistemas corporativos: sistemas de operação, ou finalísticos, que se coadunam com os fins da Previdência Social. Assim, entende-se que este conceito comporta o conjunto de sistemas e subsistemas que garantem a operação dos regimes geral e próprio de previdência social, inclusive de previdência complementar;

XXVIII - sistemas legados: compreendem o conjunto de aplicações desenvolvidas com tecnologias obsoletas que permanecem em operação no INSS;

XXIX - usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal-APF, formalizada por meio da assinatura do Termo de Responsabilidade;

XXX - usuário interno: servidor do quadro do INSS lotado em uma Unidade Orgânica – UO, que se utiliza dos sistemas corporativos do Instituto;

XXXI - usuário externo: usuários vinculados a uma Entidade Externa, que se utiliza dos sistemas corporativos do Instituto por meio de um perfil de acesso concedido por um Gestor de Acesso Externo;

Art. 3º São diretrizes desta NCAL-INSS:

I - o acesso à rede e aos sistemas corporativos do INSS dar-se-á por meio de autenticação integrada de domínio baseado em serviço de diretório, administrado por meio de uma ferramenta de gestão de identidades;

II - as concessões de acesso à rede de dados e aos sistemas corporativos são distintas. Sendo assim, o usuário pode obter permissão de acesso apenas à rede de dados, ou apenas a determinado(s) sistema(s) corporativo(s);

III - as credenciais de acesso a rede de dados e aos sistemas corporativos do INSS são conferidas aos usuários com base na necessidade de conhecer, para viabilizar o exercício de suas atribuições funcionais e atividades a serem desenvolvidas no âmbito do INSS; e

IV - o uso indevido de informações dos sistemas corporativos do INSS sujeitará o agente às penalidades previstas na legislação.

Art. 4º Base Cadastral:

I - as bases de dados do Serviço de Diretórios (acesso à rede de dados), do Sistema de Gestão de Acessos (sistemas corporativos) e sistemas legados devem ser alimentadas por informações disponibilizadas pelo INSS;

II - para tanto, a área responsável pela gestão de pessoas do INSS disponibilizará semanalmente as informações extraídas do Sistema Integrado de Administração de Recursos Humanos – SIAPE para a empresa prestadora de serviços tecnológicos contratada pelo Instituto, com a supervisão da área de gestão de TI do INSS, contendo, minimamente, os seguintes dados:

Tabela 1: Informações Usuários

Item	Informação	Campo	Descrição
1	GR-MATRICULA	N 0012	GRUPO NUMÉRICO COMPOSTO DE NÚMERO DO ÓRGÃO (N0005) E NÚMERO DE MATRÍCULA DO SERVIDOR (N0007)
2	IT-NU-IDEN-SERV-ORIGEM	A 0008	NÚMERO DE IDENTIFICAÇÃO DO SERVIDOR NA ORIGEM - NÚMERO VINCULADO AO CARGO EFETIVO OU EM COMISSÃO
3	IT-NO-SERVIDOR	A 0060	NOME
4	IT-DA-NASCIMENTO	N 0008	DATA DE NASCIMENTO
5	IT-NU-CPF	N 0011	NÚMERO DO CPF
6	IT-NU-PIS-PASEP	N 0011	NÚMERO DO PIS
7	IT-IN-SUPRESSAO-PAGAMENTO	A 0001	INDICATIVO DE SUPRESSÃO DE PAGAMENTO
8	IT-CO-SITUACAO-SERVIDOR	N 0002	CÓDIGO DE SITUAÇÃO FUNCIONAL DO SERVIDOR
9	IT-CO-GRUPO-OCOR-AFASTAMENTO	N 0002	CÓDIGO DE OCORRÊNCIA DE AFASTAMENTO
10	IT-DA-INICIO-OCOR-AFASTAMENTO	N 0008	DATA DO INÍCIO DA OCORRÊNCIA DE AFASTAMENTO
11	IT-DA-TERMINO-OCOR-AFASTAMENTO	N 0008	DATA DE TÉRMINO DA OCORRÊNCIA DE AFASTAMENTO
12	IT-CO-GRUPO-OCOR-EXCLUSAO	N 0002	CÓDIGO DE OCORRÊNCIA DE EXCLUSÃO
13	IT-CO-UORG-LOTACAO-SERVIDOR	N 0009	CÓDIGO DA UORG DE LOTAÇÃO DO SERVIDOR

14	IT-CO-ORGAO-REQUISITANTE	N 0005	CÓDIGO DO ÓRGÃO REQUISITANTE

III - a Diretoria de Tecnologia da Informação e Inovação procederá com a atualização das bases cadastrais do serviço de diretórios e dos sistemas corporativos, bem como realizará a validação das informações disponibilizados pelo INSS por meio de outras bases, na periodicidade do envio das informações; e

IV - a área responsável pela gestão de pessoas do INSS poderá acordar, com a área responsável pela gestão de TI do INSS, a revisão das informações necessárias à administração de contas de usuários.

Art. 5º Credenciais e perfis de acesso:

I - a emissão de uma credencial permite ao usuário acessar a rede de dados corporativa do INSS. Para que o mesmo obtenha acesso aos sistemas corporativos a credencial deve ser associada a um perfil de acesso;

II - o processo de credenciamento de usuário aos ativos de informação deve ser feito observando os seguintes critérios:

a) a credencial de acesso concedida para acesso à rede de dados e sistemas corporativos do INSS é de caráter pessoal e intransferível;

b) as credenciais de acesso devem ser concedidas após a data de contratação ou entrada em exercício do usuário; e

c) as mesmas credenciais de acesso devem ser utilizadas para o acesso à rede de dados e aos sistemas corporativos do INSS, mediante autenticação que permita ao usuário acessar vários sistemas, por meio de ferramenta de gestão de identidades e acessos.

III - a área responsável pela gestão de pessoas do INSS deverá utilizar os canais de atendimento disponibilizados pela empresa prestadora de serviços tecnológicos contratada pelo Instituto, ou outro canal informado pela DTI, para:

a) solicitar o credenciamento de usuários do quadro de pessoal do INSS na data do ato administrativo de retorno ou ingresso no órgão, para acesso à rede, e de estagiários, após assinatura do contrato de prestação de serviço, para acesso à rede;

b) solicitar a revogação de credenciais de acesso de servidores do quadro de pessoal do INSS cedidos a outros órgãos;

c) solicitar a desativação de usuários do quadro de pessoal do INSS na data do ato administrativo ou de ocorrências que ensejem desligamento para fins de acesso lógico; e

d) solicitar a desativação do acesso de usuários do quadro de pessoal em atividade do INSS afastados ou com licença programada de suas funções por mais de sessenta dias ininterruptos;

IV - quanto ao processo de formação das credenciais de acesso fica estabelecido que:

a) o nome do usuário será composto de acordo com os padrões estabelecidos no Guia de Interoperabilidade do Governo Eletrônico – e-Ping, mais especificamente no documento “Caixas Individuais-Fundacionais no Governo Federal” (Rede do Governo, 2010) que define regras de formação de nomes para a composição de endereços eletrônicos;

b) quanto às senhas de acesso:

1. deverão ter no mínimo oito caracteres e conter, obrigatoriamente, caracteres alfanuméricos (combinação de letras e números). O usuário poderá acrescentar caracteres especiais (espaços em branco, símbolos, sinais de pontuação, etc);

2. é vedada a reutilização das últimas quatro senhas utilizadas pelo usuário;

3. podem ser alteradas sempre que preciso ou quando o usuário achar necessário;

4. o prazo de validade não deve ultrapassar noventa dias; e

5. o usuário receberá por meio de comunicado direto (via interface do sistema ou por mensagem no correio eletrônico) a informação do prazo próximo de vencimento da senha, quando esta estiver a 15 dias da sua data de expiração.

V - os perfis de acesso aos sistemas corporativos deverão contemplar um conjunto de permissões e ações vinculadas às atividades desenvolvidas pelo usuário;

VI- caberá à área responsável pela gestão de TI do INSS estabelecer, em conjunto com as áreas responsáveis pela gestão dos sistemas corporativos, a norma de criação dos perfis de acesso;

VII - as áreas responsáveis pela gestão dos sistemas corporativos, são responsáveis pelas permissões, transações e ações que devem compor cada perfil de acesso;

VIII - os perfis de acesso e perfis de gestão concedidos para usuários interno e externos deverão ser objeto de revisão contínua pelos gestores responsáveis, não podendo ultrapassar o prazo máximo de 30 (trinta) meses;

IX - quanto à utilização das credenciais e perfis de acesso, o usuário:

- a) deve ter conhecimento prévio desta Norma de Controle de Acesso Lógico e preencher os requisitos estabelecidos na mesma;
- b) deve estar devidamente autorizado a utilizar a rede corporativa e/ou os sistemas corporativos, de acordo com os requisitos estabelecidos nesta Norma;
- c) deve utilizar os serviços e as informações obtidas, por meio do perfil de acesso, única e exclusivamente em razão do exercício da função pública e para os fins que lhe foi designado, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal;
- d) não pode divulgar, nem mesmo compartilhar, os códigos de segurança que lhe forem atribuídos (credenciais de acesso), os quais são pessoais e intransferíveis;
- e) não pode utilizar as credenciais para acessar os recursos disponíveis em mais de uma estação de trabalho simultaneamente;
- f) não pode fazer uso das credenciais de acesso de outros usuários;
- g) deve fornecer informações acessadas nos sistemas e na rede de dados corporativos do INSS somente mediante demanda formalizada de quem tenha competência para tal;
- h) deve comunicar a chefia imediata ou responsável pela administração do sistema ou rede corporativa quaisquer violações ou incidentes referentes à proteção do equipamento utilizado, do software ou de outros ativos da informação; e
- i) deve, sempre que for necessário afastar-se da estação de trabalho, certificar-se de que a sessão de rede ou acesso ao sistema corporativo esteja encerrado ou bloqueado.

X - o processo de autenticação de usuários deve ser definido pela área responsável pela gestão de Tecnologia da Informação do Instituto e poderá ser baseada em autenticação simples (nome de usuário e senha) agregada a autenticação multifator (certificação digital ou outros meios disponíveis);

XI - o usuário deverá, obrigatoriamente, efetuar processo de alteração da sua senha em seu primeiro acesso à rede de dados corporativa; e

XII - no ato do primeiro acesso, bem como após cada atualização desta Norma, o usuário deverá manifestar concordância com os termos dispostos na mesma.

XIII - Credenciamento de Usuários Internos:

a) o cadastro de novos servidores ou ocupantes de cargo em comissão, no âmbito do Instituto, pode ser solicitado por servidor vinculado à área responsável pela gestão de pessoas ou pela chefia imediata do usuário; e

b) esse cadastro deve ser solicitado por meio dos canais de atendimento disponibilizados pela prestadora de serviços tecnológicos contratada pelo Instituto ou outro informado pela DTI.

XIV - credenciamento de estagiários:

a) a emissão de credencial de acesso se dará tendo como requisito as seguintes condições:

1. a empresa que atuar como agente de integração do estágio supervisionado deve manter contrato com o INSS; e
2. o contrato de estágio supervisionado deverá conter cláusula de confidencialidade e sigilo de informações preestabelecidos com a Administração Pública.

b) para viabilizar o acesso de estagiários aos sistemas corporativos, os gestores dos sistemas corporativos deverão criar perfis específicos e restritos às atividades do estagiário;

c) é vedada a concessão de perfis de acesso aos sistemas corporativos para estagiários com permissão de alteração das bases de dados institucionais;

d) o acesso será concedido mediante solicitação expressa de servidor do quadro do INSS, responsável pela supervisão do estágio, que deverá:

1. avaliar os riscos de utilização indevida de informações institucionais e as eventuais restrições referentes aos dias e horários para a realização dos acessos.

e) o acesso será precedido da assinatura do Termo de Confidencialidade e de Manutenção de Sigilo – TCMS, Anexo II, o qual deverá ser firmado pelo estagiário ou pelo estagiário e seu responsável legal, no caso de se tratar de estagiário menor de dezoito anos;

f) as solicitações de acesso à rede para estagiários devem ser procedidas por meio dos canais remotos de atendimento disponibilizados pela empresa prestadora de serviços tecnológicos contratada pelo Instituto ou outro canal informado pela DTI, pela unidade de gestão de pessoas, pela chefia imediata do educando ou pelo responsável por sua supervisão;

g) os gestores de sistemas devem criar perfis diferenciados para estagiários de nível médio e nível superior;

h) o supervisor do estagiário deverá, periodicamente, orientá-lo quanto ao uso responsável e adequado do acesso aos sistemas corporativos; e

i) o acesso do estagiário limitar-se-á à data final do contrato ou imediatamente cessado na hipótese de rescisão antecipada do estágio, cabendo ao supervisor do estagiário, em quaisquer dos casos, adotar as providências necessárias ao bloqueio do acesso, tão logo finde a contratação.

XV - credenciamento de usuários externos:

a) as credenciais de acesso para usuários externos devem ser emitidas tendo em vista o interesse do INSS, devidamente justificadas e previstas no convênio, acordo de cooperação técnica ou instrumento congênere;

b) as solicitações de emissão de credenciais de acesso à rede corporativa para usuários amparados por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica, contrato ou instrumento congênere devem:

1. ser feitas pelo gestor da unidade/área responsável pela gestão do instrumento legal; e

2. ser atendidas somente após validação das credenciais do gestor solicitante do Instituto, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700).

c) a emissão de credenciais de acesso à rede corporativa para prestadores de serviço terceirizados ou equiparados nas dependências do INSS, quando necessária, será provida unicamente pelo interesse do INSS. Para tanto, devem ser atendidos os seguintes requisitos:

1. a organização a qual o usuário é vinculado deve manter contrato, acordo de cooperação, convênio ou instrumento congênere vigente com o INSS;

2. instrumento deve conter cláusulas prevendo:

2.1. necessidade e justificativa para acesso à rede corporativa;

2.2. a confidencialidade e sigilo de informações preestabelecidas junto ao Instituto;

2.3. a obrigatoriedade da organização ou do ente contratado informar previamente ao representante legal do INSS, responsável pela gestão do contrato, quaisquer alterações em seu corpo de colaboradores que impacte na emissão/exclusão das contas de acesso;

2.4. a organização ou ente contratado também deverá manter com seus colaboradores Termo de Confidencialidade de Manutenção de Sigilo – TCMS; e

2.5. o gestor do contrato pelo INSS deve fundamentar a necessidade do acesso à rede para prestadores de serviço terceirizados ou equiparados, definindo os recursos que devem ser disponibilizados e eventuais restrições a dias e horas para realização do acesso à rede.

3. os TCMS deverão ser arquivados junto aos instrumentos assinados com o INSS e uma cópia ou link eletrônico deverá ser encaminhada ao Gestor do Contrato. O mesmo deve ocorrer para quaisquer alterações ocorridas na vigência dos contratos, acordos ou convênios;

3.1 caso os Termos sejam gerados de forma eletrônica, deverá ser disponibilizado o arquivo correspondente, atendendo aos requisitos necessários para garantia de integridade e disponibilidade de acesso, assim como os requisitos específicos previstos em contrato; e

4. a emissão de credenciais de acesso poderá ser feita pelo gestor do contrato, representante legal do INSS, ou pelo gestor da unidade responsável pela gestão do contrato, convênio, acordo de cooperação técnica ou instrumento congênere e serão atendidas somente após validação das credenciais do solicitante, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700).

d) o acesso aos prestadores de serviço vinculados à Central de Atendimento 135 se dará observando as seguintes condições:

1. a empresa deve manter contrato com o INSS;

2. o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

3. a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade - TCMS;

4. o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte do INSS, definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;

5. os acessos deverão ser realizados única e exclusivamente por necessidade de serviço; e

6. Os contratos de prestação de serviços de teleatendimento devem conter documento a ser utilizado para formalização das indicações de gestores de acesso aos sistemas corporativos do Instituto;

7. o INSS pode disponibilizar, de forma restrita, às centrais 135 uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

e) nos casos referentes a prestadores de serviço vinculados à Ouvidoria do Ministério da Economia, o acesso se dará observando-se as seguintes condições:

1. a empresa deve manter Contrato direto com a Ouvidoria do Ministério da Economia;
2. o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;
3. a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade;
4. o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte da Ouvidoria do Ministério da Economia, definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;
5. os acessos deverão ser realizados única e exclusivamente por necessidade de serviço; e
6. o INSS pode disponibilizar, de forma restrita, à Ouvidoria do Ministério da Economia uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

f) o acesso à rede corporativa por servidores vinculados a órgãos de controle externo, envolvidos em ações de auditoria no âmbito do INSS, será concedido mediante apresentação da equipe de auditoria por meio de documento formal que conste:

1. dados necessários ao cadastro de usuários externos;
2. informações acerca dos objetivos dos trabalhos a serem executados;
3. os prazos envolvidos; e
4. informações complementares.

g) este tipo de acesso deverá observar as parcerias institucionalmente estabelecidas entre esses órgãos e o INSS no que tange à cobertura/previsão de acesso à rede corporativa do Instituto; e

h) o atendimento de pedido de solicitação de informações advindo de pessoas físicas ou jurídicas externas, respeitadas as restrições de acesso às informações previstas na Lei nº 12.527, de 18 de novembro de 2011, serão analisadas pela área designada para responder as demandas dos cidadãos por meio do e-SIC.

XVI - os procedimentos referentes às solicitações de inclusão, exclusão, inativação e suspensão de contas de acesso de usuários devem ser executados tendo como premissa a preservação dos registros para efeito de auditoria.

XVII - bloqueio administrativo:

a) o responsável pela Corregedoria-Geral do INSS, quando necessário, poderão solicitar a suspensão, bloqueio ou inativação imediata de contas de acesso de usuários que estiverem envolvidos em inquérito penal, em Processo Administrativo Disciplinar – PAD – ou em Sindicância, decorrente de infrações cometidas no exercício das atribuições do cargo;

b) estas solicitações deverão ser efetuadas mediante comunicação formal da Corregedoria-Geral para a prestadora de serviços tecnológicos contratada pelo Instituto, ou outro canal informado pela DTI, a qual procederá a imediata implementação da mudança.

c) para disciplinar o disposto na "alínea a", é considerado possível de ter a senha bloqueada, o usuário que estiver na seguinte situação:

1. afastado temporariamente do cargo ou função pública em razão de ato que se encontra sob apuração;
2. indiciado em processo administrativo disciplinar, por incursão nos incisos IX, XI, XII, XV, XVI e XVII do art. 117 e arts. 130 e 132 da Lei nº 8.112, de 11 de dezembro de 1990, ou cuja proposta pela Comissão Processante, no relatório final, seja pela aplicação de penalidade a partir de suspensão de trinta dias; e
3. submetido à prisão em flagrante, temporária ou preventiva decorrente do cometimento de infração no exercício das atribuições do cargo, enquanto estiver em apuração de inquérito policial ou pelo Ministério Público Federal.

d) o bloqueio de acessos, tratados nas situações da "alínea c", será efetivado no âmbito da ferramenta de gestão de acessos nas seguintes situações:

1. usuário afastado temporariamente do cargo ou função, enquanto durar o afastamento; e
2. usuário indiciado nos termos do subitem "alínea c", desta Norma, até o efetivo cumprimento da penalidade porventura aplicada ou, em caso de não aplicação de penalidade, enquanto durar o processo.

Art. 6º Rede de Dados Corporativa:

I - infraestrutura de rede:

a) a infraestrutura de rede do INSS é disponibilizada para uso Institucional. Sendo assim, apenas equipamentos de propriedade do Instituto são autorizados e devem ser conectados à rede corporativa;

1. em casos excepcionais, a conexão de equipamentos particulares à rede corporativa deve ser feita em razão do interesse do Instituto e sob prévia autorização do responsável pela gestão da unidade em que o equipamento estiver localizado.

b) o INSS poderá disponibilizar o acesso à rede de dados corporativa por meio de tecnologia *Wireless* (sem fio). Para tanto os seguintes critérios deverão ser adotados:

1. os projetos que envolvam a utilização de pontos de acesso sem fio à rede corporativa no âmbito do Instituto deverão ser devidamente registrados e aprovados pela área responsável pela gestão de TI do INSS;

2. os pontos de acesso à rede de dados corporativa sem fio poderão ser objeto de testes periódicos de penetração e de auditoria a critério da área responsável pela gestão de TI no INSS;

3. as conexões à rede sem fio serão avaliadas pela área responsável pela gestão de TI do INSS em relação aos requisitos de segurança e deverão atender ao princípio do privilégio mínimo;

4. a área responsável pela gestão de TI do INSS poderá disponibilizar rede sem fio com regras específicas de acesso para visitantes nas diversas unidades do Instituto;

5. os dispositivos conectados à rede do INSS por meio de conexão sem fio deverão suportar configurações de criptografia estabelecidas pela área responsável pela gestão de TI no âmbito do INSS;

6. qualquer tecnologia de acesso sem fio implementada no INSS deverá suportar autenticação forte, com possibilidade de efetuar checagens em bancos de dados externos.

c) a área responsável pela gestão de TI do INSS deve dispor de mecanismos automáticos que possibilitem:

1. a detecção e bloqueio de equipamentos externos conectados à rede corporativa; e

2. a identificação e rastreamento dos endereços IP de origem e destino, bem como os serviços utilizados na rede corporativa inclusive nos acessos remotos.

II - administração da rede corporativa:

a) a operacionalização da administração da rede do INSS é realizada por empresa prestadora de serviços tecnológicos contratada pelo Instituto;

1. os ativos e serviços que compõem a rede de dados corporativa são providos, gerenciados e operacionalizados por tal prestadora de serviços; e

2. os acessos à rede de dados corporativa realizados pelos usuários do INSS são gerenciados e monitorados pela empresa prestadora de serviços de tecnologia contratada pelo Instituto, contudo seguem as regras desta Norma.

b) quanto ao processo de geração de contas de serviço fica estabelecido que:

1. os critérios para a emissão de contas de serviços serão vinculados a um processo formal estabelecido pela área responsável pela gestão de TI do INSS;

2. a concessão de contas de serviços deve ser feita conforme a necessidade de uso de acordo com os critérios estabelecidos nesta Norma de Controle de Acesso;

3. o direito de acesso privilegiado, por meio de contas de serviços, associado a sistemas ou processos, deve ser identificado;

4. deve ser viabilizada ferramenta que possibilite a gestão das contas de serviço de forma automatizada, possibilitando o registro e verificação de todos os privilégios concedidos;

5. as contas de serviço fornecidas devem ser utilizadas exclusivamente para os fins aos quais foram concedidas;

6. as contas de serviço emitidas devem ser revalidadas periodicamente com base na função exercida e na área de atuação do servidor; e

7. as contas de serviço com credenciais de acesso de uso compartilhado devem ter suas senhas alteradas periodicamente, conforme estabelecido nesta Norma de Controle de Acesso Lógico, ou sempre que ocorrerem mudanças no grupo de usuários que utilizam as mesmas.

C) é vedado o uso da rede corporativa para:

1. acesso por meio de equipamento não homologado ou não autorizado pelo INSS;

2. fazer download, instalar e/ou utilizar sistemas ou aplicativos não homologados pela área responsável pela gestão de TI do INSS nos equipamentos de propriedade do Instituto;

3. a utilização de softwares particulares em equipamentos do INSS sem autorização expressa;

4. a instalação e conexão de equipamentos particulares à rede corporativa do Instituto sem a prévia autorização do gestor responsável pela unidade ou da área responsável pela gestão de TI do INSS;

5. o uso dos recursos de rede para fins particulares ou de terceiros alheios aos interesses do INSS, em especial quando tal procedimento prejudique o tráfego da rede de dados;

6. o uso para fins de divulgação ou distribuição de material que não possua vínculo com as atividades desenvolvidas pelo Instituto;

7. a instalação ou utilização de ferramentas de monitoramento de rede sem a anuência e autorização expressa da área responsável pela gestão de TI no Instituto;

8. a instalação de dispositivos de comunicação ou de compartilhamento de dados sem fio, particulares, à rede corporativa do Instituto, sem autorização expressa da área responsável pela gestão de TI do INSS; e

9. burlar as regras de acesso a internet configuradas em proxy ou ferramenta similar de gerenciamento de conteúdo *web*;

d) cabe à área responsável pela gestão de TI no âmbito do INSS definir os aspectos relacionados à plataforma tecnológica, gestão operacional, forma de autenticação e sustentação do domínio de rede do INSS.

Art. 7º Gestão do Acesso aos Sistemas Corporativos:

I - sistemas legados:

a) as regras estabelecidas nesta norma devem ser aplicadas, guardando-se as devidas limitações tecnológicas, aos sistemas legados; e

b) o controle de acesso aos sistemas legados é efetuado por base própria.

II - sistemas de apoio à administração:

a) os ambientes de hospedagem desses sistemas são suportados por terceiros;

b) o ambiente deverá ser gerenciado e operacionalizado pela área de gestão de TI do INSS;

c) o acesso pelos usuários a esses sistemas deverá ser autenticado pelo serviço de diretório utilizado pelo Instituto; e

d) as regras de hospedagem de sistemas serão definidas, em ato próprio, pela área de gestão de TI do INSS.

III - armazenamento de registros logs:

a) as áreas responsáveis pela gestão de sistemas corporativos e demais aplicações devem definir, em conjunto com a área responsável pela gestão de TI, a temporalidade de registro dos logs de acesso e transações, e quais registros devem ser armazenados por um período maior que o estipulado no Inciso I do Art. 8º desta Norma;

b) o INSS poderá alterar a temporalidade destes dados em norma específica;

c) Os logs de acesso devem contemplar minimamente os registros relacionados no ANEXO III desta norma.

IV - administração da ferramenta de gestão de acesso:

a) com o objetivo de operacionalizar a gestão dos acessos aos sistemas corporativos no âmbito do INSS, serão criados os seguintes papéis:

1. administrador de sistema INSS: Servidor do quadro, lotado na área responsável pela gestão de TI, designado por meio de Portaria do Diretor de Tecnologia da Informação e Inovação, a ser publicada em Boletim de Serviço – BS, responsável pela administração da ferramenta de gestão de acesso aos sistemas corporativos no âmbito do INSS;

2. gestor de sistema: Servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em Boletim de Serviço, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedoria-Geral e Procuradoria Federal Especializada. É responsável pela implementação de sistemas corporativos no âmbito do INSS;

3. gestor de acesso central: Servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em Boletim de Serviço, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedoria-Geral e Procuradoria Federal Especializada. É responsável pela manutenção dos perfis de gestão dos usuários nas áreas que compõem a Administração Central e, quando necessário, dos gestores de acesso das Superintendências Regionais;

4. gestor de acesso interno: Servidor do quadro, lotado na Administração Central, Superintendência Regional, Gerência Executiva, Agência da Previdência Social, indicado pelo Gestor de Acesso Central ou por um Gestor de Acesso, responsável pela atribuição do perfil de acesso e de gestão dos usuários no INSS; e

5. gestor de acesso externo: Pessoa formalmente indicada, por documento previsto no instrumento legal que firmou a parceria ou por meio de Ofício de lavra do representante máximo de uma Entidade Externa, responsável pelo cadastro de usuários externos e a gestão dos acessos aos sistemas corporativos do Instituto.

b) Os perfis de acesso serão atribuídos de acordo com a necessidade do fluxo de operação definido para cada sistema corporativo;

c) a indicação e processo de substituição dos responsáveis pela gestão dos acessos aos sistemas corporativos no âmbito do INSS poderá ser procedida das seguintes formas:

1. a autoridade responsável pela indicação do gestor de acessos pode indicar opcionalmente o substituto;

2. o próprio gestor de acessos pode designar, a qualquer momento, por meio da ferramenta de gestão de acessos um substituto; ou

3. quando não houver um gestor responsável, ou substituto, por uma unidade devidamente designado, a gestão dos usuários será transferida, preferencialmente de forma automática, para o responsável pela área da abrangência daquela unidade e assim subsequentemente; e

4. o Gestor de Acesso é corresponsável com os perfis de gestão ou acesso que ele atribuir aos usuários.

d) ao usuário interno cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Norma de Controle de Acesso Lógico e suas normas complementares;

2. solicitar, ao Gestor de Acesso responsável pela gestão da unidade de lotação a qual é vinculado, a suspensão do seu perfil de acesso nos períodos de afastamento do serviço por mais de trinta dias consecutivos;

3. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e

4. ter conhecimento e estar de acordo com o disposto nesta Norma.

e) ao usuário externo cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Norma de Controle de Acesso Lógico;

2. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e

3. ter conhecimento e estar de acordo com o disposto nesta Norma.

f) ao administrador do sistema INSS cabe:

1. criar os sistemas e subsistemas, devidamente homologados pela área de negócio responsável, no ambiente de produção, por meio de ferramenta de gestão de acesso;

2. mediante apresentação de Portaria de designação para Gestores de Acesso Central, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores quanto à atribuição dos perfis de gestão; e

3. mediante apresentação de Portaria de designação para Gestores de Sistema, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores acerca do processo de implementação dos sistemas corporativos no âmbito do INSS.

g) ao gestor de sistema cabe:

1. efetuar os procedimentos de importação, inclusão, alteração e exclusão de papéis e permissões nos sistemas corporativos em ambiente de produção; e

2. atuar, em conjunto com o Administrador do Sistema INSS e a prestadora de serviços tecnológicos contratada pelo Instituto, no planejamento e execução do processo de implementação dos sistemas corporativos dos quais for designado responsável.

h) ao gestor de acesso central cabe:

1. efetuar o credenciamento, suspensão ou exclusão de perfis de gestão dos sistemas corporativos aos Gestores de Acesso na Administração Central e, quando necessário, dos Gestores de Acesso da Superintendência Regional, Gerência Executiva, Agência da Previdência Social e demais usuários de sua abrangência; e

2. orientar os usuários de sua abrangência e os gestores da Administração Central e Superintendências Regionais, Gerências Executivas e Agências da Previdência Social acerca das regras para o acesso aos sistemas corporativos do INSS.

i) ao gestor de acesso interno cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários da Administração Central, Superintendência Regional, Gerência Executiva, Agência da Previdência Social;

2. atribuir, alterar ou excluir os perfis de acesso aos usuários da Administração Central, Superintendência Regional, Gerência Executiva, Agência da Previdência Social; e

3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS.

j) ao gestor de acesso externo cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários do seu Órgão/Entidade;

2. atribuir, alterar ou excluir os perfis de acesso aos usuários do seu Órgão/Entidade; e

3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS.

V - configura-se mau uso, sujeito a responsabilidade penal, civil e disciplinar:

a) a divulgação, sem autorização expressa da chefia imediata ou do gestor de acesso de sua abrangência, de informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS;

b) acessar sistemas corporativos sem autorização prévia, de acordo com os requisitos estabelecidos nesta Norma;

c) utilizar-se das informações obtidas por meio de acesso concedido em desacordo com os procedimentos dispostos nesta Norma e demais normas vigentes na Administração Pública Federal;

d) compartilhar ou fazer uso das credenciais de acesso, aos sistemas corporativos, de outros usuários;

e) a instalação de sistemas corporativos em equipamentos particulares; e

f) em casos excepcionais, a área responsável pela gestão de TI do INSS, mediante ato formal, poderá autorizar a adoção das medidas descritas no Inciso III do Art.8º.

Art. 8º Disposições Gerais:

I - todo acesso à rede de dados e aos sistemas corporativos deve ser registrado e monitorado de modo que permita a rastreabilidade, a identificação e o bloqueio de usuários e equipamentos não autorizados. Estas informações devem ser armazenadas por um período de, no mínimo, doze meses, observando o disposto no Inciso III do art. 7º desta norma;

II - as ocorrências de mau uso do acesso aos recursos disponíveis na rede e sistemas corporativos não previstas nesta norma e os casos omissos serão encaminhados para a área responsável pela gestão de TI no âmbito do INSS para análise e pronunciamento;

III - identificada irregularidade de mau uso dos recursos de rede poderá ocorrer:

a) o bloqueio preventivo do acesso pela DTI, o encaminhamento de dossiê com as informações para a Corregedoria-Geral do INSS ou Corregedorias Regionais, nas suas áreas de abrangências, a fim de que seja realizada a análise no âmbito disciplinar; e

b) ressalta-se que o descumprimento dessa Norma poderá resultar em sanções administrativas, civis e criminais.

IV - esta norma deve ser revisada num período máximo de três anos.

ANEXO II

RESOLUÇÃO Nº 3/CEGOV/INSS, DE DE DE 2020

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF: _____, identidade _____, expedida pelo _____, em _____, e lotado no(a) _____ do Instituto Nacional do Seguro Social – INSS, DECLARO, sob pena das sanções cabíveis nos termos da Política de Segurança da Informação - POSIN do INSS que assumo a responsabilidade por:

I - tratar o(s) ativo(s) de informação como patrimônio do Instituto Nacional do Seguro Social;

II - utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do INSS;

III - contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que disciplina a gestão de segurança da informação na Administração Pública Federal, direta e indireta, e dá outras providências;

IV - utilizar as credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do INSS;

V - responder, perante o INSS, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

_____, _____ de _____ de _____

Assinatura do usuário

Nome do usuário:	Unidade de Lotação:
Nome da Autoridade Responsável pela Autorização do Acesso:	

Assinatura e Carimbo do Responsável pela Autorização de Acesso

ANEXO III

RESOLUÇÃO Nº 3/CEGOV/INSS, DE _____ DE _____ DE 2020

REGISTROS DE LOGS

1. Relação dos campos de registros de logs do GERID
 - 1.1. Dados Gerais
 - 1.1.1. Data
 - 1.1.2. Sistema
 - 1.1.3. Ambiente
 - 1.1.4. IP destino
 - 1.1.5. IP origem
 - 1.1.6. CPF usuário
 - 1.1.7. URL de origem
 2. Ações:
 - 2.1. CAS (autenticação): Central Authentication Service - Serviço Central de Autenticação
 - 2.1.1. Criação de service ticket (ST)
 - 2.1.2. Criação de ticket granting ticket (TGT)
 - 2.1.3. validação de ST
 - 2.1.4. Exclusão de ticket TGT
 - 2.1.5. Autenticação com sucesso (login+password)
 - 2.1.6. Autenticação com sucesso (certificado digital)
 - 2.1.7. Autenticação com falha
 - 2.2. GPA: Gerenciamento de Permissão de Acesso
 - 2.2.1. Início de sessão
 - 2.2.2. Dados do usuário em sessão (CPF, NOME, PAPEL)
 - 2.2.3. Requisição de logout
 - 2.2.4. Dados de credenciais
 - 2.2.5. Concessão de credenciais
 - 2.2.6. Alteração de Credenciais
 - 2.2.7. Dados de receptor (CPF, NOME, Lotação)
 - 2.2.8. Inserção de credencial no usuário
 - 2.2.9. Revogação de Credenciais
 - 2.2.10. Pesquisa de credenciais

- 2.2.11. Pesquisa de usuários
- 2.2.12. Substituição de gestor



INSTITUTO NACIONAL DO SEGURO SOCIAL
MINUTA DE RESOLUÇÃO

MINUTA DE RESOLUÇÃO

**RESOLUÇÃO Nº 4/CEGOV/INSS, DE DE
DE 2020**

Institui a Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR do Instituto Nacional do Seguro Social.

O **COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS**, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída a Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR do INSS.

Art. 2º Os Anexos a esta Portaria serão publicados em Boletim de Serviço.

Art. 3º Esta Portaria complementa Política de Segurança da Informação POSIN-INSS vigente.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretora de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **ALEXINALDO MESSIAS CERQUEIRA**, **Chefe de Serviço**, em 24/07/2020, às 18:35, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1328742** e o código CRC **3C0B39CB**.

ANEXO I

RESOLUÇÃO Nº 4/CEGOV/INSS, DE DE DE 2020
EQUIPE DE TRATAMENTO DE INCIDENTES DE REDES COMPUTACIONAIS - ETIR

Art. 1º Para os efeitos desta norma ficam estabelecidos os seguintes conceitos e definições:

I - agente responsável: Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

II - artefato malicioso: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

III - comunidade ou Público Alvo: é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

IV - CTIR GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI;

V - equipe de tratamento e resposta a incidentes em redes computacionais – ETIR: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

VI - incidente de segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VII - serviço: é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

VIII - tratamento de Incidentes de Segurança em Redes Computacionais: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

XI - usuário: pessoas que fazem uso de serviços de TI e sistemas de informação de propriedade do INSS, independente do cargo ocupado (contratados, consultores, conselheiros, servidores, temporários e etc); e

X - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou por uma organização, os quais podem ser evitados por uma ação interna de segurança da informação.

Art. 2º Esta norma tem a missão de:

Parágrafo único. Agir proativamente, receber, analisar, monitorar, coordenar e propor respostas a notificações e atividades relacionadas a incidentes de segurança da informação e comunicações no âmbito do Instituto.

Art. 3º Esta norma tem como público alvo:

I - a abrangência das atividades pertinentes à ETIR-INSS inclui os usuários dos serviços de Tecnologia da Informação - TI, e os sistemas de informação do INSS;

II - as atividades pertinentes à ETIR-INSS serão realizadas com intercâmbio de informações e em cooperação com as seguintes instâncias:

a) o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR GOV;

b) a Equipe de Resposta e Tratamento de Incidentes em Redes Computacionais – ETIR, de empresas prestadoras de serviços de tecnologia contratadas pelo Instituto;

c) equipes de tratamento de incidentes de redes computacionais dos demais órgãos, entidades e empresas, públicas ou privadas, que tenham contratos, acordos, convênios ou instrumentos congêneres com o INSS; e

d) o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República – GSI/PR.

Art. 4º a implementação e o funcionamento da ETIR-INSS seguirão a metodologia definida pelo Gabinete de Segurança Institucional da Presidência da República, conforme definido a seguir:

I - o modelo de implementação no qual a ETIR-INSS se baseia é o “Modelo 1 – Utilizando a equipe de Tecnologia da Informação”, conforme definido pelo GSI/PR;

II - a equipe será composta por profissionais da área de Tecnologia da Informação, lotados na Diretoria de Tecnologia da Informação e Inovação – DTI, sem prejuízo de suas atribuições típicas do cargo, com experiência e conhecimentos técnicos compatíveis com a importância da missão da ETIR-INSS;

III - a equipe será composta por servidores públicos efetivos;

IV - a ETIR-INSS ficará vinculada tecnicamente à Coordenação-Geral de Infraestrutura e Operações – CGIN, da Diretoria de Tecnologia da Informação e Inovação - DTI; e

V - o Coordenador da ETIR-INSS será nomeado por meio de ato do Diretor de Tecnologia da Informação e Inovação - DTI;

VI - Caso o Coordenador da ETIR-INSS não seja formalmente nomeado, as atribuições relacionadas à coordenação da equipe serão desempenhadas pelo Coordenador-Geral de Infraestrutura e Operações.

Art. 5º A ETIR-INSS será composta por membros:

I - permanentes: que efetivamente atuarão em todos os incidentes registrados;

II - colaboradores: que atuarão, de forma esporádica, no tratamento de incidentes relacionados às suas áreas de atuação; e

III - Opcionais: servidores das unidades descentralizadas sob supervisão da DTI.

IV - sendo assim, a ETIR-INSS será formada por servidores lotados na área de TI, de acordo com os papéis abaixo:

Quantidade	Papel	Setor
2	Permanente	Serviço de Segurança de TIC
2	Colaborador	Coordenação-Geral de Infraestrutura e Operações
2	Colaborador	Coordenação-Geral de Projetos e Soluções Digitais
2	Opcional	Unidades descentralizadas

V - Os membros da ETIR-INSS serão designados por meio de ato do Diretor de Tecnologia da Informação e Inovação.

Art. 6º Quanto autonomia da ETIR-INSS:

I - terá autonomia limitada para o tratamento de incidentes de Segurança da Informação, devendo implementar ações que possam impactar outras áreas do Instituto somente com anuência do Diretor de Tecnologia da Informação e Inovação e do gestor responsável pela área/sistema afetada; e

II - poderá, ainda, gerar relatórios técnicos sugerindo a adoção de medidas para resolução de incidentes.

Art. 7º A ETIR-INSS fornecerá o serviço de Tratamento de Incidentes de Segurança em Redes Computacionais:

I - este serviço compreende basicamente as seguintes ações:

- a) recepção: receber solicitações e alertas diversos. Para tanto o Instituto disponibilizará como canal de comunicação a caixa postal etir@inss.gov.br;
- b) filtrar: todo conteúdo direcionado para a ETIR deve ser verificado, a partir desta análise deve ser tratado pela equipe ou, não se tratando de um incidente de segurança em redes computacionais, encaminhado para a área competente;
- c) catalogar: os incidentes devem ser catalogados em ferramenta a ser indicada pela DTI, com nível de acesso restrito;
- d) classificar: os incidentes devem ser classificados quanto ao nível de severidade e impacto;
- e) tratar o incidente: indicar o tratamento do incidente com medidas corretivas e formas de se evitar que ocorra novamente;
- f) responder: as solicitações e alertas encaminhados para a ETIR devem ser devidamente respondidos; e
- g) monitorar: monitorar a aplicação do tratamento dos incidentes indicados.

II - a ETIR deve analisar os incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências; e

III - o detalhamento dos serviços prestados pela ETIR-INSS deve ser publicado em página específica da Intranet do Instituto no prazo de 30 dias a partir da publicação desta portaria.



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 5/CEGOV/INSS, DE DE DE 2020

Disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis Internet, competências e conteúdo de acesso para cada perfil.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída, nos termos do Anexo I desta Portaria, norma que estabelece critérios para uso da Internet no âmbito do Instituto Nacional do Seguro Social - INSS.

Art. 2º Os Anexos a esta Portaria serão publicados em Boletim de Serviço.

Art. 3º Esta Portaria complementa a Política de Segurança da Informação POSIN-INSS vigente.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretora de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **ALEXINALDO MESSIAS CERQUEIRA**, **Chefe de Serviço**, em 24/07/2020, às 18:36, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1329042** e o código CRC **C003C089**.

ANEXO I

RESOLUÇÃO Nº 5/CEGOV/INSS, DE DE DE 2020

NORMA DE USO DA INTERNET

Art. 1º Esta norma se aplica a todos os servidores e colaboradores, vinculados direta ou indiretamente ao INSS, bem como a servidores e empregados de entidades e órgãos da Administração Pública ou privadas que necessitem ou estejam autorizados a acessar a Internet a partir da rede corporativa do Instituto.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União – AGU que atuarem na consultoria e no assessoramento jurídico, e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta norma, ficam estabelecidos os seguintes conceitos e definições:

I - autorizador: ocupantes de cargos que serão responsáveis pela autorização da concessão de perfis de acesso para usuários finais de sua área de abrangência;

II - internet: é a rede mundial que interliga computadores de diferentes tipos e dimensões e permite a comunicação entre pessoas e organizações, independentemente da localização geográfica;

III - intranet: é a rede de computadores administrada pelo INSS, que utiliza os mesmos serviços e tecnologias disponíveis na rede mundial, podendo ser definida como um tipo de Internet Local do Instituto;

IV - perfil de acesso: atributo que estabelece as categorias de sítios acessíveis e tipos de arquivos que podem ser recebidos ou transmitidos pelos usuários;

V - proxy: desempenha a função de conexão do computador (local) à rede externa (Internet). Como os endereços locais do computador não são válidos para acessos externos, cabe ao proxy enviar a solicitação do endereço local para o servidor, traduzindo e repassando-a para o seu computador;

VI - sítio: um conjunto de informações ou serviços disponíveis na Internet ou na Intranet, organizados em páginas eletrônicas e acessíveis por meio de endereços que identificam, de forma padronizada, sua origem e conteúdo;

VII - usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal-APF, formalizada por meio da assinatura do Termo de Responsabilidade; e

VIII - VPN: Trata-se de uma Rede Privada Virtual (Virtual Private Network) construída sobre a infraestrutura de uma rede pública. Essa é uma forma de conectar dois computadores por meio de uma rede pública, como a Internet;

Art. 3º Essa norma tem como diretrizes:

I - o acesso à Internet disponibilizado pelo Instituto Nacional do Seguro Social aos usuários deve ser utilizado exclusivamente em razão de trabalho, cumprindo os procedimentos dispostos nesta norma;

II - os recursos disponibilizados pelo Instituto, não poderão ser usados para quaisquer propósitos que sejam ilegais ou proibidos, de modo a danificar, desativar, sobrecarregar ou prejudicar qualquer área, serviço ou conteúdo, ou interferir no uso e execução das atividades laborais de outros usuários;

III - o volume de tráfego de Internet e os endereços *web* visitados poderão ser monitorados, visando assegurar o cumprimento desta norma; e

IV - o acesso à Internet para propósitos particulares ou estranhos às atividades do INSS poderá ser bloqueado, sem prévia comunicação ao usuário e sem prejuízo das demais sanções aplicáveis.

Art. 4º Quando aos Perfis de Acesso:

I - o acesso aos sítios da Internet para todos os usuários será realizado mediante a atribuição de perfis de acesso;

II - o processo de solicitação e autorização de perfil de acesso à Internet do INSS compreenderá os seguintes perfis:

a) Perfil 1 - Perfil Restrito, deve ser inicialmente atribuído para usuários com maior restrição de acesso à internet, permitido acessar somente sítios governamentais, instituições bancárias e sítios considerados de interesse do INSS;

b) Perfil 2 - Perfil Básico, deve ser inicialmente atribuído para estagiários, recepcionistas e usuários externos. O usuário poderá acessar todos os sítios permitidos pelo Perfil 1, sítios de provedores de e-mail pessoal e instituições de ensino;

c) Perfil 3 - Perfil Padrão, para os servidores do quadro do Instituto. O usuário poderá acessar a todos sítios da internet sem a veiculação de material em áudio e vídeo; e

d) Perfil 4 - Perfil Avançado, deve ser atribuído preferencialmente para servidores do quadro do Instituto e estagiários que desempenham funções relacionadas à Comunicação Social, Desenvolvimento de Pessoas e gestores, respeitado o princípio da necessidade de conhecer, designados pelos Autorizadores deste perfil. O usuário poderá acessar todos os sítios da Internet, incluindo sítios que veiculam material em áudio e vídeo (*streaming*), sítios de compartilhamento de vídeos, blogs e redes sociais.

III - o perfil concedido a agentes externos é de caráter temporário, com validade equivalente à vigência do trabalho a ser executado;

IV - o processo de alterações, bloqueios, liberações e categorizações de sítios, assim como a criação e/ou alterações de perfis de acesso descritos nesta norma, quando necessários, serão definidos pela Diretoria de Tecnologia da Informação e Inovação – DTI, e publicado no Portal do INSS na Intranet; e

V - os novos usuários que não tiverem um perfil de acesso atribuído, devem ser direcionados para uma página da intranet contendo orientações e normas relacionadas ao acesso à internet no INSS, entre outras informações definidas pela DTI.

Art. 5º Acesso de Usuários Externos:

I - quanto ao acesso de servidores ou funcionários públicos externos:

a) o acesso à Intranet e Internet a partir da rede de dados corporativa, nas dependências do INSS, aos demais órgãos da Administração Pública Direta e Indireta, de qualquer das esferas de governo, será concedido exclusivamente para servidores e empregados públicos, efetivos ou ocupantes de cargo em comissão;

b) os acessos dos usuários externos das entidades que compõem o Poder Público serão concedidos mediante o estabelecimento de acordos ou convênios

específicos firmados com o INSS;

c) o gestor ou Coordenador-Geral da área responsável pelo convênio, contrato, ACT ou instrumento congênere, assumirá o papel de Autorizador do serviço de acesso à internet para usuários externos e deverá fundamentar as solicitações com base no instrumento; e

d) poderão ser concedidos acessos temporários para auditores de controle interno e externo, vinculados à Controladoria-Geral da União – CGU ou do Tribunal de Contas da União - TCU, no uso de suas atribuições.

II - quanto ao acesso de terceirizados:

a) o acesso à Internet por terceirizados deve ser provido pela empresa contratada;

b) em caráter de exceção, será concedido o acesso aos terceirizados a partir da infraestrutura de rede do INSS, desde que preenchidos os seguintes requisitos:

1. o contrato de prestação de serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

2. a empresa contratada deverá manter com seus funcionários Termo de Confidencialidade;

3. o contrato deve prever a necessidade de acesso à internet a partir das dependências do Instituto; e

4. o Autorizador, que para estes fins será o gestor do contrato ou o responsável pela área requisitante do serviço, deverá fundamentar as necessidades de acesso do contratado, definindo os recursos que devem ser disponibilizados, endereços da Intranet e Internet necessários para o desenvolvimento das atividades, bem como eventuais restrições a dias e horários para realização do acesso.

III - quanto ao acesso de visitantes:

a) a conexão de equipamentos pessoais à rede do Instituto, quando necessária e motivada pelo interesse da Administração, deve ser previamente autorizada pelo gestor da unidade onde o equipamento será utilizado;

b) só será permitida a utilização da rede local por equipamentos que atendam a todos os requisitos estabelecidos pela DTI; e

c) o acesso se dará, exclusivamente, à Internet, sendo vedado o acesso ao conteúdo disponibilizado na intranet.

Art. 6º A todos os perfis de acesso descritos nesta norma aplicam-se as restrições de acesso a sítios que:

I - contenham material pornográfico ou obsceno;

II - contenham material ilegal;

III - disponibilizem jogos, inclusive os da Internet (online);

IV - contenham material impróprio, ofensivo, preconceituoso ou discriminatório, que façam apologia à violência, ao terrorismo e às drogas; e

V - contenha e/ou divulgue conteúdo de violação de direito autoral (pirataria) e/ou execução de quaisquer tipos ou formas de fraudes.

Art. 7º Quanto ao processo de atribuição de acesso à Internet:

I - a atribuição dos perfis de acesso à Internet serão feitas pelos Autorizadores, de forma fundamentada respeitando o princípio da necessidade de conhecer, de acordo com a tabela abaixo:

Perfil	Autorizador
Perfil 1, 2 e 3	Gerente de APS, Gerente Executivo, Superintendentes Regionais, Procuradores Regionais, Coordenadores-Gerais, Superintendentes Regionais, Presidente do INSS, Auditor-Geral, Coordenadores-Gerais, Corregedoria-Geral, Procurador-Chefe da PFE-INSS, Diretores, Gestor ou chefe da área responsável pelo Contrato ou ato administrativo similar no âmbito do INSS.
Perfil 4	Chefes de Assessoria de Comunicação Social nas Superintendências Regionais, Assessor de Comunicação Social (Administração Central), Diretor de Tecnologia da Informação e Inovação, Diretor de Gestão de Pessoas e Administração e Presidente do INSS.

II - nos casos de novos usuários de rede (LDAP), criados por meio de registro de chamado técnico, quando o solicitante não indicar o perfil de acesso à internet, será atribuído o Perfil 1;

III - para proceder a alteração do perfil de acesso, os usuários deverão preencher “Formulário de Acesso à Internet” (Anexo II) e providenciar a assinatura pelo Autorizador do acesso; e

IV - ao registrar a solicitação, deve-se anexar o Formulário de Solicitação de Acesso à Internet devidamente preenchido e assinado (pelo solicitante e Autorizador), conforme documento nato digital ou digitalizado no formato PDF.

Art. 8º A solicitação para perfis de acesso em caráter temporário devem indicar no Formulário de Solicitação de Acesso à Internet, a motivação da necessidade e a data de expiração do acesso.

Art. 9º Responsabilidades:

I - o usuário deve:

- a) preencher os requisitos e termos estabelecidos nesta norma;
- b) estar devidamente autorizado a utilizar a Internet nas formas estabelecidas nesta norma;
- c) fazer uso da Internet de forma responsável e segura, utilizando o acesso exclusivamente em razão de trabalho, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal; e
- d) impedir a divulgação e compartilhamento das chaves de segurança atribuídas, que são pessoais e intransferíveis.

II - o autorizador deve:

- a) conceder os perfis de acesso à internet rigorosamente de acordo com as atribuições dos usuários de sua abrangência, observando os normativos do INSS;
- b) verificar periodicamente o uso dos acessos concedidos e, sempre que necessário, solicitar alteração dos perfis de acesso dos usuários de sua abrangência; e
- c) reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à equipe de tratamento de incidentes de rede do INSS.

III - a área responsável pela gestão de TI no INSS deve:

- a) monitorar os acessos à internet e sua utilização de acordo com as diretrizes estabelecidas nesta norma; e
- b) identificar os casos de mau uso da Internet e adotar uma ou mais das seguintes providências:
 - 1. alertar ao usuário, responsável pelo acesso, e ao Autorizador, responsável pela concessão, acerca do uso indevido da internet;
 - 2. nos casos de reincidência, solicitar a revogação do acesso à internet concedido ao usuário; e
 - 3. encaminhar a documentação que comprova a má utilização do acesso concedido para Corregedoria do INSS, para análise e adoção das medidas cabíveis.

Art. 10º As seguintes práticas configuram-se como uso indevido da internet:

I - acessar a internet disponibilizada pelo Instituto sem estar devidamente autorizado, conforme estabelecido nesta norma;

II - não manifestar concordância com as regras estabelecidas nesta norma e nas demais aplicáveis;

III - fazer uso dos recursos de Internet disponibilizado pelo Instituto para fins alheios ao trabalho, em discordância com os procedimentos dispostos nesta norma, sem prejuízo de demais normatizações vigentes na Administração Pública Federal;

IV - utilizar os serviços extrapolando os privilégios do perfil de acesso que lhe foi designado;

V - divulgação e compartilhamento das chaves de segurança, que são pessoais e intransferíveis, permitindo a utilização por terceiros do perfil que lhe foi atribuído;

VI - praticar atos de comercialização de produtos e serviços, em proveito próprio ou de terceiros, que não atendam os interesses do INSS;

VII - utilizar recursos ou dispositivos para acesso a computadores ou redes externas ao Instituto, com o objetivo de obter informações não autorizadas ou provocar a interrupção de serviços de rede;

VIII - utilizar modem ou dispositivo de rede que interligue a rede interna do INSS a outras redes ou à Internet;

IX - a exposição, o armazenamento, a distribuição, a edição, a gravação e o compartilhamento, através do uso dos recursos computacionais e de comunicação do INSS, de arquivos estranhos às atividades do Instituto e não autorizados pela chefia imediata;

X - realizar qualquer atividade que apoie ou facilite os vazamentos de dados;

XI - baixar arquivos ou programas da Internet que contrariem as diretrizes da Política de Segurança da Informação - POSIN vigente; e

XII - utilizar *proxy* não disponibilizado pelo INSS.

Art. 11 O acesso à Internet é passível de registro e monitoração, incluindo quaisquer dados transmitidos pela rede do INSS.

Art. 12 Disposições Gerais:

I - em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a ETIR deverá ser imediatamente acionada, para tomar as providências necessárias a fim de sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação do INSS;

II - as ocorrências de mau uso do acesso à internet não previstas nesta norma, assim como os casos de dúvidas em relação à aplicação das disposições aqui estabelecidas, devem ser encaminhadas à DTI para registro, análise e avaliação da necessidade de alterações de acordo com o processo de governança em vigência no Instituto;

III - o descumprimento desta norma, poderá acarretar ao usuário as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei, responsabilidade administrativa, civil e criminal; e

IV - esta norma deve ser atualizada periodicamente, não excedendo o prazo máximo de 3 anos.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

DESPACHO

Diretoria De Tecnologia da Informação e Inovação, em 24/07/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Solicita ajuste nas
normas de segurança da
informação apresentadas
na Reunião Ordinárias
CEGOV nº 6/2020.

1. Em atenção ao Despacho CEGOV (SEI 1322316), informa-se que os ajustes nos normativos de Segurança da Informação solicitados a partir da 6ª Reunião Ordinária do CEGOV foram efetuados, conforme Despacho SSEG (SEI 1326078).
2. Encaminha-se o presente ao Comitê Estratégico de Governança - CEGOV, com ciência ao Comitê Temático de Governança Digital - CTGD, para prosseguimento do processo.

CLAUDIO AUGUSTO NOVAIS FERRAZ

Diretor de Tecnologia da Informação e Inovação - Substituto



Documento assinado eletronicamente por **Claudio Augusto Novais Ferraz, Diretor(a) de Tecnologia da Informação e Inovação Substituto(a)**, em 24/07/2020, às 19:39, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site
https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1331599** e o código CRC **2A1A80F7**.



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria De Integridade, Governança e Gerenciamento De Riscos
Comitê Estratégico de Governança

DESPACHO

Comitê Estratégico de Governança, em 03/08/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO, COMITÊ
ESTRATÉGICO DE
GOVERNANÇA

Ass.: Ajuste nas normas
de segurança da
informação apresentadas
na Reunião Ordinárias
CEGOV nº 6/2020.

1. Trata-se dos normativos para instituição de políticas e normas de segurança da informação do Instituto Nacional do Seguro Social - INSS (documentos SEI nº 1249859, 1249899, 1250265 e 1253280) que foram discutidos na 6ª Reunião Ordinária do Comitê Estratégico de Governança - CEGOV, realizada no dia 22/07/2020 (Processo SEI nº 35014.164930/2020-78).
2. Tendo em vista o término do prazo para encaminhamento de sugestões por parte dos membros do CEGOV, conforme acordado na 6ª Reunião do CEGOV, registra-se que não houveram manifestações dos integrantes do CEGOV para ajustes nas normas.
3. Encaminhe-se os autos à Diretoria de Tecnologia da Informação e Inovação para demais providências.

RENATO DO CARMO DAS NEVES ALVES
Coordenador-Geral de Governança - Substituto
Secretaria-Executiva do Comitê Estratégico de Governança



Documento assinado eletronicamente por **RENATO DO CARMO DAS NEVES ALVES, Técnico do Seguro Social**, em 03/08/2020, às 10:55, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1381491** e o código CRC **A23A31A7**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1381491



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações

DESPACHO

Coordenação-Geral De Infraestrutura e Operações, em 03/08/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Solicita ajuste nas
normas de segurança da
informação apresentadas
na Reunião Ordinárias
CEGOV nº 6/2020.

1. Ciente do Despacho CEGOV (SEI 1381491).
2. Encaminha-se para o Serviço de Segurança em Tecnologia da Informação (SSEG) a fim de atualizar nomenclatura da ETIR nas minutas em conformidade com a IN nº 02, de 24 de julho de 2020, do GSI/PR, e disponibilizar no presente processo a versão final das minutas.

CLAUDIO AUGUSTO NOVAIS FERRAZ

Coordenador-Geral de Infraestrutura e Operações



Documento assinado eletronicamente por **Claudio Augusto Novais Ferraz, Coordenador(a) Geral**, em 03/08/2020, às 18:54, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1384034** e o código CRC **66D603DF**.



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações
Coordenação De Suporte e Infraestrutura De Tecnologia da Informação e Comunicação
Serviço De Segurança em Tecnologia da Informação e Comunicação

DESPACHO

Serviço De Segurança em Tecnologia da Informação e Comunicação, em 04/08/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Solicita ajuste nas
normas de segurança da
informação apresentadas
na Reunião Ordinárias
CEGOV nº 6/2020.

1. Trata-se de proposta de normativos para instituição de políticas e normas de segurança da informação do Instituto Nacional do Seguro Social - INSS (documentos SEI nº 1249859, 1249899, 1250265 e 1253280) que foram discutidos na 6ª Reunião Ordinária do Comitê Estratégico de Governança - CEGOV, realizada no dia 22/07/2020 (Processo SEI nº 35014.164930/2020-78).
2. Retornam os autos ao Serviço de Segurança em Tecnologia da Informação - SSEG, para que sejam procedidas as atualizações necessárias para adequação, da documentação sob análise, às diretrizes estabelecidas pela IN nº 02, de 24 de julho de 2020, publicada pelo Gabinete de Segurança Institucional da Presidência da República - GSI/PR, e para que sejam disponibilizadas no presente processo as versões finais das minutas.
3. Informo que este SSEG, promoveu as alterações necessárias, para adequação à norma supracitada, nos normativos propostos. E que versões atualizadas das minutas foram acostadas ao presente processo (documentos SEI nº 1391885, 1392067, 1392184 e 1394150).
4. Encaminhe-se, em devolução, à Coordenação-Geral de Infraestrutura e Operações - CGIN, para análise e providências.

ALEXINALDO MESSIAS CERQUEIRA

Chefe do Serviço de Segurança em Tecnologia da Informação e Comunicação



Documento assinado eletronicamente por **ALEXINALDO MESSIAS CERQUEIRA, Chefe de Serviço**, em 04/08/2020, às 12:58, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1391862** e o código CRC **263F2E01**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1391862



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 2/CEGOV/INSS, DE DE DE 2020

Atualiza a Política de Segurança da Informação do Instituto Nacional do Seguro Social

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída no âmbito do INSS e nos termos do Anexo a esta Resolução, a Política de Segurança da Informação POSIN-INSS.

Art. 2º Esta Resolução entra em vigor na data de sua publicação e seu Anexo será publicado em Boletim de Serviço.

Art. 3º Fica revogada a Resolução nº 672/PRES/INSS, de 27 de dezembro de 2018.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretora de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por ALEXINALDO MESSIAS CERQUEIRA, Chefe de Serviço, em 04/08/2020, às 12:58, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador 1391885 e o código CRC 510F9405.

ANEXO I

RESOLUÇÃO Nº 2/CEGOV/INSS, DE DE DE 2020

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO INSTITUTO NACIONAL DO SEGURO SOCIAL – POSIN-INSS .

Art. 1º A Política de Segurança da Informação do Instituto Nacional do Seguro Social – POSIN-INSS, tem por objetivo estabelecer e difundir diretrizes e princípios de Segurança da Informação – SI, com vistas à orientação para uso e proteção adequados das informações produzidas e custodiadas pelo Instituto, preservando sua disponibilidade, integridade, confidencialidade e autenticidade.

Parágrafo único. A Política de que trata o caput e suas normas complementares aplicam-se a todos os agentes públicos que têm vínculo direto e/ou indireto com o Instituto.

Art. 2º Para os efeitos da POSIN-INSS, entende-se:

I - agente público: Todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da APF, direta e indireta;

II - atividade crítica - atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo;

III - ativos de informação: meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV - dados processados: dados submetidos a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação;

V - gestor de Segurança da Informação: é o responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da APF;

formato; VI - Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou

VII - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

VIII - necessidade de conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

IX - riscos de segurança da informação: potencial associado à exploração de uma ou mais vulnerabilidades nos ativos de informação, em razão de ameaças, com impacto negativo às atividades do Instituto;

X - segurança da informação – SI: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e autenticidades das informações;

XI - vínculo direto: agentes públicos contratados diretamente pelo INSS;

XII - vínculo indireto: agentes privados ou públicos pertencentes a órgãos ou unidades da Administração Pública Federal, Estadual ou Municipal que mantenham contrato, convênio, acordo de cooperação técnica ou instrumento congêneros com o INSS; e

Art. 3º Esta POSIN-INSS foi elaborada com base nos seguintes documentos:

I - Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;

II - Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto na Constituição Federal;

III - Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

IV - Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais;

V - Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

VI - Decreto nº 7.724, de 16 de maio de 2012, regulamenta a Lei nº 12.527, de 18 de novembro de 2011;

VII - Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

VIII - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

IX - Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

X - Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que disciplina a gestão de segurança da informação na Administração Pública Federal, direta e indireta, e dá outras providências;

XI - Instruções normativas relacionadas à segurança da informação, publicadas pelo Gabinete de Segurança Institucional da Presidência da República;

XII - Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação;

XIII - NBR ISO/IEC 27002:2013, que institui código de melhores práticas para a Gestão de Segurança da Informação;

Art. 4º Esta POSIN-INSS foi elaborada com base nos seguintes princípios:

I - a preservação da imagem do Instituto e de seus agentes públicos;

II - a salvaguarda das informações do cidadão;

III - ações de segurança orientadas pela gestão de riscos;

IV - continuidade assegurada dos serviços ao cidadão;

V - o alinhamento com a missão institucional e seu planejamento estratégico; e

VI - respeito à natureza e finalidade de cada área do Instituto.

Art. 5º São diretrizes gerais da POSIN-INSS:

I - Tratamento da Informação:

- a) toda informação produzida pelos agentes públicos, no exercício de suas atividades, é de propriedade do INSS e deve ser protegida;
- b) informações produzidas, armazenadas e tratadas pelo Instituto, especialmente as informações pessoais e custodiadas, devem receber o devido tratamento para assegurar sua proteção durante todo o ciclo de vida; e
- c) somente os canais de comunicação disponibilizados pelo INSS devem ser utilizados para trafegar informações institucionais.

II - Tratamento de Incidentes de Segurança da Informação (SI):

- a) todo incidente de segurança da informação deve ser imediatamente relatado à área responsável pela gestão de segurança da informação de TI, observando-se a apropriada coleta de evidências.

III - Gestão de Riscos de Segurança:

- a) os riscos de segurança da informação devem ser identificados e tratados; e
- b) os critérios para a gestão de risco devem ser definidos e comunicados a toda instituição.

IV - Gestão de Continuidade:

- a) os ativos de informação que suportam as atividades críticas do Instituto devem ser suportados por ambiente de alta disponibilidade e ter capacidade de recuperação em prazos e condições previamente definidos para situações de contingência, em conformidade com o processo de continuidade; e
- b) a continuidade das operações e serviços de Tecnologia da Informação – TI, deve estar prevista nos contratos, assim como os prazos e condições devem estar formalmente estabelecidos.

V - Controles de Acesso:

- a) todo acesso à informação deve ser motivado pela necessidade de conhecer;
- b) os sistemas de informação e as instalações físicas devem ter capacidade de controlar os acessos, com fins de responsabilização pelo seu uso; e
- c) as autorizações de acesso às informações, sistemas e instalações físicas devem ter critérios de acesso definidos e divulgados a todos da instituição.

VI - Recursos Computacionais:

a) correio eletrônico:

- 1. o correio eletrônico, *e-mail*, é uma forma de comunicação oficial e deve ser utilizado exclusivamente no desempenho das atividades funcionais; e
- 2. ao produzir, responder ou encaminhar mensagem em caixa de correio eletrônico institucional, o servidor deverá se identificar, subscrevendo, ao menos, seu nome, cargo e telefone de contato institucional.

b) Acesso à Internet:

- 1. o acesso à Internet, por meio da rede de dados do INSS, é uma concessão e deve ter seu uso orientado para a execução das atividades do Instituto; e
- 2. os acessos serão liberados de acordo com perfis previamente definidos pelo órgão responsável pelos serviços de TI.

c) Gestão de Mudanças de TI:

- 1. toda mudança nos sistemas de informação do INSS deve ser previamente e formalmente autorizada; e
- 2. a gestão de mudanças deve prever, no mínimo, a guarda dos registros, realização de testes e a possibilidade de recuperação do ambiente.

d) Computação em Nuvem:

- 1. o ambiente de computação em nuvem, sua infraestrutura e canal de comunicação devem estar aderentes às diretrizes e normas de SI, estabelecidas pelo instituto, e às legislações vigentes.

2. o contrato de prestação de serviço, quando for o caso, deverá conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço.

VII - Educação e Conscientização:

- a) esta Política e seus normativos complementares devem ser periodicamente divulgados a todos os agentes públicos do Instituto;
- b) o Instituto deve manter programa contínuo de conscientização dos agentes públicos em Segurança da Informação— SI; e
- c) deve ser mantido plano de capacitação especializado aos profissionais que atuam na gestão de SI.

VIII - Auditoria e Conformidade:

- a) o cumprimento desta Política e de suas normas complementares deve ser avaliado periodicamente, por meio de verificações de conformidade; e
- b) o uso dos recursos de TI disponibilizados pelo Instituto é passível de monitoramento e auditoria.

IX - Responsabilidade pela gestão das informações:

- a) Os responsáveis pela gestão dos ativos da informação e sistemas corporativos devem descrever os requisitos de segurança;
- b) Os sistemas de informação devem ser concebidos possibilitando a segregação de funções.

X - Segurança física e do ambiente:

- a) As instalações em que as informações críticas ou sensíveis serão processadas deverão ser mantidas em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção física;
- b) Os ativos da organização devem ser protegidos contra acesso físico não autorizado, danos, perdas, furto e interferência. As proteções devem estar alinhadas aos riscos identificados.

XI - Gestão de ativos da informação

- a) os ativos de informação devem:

- 1. ser inventariados e protegidos;
- 2. ter identificados os seus proprietários e custodiantes;
- 3. ter a sua entrada e saída nas dependências do Instituto autorizadas e registradas por autoridade competente;
- 4. ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 6º A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas, cíveis e penais, previstas na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), no Código Penal, no Código Civil, e, ainda, em legislação que regule ou venha regular a matéria.

Art. 7º Competências e Responsabilidades:

I - Cabe ao Gestor de Segurança da Informação:

- a) promover cultura de segurança da informação;
- b) acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
- c) propor os recursos necessários à implementação das ações de SI;
- d) coordenar o CSI ou estrutura equivalente;
- e) acompanhar os trabalhos e a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR-INSS;
- f) propor o detalhamento das diretrizes desta Política, por meio de normas e procedimentos, e acompanhar sua implementação;

- g) assessorar a alta administração na implementação da Política de Segurança da Informação;
- h) estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;
- i) promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no INSS;
- j) incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;
- k) verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;
- l) acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e
- m) manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

II - Cabe ao Presidente do Instituto nomear o Gestor de SI;

III - Caso o Gestor de SI não seja nomeado, as atribuições relacionadas no art. 7º inciso I serão desempenhadas pelo Diretor de Tecnologia da Informação e Inovação;

IV - A ETIR-INSS deve analisar e propor respostas a notificações e atividades relacionadas a incidentes de SI, no âmbito do Instituto; e

V - É responsabilidade de todos os agentes públicos, diretos e indiretos, conhecer e cumprir as diretrizes desta Política e demais normas e procedimentos complementares de SI;

VI - Tendo em vista o Sistema de Governança do INSS, instituído pela Portaria nº 3.213/PRES/INSS/2019, compete ao Comitê Estratégico de Governança - CEGOV - deliberar sobre políticas e normas de segurança da informação, assessorado pelo Comitê Temático de Governança Digital.

Parágrafo único. O Comitê Temático de Gestão da Informação é responsável pela aprovação de procedimentos e de normas internas que orientem o compartilhamento de dados sob gestão do INSS e pela aprovação da categorização dos níveis de compartilhamento de dados com outras entidades públicas (federais ou de outras esferas e poderes) da sociedade civil (Vide atribuições do CTGI, no Art. 6º do Anexo da Portaria nº 3.213/PRES/INSS/2019).

Art. 8º Esta Política e seus normativos devem ser revisados sempre que necessário, não excedendo o período máximo de três anos.



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 3/CEGOV/INSS, DE DE DE 2020

Define regras para a emissão de credenciais de acesso lógico no âmbito do INSS

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída a Norma de Controle de Acesso Lógico - NCAL, do Instituto Nacional do Seguro Social – INSS.

Art. 2º Esta Resolução, bem como seus anexos, serão publicados em Boletim de Serviço, nos termos do Inciso I do Art. 16, da Resolução n.708/INSS/PRES, de 6 de novembro de 2019.

Art. 3º Revogar a RESOLUÇÃO Nº 413/PRES/INSS, DE 20 DE MAIO DE 2014.

Art. 4º Esta Resolução entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretora de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por ALEXINALDO MESSIAS CERQUEIRA, Chefe de Serviço, em 04/08/2020, às 12:58, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador 1392067 e o código CRC 59B66EB9.

ANEXO I

RESOLUÇÃO Nº 3/CEGOV/INSS, DE DE DE 2020

NORMA DE CONTROLE DE ACESSO LÓGICO – INSS

Art. 1º Os termos definidos nesta norma aplicam-se a todos os agentes públicos e privados com vínculo direto ou indireto, permanente ou temporário com o INSS.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União – AGU que atuarem na consultoria e no assessoramento jurídico, e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta Norma de Controle de Acesso Lógico são estabelecidos os seguintes conceitos e definições:

I - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

II - administrador de Domínio: Usuário responsável pela administração de um domínio por meio da aplicação de políticas globais, criação, edição e exclusão de usuários e grupos, e instalação de programas em um grande número de estações de trabalho;

III - administrador Local: Usuário responsável pela administração de partes de um domínio (geralmente restrito a um setor ou abrangência), por meio de políticas locais, edição de grupos e usuários locais, e instalação de programas em estações de trabalho limitadas a um setor ou abrangência;

IV - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta;

V - ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VI - contas de serviço: contas de acesso à rede corporativa de computadores, necessárias para a execução de procedimentos automáticos (aplicação, script, etc) sem qualquer intervenção humana no seu uso;

VII - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais;

VIII - credenciamento: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer;

IX - credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física, como crachá, cartão e selo ou lógica como identificação usuário e senha;

X - dado: Sugestão de Alteração "O dado é um elemento informativo concreto e sua forma plural expressa uma informação" é o registro do atributo de um ente objeto ou fenômeno onde registro indica o ato de registrar, ou seja, é a gravação ou a impressão de caracteres ou símbolos que tenham um significado em algum documento ou suporte físico;

XI - domínio: agrupamento lógico de computadores em rede que compartilham recursos em um banco de dados de segurança, comum, onde a administração e autenticação são centralizadas. Desta forma um usuário precisa de uma conta para ter acesso ao domínio e aos recursos compartilhados;

XII - endereço IP: conjunto de elementos numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores. Sequência de números associada a cada computador conectado à Internet. No caso de IPv4, o endereço IP é dividido em quatro grupos, separados por "." e compostos por números entre 0 e 255. No caso de IPv6, o endereço IP é dividido em até oito grupos, separados por ":" e compostos por números hexadecimais (números e letras de "A" a "F") entre 0 e FFFF;

XIII - entidade externa: Organização governamental, não governamental ou privada amparada por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica ou instrumento congênera com o INSS;

XIV - e-SIC: Sistema Eletrônico do Serviço de Informações ao Cidadão, aplicação disponibilizada na internet, que centraliza todos os pedidos de informações dirigidos ao Poder Executivo Federal;

XV - estagiário: educando que esteja frequentando o ensino regular, em instituições de educação superior, de educação profissional, de ensino médio, de educação especial e dos anos finais do ensino fundamental, na modalidade profissional da educação de jovens e adultos, que desenvolve as atividades relacionadas à sua área de formação profissional junto as pessoas Jurídicas de Direito Privado, órgãos da Administração Pública e Instituições de Ensino, que tenham condições de proporcionar experiência prática na sua linha de formação;

XVI - estágio Supervisionado: ato educativo escolar supervisionado, desenvolvido no ambiente de trabalho, que visa a preparação para o trabalho produtivo de educandos;

XVII - ferramenta de gestão de acessos: Software que possibilita a gestão integrada de papéis e permissões de acesso dos usuários nos sistemas corporativos;

XVIII - gestor da informação: usuário que gerou a informação, que responde pelo seu conteúdo ou que foi formalmente designado para definir, alterar a sua classificação nos graus de sigilo e perfil de acesso dos demais usuários e processos;

XIX - gestão de identidades: Combinação de sistemas técnicos, regras e procedimentos que definem a posse, utilização e segurança de uma identidade. Seu objetivo primário é estabelecer a confiança na associação de atributos a uma identidade digital e conectar esta identidade com uma entidade individual;

XX - Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXI - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

XXII - Log ou Registro de Auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional;

XXIII - necessidade de conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

XXIV - perfil de Acesso do Usuário: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

XXV - recursos de rede: Dispositivos (impressoras, scanners, multifuncionais, etc) ou serviços (sistemas, portais, etc) disponibilizados para os usuários por meio de uma rede de dados;

XXVI - serviço de diretório: serviço que armazena e organiza informações relativas a recursos disponíveis e usuários de uma rede de dados. Permite que o

administrador da rede gerencie o acesso de usuários e sistemas aos recursos disponíveis;

XXVII - sistemas corporativos: sistemas de operação, ou finalísticos, que se coadunam com os fins da Previdência Social. Assim, entende-se que este conceito comporta o conjunto de sistemas e subsistemas que garantem a operação dos regimes geral e próprio de previdência social, inclusive de previdência complementar;

XXVIII - sistemas legados: compreendem o conjunto de aplicações desenvolvidas com tecnologias obsoletas que permanecem em operação no INSS;

XXIX - usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal-APF, formalizada por meio da assinatura do Termo de Responsabilidade;

XXX - usuário interno: servidor do quadro do INSS lotado em uma Unidade Orgânica – UO, que se utiliza dos sistemas corporativos do Instituto;

XXXI - usuário externo: usuários vinculados a uma Entidade Externa, que se utiliza dos sistemas corporativos do Instituto por meio de um perfil de acesso concedido por um Gestor de Acesso Externo;

Art. 3º São diretrizes desta NCAL-INSS:

I - o acesso à rede e aos sistemas corporativos do INSS dar-se-á por meio de autenticação integrada de domínio baseado em serviço de diretório, administrado por meio de uma ferramenta de gestão de identidades;

II - as concessões de acesso à rede de dados e aos sistemas corporativos são distintas. Sendo assim, o usuário pode obter permissão de acesso apenas à rede de dados, ou apenas a determinado(s) sistema(s) corporativo(s);

III - as credenciais de acesso a rede de dados e aos sistemas corporativos do INSS são conferidas aos usuários com base na necessidade de conhecer, para viabilizar o exercício de suas atribuições funcionais e atividades a serem desenvolvidas no âmbito do INSS; e

IV - o uso indevido de informações dos sistemas corporativos do INSS sujeitará o agente às penalidades previstas na legislação.

Art. 4º Base Cadastral:

I - as bases de dados do Serviço de Diretórios (acesso à rede de dados), do Sistema de Gestão de Acessos (sistemas corporativos) e sistemas legados devem ser alimentadas por informações disponibilizadas pelo INSS;

II - para tanto, a área responsável pela gestão de pessoas do INSS disponibilizará semanalmente as informações extraídas do Sistema Integrado de Administração de Recursos Humanos – SIAPE para a empresa prestadora de serviços tecnológicos contratada pelo Instituto, com a supervisão da área de gestão de TI do INSS, contendo, minimamente, os seguintes dados:

Tabela 1: Informações Usuários

Item	Informação	Campo	Descrição
1	GR-MATRICULA	N 0012	GRUPO NUMÉRICO COMPOSTO DE NÚMERO DO ÓRGÃO (N0005) E NÚMERO DE MATRÍCULA DO SERVIDOR (N0007)
2	IT-NU-IDEN-SERV-ORIGEM	A 0008	NÚMERO DE IDENTIFICAÇÃO DO SERVIDOR NA ORIGEM - NÚMERO VINCULADO AO CARGO EFETIVO OU EM COMISSÃO
3	IT-NO-SERVIDOR	A 0060	NOME
4	IT-DA-NASCIMENTO	N 0008	DATA DE NASCIMENTO
5	IT-NU-CPF	N 0011	NÚMERO DO CPF
6	IT-NU-PIS-PASEP	N 0011	NÚMERO DO PIS
7	IT-IN-SUPRESSAO-PAGAMENTO	A 0001	INDICATIVO DE SUPRESSÃO DE PAGAMENTO
8	IT-CO-SITUACAO-SERVIDOR	N 0002	CÓDIGO DE SITUAÇÃO FUNCIONAL DO SERVIDOR
9	IT-CO-GRUPO-OCOR-AFASTAMENTO	N 0002	CÓDIGO DE OCORRÊNCIA DE AFASTAMENTO
10	IT-DA-INICIO-OCOR-AFASTAMENTO	N 0008	DATA DO INÍCIO DA OCORRÊNCIA DE AFASTAMENTO
11	IT-DA-TERMINO-OCOR-AFASTAMENTO	N 0008	DATA DE TÉRMINO DA OCORRÊNCIA DE AFASTAMENTO
12	IT-CO-GRUPO-OCOR-EXCLUSAO	N 0002	CÓDIGO DE OCORRÊNCIA DE EXCLUSÃO
13	IT-CO-UORG-LOTACAO-SERVIDOR	N 0009	CÓDIGO DA UORG DE LOTAÇÃO DO SERVIDOR

14	IT-CO-ORGAO-REQUISITANTE	N 0005	CÓDIGO DO ÓRGÃO REQUISITANTE

III - a Diretoria de Tecnologia da Informação e Inovação procederá com a atualização das bases cadastrais do serviço de diretórios e dos sistemas corporativos, bem como realizará a validação das informações disponibilizados pelo INSS por meio de outras bases, na periodicidade do envio das informações; e

IV - a área responsável pela gestão de pessoas do INSS poderá acordar, com a área responsável pela gestão de TI do INSS, a revisão das informações necessárias à administração de contas de usuários.

Art. 5º Credenciais e perfis de acesso:

I - a emissão de uma credencial permite ao usuário acessar a rede de dados corporativa do INSS. Para que o mesmo obtenha acesso aos sistemas corporativos a credencial deve ser associada a um perfil de acesso;

II - o processo de credenciamento de usuário aos ativos de informação deve ser feito observando os seguintes critérios:

a) a credencial de acesso concedida para acesso à rede de dados e sistemas corporativos do INSS é de caráter pessoal e intransferível;

b) as credenciais de acesso devem ser concedidas após a data de contratação ou entrada em exercício do usuário; e

c) as mesmas credenciais de acesso devem ser utilizadas para o acesso à rede de dados e aos sistemas corporativos do INSS, mediante autenticação que permita ao usuário acessar vários sistemas, por meio de ferramenta de gestão de identidades e acessos.

III - a área responsável pela gestão de pessoas do INSS deverá utilizar os canais de atendimento disponibilizados pela empresa prestadora de serviços tecnológicos contratada pelo Instituto, ou outro canal informado pela DTI, para:

a) solicitar o credenciamento de usuários do quadro de pessoal do INSS na data do ato administrativo de retorno ou ingresso no órgão, para acesso à rede, e de estagiários, após assinatura do contrato de prestação de serviço, para acesso à rede;

b) solicitar a revogação de credenciais de acesso de servidores do quadro de pessoal do INSS cedidos a outros órgãos;

c) solicitar a desativação de usuários do quadro de pessoal do INSS na data do ato administrativo ou de ocorrências que ensejem desligamento para fins de acesso lógico; e

d) solicitar a desativação do acesso de usuários do quadro de pessoal em atividade do INSS afastados ou com licença programada de suas funções por mais de sessenta dias ininterruptos;

IV - quanto ao processo de formação das credenciais de acesso fica estabelecido que:

a) o nome do usuário será composto de acordo com os padrões estabelecidos no Guia de Interoperabilidade do Governo Eletrônico – e-Ping, mais especificamente no documento “Caixas Individuais-Fundacionais no Governo Federal” (Rede do Governo, 2010) que define regras de formação de nomes para a composição de endereços eletrônicos;

b) quanto às senhas de acesso:

1. deverão ter no mínimo oito caracteres e conter, obrigatoriamente, caracteres alfanuméricos (combinação de letras e números). O usuário poderá acrescentar caracteres especiais (espaços em branco, símbolos, sinais de pontuação, etc);

2. é vedada a reutilização das últimas quatro senhas utilizadas pelo usuário;

3. podem ser alteradas sempre que preciso ou quando o usuário achar necessário;

4. o prazo de validade não deve ultrapassar noventa dias; e

5. o usuário receberá por meio de comunicado direto (via interface do sistema ou por mensagem no correio eletrônico) a informação do prazo próximo de vencimento da senha, quando esta estiver a 15 dias da sua data de expiração.

V - os perfis de acesso aos sistemas corporativos deverão contemplar um conjunto de permissões e ações vinculadas às atividades desenvolvidas pelo usuário;

VI- caberá à área responsável pela gestão de TI do INSS estabelecer, em conjunto com as áreas responsáveis pela gestão dos sistemas corporativos, a norma de criação dos perfis de acesso;

VII - as áreas responsáveis pela gestão dos sistemas corporativos, são responsáveis pelas permissões, transações e ações que devem compor cada perfil de acesso;

VIII - os perfis de acesso e perfis de gestão concedidos para usuários interno e externos deverão ser objeto de revisão contínua pelos gestores responsáveis, não podendo ultrapassar o prazo máximo de 30 (trinta) meses;

IX - quanto à utilização das credenciais e perfis de acesso, o usuário:

- a) deve ter conhecimento prévio desta Norma de Controle de Acesso Lógico e preencher os requisitos estabelecidos na mesma;
- b) deve estar devidamente autorizado a utilizar a rede corporativa e/ou os sistemas corporativos, de acordo com os requisitos estabelecidos nesta Norma;
- c) deve utilizar os serviços e as informações obtidas, por meio do perfil de acesso, única e exclusivamente em razão do exercício da função pública e para os fins que lhe foi designado, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal;
- d) não pode divulgar, nem mesmo compartilhar, os códigos de segurança que lhe forem atribuídos (credenciais de acesso), os quais são pessoais e intransferíveis;
- e) não pode utilizar as credenciais para acessar os recursos disponíveis em mais de uma estação de trabalho simultaneamente;
- f) não pode fazer uso das credenciais de acesso de outros usuários;
- g) deve fornecer informações acessadas nos sistemas e na rede de dados corporativos do INSS somente mediante demanda formalizada de quem tenha competência para tal;
- h) deve comunicar a chefia imediata ou responsável pela administração do sistema ou rede corporativa quaisquer violações ou incidentes referentes à proteção do equipamento utilizado, do software ou de outros ativos da informação; e
- i) deve, sempre que for necessário afastar-se da estação de trabalho, certificar-se de que a sessão de rede ou acesso ao sistema corporativo esteja encerrado ou bloqueado.

X - o processo de autenticação de usuários deve ser definido pela área responsável pela gestão de Tecnologia da Informação do Instituto e poderá ser baseada em autenticação simples (nome de usuário e senha) agregada a autenticação multifator (certificação digital ou outros meios disponíveis);

XI - o usuário deverá, obrigatoriamente, efetuar processo de alteração da sua senha em seu primeiro acesso à rede de dados corporativa; e

XII - no ato do primeiro acesso, bem como após cada atualização desta Norma, o usuário deverá manifestar concordância com os termos dispostos na mesma.

XIII - Credenciamento de Usuários Internos:

a) o cadastro de novos servidores ou ocupantes de cargo em comissão, no âmbito do Instituto, pode ser solicitado por servidor vinculado à área responsável pela gestão de pessoas ou pela chefia imediata do usuário; e

b) esse cadastro deve ser solicitado por meio dos canais de atendimento disponibilizados pela prestadora de serviços tecnológicos contratada pelo Instituto ou outro informado pela DTI.

XIV - credenciamento de estagiários:

a) a emissão de credencial de acesso se dará tendo como requisito as seguintes condições:

1. a empresa que atuar como agente de integração do estágio supervisionado deve manter contrato com o INSS; e
2. o contrato de estágio supervisionado deverá conter cláusula de confidencialidade e sigilo de informações preestabelecidos com a Administração Pública.

b) para viabilizar o acesso de estagiários aos sistemas corporativos, os gestores dos sistemas corporativos deverão criar perfis específicos e restritos às atividades do estagiário;

c) é vedada a concessão de perfis de acesso aos sistemas corporativos para estagiários com permissão de alteração das bases de dados institucionais;

d) o acesso será concedido mediante solicitação expressa de servidor do quadro do INSS, responsável pela supervisão do estágio, que deverá:

1. avaliar os riscos de utilização indevida de informações institucionais e as eventuais restrições referentes aos dias e horários para a realização dos acessos.

e) o acesso será precedido da assinatura do Termo de Confidencialidade e de Manutenção de Sigilo – TCMS, Anexo II, o qual deverá ser firmado pelo estagiário ou pelo estagiário e seu responsável legal, no caso de se tratar de estagiário menor de dezoito anos;

f) as solicitações de acesso à rede para estagiários devem ser procedidas por meio dos canais remotos de atendimento disponibilizados pela empresa prestadora de serviços tecnológicos contratada pelo Instituto ou outro canal informado pela DTI, pela unidade de gestão de pessoas, pela chefia imediata do educando ou pelo responsável por sua supervisão;

g) os gestores de sistemas devem criar perfis diferenciados para estagiários de nível médio e nível superior;

h) o supervisor do estagiário deverá, periodicamente, orientá-lo quanto ao uso responsável e adequado do acesso aos sistemas corporativos; e

i) o acesso do estagiário limitar-se-á à data final do contrato ou imediatamente cessado na hipótese de rescisão antecipada do estágio, cabendo ao supervisor do estagiário, em quaisquer dos casos, adotar as providências necessárias ao bloqueio do acesso, tão logo finde a contratação.

XV - credenciamento de usuários externos:

a) as credenciais de acesso para usuários externos devem ser emitidas tendo em vista o interesse do INSS, devidamente justificadas e previstas no convênio, acordo de cooperação técnica ou instrumento congênere;

b) as solicitações de emissão de credenciais de acesso à rede corporativa para usuários amparados por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica, contrato ou instrumento congênere devem:

1. ser feitas pelo gestor da unidade/área responsável pela gestão do instrumento legal; e

2. ser atendidas somente após validação das credenciais do gestor solicitante do Instituto, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700).

c) a emissão de credenciais de acesso à rede corporativa para prestadores de serviço terceirizados ou equiparados nas dependências do INSS, quando necessária, será provida unicamente pelo interesse do INSS. Para tanto, devem ser atendidos os seguintes requisitos:

1. a organização a qual o usuário é vinculado deve manter contrato, acordo de cooperação, convênio ou instrumento congênere vigente com o INSS;

2. instrumento deve conter cláusulas prevendo:

2.1. necessidade e justificativa para acesso à rede corporativa;

2.2. a confidencialidade e sigilo de informações preestabelecidas junto ao Instituto;

2.3. a obrigatoriedade da organização ou do ente contratado informar previamente ao representante legal do INSS, responsável pela gestão do contrato, quaisquer alterações em seu corpo de colaboradores que impacte na emissão/exclusão das contas de acesso;

2.4. a organização ou ente contratado também deverá manter com seus colaboradores Termo de Confidencialidade de Manutenção de Sigilo – TCMS; e

2.5. o gestor do contrato pelo INSS deve fundamentar a necessidade do acesso à rede para prestadores de serviço terceirizados ou equiparados, definindo os recursos que devem ser disponibilizados e eventuais restrições a dias e horas para realização do acesso à rede.

3. os TCMS deverão ser arquivados junto aos instrumentos assinados com o INSS e uma cópia ou link eletrônico deverá ser encaminhada ao Gestor do Contrato. O mesmo deve ocorrer para quaisquer alterações ocorridas na vigência dos contratos, acordos ou convênios;

3.1 caso os Termos sejam gerados de forma eletrônica, deverá ser disponibilizado o arquivo correspondente, atendendo aos requisitos necessários para garantia de integridade e disponibilidade de acesso, assim como os requisitos específicos previstos em contrato; e

4. a emissão de credenciais de acesso poderá ser feita pelo gestor do contrato, representante legal do INSS, ou pelo gestor da unidade responsável pela gestão do contrato, convênio, acordo de cooperação técnica ou instrumento congênere e serão atendidas somente após validação das credenciais do solicitante, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700).

d) o acesso aos prestadores de serviço vinculados à Central de Atendimento 135 se dará observando as seguintes condições:

1. a empresa deve manter contrato com o INSS;

2. o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

3. a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade - TCMS;

4. o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte do INSS, definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;

5. os acessos deverão ser realizados única e exclusivamente por necessidade de serviço; e

6. Os contratos de prestação de serviços de teleatendimento devem conter documento a ser utilizado para formalização das indicações de gestores de acesso aos sistemas corporativos do Instituto;

7. o INSS pode disponibilizar, de forma restrita, às centrais 135 uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

e) nos casos referentes a prestadores de serviço vinculados à Ouvidoria do Ministério da Economia, o acesso se dará observando-se as seguintes condições:

1. a empresa deve manter Contrato direto com a Ouvidoria do Ministério da Economia;
2. o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;
3. a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade;
4. o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte da Ouvidoria do Ministério da Economia, definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;
5. os acessos deverão ser realizados única e exclusivamente por necessidade de serviço; e
6. o INSS pode disponibilizar, de forma restrita, à Ouvidoria do Ministério da Economia uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

f) o acesso à rede corporativa por servidores vinculados a órgãos de controle externo, envolvidos em ações de auditoria no âmbito do INSS, será concedido mediante apresentação da equipe de auditoria por meio de documento formal que conste:

1. dados necessários ao cadastro de usuários externos;
2. informações acerca dos objetivos dos trabalhos a serem executados;
3. os prazos envolvidos; e
4. informações complementares.

g) este tipo de acesso deverá observar as parcerias institucionalmente estabelecidas entre esses órgãos e o INSS no que tange à cobertura/previsão de acesso à rede corporativa do Instituto; e

h) o atendimento de pedido de solicitação de informações advindo de pessoas físicas ou jurídicas externas, respeitadas as restrições de acesso às informações previstas na Lei nº 12.527, de 18 de novembro de 2011, serão analisadas pela área designada para responder as demandas dos cidadãos por meio do e-SIC.

XVI - os procedimentos referentes às solicitações de inclusão, exclusão, inativação e suspensão de contas de acesso de usuários devem ser executados tendo como premissa a preservação dos registros para efeito de auditoria.

XVII - bloqueio administrativo:

a) o responsável pela Corregedoria-Geral do INSS, quando necessário, poderão solicitar a suspensão, bloqueio ou inativação imediata de contas de acesso de usuários que estiverem envolvidos em inquérito penal, em Processo Administrativo Disciplinar – PAD – ou em Sindicância, decorrente de infrações cometidas no exercício das atribuições do cargo;

b) estas solicitações deverão ser efetuadas mediante comunicação formal da Corregedoria-Geral para a prestadora de serviços tecnológicos contratada pelo Instituto, ou outro canal informado pela DTI, a qual procederá a imediata implementação da mudança.

c) para disciplinar o disposto na "alínea a", é considerado possível de ter a senha bloqueada, o usuário que estiver na seguinte situação:

1. afastado temporariamente do cargo ou função pública em razão de ato que se encontra sob apuração;
2. indiciado em processo administrativo disciplinar, por incursão nos incisos IX, XI, XII, XV, XVI e XVII do art. 117 e arts. 130 e 132 da Lei nº 8.112, de 11 de dezembro de 1990, ou cuja proposta pela Comissão Processante, no relatório final, seja pela aplicação de penalidade a partir de suspensão de trinta dias; e
3. submetido à prisão em flagrante, temporária ou preventiva decorrente do cometimento de infração no exercício das atribuições do cargo, enquanto estiver em apuração de inquérito policial ou pelo Ministério Público Federal.

d) o bloqueio de acessos, tratados nas situações da "alínea c", será efetivado no âmbito da ferramenta de gestão de acessos nas seguintes situações:

1. usuário afastado temporariamente do cargo ou função, enquanto durar o afastamento; e
2. usuário indiciado nos termos do subitem "alínea c", desta Norma, até o efetivo cumprimento da penalidade porventura aplicada ou, em caso de não aplicação de penalidade, enquanto durar o processo.

Art. 6º Rede de Dados Corporativa:

I - infraestrutura de rede:

a) a infraestrutura de rede do INSS é disponibilizada para uso Institucional. Sendo assim, apenas equipamentos de propriedade do Instituto são autorizados e devem ser conectados à rede corporativa;

1. em casos excepcionais, a conexão de equipamentos particulares à rede corporativa deve ser feita em razão do interesse do Instituto e sob prévia autorização do responsável pela gestão da unidade em que o equipamento estiver localizado.

b) o INSS poderá disponibilizar o acesso à rede de dados corporativa por meio de tecnologia *Wireless* (sem fio). Para tanto os seguintes critérios deverão ser adotados:

1. os projetos que envolvam a utilização de pontos de acesso sem fio à rede corporativa no âmbito do Instituto deverão ser devidamente registrados e aprovados pela área responsável pela gestão de TI do INSS;

2. os pontos de acesso à rede de dados corporativa sem fio poderão ser objeto de testes periódicos de penetração e de auditoria a critério da área responsável pela gestão de TI no INSS;

3. as conexões à rede sem fio serão avaliadas pela área responsável pela gestão de TI do INSS em relação aos requisitos de segurança e deverão atender ao princípio do privilégio mínimo;

4. a área responsável pela gestão de TI do INSS poderá disponibilizar rede sem fio com regras específicas de acesso para visitantes nas diversas unidades do Instituto;

5. os dispositivos conectados à rede do INSS por meio de conexão sem fio deverão suportar configurações de criptografia estabelecidas pela área responsável pela gestão de TI no âmbito do INSS;

6. qualquer tecnologia de acesso sem fio implementada no INSS deverá suportar autenticação forte, com possibilidade de efetuar checagens em bancos de dados externos.

c) a área responsável pela gestão de TI do INSS deve dispor de mecanismos automáticos que possibilitem:

1. a detecção e bloqueio de equipamentos externos conectados à rede corporativa; e

2. a identificação e rastreamento dos endereços IP de origem e destino, bem como os serviços utilizados na rede corporativa inclusive nos acessos remotos.

II - administração da rede corporativa:

a) a operacionalização da administração da rede do INSS é realizada por empresa prestadora de serviços tecnológicos contratada pelo Instituto;

1. os ativos e serviços que compõem a rede de dados corporativa são providos, gerenciados e operacionalizados por tal prestadora de serviços; e

2. os acessos à rede de dados corporativa realizados pelos usuários do INSS são gerenciados e monitorados pela empresa prestadora de serviços de tecnologia contratada pelo Instituto, contudo seguem as regras desta Norma.

b) quanto ao processo de geração de contas de serviço fica estabelecido que:

1. os critérios para a emissão de contas de serviços serão vinculados a um processo formal estabelecido pela área responsável pela gestão de TI do INSS;

2. a concessão de contas de serviços deve ser feita conforme a necessidade de uso de acordo com os critérios estabelecidos nesta Norma de Controle de Acesso;

3. o direito de acesso privilegiado, por meio de contas de serviços, associado a sistemas ou processos, deve ser identificado;

4. deve ser viabilizada ferramenta que possibilite a gestão das contas de serviço de forma automatizada, possibilitando o registro e verificação de todos os privilégios concedidos;

5. as contas de serviço fornecidas devem ser utilizadas exclusivamente para os fins aos quais foram concedidas;

6. as contas de serviço emitidas devem ser revalidadas periodicamente com base na função exercida e na área de atuação do servidor; e

7. as contas de serviço com credenciais de acesso de uso compartilhado devem ter suas senhas alteradas periodicamente, conforme estabelecido nesta Norma de Controle de Acesso Lógico, ou sempre que ocorrerem mudanças no grupo de usuários que utilizam as mesmas.

C) é vedado o uso da rede corporativa para:

1. acesso por meio de equipamento não homologado ou não autorizado pelo INSS;

2. fazer download, instalar e/ou utilizar sistemas ou aplicativos não homologados pela área responsável pela gestão de TI do INSS nos equipamentos de propriedade do Instituto;

3. a utilização de softwares particulares em equipamentos do INSS sem autorização expressa;

4. a instalação e conexão de equipamentos particulares à rede corporativa do Instituto sem a prévia autorização do gestor responsável pela unidade ou da área responsável pela gestão de TI do INSS;

5. o uso dos recursos de rede para fins particulares ou de terceiros alheios aos interesses do INSS, em especial quando tal procedimento prejudique o tráfego da rede de dados;

6. o uso para fins de divulgação ou distribuição de material que não possua vínculo com as atividades desenvolvidas pelo Instituto;

7. a instalação ou utilização de ferramentas de monitoramento de rede sem a anuência e autorização expressa da área responsável pela gestão de TI no Instituto;

8. a instalação de dispositivos de comunicação ou de compartilhamento de dados sem fio, particulares, à rede corporativa do Instituto, sem autorização expressa da área responsável pela gestão de TI do INSS; e

9. burlar as regras de acesso a internet configuradas em proxy ou ferramenta similar de gerenciamento de conteúdo *web*;

d) cabe à área responsável pela gestão de TI no âmbito do INSS definir os aspectos relacionados à plataforma tecnológica, gestão operacional, forma de autenticação e sustentação do domínio de rede do INSS.

Art. 7º Gestão do Acesso aos Sistemas Corporativos:

I - sistemas legados:

a) as regras estabelecidas nesta norma devem ser aplicadas, guardando-se as devidas limitações tecnológicas, aos sistemas legados; e

b) o controle de acesso aos sistemas legados é efetuado por base própria.

II - sistemas de apoio à administração:

a) os ambientes de hospedagem desses sistemas são suportados por terceiros;

b) o ambiente deverá ser gerenciado e operacionalizado pela área de gestão de TI do INSS;

c) o acesso pelos usuários a esses sistemas deverá ser autenticado pelo serviço de diretório utilizado pelo Instituto; e

d) as regras de hospedagem de sistemas serão definidas, em ato próprio, pela área de gestão de TI do INSS.

III - armazenamento de registros logs:

a) as áreas responsáveis pela gestão de sistemas corporativos e demais aplicações devem definir, em conjunto com a área responsável pela gestão de TI, a temporalidade de registro dos logs de acesso e transações, e quais registros devem ser armazenados por um período maior que o estipulado no Inciso I do Art. 8º desta Norma;

b) o INSS poderá alterar a temporalidade destes dados em norma específica;

c) Os logs de acesso devem contemplar minimamente os registros relacionados no ANEXO III desta norma.

IV - administração da ferramenta de gestão de acesso:

a) com o objetivo de operacionalizar a gestão dos acessos aos sistemas corporativos no âmbito do INSS, serão criados os seguintes papéis:

1. administrador de sistema INSS: Servidor do quadro, lotado na área responsável pela gestão de TI, designado por meio de Portaria do Diretor de Tecnologia da Informação e Inovação, a ser publicada em Boletim de Serviço – BS, responsável pela administração da ferramenta de gestão de acesso aos sistemas corporativos no âmbito do INSS;

2. gestor de sistema: Servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em Boletim de Serviço, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedoria-Geral e Procuradoria Federal Especializada. É responsável pela implementação de sistemas corporativos no âmbito do INSS;

3. gestor de acesso central: Servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em Boletim de Serviço, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedoria-Geral e Procuradoria Federal Especializada. É responsável pela manutenção dos perfis de gestão dos usuários nas áreas que compõem a Administração Central e, quando necessário, dos gestores de acesso das Superintendências Regionais;

4. gestor de acesso interno: Servidor do quadro, lotado na Administração Central, Superintendência Regional, Gerência Executiva, Agência da Previdência Social, indicado pelo Gestor de Acesso Central ou por um Gestor de Acesso, responsável pela atribuição do perfil de acesso e de gestão dos usuários no INSS; e

5. gestor de acesso externo: Pessoa formalmente indicada, por documento previsto no instrumento legal que firmou a parceria ou por meio de Ofício de lavra do representante máximo de uma Entidade Externa, responsável pelo cadastro de usuários externos e a gestão dos acessos aos sistemas corporativos do Instituto.

b) Os perfis de acesso serão atribuídos de acordo com a necessidade do fluxo de operação definido para cada sistema corporativo;

c) a indicação e o processo de substituição dos responsáveis pela gestão dos acessos aos sistemas corporativos no âmbito do INSS poderá ser procedida das seguintes formas:

1. a autoridade responsável pela indicação do gestor de acessos pode indicar opcionalmente o substituto;

2. o próprio gestor de acessos pode designar, a qualquer momento, por meio da ferramenta de gestão de acessos um substituto; ou

3. quando não houver um gestor responsável, ou substituto, por uma unidade devidamente designado, a gestão dos usuários será transferida, preferencialmente de forma automática, para o responsável pela área da abrangência daquela unidade e assim subsequentemente; e

4. o Gestor de Acesso é corresponsável com os perfis de gestão ou acesso que ele atribuir aos usuários.

d) ao usuário interno cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Norma de Controle de Acesso Lógico e suas normas complementares;

2. solicitar, ao Gestor de Acesso responsável pela gestão da unidade de lotação a qual é vinculado, a suspensão do seu perfil de acesso nos períodos de afastamento do serviço por mais de trinta dias consecutivos;

3. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e

4. ter conhecimento e estar de acordo com o disposto nesta Norma.

e) ao usuário externo cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Norma de Controle de Acesso Lógico;

2. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e

3. ter conhecimento e estar de acordo com o disposto nesta Norma.

f) ao administrador do sistema INSS cabe:

1. criar os sistemas e subsistemas, devidamente homologados pela área de negócio responsável, no ambiente de produção, por meio de ferramenta de gestão de acesso;

2. mediante apresentação de Portaria de designação para Gestores de Acesso Central, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores quanto à atribuição dos perfis de gestão; e

3. mediante apresentação de Portaria de designação para Gestores de Sistema, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores acerca do processo de implementação dos sistemas corporativos no âmbito do INSS.

g) ao gestor de sistema cabe:

1. efetuar os procedimentos de importação, inclusão, alteração e exclusão de papéis e permissões nos sistemas corporativos em ambiente de produção; e

2. atuar, em conjunto com o Administrador do Sistema INSS e a prestadora de serviços tecnológicos contratada pelo Instituto, no planejamento e execução do processo de implementação dos sistemas corporativos dos quais for designado responsável.

h) ao gestor de acesso central cabe:

1. efetuar o credenciamento, suspensão ou exclusão de perfis de gestão dos sistemas corporativos aos Gestores de Acesso na Administração Central e, quando necessário, dos Gestores de Acesso da Superintendência Regional, Gerência Executiva, Agência da Previdência Social e demais usuários de sua abrangência; e

2. orientar os usuários de sua abrangência e os gestores da Administração Central e Superintendências Regionais, Gerências Executivas e Agências da Previdência Social acerca das regras para o acesso aos sistemas corporativos do INSS.

i) ao gestor de acesso interno cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários da Administração Central, Superintendência Regional, Gerência Executiva, Agência da Previdência Social;

2. atribuir, alterar ou excluir os perfis de acesso aos usuários da Administração Central, Superintendência Regional, Gerência Executiva, Agência da Previdência Social; e

3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS.

j) ao gestor de acesso externo cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários do seu Órgão/Entidade;

2. atribuir, alterar ou excluir os perfis de acesso aos usuários do seu Órgão/Entidade; e

3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS.

V - configura-se mau uso, sujeito a responsabilidade penal, civil e disciplinar:

a) a divulgação, sem autorização expressa da chefia imediata ou do gestor de acesso de sua abrangência, de informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS;

b) acessar sistemas corporativos sem autorização prévia, de acordo com os requisitos estabelecidos nesta Norma;

c) utilizar-se das informações obtidas por meio de acesso concedido em desacordo com os procedimentos dispostos nesta Norma e demais normas vigentes na Administração Pública Federal;

d) compartilhar ou fazer uso das credenciais de acesso, aos sistemas corporativos, de outros usuários;

e) a instalação de sistemas corporativos em equipamentos particulares; e

f) em casos excepcionais, a área responsável pela gestão de TI do INSS, mediante ato formal, poderá autorizar a adoção das medidas descritas no Inciso III do Art.8º.

Art. 8º Disposições Gerais:

I - todo acesso à rede de dados e aos sistemas corporativos deve ser registrado e monitorado de modo que permita a rastreabilidade, a identificação e o bloqueio de usuários e equipamentos não autorizados. Estas informações devem ser armazenadas por um período de, no mínimo, doze meses, observando o disposto no Inciso III do art. 7º desta norma;

II - as ocorrências de mau uso do acesso aos recursos disponíveis na rede e sistemas corporativos não previstas nesta norma e os casos omissos serão encaminhados para a área responsável pela gestão de TI no âmbito do INSS para análise e pronunciamento;

III - identificada irregularidade de mau uso dos recursos de rede poderá ocorrer:

a) o bloqueio preventivo do acesso pela DTI, o encaminhamento de dossiê com as informações para a Corregedoria-Geral do INSS ou Corregedorias Regionais, nas suas áreas de abrangências, a fim de que seja realizada a análise no âmbito disciplinar; e

b) ressalta-se que o descumprimento dessa Norma poderá resultar em sanções administrativas, civis e criminais.

IV - esta norma deve ser revisada num período máximo de três anos.

ANEXO II

RESOLUÇÃO Nº 3/CEGOV/INSS, DE DE DE 2020

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF: _____, identidade _____, expedida pelo _____, em _____, e lotado no(a) _____ do Instituto Nacional do Seguro Social – INSS, DECLARO, sob pena das sanções cabíveis nos termos da Política de Segurança da Informação - POSIN do INSS que assumo a responsabilidade por:

I - tratar o(s) ativo(s) de informação como patrimônio do Instituto Nacional do Seguro Social;

II - utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do INSS;

III - contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que disciplina a gestão de segurança da informação na Administração Pública Federal, direta e indireta, e dá outras providências;

IV - utilizar as credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do INSS;

V - responder, perante o INSS, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

_____, _____ de _____ de _____

Assinatura do usuário

Nome do usuário:	Unidade de Lotação:
Nome da Autoridade Responsável pela Autorização do Acesso:	

Assinatura e Carimbo do Responsável pela Autorização de Acesso

ANEXO III

RESOLUÇÃO Nº 3/CEGOV/INSS, DE _____ DE _____ DE 2020

REGISTROS DE LOGS

1. Relação dos campos de registros de logs do GERID
 - 1.1. Dados Gerais
 - 1.1.1. Data
 - 1.1.2. Sistema
 - 1.1.3. Ambiente
 - 1.1.4. IP destino
 - 1.1.5. IP origem
 - 1.1.6. CPF usuário
 - 1.1.7. URL de origem
 2. Ações:
 - 2.1. CAS (autenticação): Central Authentication Service - Serviço Central de Autenticação
 - 2.1.1. Criação de service ticket (ST)
 - 2.1.2. Criação de ticket granting ticket (TGT)
 - 2.1.3. validação de ST
 - 2.1.4. Exclusão de ticket TGT
 - 2.1.5. Autenticação com sucesso (login+password)
 - 2.1.6. Autenticação com sucesso (certificado digital)
 - 2.1.7. Autenticação com falha
 - 2.2. GPA: Gerenciamento de Permissão de Acesso
 - 2.2.1. Início de sessão
 - 2.2.2. Dados do usuário em sessão (CPF, NOME, PAPEL)
 - 2.2.3. Requisição de logout
 - 2.2.4. Dados de credenciais
 - 2.2.5. Concessão de credenciais
 - 2.2.6. Alteração de Credenciais
 - 2.2.7. Dados de receptor (CPF, NOME, Lotação)
 - 2.2.8. Inserção de credencial no usuário
 - 2.2.9. Revogação de Credenciais
 - 2.2.10. Pesquisa de credenciais

- 2.2.11. Pesquisa de usuários
- 2.2.12. Substituição de gestor



INSTITUTO NACIONAL DO SEGURO SOCIAL
MINUTA DE RESOLUÇÃO

MINUTA DE RESOLUÇÃO

**RESOLUÇÃO Nº 4/CEGOV/INSS, DE DE
DE 2020**

Institui a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos
Instituto Nacional do Seguro Social.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR do INSS.

Art. 2º Os Anexos a esta Portaria serão publicados em Boletim de Serviço.

Art. 3º Esta Portaria complementa Política de Segurança da Informação POSIN-INSS vigente.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretora de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **ALEXINALDO MESSIAS CERQUEIRA**, **Chefe de Serviço**, em 04/08/2020, às 12:59, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1392184** e o código CRC **BDC8C17F**.

ANEXO I

RESOLUÇÃO Nº 4/CEGOV/INSS, DE DE DE 2020

EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS - ETIR-INSS

Art. 1º Para os efeitos desta norma ficam estabelecidos os seguintes conceitos e definições:

I - agente responsável: Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

II - artefato malicioso: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

III - comunidade ou Público Alvo: é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos ou estrutura equivalente;

IV - CTIR GOV: Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI;

V - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

VI - incidente de segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VII - serviço: é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade pela Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

VIII - tratamento de Incidentes de Segurança em Redes Computacionais: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

XI - usuário: pessoas que fazem uso de serviços de TI e sistemas de informação de propriedade do INSS, independente do cargo ocupado (contratados, consultores, conselheiros, servidores, temporários e etc); e

X - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou por uma organização, os quais podem ser evitados por uma ação interna de segurança da informação.

Art. 2º Esta norma tem a missão de:

Parágrafo único. Agir proativamente, receber, analisar, monitorar, coordenar e propor respostas a notificações e atividades relacionadas a incidentes de segurança da informação e comunicações no âmbito do Instituto.

Art. 3º Esta norma tem como público alvo:

I - a abrangência das atividades pertinentes à ETIR-INSS inclui os usuários dos serviços de Tecnologia da Informação - TI, e os sistemas de informação do INSS;

II - as atividades pertinentes à ETIR-INSS serão realizadas com intercâmbio de informações e em cooperação com as seguintes instâncias:

a) o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR GOV;

b) a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR, de empresas prestadoras de serviços de tecnologia contratadas pelo Instituto;

c) Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos ou estrutura equivalente dos demais órgãos, entidades e empresas, públicas ou privadas, que tenham contratos, acordos, convênios ou instrumentos congêneres com o INSS; e

d) o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República – GSI/PR.

Art. 4º a implementação e o funcionamento da ETIR-INSS seguirão a metodologia definida pelo Gabinete de Segurança Institucional da Presidência da República, conforme definido a seguir:

I - o modelo de implementação no qual a ETIR-INSS se baseia é o “Modelo 1 – Utilizando a equipe de Tecnologia da Informação”, conforme definido pelo GSI/PR;

II - a equipe será composta por profissionais da área de Tecnologia da Informação, lotados na Diretoria de Tecnologia da Informação e Inovação – DTI, sem prejuízo de suas atribuições típicas do cargo, com experiência e conhecimentos técnicos compatíveis com a importância da missão da ETIR-INSS;

III - a equipe será composta por servidores públicos efetivos;

IV - a ETIR-INSS ficará vinculada tecnicamente à Coordenação-Geral de Infraestrutura e Operações – CGIN, da Diretoria de Tecnologia da Informação e Inovação - DTI; e

V - o Coordenador da ETIR-INSS será nomeado por meio de ato do Diretor de Tecnologia da Informação e Inovação - DTI;

VI - Caso o Coordenador da ETIR-INSS não seja formalmente nomeado, as atribuições relacionadas à coordenação da equipe serão desempenhadas pelo Coordenador-Geral de Infraestrutura e Operações.

Art. 5º A ETIR-INSS será composta por membros:

I - permanentes: que efetivamente atuarão em todos os incidentes registrados;

II - colaboradores: que atuarão, de forma esporádica, no tratamento de incidentes relacionados às suas áreas de atuação; e

III - Opcionais: servidores das unidades descentralizadas sob supervisão da DTI.

IV - sendo assim, a ETIR-INSS será formada por servidores lotados na área de TI, de acordo com os papéis abaixo:

Quantidade	Papel	Sector
2	Permanente	Serviço de Segurança de TIC
2	Colaborador	Coordenação-Geral de Infraestrutura e Operações
2	Colaborador	Coordenação-Geral de Projetos e Soluções Digitais
2	Opcional	Unidades descentralizadas

V - Os membros da ETIR-INSS serão designados por meio de ato do Diretor de Tecnologia da Informação e Inovação.

Art. 6º Quanto autonomia da ETIR-INSS:

I - terá autonomia limitada para o tratamento de incidentes de Segurança da Informação, devendo implementar ações que possam impactar outras áreas do Instituto somente com anuência do Diretor de Tecnologia da Informação e Inovação e do gestor responsável pela área/sistema afetada; e

II - poderá, ainda, gerar relatórios técnicos sugerindo a adoção de medidas para resolução de incidentes.

Art. 7º A ETIR-INSS fornecerá o serviço de Tratamento de Incidentes de Segurança em Redes Computacionais:

I - este serviço compreende basicamente as seguintes ações:

- a) recepção: receber solicitações e alertas diversos. Para tanto o Instituto disponibilizará como canal de comunicação a caixa postal etir@inss.gov.br;
- b) filtrar: todo conteúdo direcionado para a ETIR deve ser verificado, a partir desta análise deve ser tratado pela equipe ou, não se tratando de um incidente de segurança em redes computacionais, encaminhado para a área competente;
- c) catalogar: os incidentes devem ser catalogados em ferramenta a ser indicada pela DTI, com nível de acesso restrito;
- d) classificar: os incidentes devem ser classificados quanto ao nível de severidade e impacto;
- e) tratar o incidente: indicar o tratamento do incidente com medidas corretivas e formas de se evitar que ocorra novamente;
- f) responder: as solicitações e alertas encaminhados para a ETIR devem ser devidamente respondidos; e
- g) monitorar: monitorar a aplicação do tratamento dos incidentes indicados.

II - a ETIR deve analisar os incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências; e

III - o detalhamento dos serviços prestados pela ETIR-INSS deve ser publicado em página específica da Intranet do Instituto no prazo de 30 dias a partir da publicação desta portaria.



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 5/CEGOV/INSS, DE DE DE 2020

Disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis Internet, competências e conteúdo de acesso para cada perfil.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do processo nº 35014.034105/2019-14,

RESOLVE:

Art. 1º Fica instituída, nos termos do Anexo I desta Portaria, norma que estabelece critérios para uso da Internet no âmbito do Instituto Nacional do Seguro Social - INSS.

Art. 2º Os Anexos a esta Portaria serão publicados em Boletim de Serviço.

Art. 3º Esta Portaria complementa a Política de Segurança da Informação POSIN-INSS vigente.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretora de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **ALEXINALDO MESSIAS CERQUEIRA**, **Chefe de Serviço**, em 04/08/2020, às 12:59, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1394150** e o código CRC **3D950F20**.

ANEXO I

RESOLUÇÃO Nº 5/CEGOV/INSS, DE DE DE 2020

NORMA DE USO DA INTERNET

Art. 1º Esta norma se aplica a todos os servidores e colaboradores, vinculados direta ou indiretamente ao INSS, bem como a servidores e empregados de entidades e órgãos da Administração Pública ou privadas que necessitem ou estejam autorizados a acessar a Internet a partir da rede corporativa do Instituto.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União – AGU que atuarem na consultoria e no assessoramento jurídico, e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta norma, ficam estabelecidos os seguintes conceitos e definições:

I - autorizador: ocupantes de cargos que serão responsáveis pela autorização da concessão de perfis de acesso para usuários finais de sua área de abrangência;

II - internet: é a rede mundial que interliga computadores de diferentes tipos e dimensões e permite a comunicação entre pessoas e organizações, independentemente da localização geográfica;

III - intranet: é a rede de computadores administrada pelo INSS, que utiliza os mesmos serviços e tecnologias disponíveis na rede mundial, podendo ser definida como um tipo de Internet Local do Instituto;

IV - perfil de acesso: atributo que estabelece as categorias de sítios acessíveis e tipos de arquivos que podem ser recebidos ou transmitidos pelos usuários;

V - proxy: desempenha a função de conexão do computador (local) à rede externa (Internet). Como os endereços locais do computador não são válidos para acessos externos, cabe ao proxy enviar a solicitação do endereço local para o servidor, traduzindo e repassando-a para o seu computador;

VI - sítio: um conjunto de informações ou serviços disponíveis na Internet ou na Intranet, organizados em páginas eletrônicas e acessíveis por meio de endereços que identificam, de forma padronizada, sua origem e conteúdo;

VII - usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal-APF, formalizada por meio da assinatura do Termo de Responsabilidade; e

VIII - VPN: Trata-se de uma Rede Privada Virtual (Virtual Private Network) construída sobre a infraestrutura de uma rede pública. Essa é uma forma de conectar dois computadores por meio de uma rede pública, como a Internet;

Art. 3º Essa norma tem como diretrizes:

I - o acesso à Internet disponibilizado pelo Instituto Nacional do Seguro Social aos usuários deve ser utilizado exclusivamente em razão de trabalho, cumprindo os procedimentos dispostos nesta norma;

II - os recursos disponibilizados pelo Instituto, não poderão ser usados para quaisquer propósitos que sejam ilegais ou proibidos, de modo a danificar, desativar, sobrecarregar ou prejudicar qualquer área, serviço ou conteúdo, ou interferir no uso e execução das atividades laborais de outros usuários;

III - o volume de tráfego de Internet e os endereços *web* visitados poderão ser monitorados, visando assegurar o cumprimento desta norma; e

IV - o acesso à Internet para propósitos particulares ou estranhos às atividades do INSS poderá ser bloqueado, sem prévia comunicação ao usuário e sem prejuízo das demais sanções aplicáveis.

Art. 4º Quando aos Perfis de Acesso:

I - o acesso aos sítios da Internet para todos os usuários será realizado mediante a atribuição de perfis de acesso;

II - o processo de solicitação e autorização de perfil de acesso à Internet do INSS compreenderá os seguintes perfis:

a) Perfil 1 - Perfil Restrito, deve ser inicialmente atribuído para usuários com maior restrição de acesso à internet, permitido acessar somente sítios governamentais, instituições bancárias e sítios considerados de interesse do INSS;

b) Perfil 2 - Perfil Básico, deve ser inicialmente atribuído para estagiários, recepcionistas e usuários externos. O usuário poderá acessar todos os sítios permitidos pelo Perfil 1, sítios de provedores de e-mail pessoal e instituições de ensino;

c) Perfil 3 - Perfil Padrão, para os servidores do quadro do Instituto. O usuário poderá acessar a todos sítios da internet sem a veiculação de material em áudio e vídeo; e

d) Perfil 4 - Perfil Avançado, deve ser atribuído preferencialmente para servidores do quadro do Instituto e estagiários que desempenham funções relacionadas à Comunicação Social, Desenvolvimento de Pessoas e gestores, respeitado o princípio da necessidade de conhecer, designados pelos Autorizadores deste perfil. O usuário poderá acessar todos os sítios da Internet, incluindo sítios que veiculam material em áudio e vídeo (*streaming*), sítios de compartilhamento de vídeos, blogs e redes sociais.

III - o perfil concedido a agentes externos é de caráter temporário, com validade equivalente à vigência do trabalho a ser executado;

IV - o processo de alterações, bloqueios, liberações e categorizações de sítios, assim como a criação e/ou alterações de perfis de acesso descritos nesta norma, quando necessários, serão definidos pela Diretoria de Tecnologia da Informação e Inovação – DTI, e publicado no Portal do INSS na Intranet; e

V - os novos usuários que não tiverem um perfil de acesso atribuído, devem ser direcionados para uma página da intranet contendo orientações e normas relacionadas ao acesso à internet no INSS, entre outras informações definidas pela DTI.

Art. 5º Acesso de Usuários Externos:

I - quanto ao acesso de servidores ou funcionários públicos externos:

a) o acesso à Intranet e Internet a partir da rede de dados corporativa, nas dependências do INSS, aos demais órgãos da Administração Pública Direta e Indireta, de qualquer das esferas de governo, será concedido exclusivamente para servidores e empregados públicos, efetivos ou ocupantes de cargo em comissão;

b) os acessos dos usuários externos das entidades que compõem o Poder Público serão concedidos mediante o estabelecimento de acordos ou convênios

específicos firmados com o INSS;

c) o gestor ou Coordenador-Geral da área responsável pelo convênio, contrato, ACT ou instrumento congênere, assumirá o papel de Autorizador do serviço de acesso à internet para usuários externos e deverá fundamentar as solicitações com base no instrumento; e

d) poderão ser concedidos acessos temporários para auditores de controle interno e externo, vinculados à Controladoria-Geral da União – CGU ou do Tribunal de Contas da União - TCU, no uso de suas atribuições.

II - quanto ao acesso de terceirizados:

a) o acesso à Internet por terceirizados deve ser provido pela empresa contratada;

b) em caráter de exceção, será concedido o acesso aos terceirizados a partir da infraestrutura de rede do INSS, desde que preenchidos os seguintes requisitos:

1. o contrato de prestação de serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

2. a empresa contratada deverá manter com seus funcionários Termo de Confidencialidade;

3. o contrato deve prever a necessidade de acesso à internet a partir das dependências do Instituto; e

4. o Autorizador, que para estes fins será o gestor do contrato ou o responsável pela área requisitante do serviço, deverá fundamentar as necessidades de acesso do contratado, definindo os recursos que devem ser disponibilizados, endereços da Intranet e Internet necessários para o desenvolvimento das atividades, bem como eventuais restrições a dias e horários para realização do acesso.

III - quanto ao acesso de visitantes:

a) a conexão de equipamentos pessoais à rede do Instituto, quando necessária e motivada pelo interesse da Administração, deve ser previamente autorizada pelo gestor da unidade onde o equipamento será utilizado;

b) só será permitida a utilização da rede local por equipamentos que atendam a todos os requisitos estabelecidos pela DTI; e

c) o acesso se dará, exclusivamente, à Internet, sendo vedado o acesso ao conteúdo disponibilizado na intranet.

Art. 6º A todos os perfis de acesso descritos nesta norma aplicam-se as restrições de acesso a sítios que:

I - contenham material pornográfico ou obsceno;

II - contenham material ilegal;

III - disponibilizem jogos, inclusive os da Internet (online);

IV - contenham material impróprio, ofensivo, preconceituoso ou discriminatório, que façam apologia à violência, ao terrorismo e às drogas; e

V - contenha e/ou divulgue conteúdo de violação de direito autoral (pirataria) e/ou execução de quaisquer tipos ou formas de fraudes.

Art. 7º Quanto ao processo de atribuição de acesso à Internet:

I - a atribuição dos perfis de acesso à Internet serão feitas pelos Autorizadores, de forma fundamentada respeitando o princípio da necessidade de conhecer, de acordo com a tabela abaixo:

Perfil	Autorizador
Perfil 1, 2 e 3	Gerente de APS, Gerente Executivo, Superintendentes Regionais, Procuradores Regionais, Coordenadores-Gerais, Superintendentes Regionais, Presidente do INSS, Auditor-Geral, Coordenadores-Gerais, Corregedoria-Geral, Procurador-Chefe da PFE-INSS, Diretores, Gestor ou chefe da área responsável pelo Contrato ou ato administrativo similar no âmbito do INSS.
Perfil 4	Chefes de Assessoria de Comunicação Social nas Superintendências Regionais, Assessor de Comunicação Social (Administração Central), Diretor de Tecnologia da Informação e Inovação, Diretor de Gestão de Pessoas e Administração e Presidente do INSS.

II - nos casos de novos usuários de rede (LDAP), criados por meio de registro de chamado técnico, quando o solicitante não indicar o perfil de acesso à internet, será atribuído o Perfil 1;

III - para proceder a alteração do perfil de acesso, os usuários deverão preencher “Formulário de Acesso à Internet” (Anexo II) e providenciar a assinatura pelo Autorizador do acesso; e

IV - ao registrar a solicitação, deve-se anexar o Formulário de Solicitação de Acesso à Internet devidamente preenchido e assinado (pelo solicitante e Autorizador), conforme documento nato digital ou digitalizado no formato PDF.

Art. 8º A solicitação para perfis de acesso em caráter temporário devem indicar no Formulário de Solicitação de Acesso à Internet, a motivação da necessidade e a data de expiração do acesso.

Art. 9º Responsabilidades:

I - o usuário deve:

- a) preencher os requisitos e termos estabelecidos nesta norma;
- b) estar devidamente autorizado a utilizar a Internet nas formas estabelecidas nesta norma;
- c) fazer uso da Internet de forma responsável e segura, utilizando o acesso exclusivamente em razão de trabalho, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal; e
- d) impedir a divulgação e compartilhamento das chaves de segurança atribuídas, que são pessoais e intransferíveis.

II - o autorizador deve:

- a) conceder os perfis de acesso à internet rigorosamente de acordo com as atribuições dos usuários de sua abrangência, observando os normativos do INSS;
- b) verificar periodicamente o uso dos acessos concedidos e, sempre que necessário, solicitar alteração dos perfis de acesso dos usuários de sua abrangência; e
- c) reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR-INSS.

III - a área responsável pela gestão de TI no INSS deve:

- a) monitorar os acessos à internet e sua utilização de acordo com as diretrizes estabelecidas nesta norma; e
- b) identificar os casos de mau uso da Internet e adotar uma ou mais das seguintes providências:
 - 1. alertar ao usuário, responsável pelo acesso, e ao Autorizador, responsável pela concessão, acerca do uso indevido da internet;
 - 2. nos casos de reincidência, solicitar a revogação do acesso à internet concedido ao usuário; e
 - 3. encaminhar a documentação que comprova a má utilização do acesso concedido para Corregedoria do INSS, para análise e adoção das medidas cabíveis.

Art. 10º As seguintes práticas configuram-se como uso indevido da internet:

I - acessar a internet disponibilizada pelo Instituto sem estar devidamente autorizado, conforme estabelecido nesta norma;

II - não manifestar concordância com as regras estabelecidas nesta norma e nas demais aplicáveis;

III - fazer uso dos recursos de Internet disponibilizado pelo Instituto para fins alheios ao trabalho, em discordância com os procedimentos dispostos nesta norma, sem prejuízo de demais normatizações vigentes na Administração Pública Federal;

IV - utilizar os serviços extrapolando os privilégios do perfil de acesso que lhe foi designado;

V - divulgação e compartilhamento das chaves de segurança, que são pessoais e intransferíveis, permitindo a utilização por terceiros do perfil que lhe foi atribuído;

VI - praticar atos de comercialização de produtos e serviços, em proveito próprio ou de terceiros, que não atendam os interesses do INSS;

VII - utilizar recursos ou dispositivos para acesso a computadores ou redes externas ao Instituto, com o objetivo de obter informações não autorizadas ou provocar a interrupção de serviços de rede;

VIII - utilizar modem ou dispositivo de rede que interligue a rede interna do INSS a outras redes ou à Internet;

IX - a exposição, o armazenamento, a distribuição, a edição, a gravação e o compartilhamento, através do uso dos recursos computacionais e de comunicação do INSS, de arquivos estranhos às atividades do Instituto e não autorizados pela chefia imediata;

X - realizar qualquer atividade que apoie ou facilite os vazamentos de dados;

XI - baixar arquivos ou programas da Internet que contrariem as diretrizes da Política de Segurança da Informação - POSIN vigente; e

XII - utilizar *proxy* não disponibilizado pelo INSS.

Art. 11 O acesso à Internet é passível de registro e monitoração, incluindo quaisquer dados transmitidos pela rede do INSS.

Art. 12 Disposições Gerais:

I - em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a ETIR-INSS deverá ser imediatamente acionada, para tomar as providências necessárias a fim de sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação do INSS;

II - as ocorrências de mau uso do acesso à internet não previstas nesta norma, assim como os casos de dúvidas em relação à aplicação das disposições aqui estabelecidas, devem ser encaminhadas à DTI para registro, análise e avaliação da necessidade de alterações de acordo com o processo de governança em vigência no Instituto;

III - o descumprimento desta norma, poderá acarretar ao usuário as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei, responsabilidade administrativa, civil e criminal; e

IV - esta norma deve ser atualizada periodicamente, não excedendo o prazo máximo de 3 anos.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações

DESPACHO

Coordenação-Geral De Infraestrutura e Operações, em 04/08/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Ajustes nas normas
de segurança da
informação apresentadas
na Reunião Ordinárias
CEGOV nº 6/2020.

1. Trata-se dos normativos para instituição de políticas e normas de segurança da informação do Instituto Nacional do Seguro Social - INSS que foram discutidos na 6ª Reunião Ordinária do Comitê Estratégico de Governança - CEGOV, realizada no dia 22/07/2020 (Processo SEI nº 35014.164930/2020-78).
2. Tendo em vista o término do prazo para encaminhamento de sugestões por parte dos membros do CEGOV e a devolução do processo à Diretoria de Tecnologia da Informação e Inovação, procedeu-se com a atualização de nomeclaturas nos normativos, conforme a IN nº 02, de 24 de julho de 2020, do GSI/PR e acostou-se aos autos do presente processo as minutas atualizadas (SEI nº 1391885, 1392067, 1392184 e 1394150) conforme Despacho SSEG (SEI 1391862).
3. Ressalta-se que após os ajustes formais no texto das minutas e antes da publicação dos normativos, a necessidade de uma ação coordenada desta DTI junto ao prestador de serviço para providenciar as mudanças tecnológicas necessárias, além de um plano de comunicação das referidas mudanças.
3. Feitas as considerações, encaminhe-se ao Comitê Estratégico de Governança - CEGOV, com ciência da Diretoria de Tecnologia da Informação e Inovação e do Comitê Temático de Governança Digital, para as tratativas necessárias para prosseguimento do presente processo.

CLAUDIO AUGUSTO NOVAIS FERRAZ

Coordenador-Geral de Infraestrutura e Operações



Documento assinado eletronicamente por **Claudio Augusto Novais Ferraz, Coordenador(a) Geral**, em 04/08/2020, às 19:30, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1399902** e o código CRC **9D3D2E61**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1399902



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria De Integridade, Governança e Gerenciamento De Riscos
Comitê Estratégico de Governança

DESPACHO

Comitê Estratégico de Governança, em 05/08/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO, COMITÊ
ESTRATÉGICO DE
GOVERNANÇA

A s s . : Minuta de
Resolução de políticas e
normas de segurança da
informação do Instituto
Nacional do Seguro Social
- INSS.

1. Trata-se dos normativos para instituição de políticas e normas de segurança da informação do Instituto Nacional do Seguro Social - INSS que foram discutidos na 6ª Reunião Ordinária do Comitê Estratégico de Governança - CEGOV, realizada no dia 22/07/2020 (Processo SEI nº 35014.164930/2020-78).
2. A Diretoria de Tecnologia da Informação e Inovação - DTI, justificou a necessidade de retorno dos autos para fins de atualização de nomenclaturas nos normativos, em atendimento ao estabelecido na Instrução Normativa nº 02, de 24 de julho de 2020, do Gabinete de Segurança Institucional da Presidência da República - GSI/PR.
3. Os ajustes foram procedidos aos normativos e as minutas atualizadas foram acostadas ao presente processo (SEI nº 1391885, 1392067, 1392184 e 1394150) conforme Despacho do Serviço de Segurança em Tecnologia da Informação e Comunicação - SSEG/CGIN/DTI (SEI 1391862).
4. Isto posto, vem-se apresentar as minutas de Resoluções para análise da Coordenação de Suporte ao Gabinete - CSG, como preceitua a Resolução nº 708/PRES/INSS/2019.
5. Após a análise das minutas, solicita-se que os autos sejam retornados ao CEGOV, antes da publicação dos normativos.

RENATO DO CARMO DAS NEVES ALVES

Coordenador-Geral de Governança - Substituto



Documento assinado eletronicamente por **RENATO DO CARMO DAS NEVES ALVES**, Técnico do Seguro Social, em 14/08/2020, às 16:12, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1406246** e o código CRC **E754C934**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1406246



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 9/CEGOV/INSS, DE DE AGOSTO DE 2020

Atualiza a
Política de
Segurança
da
Informação
do Instituto
Nacional
do Seguro
Social –
POSIN-
INSS.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do Processo Administrativo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Instituir, no âmbito do INSS, e nos termos do Anexo a esta Resolução, a Política de Segurança da Informação POSIN-INSS.

Art. 2º Fica revogada a Resolução nº 672/PRES/INSS, de 27 de dezembro de 2018, publicada no Diário Oficial da União nº 250, de 31 de dezembro de 2018, Seção 1, pág. 151.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

**ALESSANDRO ROOSEVELT SILVA
RIBEIRO**
Diretor de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração



Documento assinado eletronicamente por **DIOGO FREITAS FIGUEIREDO, Coordenador(a)**, em 26/08/2020, às 17:15, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1488248** e o código CRC **7116B590**.

ANEXO I

RESOLUÇÃO Nº 9/CEGOV/INSS, DE DE AGOSTO DE 2020

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO INSTITUTO NACIONAL DO SEGURO SOCIAL – POSIN-INSS.

Art. 1º A POSIN-INSS tem por objetivo estabelecer e difundir diretrizes e princípios de Segurança da Informação – SI, com vistas à orientação para uso e proteção adequados das informações produzidas e custodiadas pelo Instituto, preservando sua disponibilidade, integridade, confidencialidade e autenticidade.

Parágrafo único. A Política de que trata o **caput** e suas normas complementares aplicam-se a todos os agentes públicos que têm vínculo direto e/ou indireto com o Instituto.

Art. 2º Para os efeitos da POSIN-INSS, entende-se:

I - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta;

II - atividades críticas: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade, de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo;

III - ativos de informação: meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV - dados processados: dados submetidos a qualquer operação ou tratamento, por meio de

processamento eletrônico ou automatizado, com o emprego de tecnologia da informação;

V - gestor de Segurança da Informação: é o responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da Administração Pública Federal;

VI - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

VII - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

VIII - necessidade de conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

IX - riscos de segurança da informação: potencial associado à exploração de uma ou mais vulnerabilidades nos ativos de informação, em razão de ameaças, com impacto negativo às atividades do Instituto;

X - Segurança da Informação – SI: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e autenticidades das informações;

XI - vínculo direto: agentes públicos contratados diretamente pelo INSS; e

XII - vínculo indireto: agentes privados ou públicos pertencentes a órgãos ou unidades da Administração Pública Federal, Estadual ou Municipal que mantenham contrato, convênio, acordo de cooperação técnica ou instrumento congênere com o INSS.

Art. 3º Esta POSIN-INSS foi elaborada com base nos seguintes normativos:

I - Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;

II - Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto na Constituição Federal;

III - Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

IV - Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais;

V - Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

VI - Decreto nº 7.724, de 16 de maio de 2012, regulamenta a Lei nº 12.527, de 18 de novembro de 2011;

VII - Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

VIII - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

IX - Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

X - Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que disciplina a gestão de segurança da informação na Administração Pública Federal, direta e indireta, e dá outras providências;

XI - instruções normativas relacionadas à segurança da informação, publicadas pelo Gabinete de Segurança Institucional da Presidência da República;

XII - Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação; e

XIII - NBR ISO/IEC 27002:2013, que institui código de melhores práticas para a Gestão de Segurança da Informação.

Art. 4º Esta POSIN-INSS foi elaborada com base nos seguintes princípios:

I - a preservação da imagem do Instituto e de seus agentes públicos;

II - a salvaguarda das informações do cidadão;

III - ações de segurança orientadas pela gestão de riscos;

IV - continuidade assegurada dos serviços ao cidadão;

V - o alinhamento com a missão institucional e seu planejamento estratégico; e

VI - respeito à natureza e finalidade de cada área do Instituto.

Art. 5º São diretrizes gerais da POSIN-INSS:

I - tratamento da informação:

a) toda informação produzida pelos agentes públicos, no exercício de suas atividades, é de propriedade do INSS e deve ser protegida;

b) informações produzidas, armazenadas e tratadas pelo Instituto, especialmente as informações pessoais e custodiadas, devem receber o devido tratamento para assegurar sua proteção durante todo o ciclo de vida; e

c) somente os canais de comunicação disponibilizados pelo INSS devem ser utilizados para trafegar informações institucionais;

II - tratamento de incidentes de SI: todo incidente de segurança da informação deve ser imediatamente relatado à área responsável pela gestão de segurança da informação de Tecnologia da Informação – TI, observando-se a apropriada coleta de evidências;

III - gestão de riscos de segurança:

a) os riscos de segurança da informação devem ser identificados e tratados; e

b) os critérios para a gestão de risco devem ser definidos e comunicados à toda Instituição;

IV - gestão de continuidade:

a) os ativos de informação que suportam as atividades críticas do Instituto devem ser suportados por ambiente de alta disponibilidade e ter capacidade de recuperação em prazos e condições previamente definidos para situações de contingência, em conformidade com o processo de continuidade; e

b) a continuidade das operações e serviços de TI deve estar prevista nos contratos, assim como os prazos e condições devem estar formalmente estabelecidos;

V - controles de acesso:

a) todo acesso à informação deve ser motivado pela necessidade de conhecer;

b) os sistemas de informação e as instalações físicas devem ter capacidade de controlar os acessos, com fins de responsabilização pelo seu uso; e

c) as autorizações de acesso às informações, sistemas e instalações físicas devem ter critérios de acesso definidos e divulgados a todos da Instituição;

VI - recursos computacionais:

a) correio eletrônico:

1. o correio eletrônico, e-mail, é uma forma de comunicação oficial e deve ser utilizado exclusivamente no desempenho das atividades funcionais; e

2. ao produzir, responder ou encaminhar mensagem em caixa de correio eletrônico institucional, o servidor deverá se identificar, subscrevendo, ao menos, seu nome, cargo e telefone de contato institucional;

b) acesso à Internet:

1. o acesso à Internet, por meio da rede de dados do INSS, é uma concessão e deve ter seu uso orientado para a execução das atividades do Instituto; e

2. os acessos serão liberados de acordo com perfis previamente definidos pelo órgão responsável pelos serviços de TI;

c) gestão de mudanças de TI:

1. toda mudança nos sistemas de informação do INSS deve ser previamente e formalmente autorizada; e

2. a gestão de mudanças deve prever, no mínimo, a guarda dos registros, realização de testes e a possibilidade de recuperação do ambiente;

d) computação em nuvem:

1. o ambiente de computação em nuvem, sua infraestrutura e canal de comunicação devem estar aderentes às diretrizes e normas de SI, estabelecidas pelo Instituto, e às legislações vigentes; e

2. o contrato de prestação de serviço, quando for o caso, deverá conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço;

VII - educação e conscientização:

a) esta Política e seus normativos complementares devem ser periodicamente divulgados a todos os agentes públicos do Instituto;

b) o Instituto deve manter programa contínuo de conscientização dos agentes públicos em

SI; e

c) deve ser mantido plano de capacitação especializado aos profissionais que atuam na gestão de SI;

VIII - auditoria e conformidade:

a) o cumprimento desta Política e de suas normas complementares deve ser avaliado periodicamente, por meio de verificações de conformidade; e

b) o uso dos recursos de TI disponibilizados pelo Instituto é passível de monitoramento e auditoria;

IX - responsabilidade pela gestão das informações:

a) os responsáveis pela gestão dos ativos da informação e sistemas corporativos devem descrever os requisitos de segurança; e

b) os sistemas de informação devem ser concebidos possibilitando a segregação de funções;

X - segurança física e do ambiente:

a) as instalações em que as informações críticas ou sensíveis serão processadas deverão ser mantidas em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção física; e

b) os ativos da organização devem ser protegidos contra acesso físico não autorizado, danos, perdas, furto e interferência. As proteções devem estar alinhadas aos riscos identificados;

XI - gestão de ativos da informação:

a) os ativos de informação devem:

1. ser inventariados e protegidos;

2. ter identificados os seus proprietários e custodiantes;

3. ter a sua entrada e saída nas dependências do Instituto autorizadas e registradas por autoridade competente; e

4. ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 6º A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas, cíveis e penais, previstas na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), no Código Penal, no Código Civil, e, ainda, em legislação que regule ou venha regular a matéria.

Art. 7º Competências e responsabilidades:

I - cabe ao Gestor de SI:

- a) promover cultura de segurança da informação;
- b) acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
- c) propor os recursos necessários à implementação das ações de SI;
- d) coordenar o Comitê de Segurança da Informação - CSI ou estrutura equivalente;
- e) acompanhar os trabalhos e a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR-INSS;
- f) propor o detalhamento das diretrizes desta Política, por meio de normas e procedimentos, e acompanhar sua implementação;
- g) assessorar a alta administração na implementação da Política de SI;
- h) estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à SI;
- i) promover a divulgação da política e das normas internas de SI do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no INSS;
- j) incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à SI;
- k) verificar os resultados dos trabalhos de auditoria sobre a gestão da SI;
- l) acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da SI; e
- m) manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à SI;

II - cabe ao Presidente do INSS nomear o Gestor de SI;

III - caso o Gestor de SI não seja nomeado, as atribuições relacionadas no inciso I do art. 7º serão desempenhadas pelo Diretor de Tecnologia da Informação e Inovação;

IV - a ETIR-INSS deve analisar e propor respostas a notificações e atividades relacionadas a incidentes de SI, no âmbito do Instituto;

V - é responsabilidade de todos os agentes públicos, diretos e indiretos, conhecer e cumprir as diretrizes desta Política e demais normas e procedimentos complementares de SI;

VI - compete ao Comitê Estratégico de Governança - CEGOV deliberar sobre políticas e normas de segurança da informação, assessorado pelo Comitê Temático de Governança Digital, tendo em vista o Sistema de Governança do INSS, instituído pela Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019.

Parágrafo único. O Comitê Temático de Gestão da Informação é responsável pela aprovação de procedimentos e de normas internas que orientem o compartilhamento de dados sob gestão do INSS e pela aprovação da categorização dos níveis de compartilhamento de dados com outras entidades públicas (federais ou de outras esferas e poderes) da sociedade civil, nos termos do art. 6º do anexo à Portaria nº 3.213/PRES/INSS, de 2019.

Art. 8º Esta Política e seus normativos devem ser revisados sempre que necessário, não excedendo o período máximo de 3 (três) anos.

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 31/12/2018 | Edição: 250 | Seção: 1 | Página: 151

Órgão: Ministério do Desenvolvimento Social/Instituto Nacional do Seguro Social/Presidência

RESOLUÇÃO Nº 672, DE 27 DE DEZEMBRO DE 2018

Atualiza a Política de Segurança da Informação e Comunicações do Instituto Nacional do Seguro Social - POSIC-INSS.

FUNDAMENTAÇÃO LEGAL:

Decreto nº 3.505, de 13 de junho de 2000;

Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008; e

Norma Complementar nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009.

O PRESIDENTE DO INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS, no uso das atribuições que lhe confere o Decreto nº 9.104, de 24 de julho de 2017, e considerando a necessidade de estabelecer diretrizes para proteção das informações geradas, processadas e armazenadas no âmbito do INSS, resolve:

Art. 1º Fica instituída, nos termos do Anexo a esta Resolução, a Política de Segurança da Informação e Comunicações do Instituto Nacional do Seguro Social - POSIC-INSS.

Parágrafo único. A Política instituída no caput será publicada em Boletim de Serviço.

Art. 2º Revoga-se a Resolução nº 323/PRES/INSS, de 22 de julho de 2013, publicada no Diário Oficial da União nº 140, de 23 de julho de 2003.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

EDISON ANTONIO COSTA BRITTO GARCIA

Este conteúdo não substitui o publicado na versão certificada.



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 10/CEGOV/INSS, DE DE AGOSTO DE 2020

Define as regras para emissão de credenciais de acesso lógico.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do Processo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Instituir, na forma do Anexo I, a Norma de Controle de Acesso Lógico - NCAL do INSS, e aprovar os Anexos II e III.

Art. 2º Fica revogada a Resolução nº 413/PRES/INSS, de 20 de maio de 2014, publicada no Diário Oficial da União nº 95, de 21 de maio de 2014, Seção 1, pág. 43/44.

Art. 3º Esta Resolução entra em na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

**ALESSANDRO ROOSEVELT SILVA
RIBEIRO**
Diretor de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e
Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **DIOGO FREITAS FIGUEIREDO, Coordenador(a)**, em 26/08/2020, às 17:15, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1490843** e o código CRC **6B1DBB66**.

ANEXO I

RESOLUÇÃO Nº 10/CEGOV/INSS, DE DE AGOSTO DE 2020

NORMA DE CONTROLE DE ACESSO LÓGICO – INSS

Art. 1º Os termos definidos nesta norma aplicam-se a todos os agentes públicos e privados com vínculo direto ou indireto, permanente ou temporário com o INSS.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Federais vinculados à Advocacia-Geral da União – AGU, que atuarem na consultoria e no assessoramento jurídico, e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta Norma de Controle de Acesso Lógico, são estabelecidos os seguintes conceitos e definições:

I - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

II - administrador de domínio: usuário responsável pela administração de um domínio por meio da aplicação de políticas globais, criação, edição e exclusão de usuários e grupos, e instalação de programas em um grande número de estações de trabalho;

III - administrador local: usuário responsável pela administração de partes de um domínio (geralmente restrito a um setor ou abrangência), por meio de políticas locais, edição de grupos e usuários locais, e instalação de programas em estações de trabalho limitadas a um setor ou abrangência;

IV - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta;

V - ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VI - contas de serviço: contas de acesso à rede corporativa de computadores, necessárias para a execução de procedimentos automáticos (aplicação, **script**, etc.), sem qualquer intervenção humana no seu uso;

VII - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais;

VIII - credenciamento: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer;

IX - necessidade de conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

X - credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física, como crachá, cartão e selo ou lógica como identificação usuário e senha;

XI - dado: é um elemento informativo concreto e sua forma plural expressa uma informação, é o registro do atributo de um ente objeto ou fenômeno onde registro indica o ato de registrar, ou seja, é a gravação ou a impressão de caracteres ou símbolos que tenham um significado em algum documento ou suporte físico;

XII - domínio: agrupamento lógico de computadores em rede que compartilham recursos em um banco de dados de segurança, comum, onde a administração e autenticação são centralizadas. Desta forma um usuário precisa de uma conta para ter acesso ao domínio e aos recursos compartilhados;

XIII - endereço IP (**Internet Protocol**): conjunto de elementos numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores. Sequência de números associada a cada computador conectado à Internet. No caso de IPv4, o endereço IP é dividido em quatro grupos, separados por "." e compostos por números entre 0 e 255. No caso de IPv6, o endereço IP é dividido em até oito grupos, separados por ":" e compostos por números hexadecimais (números e letras de "A" a "F") entre 0 e FFFF;

XIV - entidade externa: organização governamental, não governamental ou privada, amparada por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica ou instrumento congênere com o INSS;

XV - e-SIC: Sistema Eletrônico do Serviço de Informações ao Cidadão, aplicação disponibilizada na internet, que centraliza todos os pedidos de informações dirigidos ao Poder Executivo Federal;

XVI - estagiário: educando que esteja frequentando o ensino regular, em instituições de educação superior, de educação profissional, de ensino médio, de educação especial e dos anos finais do ensino fundamental, na modalidade profissional da educação de jovens e adultos, que desenvolve as atividades relacionadas à sua área de formação profissional junto as pessoas Jurídicas de Direito Privado, órgãos da Administração Pública e Instituições de Ensino, que tenham condições de proporcionar experiência prática na sua linha de formação;

XVII - estágio supervisionado: ato educativo escolar supervisionado, desenvolvido no ambiente de trabalho, que visa a preparação para o trabalho produtivo de educandos;

XVIII - ferramenta de gestão de acessos: **software** que possibilita a gestão integrada de papéis e permissões de acesso dos usuários nos sistemas corporativos;

XIX - gestor da informação: usuário que gerou a informação, que responde pelo seu conteúdo ou que foi formalmente designado para definir, alterar a sua classificação nos graus de sigilo e perfil de acesso dos demais usuários e processos;

XX - gestão de identidades: combinação de sistemas técnicos, regras e procedimentos que definem a posse, utilização e segurança de uma identidade. Seu objetivo primário é estabelecer a confiança na associação de atributos a uma identidade digital e conectar esta identidade com uma entidade individual;

XXI - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXII - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

XXIII - **log** ou registro de auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional;

XXIV - perfil de acesso do usuário: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

XXV - recursos de rede: dispositivos (impressoras, **scanners**, multifuncionais, etc) ou serviços (sistemas, portais, etc) disponibilizados para os usuários por meio de uma rede de dados;

XXVI - serviço de diretório: serviço que armazena e organiza informações relativas a recursos disponíveis e usuários de uma rede de dados. Permite que o administrador da rede gerencie o acesso de usuários e sistemas aos recursos disponíveis;

XXVII - sistemas corporativos: sistemas de operação, ou finalísticos, que se coadunam com os fins da Previdência Social. Assim, entende-se que este conceito comporta o conjunto de sistemas e subsistemas que garantem a operação dos Regimes Geral e Próprio de Previdência Social, inclusive de previdência complementar;

XXVIII - sistemas legados: compreendem o conjunto de aplicações desenvolvidas com tecnologias obsoletas que permanecem em operação no INSS;

XXIX - usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal, formalizada por meio da

assinatura do Termo de Responsabilidade;

XXX - usuário interno: servidor do quadro do INSS lotado em uma Unidade Orgânica – UO, que se utiliza dos sistemas corporativos do Instituto; e

XXXI - usuário externo: usuários vinculados a uma Entidade Externa, que se utiliza dos sistemas corporativos do Instituto por meio de um perfil de acesso concedido por um Gestor de Acesso Externo.

Art. 3º São diretrizes desta NCAL-INSS:

I - o acesso à rede e aos sistemas corporativos do INSS dar-se-á por meio de autenticação integrada de domínio baseado em serviço de diretório, administrado por meio de uma ferramenta de gestão de identidades;

II - as concessões de acesso à rede de dados e aos sistemas corporativos são distintas. Sendo assim, o usuário pode obter permissão de acesso apenas à rede de dados, ou apenas a determinado (s) sistema (s) corporativo (s);

III - as credenciais de acesso a rede de dados e aos sistemas corporativos do INSS são conferidas aos usuários com base na necessidade de conhecer, para viabilizar o exercício de suas atribuições funcionais e atividades a serem desenvolvidas no âmbito do INSS; e

IV - o uso indevido de informações dos sistemas corporativos do INSS sujeitará o agente às penalidades previstas na legislação.

Art. 4º Base Cadastral é a base de dados do Serviço de Diretórios (acesso à rede de dados), do Sistema de Gestão de Acessos (sistemas corporativos) e dos sistemas legados, que devem ser alimentadas por informações disponibilizadas pelo INSS. Para tanto, a área responsável pela gestão de pessoas do INSS disponibilizará semanalmente as informações extraídas do Sistema Integrado de Administração de Recursos Humanos – SIAPE para a empresa prestadora de serviços tecnológicos contratada pelo Instituto, com a supervisão da área de gestão de TI do INSS, contendo, minimamente, os seguintes dados:

Tabela 1: Informações Usuários

ITEM	INFORMAÇÃO	CAMPO	DESCRIÇÃO
1	GR-MATRICULA	N 0012	GRUPO NUMÉRICO COMPOSTO DE NÚMERO DO ÓRGÃO (N0005) E NÚMERO DE MATRÍCULA DO SERVIDOR (N0007)
2	IT-NU-IDEN-SERV-ORIGEM	A 0008	NÚMERO DE IDENTIFICAÇÃO DO SERVIDOR NA ORIGEM - NÚMERO VINCULADO AO CARGO EFETIVO OU EM COMISSÃO
3	IT-NO-SERVIDOR	A 0060	NOME

4	IT-DA-NASCIMENTO	N 0008	DATA DE NASCIMENTO
5	IT-NU-CPF	N 0011	NÚMERO DO CPF
6	IT-NU-PIS-PASEP	N 0011	NÚMERO DO PIS
7	IT-IN-SUPRESSAO-PAGAMENTO	A 0001	INDICATIVO DE SUPRESSÃO DE PAGAMENTO
8	IT-CO-SITUACAO-SERVIDOR	N 0002	CÓDIGO DE SITUAÇÃO FUNCIONAL DO SERVIDOR
9	IT-CO-GRUPO-OCOR-AFASTAMENTO	N 0002	CÓDIGO DE OCORRÊNCIA DE AFASTAMENTO
10	IT-DA-INICIO-OCOR-AFASTAMENTO	N 0008	DATA DO INÍCIO DA OCORRÊNCIA DE AFASTAMENTO
11	IT-DA-TERMINO-OCOR-AFASTAMENTO	N 0008	DATA DE TÉRMINO DA OCORRÊNCIA DE AFASTAMENTO
12	IT-CO-GRUPO-OCOR-EXCLUSAO	N 0002	CÓDIGO DE OCORRÊNCIA DE EXCLUSÃO
13	IT-CO-UORG-LOTACAO-SERVIDOR	N 0009	CÓDIGO DA UORG DE LOTAÇÃO DO SERVIDOR
14	IT-CO-ORGAO-REQUISITANTE	N 0005	CÓDIGO DO ÓRGÃO REQUISITANTE

Parágrafo único. A Diretoria de Tecnologia da Informação e Inovação procederá com a atualização das bases cadastrais do serviço de diretórios e dos sistemas corporativos, bem como realizará a validação das informações disponibilizados pelo INSS por meio de outras bases, na periodicidade do envio das informações, e a área responsável pela gestão de pessoas do INSS poderá acordar, com a área responsável pela gestão de TI do INSS, a revisão das informações necessárias à administração de contas de usuários.

Art. 5º Sobre credenciais e perfis de acesso, verifica-se que a emissão de uma credencial permite ao usuário acessar a rede de dados corporativa do INSS. Para que o mesmo obtenha acesso aos sistemas corporativos, a credencial deve ser associada a um perfil de acesso, e o o processo de credenciamento de usuário aos ativos de informação deve ser feito observando os seguintes critérios:

I - a credencial de acesso concedida para acesso à rede de dados e sistemas corporativos do INSS é de caráter pessoal e intransferível;

II - as credenciais de acesso devem ser concedidas após a data de contratação ou entrada em exercício do usuário; e

III - as mesmas credenciais de acesso devem ser utilizadas para o acesso à rede de dados e aos sistemas corporativos do INSS, mediante autenticação que permita ao usuário acessar vários sistemas, por meio de ferramenta de gestão de identidades e acessos.

§ 1º A área responsável pela gestão de pessoas do INSS deverá utilizar os canais de atendimento disponibilizados pela empresa prestadora de serviços tecnológicos contratada pelo Instituto, ou outro canal informado pela DTI, para solicitar:

I - o credenciamento de usuários do quadro de pessoal do INSS na data do ato administrativo de retorno ou ingresso no órgão, para acesso à rede, e de estagiários, após assinatura do contrato de prestação de serviço, para acesso à rede;

II - a revogação de credenciais de acesso de servidores do quadro de pessoal do INSS cedidos a outros órgãos;

III - a desativação de usuários do quadro de pessoal do INSS na data do ato administrativo ou de ocorrências que ensejem desligamento para fins de acesso lógico; e

IV - a desativação do acesso de usuários do quadro de pessoal em atividade do INSS afastados ou com licença programada de suas funções por mais de sessenta dias ininterruptos.

§ 2º Quanto ao processo de formação das credenciais de acesso fica estabelecido que o nome do usuário será composto de acordo com os padrões estabelecidos no Guia de Interoperabilidade do Governo Eletrônico – e-Ping, mais especificamente no documento “Caixas Individuais-Fundacionais no Governo Federal” (Rede do Governo, 2010) que define regras de formação de nomes para a composição de endereços eletrônicos.

§ 3º Com relação às senhas de acesso, deve se observar que:

I - deverão ter no mínimo oito caracteres e conter, obrigatoriamente, caracteres alfanuméricos (combinação de letras e números). O usuário poderá acrescentar caracteres especiais (espaços em branco, símbolos, sinais de pontuação, etc.);

II - é vedada a reutilização das últimas quatro senhas utilizadas pelo usuário;

III - podem ser alteradas sempre que preciso ou quando o usuário achar necessário;

IV - o prazo de validade não deve ultrapassar 90 (noventa) dias; e

V - o usuário receberá, por meio de comunicado direto (via interface do sistema ou por mensagem no correio eletrônico), a informação do prazo próximo de vencimento da senha, quando esta estiver a 15 (quinze) dias da sua data de expiração.

§ 4º Os perfis de acesso aos sistemas corporativos deverão contemplar um conjunto de permissões e ações vinculadas às atividades desenvolvidas pelo usuário, sendo que:

I - caberá à área responsável pela gestão de TI do INSS estabelecer, em conjunto com as áreas responsáveis pela gestão dos sistemas corporativos, a norma de criação dos perfis de acesso;

II - as áreas responsáveis pela gestão dos sistemas corporativos são responsáveis pelas permissões, transações e ações que devem compor cada perfil de acesso; e

III - os perfis de acesso e de gestão concedidos para usuários internos e externos deverão ser objeto de revisão contínua pelos gestores responsáveis, não podendo ultrapassar o prazo máximo de 30 (trinta) meses.

§ 5º Quanto à utilização das credenciais e perfis de acesso, o usuário:

I - deve ter conhecimento prévio desta Norma de Controle de Acesso Lógico e preencher os requisitos estabelecidos na mesma;

II - deve estar devidamente autorizado a utilizar a rede corporativa e/ou os sistemas corporativos, de acordo com os requisitos estabelecidos nesta Norma;

III - deve utilizar os serviços e as informações obtidas, por meio do perfil de acesso, única e exclusivamente em razão do exercício da função pública e para os fins que lhe foi designado, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal;

IV - não pode divulgar, nem mesmo compartilhar, os códigos de segurança que lhe forem atribuídos (credenciais de acesso), os quais são pessoais e intransferíveis;

V - não pode utilizar as credenciais para acessar os recursos disponíveis em mais de uma estação de trabalho simultaneamente;

VI - não pode fazer uso das credenciais de acesso de outros usuários;

VII - deve fornecer informações acessadas nos sistemas e na rede de dados corporativos do INSS somente mediante demanda formalizada de quem tenha competência para tal;

VIII - deve comunicar à chefia imediata ou responsável pela administração do sistema ou rede corporativa quaisquer violações ou incidentes referentes à proteção do equipamento utilizado, do **software** ou de outros ativos da informação;

IX - deve, sempre que for necessário, afastar-se da estação de trabalho, certificar-se de que a sessão de rede ou acesso ao sistema corporativo esteja encerrado ou bloqueado;

X - deverá, obrigatoriamente, efetuar processo de alteração da sua senha em seu primeiro acesso à rede de dados corporativa; e

XI - no ato do primeiro acesso, bem como após cada atualização desta Norma, o usuário deverá manifestar concordância com os termos dispostos na mesma.

§ 6º O processo de autenticação de usuários deve ser definido pela área responsável pela gestão de Tecnologia da Informação do Instituto e poderá ser baseada em autenticação simples (nome de usuário e senha) agregada a autenticação multifator (certificação digital ou outros meios disponíveis).

§ 7º O credenciamento de usuários internos se dá pelo cadastro de novos servidores ou ocupantes de cargo em comissão, no âmbito do Instituto, pode ser solicitado por servidor vinculado à área responsável pela gestão de pessoas ou pela chefia imediata do usuário.

§ 8º O cadastro de que trata o § 7º deve ser solicitado por meio dos canais de atendimento disponibilizados pela prestadora de serviços tecnológicos contratada pelo Instituto ou outro informado pela DTI.

§ 9º O credenciamento de estagiários, se dará com a emissão de credencial de acesso, tendo como requisito as seguintes condições:

I - a empresa que atuar como agente de integração do estágio supervisionado deve manter contrato com o INSS;

II - o contrato de estágio supervisionado deverá conter cláusula de confidencialidade e sigilo de informações preestabelecidos com a Administração Pública;

III - a criação de perfis específicos e restritos às atividades do estagiário pelos gestores dos sistemas corporativos para o acesso dos estagiários;

IV - é vedada a concessão de perfis de acesso aos sistemas corporativos para estagiários com permissão de alteração das bases de dados institucionais;

V - o acesso será concedido mediante solicitação expressa de servidor do quadro do INSS, responsável pela supervisão do estágio, que deverá avaliar os riscos de utilização indevida de informações institucionais e as eventuais restrições referentes aos dias e horários para a realização dos acessos;

VI - o acesso será precedido da assinatura do Termo de Confidencialidade e de Manutenção de Sigilo – TCMS, Anexo II, o qual deverá ser firmado pelo estagiário ou pelo estagiário e seu responsável legal, no caso de se tratar de estagiário menor de 18 (dezoito) anos;

VII - as solicitações de acesso à rede para estagiários devem ser procedidas por meio dos canais remotos de atendimento disponibilizados pela empresa prestadora de serviços tecnológicos contratada pelo Instituto ou outro canal informado pela DTI, pela unidade de gestão de pessoas, pela chefia imediata do educando ou pelo responsável por sua supervisão;

VIII - os gestores de sistemas devem criar perfis diferenciados para estagiários de nível médio e nível superior;

IX - o supervisor do estagiário deverá, periodicamente, orientá-lo quanto ao uso responsável e adequado do acesso aos sistemas corporativos; e

X - o acesso do estagiário limitar-se-á à data final do contrato ou imediatamente cessado na hipótese de rescisão antecipada do estágio, cabendo ao supervisor do estagiário, em quaisquer dos casos, adotar as providências necessárias ao bloqueio do acesso, tão logo finde a contratação.

§ 10. O credenciamento de usuários externos, obedecerá as seguintes diretrizes:

I - as credenciais de acesso para usuários externos devem ser emitidas tendo em vista o interesse do INSS, devidamente justificadas e previstas no convênio, acordo de cooperação técnica ou instrumento congênere;

II - as solicitações de emissão de credenciais de acesso à rede corporativa para usuários amparados por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica, contrato ou instrumento congênere devem:

a) ser feitas pelo gestor da unidade/área responsável pela gestão do instrumento legal; e

b) ser atendidas somente após validação das credenciais do gestor solicitante do Instituto, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700);

III - a emissão de credenciais de acesso à rede corporativa para prestadores de serviço terceirizados ou equiparados nas dependências do INSS, quando necessária, será provida unicamente pelo interesse do INSS, devendo ser atendidos os seguintes requisitos:

a) a organização a qual o usuário é vinculado deve manter contrato, acordo de cooperação, convênio ou instrumento congênere vigente com o INSS;

b) instrumento deve conter cláusulas prevendo:

1. a necessidade e justificativa para acesso à rede corporativa;

2. a confidencialidade e sigilo de informações preestabelecidas junto ao Instituto; e

3. a obrigatoriedade da organização ou do ente contratado informar previamente ao representante legal do INSS, responsável pela gestão do contrato, quaisquer alterações em seu corpo de colaboradores que impacte na emissão/exclusão das contas de acesso;

c) a organização ou ente contratado também deverá manter com seus colaboradores Termo

de Confidencialidade de Manutenção de Sigilo – TCMS; e

d) o gestor do contrato pelo INSS deve fundamentar a necessidade do acesso à rede para prestadores de serviço terceirizados ou equiparados, definindo os recursos que devem ser disponibilizados e eventuais restrições a dias e horas para realização do acesso à rede;

IV - os TCMS deverão ser arquivados junto aos instrumentos assinados com o INSS e uma cópia ou **link** eletrônico deverá ser encaminhada ao Gestor do Contrato. O mesmo deve ocorrer para quaisquer alterações ocorridas na vigência dos contratos, acordos ou convênios;

V - caso os Termos sejam gerados de forma eletrônica, deverá ser disponibilizado o arquivo correspondente, atendendo aos requisitos necessários para garantia de integridade e disponibilidade de acesso, assim como os requisitos específicos previstos em contrato; e

VI - a emissão de credenciais de acesso poderá ser feita pelo gestor do contrato, representante legal do INSS, ou pelo gestor da unidade responsável pela gestão do contrato, convênio, acordo de cooperação técnica ou instrumento congênere e serão atendidas somente após validação das credenciais do solicitante, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700).

§ 11. O acesso aos prestadores de serviço vinculados à Central de Atendimento 135 se dará observando as seguintes condições:

I - a empresa deve manter contrato com o INSS;

II - o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

III - a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade - TCMS;

IV - o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte do INSS, definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;

V - os acessos deverão ser realizados única e exclusivamente por necessidade de serviço;

VI - os contratos de prestação de serviços de teleatendimento devem conter documento a ser utilizado para formalização das indicações de gestores de acesso aos sistemas corporativos do Instituto; e

VII - o INSS pode disponibilizar, de forma restrita, às centrais 135, uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

§ 12. Nos casos referentes a prestadores de serviço vinculados à Ouvidoria do Ministério da Economia, o acesso se dará observando-se as seguintes condições:

I - a empresa deve manter contrato direto com a Ouvidoria do Ministério da Economia;

II - o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

III - a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade;

IV - o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte da Ouvidoria do Ministério da Economia, definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;

V - os acessos deverão ser realizados única e exclusivamente por necessidade de serviço; e

VI - o INSS pode disponibilizar, de forma restrita, à Ouvidoria do Ministério da Economia, uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

§ 13. O acesso à rede corporativa por servidores vinculados a órgãos de controle externo, envolvidos em ações de auditoria no âmbito do INSS, será concedido mediante apresentação da equipe de auditoria por meio de documento formal que conste:

I - dados necessários ao cadastro de usuários externos;

II - informações acerca dos objetivos dos trabalhos a serem executados;

III - os prazos envolvidos; e

IV - informações complementares.

§ 14. O tipo de acesso de que trata o § 12 deverá observar:

I - as parcerias institucionalmente estabelecidas entres esses órgãos e o INSS no que tange à cobertura/previsão de acesso à rede corporativa do Instituto;

II - o atendimento de pedido de solicitação de informações advindo de pessoas físicas ou jurídicas externas, respeitadas as restrições de acesso às informações previstas na Lei nº 12.527, de 18 de novembro de 2011, serão analisadas pela área designada para responder as demandas dos cidadãos por meio do e-SIC; e

III - os procedimentos referentes às solicitações de inclusão, exclusão, inativação e suspensão de contas de acesso de usuários devem ser executados tendo como premissa a preservação dos registros para efeito de auditoria.

§ 15. O bloqueio administrativo se dará da seguinte forma:

I - o responsável pela Corregedoria-Geral do INSS, quando necessário, poderá solicitar a suspensão, bloqueio ou inativação imediata de contas de acesso de usuários que estiverem envolvidos em inquérito penal, em Processo Administrativo Disciplinar – PAD ou em Sindicância, decorrente de infrações cometidas no exercício das atribuições do cargo, quando o usuário estiver na seguinte situação:

a) afastado temporariamente do cargo ou função pública em razão de ato que se encontra sob apuração;

b) indiciado em processo administrativo disciplinar, por incursão nos incisos IX, XI, XII, XV, XVI e XVII do art. 117 e arts. 130 e 132 da Lei nº 8.112, de 11 de dezembro de 1990, ou cuja proposta pela Comissão Processante, no relatório final, seja pela aplicação de penalidade a partir de suspensão de 30 (trinta) dias; e

c) submetido à prisão em flagrante, temporária ou preventiva decorrente do cometimento de infração no exercício das atribuições do cargo, enquanto estiver em apuração de inquérito policial ou pelo Ministério Público Federal;

II - as solicitações de que tratam o inciso I deverão ser efetuadas mediante comunicação formal da Corregedoria-Geral para a prestadora de serviços tecnológicos contratada pelo Instituto, ou outro canal informado pela DTI, a qual procederá a imediata implementação da mudança;

III - o bloqueio de acessos tratados nas situações do inciso I serão efetivados no âmbito da ferramenta de gestão de acessos nas seguintes situações:

a) usuário afastado temporariamente do cargo ou função, enquanto durar o afastamento; e

b) usuário indiciado nos termos da alínea "c" do inciso I do § 15, até o efetivo cumprimento da penalidade porventura aplicada ou, em caso de não aplicação de penalidade, enquanto durar o processo.

Art. 6º A Rede de Dados Corporativa compõe a infraestrutura de rede, que é disponibilizada para uso institucional, logo, apenas equipamentos de propriedade do Instituto são autorizados e devem ser conectados à rede corporativa.

§ 1º Em casos excepcionais, a conexão de equipamentos particulares à rede corporativa deve ser feita em razão do interesse do Instituto e sob prévia autorização do responsável pela gestão da unidade em que o equipamento estiver localizado.

§ 2º O INSS poderá disponibilizar o acesso à rede de dados corporativa por meio de tecnologia **Wireless** (sem fio). Para tanto os seguintes critérios deverão ser adotados:

I - os projetos que envolvam a utilização de pontos de acesso sem fio à rede corporativa no âmbito do Instituto deverão ser devidamente registrados e aprovados pela área responsável pela gestão de TI do INSS;

II - os pontos de acesso à rede de dados corporativa sem fio poderão ser objeto de testes periódicos de penetração e de auditoria a critério da área responsável pela gestão de TI no INSS; e

III - as conexões à rede sem fio serão avaliadas pela área responsável pela gestão de TI do INSS em relação aos requisitos de segurança e deverão atender ao princípio do privilégio mínimo.

§ 3º A área responsável pela gestão de TI do INSS poderá disponibilizar rede sem fio com regras específicas de acesso para visitantes nas diversas unidades do Instituto.

§ 4º Os dispositivos conectados à rede do INSS por meio de conexão sem fio deverão suportar configurações de criptografia estabelecidas pela área responsável pela gestão de TI no âmbito do INSS;

§ 5º Qualquer tecnologia de acesso sem fio implementada no INSS deverá suportar autenticação forte, com possibilidade de efetuar checagens em bancos de dados externos, e a área responsável pela gestão de TI do INSS deve dispor de mecanismos automáticos que possibilitem:

I - a detecção e bloqueio de equipamentos externos conectados à rede corporativa; e

II - a identificação e rastreamento dos endereços IP de origem e destino, bem como os serviços utilizados na rede corporativa inclusive nos acessos remotos.

§ 6º A administração da rede corporativa trata da operacionalização da rede do INSS, que é realizada por empresa prestadora de serviços tecnológicos contratada pelo Instituto e seguem as seguintes premissas:

I - prover, gerenciar e operacionalizar os ativos, acessos e serviços que compõem a rede de dados corporativa do INSS; e

II - submeter-se ao monitoramento de serviços de tecnologia contratados pelo Instituto, seguindo as regras desta Norma.

§ 7º Quanto ao processo de geração de contas de serviço, fica estabelecido que:

I - os critérios para a emissão de contas de serviços serão vinculados a um processo formal estabelecido pela área responsável pela gestão de TI do INSS;

II - a concessão de contas de serviços deve ser feita conforme a necessidade de uso de acordo com os critérios estabelecidos nesta Norma;

III - o direito de acesso privilegiado, por meio de contas de serviços, associado a sistemas

ou processos, deve ser identificado;

IV - deve ser viabilizada ferramenta que possibilite a gestão das contas de serviço de forma automatizada, possibilitando o registro e verificação de todos os privilégios concedidos;

V - as contas de serviço fornecidas devem ser utilizadas exclusivamente para os fins aos quais foram concedidas;

VI - as contas de serviço emitidas devem ser revalidadas periodicamente com base na função exercida e na área de atuação do servidor; e

VII - as contas de serviço com credenciais de acesso de uso compartilhado devem ter suas senhas alteradas periodicamente, conforme estabelecido nesta Norma de Controle de Acesso Lógico, ou sempre que ocorrerem mudanças no grupo de usuários que utilizam as mesmas.

§ 8º É vedado o uso da rede corporativa para:

I - acesso por meio de equipamento não homologado ou não autorizado pelo INSS;

II - fazer download, instalar e/ou utilizar sistemas ou aplicativos não homologados pela área responsável pela gestão de TI do INSS nos equipamentos de propriedade do Instituto;

III - a utilização de **softwares** particulares em equipamentos do INSS sem autorização expressa;

IV - a instalação e conexão de equipamentos particulares à rede corporativa do Instituto sem a prévia autorização do gestor responsável pela unidade ou da área responsável pela gestão de TI do INSS;

V - o uso dos recursos de rede para fins particulares ou de terceiros alheios aos interesses do INSS, em especial, quando tal procedimento prejudique o tráfego da rede de dados;

VI - o uso para fins de divulgação ou distribuição de material que não possua vínculo com as atividades desenvolvidas pelo Instituto;

VII - a instalação ou utilização de ferramentas de monitoramento de rede sem a anuência e autorização expressa da área responsável pela gestão de TI no Instituto;

VIII - a instalação de dispositivos de comunicação ou de compartilhamento de dados sem fio, particulares, à rede corporativa do Instituto, sem autorização expressa da área responsável pela gestão de TI do INSS; e

IX - burlar as regras de acesso a internet configuradas em **proxy** ou ferramenta similar de gerenciamento de conteúdo **web**.

§ 9º Cabe à área responsável pela gestão de TI no âmbito do INSS definir os aspectos relacionados à plataforma tecnológica, gestão operacional, forma de autenticação e sustentação do domínio de rede do INSS.

Art. 7º A Gestão do Acesso aos Sistemas Corporativos seguirá as seguintes premissas:

I - sistemas legados:

a) as regras estabelecidas nesta norma devem ser aplicadas, guardando-se as devidas limitações tecnológicas, aos sistemas legados; e

b) o controle de acesso aos sistemas legados é efetuado por base própria;

II - sistemas de apoio à administração:

a) os ambientes de hospedagem desses sistemas são suportados por terceiros;

b) o ambiente deverá ser gerenciado e operacionalizado pela área de gestão de TI do INSS;

c) o acesso pelos usuários a esses sistemas deverá ser autenticado pelo serviço de diretório utilizado pelo Instituto; e

d) as regras de hospedagem de sistemas serão definidas, em ato próprio, pela área de gestão de TI do INSS;

III - armazenamento de registros **logs**:

a) as áreas responsáveis pela gestão de sistemas corporativos e demais aplicações devem definir, em conjunto com a área responsável pela gestão de TI, a temporalidade de registro dos **logs** de acesso e transações, e quais registros devem ser armazenados por um período maior que o estipulado no **caput** do art. 8º;

b) o INSS poderá alterar a temporalidade destes dados em norma específica; e

c) os **logs** de acesso devem contemplar minimamente os registros relacionados no Anexo III;

IV - administração da ferramenta de gestão de acesso:

a) com o objetivo de operacionalizar a gestão dos acessos aos sistemas corporativos no âmbito do INSS, serão criados os seguintes papéis:

1. administrador de sistema INSS: servidor do quadro, lotado na área responsável pela gestão de TI, designado por meio de Portaria do Diretor de Tecnologia da Informação e Inovação, a ser publicada em Boletim de Serviço – BS, responsável pela administração da ferramenta de gestão de acesso aos sistemas corporativos no âmbito do INSS;

2. gestor de sistema: servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em BS, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedoria-Geral e Procuradoria Federal Especializada junto ao INSS - PFE-INSS. É responsável pela implementação de sistemas corporativos no âmbito do INSS;

3. gestor de acesso central: servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em BS, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedoria-Geral e PFE-INSS. É responsável pela manutenção dos perfis de gestão dos usuários nas áreas que compõem a Administração Central e, quando necessário, dos gestores de acesso das Superintendências-Regionais - SR;

4. gestor de acesso interno: servidor do quadro, lotado na Administração Central, SR, Gerência-Executiva - GEX, Agência da Previdência Social - APS, indicado pelo Gestor de Acesso Central ou por um Gestor de Acesso, responsável pela atribuição do perfil de acesso e de gestão dos usuários no INSS; e

5. gestor de acesso externo: pessoa formalmente indicada, por documento previsto no instrumento legal que firmou a parceria ou por meio de Ofício de lavra do representante máximo de uma Entidade Externa, responsável pelo cadastro de usuários externos e a gestão dos acessos aos sistemas corporativos do Instituto;

b) os perfis de acesso serão atribuídos de acordo com a necessidade do fluxo de operação definido para cada sistema corporativo;

c) a indicação e o processo de substituição dos responsáveis pela gestão dos acessos aos sistemas corporativos no âmbito do INSS poderá ser procedida das seguintes formas:

1. a autoridade responsável pela indicação do gestor de acessos pode indicar opcionalmente o substituto;

2. o próprio gestor de acessos pode designar, a qualquer momento, por meio da ferramenta de gestão de acessos um substituto;

3. quando não houver um gestor responsável, ou substituto, por uma unidade devidamente designado, a gestão dos usuários será transferida, preferencialmente de forma automática, para o responsável pela área da abrangência daquela unidade e assim subsequentemente; e

4. o Gestor de Acesso é corresponsável com os perfis de gestão ou acesso que ele atribuir aos usuários;

d) ao usuário interno cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Norma de Controle de Acesso Lógico e suas normas complementares;

2. solicitar, ao Gestor de Acesso responsável pela gestão da unidade de lotação a qual é vinculado, a suspensão do seu perfil de acesso nos períodos de afastamento do serviço por mais de 30 (trinta) dias consecutivos;

3. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e

4. ter conhecimento e estar de acordo com o disposto nesta Norma;

e) ao usuário externo cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Norma de Controle de Acesso Lógico;

2. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e

3. ter conhecimento e estar de acordo com o disposto nesta Norma;

f) ao administrador do sistema INSS cabe:

1. criar os sistemas e subsistemas, devidamente homologados pela área de negócio responsável, no ambiente de produção, por meio de ferramenta de gestão de acesso;

2. mediante apresentação de Portaria de designação para Gestores de Acesso Central, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores quanto à atribuição dos perfis de gestão; e

3. mediante apresentação de Portaria de designação para Gestores de Sistema, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores acerca do processo de implementação dos sistemas corporativos no âmbito do INSS;

g) ao gestor de sistema cabe:

1. efetuar os procedimentos de importação, inclusão, alteração e exclusão de papéis e permissões nos sistemas corporativos em ambiente de produção; e

2. atuar, em conjunto com o Administrador do Sistema INSS e a prestadora de serviços tecnológicos contratada pelo Instituto, no planejamento e execução do processo de implementação dos sistemas corporativos dos quais for designado responsável;

h) ao gestor de acesso central cabe:

1. efetuar o credenciamento, suspensão ou exclusão de perfis de gestão dos sistemas corporativos aos Gestores de Acesso na Administração Central e, quando necessário, dos Gestores de Acesso da SR, GEX, APS e demais usuários de sua abrangência; e

2. orientar os usuários de sua abrangência e os gestores da Administração Central e SR, GEX e APS acerca das regras para o acesso aos sistemas corporativos do INSS;

i) ao gestor de acesso interno cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários da Administração Central, SR, GEX, APS;

2. atribuir, alterar ou excluir os perfis de acesso aos usuários da Administração Central, SR, GEX, APS; e

3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS;

j) ao gestor de acesso externo cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários do seu Órgão/Entidade;

2. atribuir, alterar ou excluir os perfis de acesso aos usuários do seu Órgão/Entidade; e

3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS;

V - configura-se mau uso, sujeito a responsabilidade penal, civil e disciplinar:

a) a divulgação, sem autorização expressa da chefia imediata ou do gestor de acesso de sua abrangência, de informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS;

b) acessar sistemas corporativos sem autorização prévia, de acordo com os requisitos estabelecidos nesta Norma;

c) utilizar-se das informações obtidas por meio de acesso concedido em desacordo com os procedimentos dispostos nesta Norma e demais normas vigentes na Administração Pública Federal;

II - utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do INSS;

III - contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que disciplina a gestão de segurança da informação na Administração Pública Federal, direta e indireta, e dá outras providências;

IV - utilizar as credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do INSS;

V - responder, perante o INSS, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

_____, _____ de _____ de _____

Nome e assinatura do usuário:	Unidade de Lotação:
Nome e assinatura da Autoridade Responsável pela Autorização do Acesso:	

ANEXO III

RESOLUÇÃO Nº 10/CEGOV/INSS, DE _____ DE AGOSTO DE 2020

REGISTROS DE LOGS

1. Relação dos campos de registros de logs do GERID
 - 1.1. Dados Gerais
 - 1.1.1. Data
 - 1.1.2. Sistema
 - 1.1.3. Ambiente
 - 1.1.4. IP destino
 - 1.1.5. IP origem
 - 1.1.6. CPF usuário

- 1.1.7. URL de origem
- 2. Ações:
 - 2.1. CAS (autenticação): Central **Authentication Service** - Serviço Central de Autenticação
 - 2.1.1. Criação de **service ticket** (ST)
 - 2.1.2. Criação de **ticket granting ticket** (TGT)
 - 2.1.3. validação de ST
 - 2.1.4. Exclusão de **ticket** TGT
 - 2.1.5. Autenticação com sucesso (**login+password**)
 - 2.1.6. Autenticação com sucesso (certificado digital)
 - 2.1.7. Autenticação com falha
 - 2.2. GPA: Gerenciamento de Permissão de Acesso
 - 2.2.1. Início de sessão
 - 2.2.2. Dados do usuário em sessão (CPF, NOME, PAPEL)
 - 2.2.3. Requisição de **logout**
 - 2.2.4. Dados de credenciais
 - 2.2.5. Concessão de credenciais
 - 2.2.6. Alteração de Credenciais
 - 2.2.7. Dados de receptor (CPF, NOME, Lotação)
 - 2.2.8. Inserção de credencial no usuário
 - 2.2.9. Revogação de Credenciais
 - 2.2.10. Pesquisa de credenciais
 - 2.2.11. Pesquisa de usuários
 - 2.2.12. Substituição de gestor

RESOLUÇÃO Nº 413 /PRES/INSS, DE 20 DE MAIO DE 2014

Institui a Política de Controle de Acesso Lógico no âmbito do Instituto Nacional do Seguro Social.

FUNDAMENTAÇÃO LEGAL:

Decreto nº 7.556, de 24 de agosto de 2011;
Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008;
Norma Complementar nº 7/IN01/DSIC/GSIPR de 6 de maio de 2010;
Resolução nº 323/PRES/INSS, de 22 de julho de 2013; e
Portaria nº 947/PRES/INSS, de 29 de setembro de 2011.

O **PRESIDENTE DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS**, no uso das atribuições que lhe confere o Decreto nº 7.556, de 24 de agosto de 2011, considerando a necessidade de definir as regras para a emissão de credenciais de acesso à rede de dados e aos sistemas corporativos do INSS,

RESOLVE:

Art. 1º Fica instituída, nos termos do Anexo I desta Resolução, a Política de Controle de Acesso Lógico (PCAL) do INSS.

Art. 2º A área responsável pela gestão de Tecnologia da Informação e Comunicações (TIC) do INSS deve gerar, em articulação com as áreas responsáveis pela gestão de aplicações corporativas e com a Empresa de Tecnologia e Informações da Previdência Social (Dataprev), o Plano de Convergência do Processo de Autenticação (PCPA), documento este que detalhará as fases e os prazos envolvidos na migração do atual ambiente de autenticação para acesso aos sistemas e rede de dados corporativos para o ambiente de autenticação descrito na política ora instituída.

Parágrafo único. O PCPA deve ser publicado, por meio de portaria do responsável pela gestão de TIC do INSS.

Art. 3º Os Anexos a esta Resolução serão publicados em Boletim de Serviço.

Art. 4º Revoga-se a Resolução nº 171/PRES/INSS, de 21 de dezembro de 2011.

Art. 5º Esta Resolução entra em vigor na data de sua publicação.

LINDOLFO NETO DE OLIVEIRA SALES
Presidente

Publicada no DOU nº 95 de 21/5/2014, Seção 1, pág. 43/44



INSTITUTO NACIONAL DO SEGURO SOCIAL
RESOLUÇÃO Nº 11/CEGOV/INSS, DE DE AGOSTO DE 2020

MINUTA DE RESOLUÇÃO

Institui a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR do Instituto Nacional do Seguro Social.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do Processo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Instituir, no âmbito do INSS, e nos termos do Anexo a esta Resolução, a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR-INSS.

Art. 2º Esta Resolução complementa Política de Segurança da Informação POSIN-INSS vigente.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

**ALESSANDRO ROOSEVELT SILVA
RIBEIRO**
Diretor de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **DIOGO FREITAS FIGUEIREDO, Coordenador(a)**, em 26/08/2020, às 17:15, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1491471** e o código CRC **CAF4E4CC**.

ANEXO

RESOLUÇÃO Nº 11/CEGOV/INSS, DE DE DE 2020

EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS - ETIR-INSS

Art. 1º A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR-INSS tem por objetivo agir proativamente, receber, analisar, monitorar, coordenar e propor respostas a notificações e atividades relacionadas a incidentes de segurança da informação e comunicações no âmbito do INSS.

Art. 2º As atividades pertinentes à ETIR-INSS englobam os usuários dos serviços de Tecnologia da Informação - TI e os sistemas de informação do INSS e serão realizadas com intercâmbio de informações e em cooperação com as seguintes instâncias:

I - o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR GOV;

II - a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR de empresas prestadoras de serviços de tecnologia contratadas pelo INSS;

III - as ETIRs ou estrutura equivalente dos demais órgãos, entidades e empresas, públicas ou privadas, que tenham contratos, acordos, convênios ou instrumentos congêneres com o INSS; e

IV - o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República – GSI/PR.

Art. 3º Para os efeitos desta Resolução ficam estabelecidos os seguintes conceitos e definições:

I - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR: equipe de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

II - CTIR GOV: Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI;

III - agente responsável: servidor público ocupante de cargo efetivo de órgão ou entidade da Administração Pública Federal, direta ou indireta ou militar de carreira incumbido de chefiar e gerenciar uma ETIR;

IV - artefato malicioso: qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

V - Comunidade ou Público Alvo: conjunto de pessoas, setores, órgãos ou entidades atendidas por uma ETIR ou estrutura equivalente;

VI - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VII - serviço: conjunto de procedimentos, estruturados em processo definido, oferecido à comunidade pela ETIR;

VIII - Tratamento de Incidentes de Segurança em Redes Computacionais: serviço consistente em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

IX - usuário: pessoas que fazem uso de serviços de TI e sistemas de informação de propriedade do INSS, independentemente do cargo ocupado (contratados, consultores, conselheiros, servidores, temporários e etc.); e

X - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que possam resultar em risco para um sistema ou por uma organização, e que possam ser evitados por uma ação interna de segurança da informação.

Art. 4º A implementação e o funcionamento da ETIR-INSS seguirão metodologia definida pelo GSI/PR e as seguintes diretrizes:

I - basear-se no “Modelo 1 – Utilizando a equipe de Tecnologia da Informação”, conforme definido pelo GSI/PR;

II - os integrantes da Equipe deverão ser profissionais da área de Tecnologia da Informação, servidores públicos efetivos, lotados na Diretoria de Tecnologia da Informação e Inovação – DTI do INSS, sem prejuízo de suas atribuições típicas do cargo, com experiência e conhecimentos técnicos compatíveis com a importância da missão da ETIR-INSS;

III - a ETIR-INSS ficará vinculada tecnicamente à Coordenação-Geral de Infraestrutura e Operações – CGIN da DTI;

IV - o Coordenador da ETIR-INSS será nomeado por ato do Diretor de Tecnologia da

V - na ausência de Coordenador formalmente nomeado, as atribuições relacionadas à coordenação da equipe serão desempenhadas pelo Coordenador-Geral de Infraestrutura e Operações.

Art. 5º A ETIR-INSS será composta por membros:

I - permanentes, que efetivamente atuarão em todos os incidentes registrados;

II - colaboradores, que atuarão, de forma esporádica, no tratamento de incidentes relacionados às suas áreas de atuação; e

III - opcionais, servidores das unidades descentralizadas do INSS sob supervisão da DTI.

§ 1º Os membros da ETIR-INSS serão designados por meio de ato do Diretor de Tecnologia da Informação e Inovação.

§ 2º A distribuição dos membros da ETIR-INSS se dará da seguinte forma:

I - 2 (dois) servidores permanentes, oriundos do Serviço de Segurança de TIC;

II - 2 (dois) servidores colaboradores, oriundos da CGIN;

III - 2 (dois) servidores colaboradores, oriundos da Coordenação-Geral de Projetos e Soluções Digitais da DTI; e

IV - 2 (dois) servidores opcionais, oriundos das unidades descentralizadas do INSS.

Art. 6º A ETIR-INSS terá autonomia limitada para o tratamento de incidentes de Segurança da Informação, devendo implementar ações que possam impactar outras áreas do Instituto somente com anuência do Diretor de Tecnologia da Informação e Inovação e do Gestor responsável pela área/sistema afetada, e poderá, ainda, gerar relatórios técnicos sugerindo a adoção de medidas para resolução de incidentes.

Art. 7º A ETIR-INSS fornecerá o serviço de Tratamento de Incidentes de Segurança em Redes Computacionais, que compreende as seguintes ações:

I - recepção de solicitações e alertas diversos, utilizando como canal de comunicação a caixa postal etir@inss.gov.br, a ser disponibilizada pelo INSS;

II - filtragem de todo conteúdo direcionado à ETIR-INSS, para fins de verificação quanto à necessidade de tratamento pela Equipe e, caso não se trate de incidente de segurança em redes computacionais, encaminhar para a área competente;

III - catalogação dos incidentes detectados em ferramenta a ser indicada pela DTI, com nível de acesso restrito;

IV - classificação dos incidentes detectados quanto ao nível de severidade e impacto;

V - tratamento do incidente com medidas corretivas e indicação de formas de se evitar que ocorra novamente;

VI - resposta às solicitações e alertas encaminhados para a ETIR; e

VII - monitoramento da aplicação do tratamento dos incidentes indicados.

§ 1º A ETIR-INSS deverá analisar os incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências; e

§ 2º O detalhamento dos serviços prestados pela ETIR-INSS deverá ser publicado em página específica da Intranet do INSS, no prazo de 30 (trinta) dias a partir da publicação desta Resolução.



INSTITUTO NACIONAL DO SEGURO SOCIAL
RESOLUÇÃO Nº 12/CEGOV/INSS, DE DE AGOSTO DE 2020

MINUTA DE RESOLUÇÃO

Disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso à Internet, competências e conteúdo de acesso para cada perfil.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do Processo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Estabelecer, nos termos do Anexo a esta Resolução, os critérios para o uso da Internet no âmbito do INSS.

Art. 2º Esta Resolução complementa a Política de Segurança da Informação POSIN-INSS vigente.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES Presidente	ALESSANDRO ROOSEVELT SILVA RIBEIRO Diretor de Benefícios
JOBSON DE PAIVA SILVEIRA SALES Diretor de Atendimento	HELDER CALADO DE ARAÚJO Diretor de Gestão de Pessoas e Administração
CLÓVIS DE CASTRO JÚNIOR Diretor de Integridade, Governança e Gerenciamento de Riscos	FLÁVIO FERREIRA DOS SANTOS Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **DIOGO FREITAS FIGUEIREDO, Coordenador(a)**, em 26/08/2020, às 17:15, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1510981** e o código CRC **AF84DE92**.

ANEXO

RESOLUÇÃO Nº 12/CEGOV/INSS, DE DE AGOSTO DE 2020

NORMAS DE USO DA INTERNET

Art. 1º Esta norma se aplica a todos os servidores e colaboradores, vinculados direta ou indiretamente ao INSS, bem como a servidores e empregados de entidades e órgãos da Administração Pública ou privados que necessitem ou estejam autorizados a acessar a Internet a partir da rede corporativa do Instituto.

Paragrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União – AGU que atuarem na consultoria, assessoramento jurídico e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta norma, ficam estabelecidos os seguintes conceitos e definições:

I - autorizador: ocupantes de cargo responsáveis pela autorização da concessão de perfis de acesso para usuários finais de sua área de abrangência;

II - Internet: rede mundial que interliga computadores de diferentes tipos e dimensões e permite a comunicação entre pessoas e organizações, independentemente da localização geográfica;

III - Intranet: rede de computadores administrada pelo INSS, que utiliza os mesmos serviços e tecnologias disponíveis na rede mundial;

IV - perfil de acesso: atributo que estabelece as categorias de sítios acessíveis e tipos de arquivos que podem ser recebidos ou transmitidos pelos usuários;

V - **proxy**: ferramenta que desempenha a função de conexão do computador local à rede externa (Internet);

VI - sítio: conjunto de informações ou serviços disponíveis na Internet ou na Intranet, organizados em páginas eletrônicas e acessíveis por meio de endereços que identificam, de forma padronizada, sua origem e conteúdo;

VII - usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal-APF, formalizada por meio da assinatura do Termo de Responsabilidade; e

VIII - VPN: Rede Privada Virtual (**Virtual Private Network**) construída sobre a infraestrutura de uma rede pública, possibilitando a conexão de dois computadores por meio de uma rede pública.

Art. 3º O acesso pelos usuários à Internet disponibilizado pelo INSS deverá pautar-se pelas seguintes diretrizes:

I - seu uso se dará exclusivamente em razão de trabalho e de acordo com os procedimentos dispostos nesta Norma;

II - os recursos disponibilizados pelo INSS não poderão ser usados para quaisquer propósitos ilegais ou proibidos, que possam danificar, desativar, sobrecarregar ou prejudicar qualquer área, serviço ou conteúdo, ou interferir no uso e execução das atividades laborais de outros usuários;

III - o volume de tráfego de Internet e os endereços **web** visitados poderão ser monitorados, visando assegurar o cumprimento desta norma; e

IV - o acesso à Internet para propósitos particulares ou estranhos às atividades do INSS poderá ser bloqueado, sem prévia comunicação ao usuário e sem prejuízo das demais sanções aplicáveis.

Art. 4º O acesso aos sítios da Internet para todos os usuários será realizado mediante a atribuição de perfis de acesso, distribuídos nos seguintes níveis:

I - Perfil 1: Perfil Restrito, inicialmente atribuído a usuários com maior restrição de acesso à Internet, permitindo acesso somente a sítios governamentais, instituições bancárias e sítios considerados de interesse do INSS;

II - Perfil 2: Perfil Básico, inicialmente atribuído a estagiários, recepcionistas e usuários externos, permitindo acesso a todos os sítios permitidos pelo Perfil 1 e a sítios de provedores de e-mail pessoal e instituições de ensino;

III - Perfil 3: Perfil Padrão para os servidores do quadro do Instituto, permitindo acesso a todos os sítios da Internet,

exceto aqueles que contêm veiculação de material em áudio e vídeo; e

IV - Perfil 4: Perfil Avançado, atribuído preferencialmente a servidores do quadro do Instituto e estagiários que desempenham funções relacionadas a Comunicação Social, Desenvolvimento de Pessoas e gestores, respeitado o princípio da necessidade de conhecer e demandando designação dos Autorizadores deste Perfil. Permite acesso todos os sítios da Internet, incluindo sítios que veiculam material em áudio e vídeo (**streaming**), sítios de compartilhamento de vídeos, blogs e redes sociais.

§ 1º O perfil concedido a agentes externos será de caráter temporário, com validade equivalente à vigência do trabalho a ser executado.

§ 2º Os processos de alteração, bloqueio, liberação e categorização de sítios, assim como a criação e/ou alterações de perfis de acesso descritos nesta Norma, quando necessários, serão definidos pela Diretoria de Tecnologia da Informação e Inovação – DTI, e publicados no Portal do INSS na Intranet.

§ 3º Os novos usuários que não tiverem um perfil de acesso atribuído deverão ser direcionados para uma página da Intranet contendo orientações e normas relacionadas ao acesso à Internet no INSS, definidas pela DTI.

Art. 5º O acesso à Intranet e Internet a partir da rede de dados corporativa nas dependências do INSS e aos demais órgãos da Administração Pública Direta e Indireta, de qualquer das esferas de governo, será concedido exclusivamente a servidores e empregados públicos, efetivos ou ocupantes de cargo em comissão.

§ 1º O acesso de usuários externos das entidades que compõem o Poder Público será concedido mediante o estabelecimento em convênio, contrato, acordo de cooperação técnica ou instrumento congênere, especificamente firmados com o INSS para este fim.

§ 2º O gestor ou Coordenador-Geral da área responsável pelo convênio, contrato, acordo de cooperação técnica ou instrumento congênere assumirá o papel de Autorizador do serviço de acesso à Internet para os usuários externos, e deverá fundamentar as solicitações com base no instrumento.

§ 3º Poderão ser concedidos acessos temporários para auditores de controle interno e externo, vinculados à Controladoria-Geral da União – CGU ou do Tribunal de Contas da União - TCU, no uso de suas atribuições.

Art. 6º O acesso à Internet por terceirizados deverá ser provido pela empresa contratada.

Parágrafo único. Em caráter de exceção, poderá ser concedido o acesso aos terceirizados a partir da infraestrutura de rede do INSS, desde que preenchidos os seguintes requisitos:

I - o contrato de prestação de serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

II - a empresa contratada deverá manter com seus funcionários Termo de Confidencialidade;

III - o contrato de prestação de serviços deverá prever a necessidade de acesso à Internet a partir das dependências do INSS; e

IV - o Autorizador, que para estes fins será o gestor do contrato ou o responsável pela área requisitante do serviço, deverá fundamentar as necessidades de acesso dos empregados da contratada, definindo os recursos que serão disponibilizados, endereços da Intranet e Internet necessários para o desenvolvimento das atividades e eventuais restrições a dias e horários para realização do acesso.

Art. 7º A conexão de equipamentos pessoais de visitantes à rede do INSS, quando necessária e motivada pelo interesse da Administração, deverá ser previamente autorizada pelo gestor da unidade onde o equipamento será utilizado.

Parágrafo único. Só será permitida a utilização da rede local por visitantes caso seus equipamentos atendam a todos os requisitos estabelecidos pela DTI e o acesso se dará, exclusivamente, à Internet, sendo vedado o acesso ao conteúdo disponibilizado na Intranet.

Art. 8º A todos os perfis de acesso descritos nesta Norma aplicam-se as restrições de acesso a sítios que:

I - contenham material pornográfico ou obsceno;

II - contenham material ilegal;

III - disponibilizem jogos, inclusive os da Internet (**on line**);

IV - contenham material impróprio, ofensivo, preconceituoso ou discriminatório, que façam apologia à violência, ao terrorismo e às drogas; e

V - contenha e/ou divulgue conteúdo de violação de direito autoral (pirataria) e/ou execução de quaisquer tipos ou formas de fraudes.

Art. 9º O processo de atribuição de acesso à Internet seguirá as seguintes diretrizes:

I - a atribuição dos perfis de acesso à Internet serão feitas pelos Autorizadores, de forma fundamentada e respeitando o princípio da necessidade de conhecer, de acordo com a tabela abaixo:

Perfil	Autorizador
Perfil 1, 2 e 3	Gerente de Agência da Previdência Social - APS, Gerente-Executivo, Superintendentes-Regionais, Procuradores -Regionais, Coordenadores-Gerais, Superintendentes-Regionais, Presidente do INSS, Auditor-Geral, Corregedor-Geral, Procurador-Geral da PFE-INSS, Diretores, Gestores ou Chefes da área responsável pelo Contrato ou ato administrativo similar no âmbito do INSS.
Perfil 4	Chefes de Assessoria de Comunicação Social nas Superintendências-Regionais, Assessor de Comunicação Social (Administração Central), Diretor de Tecnologia da Informação e Inovação, Diretor de Gestão de Pessoas e Administração e Presidente do INSS.

II - nos casos de novos usuários de rede (LDAP), criados por meio de registro de chamado técnico, quando o solicitante não indicar o perfil de acesso à internet, será atribuído o Perfil 1;

III - para fins de alteração do perfil de acesso, os usuários deverão preencher o “Formulário de Acesso à Internet” (Anexo II) e providenciar a assinatura pelo Autorizador do acesso; e

IV - ao registrar a solicitação, deve-se anexar o Formulário de Solicitação de Acesso à Internet devidamente preenchido e assinado (pelo solicitante e Autorizador), conforme documento nato digital ou digitalizado no formato PDF.

Art. 10. A solicitação para perfis de acesso em caráter temporário deverá conter, no Formulário de Solicitação de Acesso à Internet, a motivação da necessidade e a data de início e de expiração do acesso.

Art. 11. Das responsabilidades:

I - O usuário deverá:

a) preencher os requisitos e termos estabelecidos nesta Norma;

b) estar devidamente autorizado a utilizar a Internet nas formas estabelecidas nesta norma;

c) fazer uso da Internet de forma responsável e segura, utilizando o acesso exclusivamente em razão de trabalho, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal; e

d) impedir a divulgação e compartilhamento das chaves de segurança atribuídas, que são pessoais e intransferíveis.

II - o autorizador deverá:

a) conceder os perfis de acesso à Internet rigorosamente de acordo com as atribuições dos usuários de sua abrangência, observando os normativos do INSS;

b) verificar periodicamente o uso dos acessos concedidos e, sempre que necessário, solicitar alteração dos perfis de acesso dos usuários de sua abrangência; e

c) reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR-INSS;

III - a área responsável pela gestão de TI no INSS deverá:

a) monitorar os acessos à internet e sua utilização de acordo com as diretrizes estabelecidas nesta norma; e

b) identificar os casos de mau uso da Internet e adotar uma ou mais das seguintes providências:

1. alertar ao usuário, responsável pelo acesso, e ao Autorizador, responsável pela concessão, acerca do uso indevido da internet; e

2. nos casos de reincidência, solicitar a revogação do acesso à internet concedido ao usuário e encaminhar a documentação que comprova a má utilização do acesso concedido para a Corregedoria do INSS, para análise e adoção das medidas cabíveis.

Art. 12. Configura-se como uso indevido da Internet:

I - acessar a Internet disponibilizada pelo INSS sem estar devidamente autorizado, conforme estabelecido nesta Norma;

II - não manifestar concordância com as regras estabelecidas nesta norma e nas demais aplicáveis;

III - fazer uso dos recursos de Internet disponibilizados pelo INSS para fins alheios ao trabalho, em discordância com os procedimentos dispostos nesta Norma, sem prejuízo de demais normatizações vigentes na Administração Pública Federal;

IV - utilizar os serviços extrapolando os privilégios do perfil de acesso que lhe foi designado;

V - divulgar e/ou compartilhar as chaves de segurança, que são pessoais e intransferíveis, permitindo a utilização por terceiros do perfil que lhe foi atribuído;

VI - praticar atos de comercialização de produtos e serviços, em proveito próprio ou de terceiros, que não atendam os interesses do INSS;

VII - utilizar recursos ou dispositivos para acesso a computadores ou redes externas ao INSS com o objetivo de obter informações não autorizadas ou provocar a interrupção de serviços de rede;

VIII - utilizar modem ou dispositivo de rede que interligue a rede interna do INSS a outras redes ou à Internet;

IX - expor, armazenar, distribuir, editar, gravar ou compartilhar, através do uso dos recursos computacionais e de comunicação do INSS, arquivos estranhos às atividades do INSS e não autorizados pela chefia imediata;

X - realizar qualquer atividade que apoie ou facilite o vazamento de dados;

XI - baixar arquivos ou programas da Internet que contrariem as diretrizes da Política de Segurança da Informação - POSIN vigente; e

XII - utilizar **proxy** não disponibilizado pelo INSS.

Art. 13. O acesso à Internet é passível de registro e monitoração, incluindo quaisquer dados transmitidos pela rede do INSS.

§ 1º Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a ETIR-INSS deverá ser imediatamente acionada, para tomar as providências necessárias a fim de sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação do INSS;

§ 2º As ocorrências de mau uso do acesso à Internet não previstas nesta norma, assim como os casos de dúvidas em relação à aplicação das disposições aqui estabelecidas, deverão ser encaminhadas à DTI para registro, análise e avaliação da necessidade de alterações de acordo com o processo de governança em vigência no INSS;

§ 3º O descumprimento desta Norma poderá acarretar ao usuário as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei, responsabilidade administrativa, civil e criminal.

Art. 14. Esta Norma deverá ser atualizada periodicamente, não excedendo o prazo máximo de 3 (três) anos.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência

Gabinete

Coordenação De Suporte ao Gabinete

DESPACHO

Coordenação De Suporte ao Gabinete, em 25/8/2020.

Ref.: Processo nº
35014.047735/2020-84.

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO, COMITÊ
ESTRATÉGICO DE
GOVERNANÇA.

A s s . : Minutas de
Resolução de políticas e
normas de segurança da
informação do Instituto
Nacional do Seguro Social
- INSS.

1. Cuidam-se de propostas de Resoluções com vistas à instituição de políticas e normas de segurança da informação no âmbito do INSS, as quais foram discutidas na 6ª Reunião Ordinária do Comitê Estratégico de Governança - CEGOV, realizada no dia 22 de julho de 2020 (Processo SEI nº 35014.164930/2020-78).

2. Em análise aos autos, verifica-se que para justificar e fundamentar a edição das Resoluções, o CEGOV emitiu a Nota Técnica nº 1/2020/CTGD - CEGOV/DIGOV/PRES-INSS (0427234), de 24 de janeiro de 2020.

3. Verifica-se, ainda, que fora invertido o trâmite previsto no art. 15 da Resolução nº 708, de 6 de novembro de 2019, sendo a análise da PFE-INSS realizada previamente à que compete a esta Coordenação, conforme preconizou a Procuradoria Federal Especializada junto ao INSS - PFE-INSS, nos itens 19 a 23 do Parecer nº 00012/2020/DAADM/PFE-INSS-SEDE/PGF/AGU (0500778).

4. Cabe salientar, ainda, que o Parecer supracitado proferiu entendimento, em síntese, *"...pela regularidade jurídico-formal das minutas apresentadas (sequencial sapiens 1 - outros 8, 9, 10, 11), considerando-a apta a produzir seus efeitos jurídicos e legais, observando-se, previamente, as considerações e sugestões deste parecer, em especial as contidas nos parágrafos 21/23, 26, 31, 32 e 33"*.

5. Em decorrência da inversão do procedimento, e efetuados os ajustes necessários pelo CEGOV, em conjunto com a Diretoria de Tecnologia da Informação e Inovação - DTI, conforme as minutas SEI nº 1391885, 1392067, 1392184 e 1394150, esta Coordenação, em seu exame, ateve-se apenas aos aspectos formais das minutas proposta, ficando a apreciação de mérito a cargo das áreas

técnicas.

6. Assim, no tocante às regras para elaboração, articulação e redação das minutas de Resolução, consigna-se a sua adequação com as regras estabelecidas na Lei Complementar nº 95, de 26 de fevereiro de 1998, no Decreto nº 9.191, de 1º de novembro de 2017, e na Resolução nº 708/PRES/INSS, de 2019, sendo analisadas e formatas por esta Coordenação, sem alteração do conteúdo minutado, cabendo ressaltar os seguintes pontos:

a) não consta na minuta o anexo citado no inciso III do art. 9º do Anexo da Minuta de Resolução 1510981;

b) quando do retorno dos autos para providências quanto à assinatura e publicação, deve-se observar, no tocante à vigência, o disposto no Decreto nº 10.139, de 28 de novembro de 2019, conforme recomendado pela PFE-INSS, na alínea "a" do item 33 do Parecer citado no item 3 do presente despacho; e

c) deve-se verificar as previsões de publicação de anexos em Boletim de Serviço, caso haja necessidade de publicação da Resolução no Diário Oficial da União, haja vista que, nos termos do art. 11 do Decreto nº 9.215, de 29 de novembro de 2017, *"Os anexos aos atos com conteúdo normativo serão publicados integralmente no Diário Oficial da União"*.

7. Diante do exposto, em atendimento ao disposto no item 5 do Despacho CEGOV SEI nº 1406246, restitua-se ao citado Comitê para conhecimento e ratificação/retificação das minutas revisadas por esta Coordenação, cujas versões finais constam dos Documentos SEI nº 1488248, nº 1490843, nº 1491471 e nº 1510981, bem como os ajustes indicados no item 6 deste Despacho.

CINTHYA DE ÁVILA OLIVEIRA TROJAN REPISO

Chefe da Divisão de Normas e Acordos

DIOGO FREITAS FIGUEIREDO

Coordenador de Suporte ao Gabinete



Documento assinado eletronicamente por **CINTHYA DE AVILA OLIVEIRA TROJAN REPISO**, **Chefe da Divisão**, em 26/08/2020, às 16:56, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **DIOGO FREITAS FIGUEIREDO**, **Coordenador(a)**, em 26/08/2020, às 17:15, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1548091** e o código CRC **02228FB0**.



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria De Integridade, Governança e Gerenciamento De Riscos
Comitê Estratégico de Governança

DESPACHO

Comitê Estratégico de Governança, em 27/08/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

A s s . : Solicita
manifestação final da
Diretoria de Tecnologia da
Informação, antes da
assinatura e publicação
das normas.

1. As normas de segurança da informação constantes dos documentos SEI nº 1488248, nº 1490843, nº 1491471 e nº 1510981 foram revisadas pela Coordenação de Suporte ao Gabinete - CSG, como determina a Resolução nº 708/PRES/INSS, de 6 de novembro de 2019, atendo-se aos aspectos formais.
2. Na análise, a CSG ressalta pontos de atenção, que constam do parágrafo 6 do Despacho CSG nº 1548091.
3. Encaminham-se, portanto, os autos à Diretoria de Tecnologia da Informação e Inovação, para que verifique as considerações da CSG, retificando e/ou ratificando os textos finais das normas.
4. Atenta-se também ao solicitado pela DTI em seu Despacho CGIN nº 1399902, que demanda, em seu parágrafo 3º, a prévia avaliação da área antes da assinatura pelos membros do CEGOV e posterior publicação das normas, para que promova uma ação coordenada junto ao prestador de serviço para providenciar as mudanças tecnológicas necessárias.
5. Ressalta-se que as normas em tela foram apreciadas e aprovadas pelo CEGOV em sua Reunião nº 6/2020, realizada em julho de 2020. Por esta razão, solicita-se agilidade da DTI quanto às tratativas necessárias, tendo em vista a importância de tais normas para a segurança da informação no Instituto.

CIBELLE CESAR DO AMARAL BRASIL
Coordenadora-Geral de Governança
Secretaria-Executiva do Comitê Estratégico de Governança



Documento assinado eletronicamente por **CIBELLE CESAR DO AMARAL BRASIL**,
Coordenador(a) Geral, em 27/08/2020, às 11:57, conforme horário oficial de Brasília, com fundamento
no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site
https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1571869** e o
código CRC **E08BBB65**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1571869



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

DESPACHO

Diretoria De Tecnologia da Informação e Inovação, em 28/08/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

A s s . : Solicita
manifestação final da
Diretoria de Tecnologia da
Informação, antes da
assinatura e publicação
das normas.

1. Ciente do despacho SEI 1571869.
2. Encaminhe-se ao Serviço de Segurança em TIC, com trâmite pela CGIN, para as tratativas necessárias.

FLÁVIO FERREIRA DOS SANTOS

Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **FLAVIO FERREIRA DOS SANTOS, Diretor(a) de Tecnologia da Informação e Inovação**, em 28/08/2020, às 09:10, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site
https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1581585** e o código CRC **F5DE934B**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1581585



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações

DESPACHO

Coordenação-Geral De Infraestrutura e Operações, em 28/08/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

A s s . : Minutas de
Resolução de políticas e
normas de segurança da
informação do Instituto
Nacional do Seguro Social
- INSS.

1. Trata-se dos normativos para instituição de políticas e normas de segurança da informação do Instituto Nacional do Seguro Social - INSS
2. Encaminha-se à SSEG para avaliação do item 6, do Despacho CGS (SEI 1548091) e Despacho CEGOV (SEI 1571869).

CLAUDIO AUGUSTO NOVAIS FERRAZ

Coordenador-Geral de Infraestrutura e Operações



Documento assinado eletronicamente por **Claudio Augusto Novais Ferraz, Coordenador(a) Geral**, em 28/08/2020, às 09:10, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site
https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1581520** e o código CRC **F1454317**.



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações
Coordenação De Suporte e Infraestrutura De Tecnologia da Informação e Comunicação
Serviço De Segurança em Tecnologia da Informação e Comunicação

DESPACHO

Serviço De Segurança em Tecnologia da Informação e Comunicação, em 28/08/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

A s s . : Minutas de
Resolução de políticas e
normas de segurança da
informação do Instituto
Nacional do Seguro Social
- INSS.

1. Trata o presente de propostas de Resoluções com vistas à instituição de políticas e normas de segurança da informação no âmbito do INSS, as quais foram discutidas na 6ª Reunião Ordinária do Comitê Estratégico de Governança - CEGOV, realizada no dia 22 de julho de 2020 (Processo SEI nº 35014.164930/2020-78).
2. Após análise da Coordenação de Suporte ao Gabinete - CSG (Documento SEI 1548091), retornam os autos para o Serviço de Segurança em Tecnologia da Informação e Comunicação - SSEG, para as devidas considerações e possíveis retificações e/ou ratificação dos textos finais das normas.
3. Sendo assim, este SSEG procedeu:
 - a) alterações necessárias nas minutas propostas para adequação ao disposto no Decreto nº 10.139, de 28 de novembro de 2019;
 - b) inclusão do Anexo II da minuta de norma que estabelece os critérios para acesso à internet (1592183);
 - c) revisão e ratificação das alterações procedidas pelo CSG, gerando assim novas versões dos atos propostos (documentos SEI 1586319, 1592201, 1592240 e 1592323).
4. Quanto ao meio de publicação dos atos (conforme os termos do art. 11 do Decreto nº 9.215, de 29 de novembro de 2017), este SSEG sugere que a Política de Segurança da Informação seja publicada no Diário Oficial da União e os demais atos e seus respectivos anexos sejam publicados em Boletim de Serviço.
5. Encaminhe-se para a Coordenação-Geral de Infraestrutura e Operações - CGIN, para conhecimento e manifestação quanto ao proposto.

ALEXINALDO MESSIAS CERQUEIRA

Chefe do Serviço de Segurança em Tecnologia da Informação e Comunicação



Documento assinado eletronicamente por **ALEXINALDO MESSIAS CERQUEIRA, Chefe de Serviço**, em 28/08/2020, às 18:51, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site

[https://sei.inss.gov.br/sei/controlador_externo.php?](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)

[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **1585512** e o código CRC **4A76FFE2**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1585512



INSTITUTO NACIONAL DO SEGURO SOCIAL
RESOLUÇÃO Nº 12/CEGOV/INSS, DE 1 DE SETEMBRO DE 2020

MINUTA DE RESOLUÇÃO

Disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso à Internet, competências e conteúdo de acesso para cada perfil.

O **COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS**, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do Processo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Estabelecer, nos termos do Anexo I a esta Resolução, os critérios para o uso da Internet no âmbito do INSS e aprovar o Anexo II.

Art. 2º Esta Resolução complementa a Política de Segurança da Informação POSIN-INSS vigente.

Art. 3º Esta Resolução entra em vigor sete dias após a data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES Presidente	ALESSANDRO ROOSEVELT SILVA RIBEIRO Diretor de Benefícios
JOBSON DE PAIVA SILVEIRA SALES Diretor de Atendimento	HELDER CALADO DE ARAÚJO Diretor de Gestão de Pessoas e Administração
CLÓVIS DE CASTRO JÚNIOR Diretor de Integridade, Governança e Gerenciamento de Riscos	FLÁVIO FERREIRA DOS SANTOS Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **ALEXINALDO MESSIAS CERQUEIRA**, **Chefe de Serviço**, em 28/08/2020, às 19:00, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1586319** e o código CRC **4FF1903F**.

ANEXO I

RESOLUÇÃO Nº 12/CEGOV/INSS, DE 1 DE SETEMBRO DE 2020

NORMAS DE USO DA INTERNET

Art. 1º Esta norma se aplica a todos os servidores e colaboradores, vinculados direta ou indiretamente ao INSS, bem como a servidores e empregados de entidades e órgãos da Administração Pública ou privados que necessitem ou estejam autorizados a

acessar a Internet a partir da rede corporativa do Instituto.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União – AGU que atuarem na consultoria, assessoramento jurídico e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta norma, ficam estabelecidos os seguintes conceitos e definições:

I - autorizador: ocupantes de cargo responsáveis pela autorização da concessão de perfis de acesso para usuários finais de sua área de abrangência;

II - Internet: rede mundial que interliga computadores de diferentes tipos e dimensões e permite a comunicação entre pessoas e organizações, independentemente da localização geográfica;

III - Intranet: rede de computadores administrada pelo INSS, que utiliza os mesmos serviços e tecnologias disponíveis na rede mundial;

IV - perfil de acesso: atributo que estabelece as categorias de sítios acessíveis e tipos de arquivos que podem ser recebidos ou transmitidos pelos usuários;

V - **proxy**: ferramenta que desempenha a função de conexão do computador local à rede externa (Internet);

VI - sítio: conjunto de informações ou serviços disponíveis na Internet ou na Intranet, organizados em páginas eletrônicas e acessíveis por meio de endereços que identificam, de forma padronizada, sua origem e conteúdo;

VII - usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal-APF, formalizada por meio da assinatura do Termo de Responsabilidade; e

VIII - VPN: Rede Privada Virtual (**Virtual Private Network**) construída sobre a infraestrutura de uma rede pública, possibilitando a conexão de dois computadores por meio de uma rede pública.

Art. 3º O acesso pelos usuários à Internet disponibilizado pelo INSS deverá pautar-se pelas seguintes diretrizes:

I - seu uso se dará exclusivamente em razão de trabalho e de acordo com os procedimentos dispostos nesta Norma;

II - os recursos disponibilizados pelo INSS não poderão ser usados para quaisquer propósitos ilegais ou proibidos, que possam danificar, desativar, sobrecarregar ou prejudicar qualquer área, serviço ou conteúdo, ou interferir no uso e execução das atividades laborais de outros usuários;

III - o volume de tráfego de Internet e os endereços **web** visitados poderão ser monitorados, visando assegurar o cumprimento desta norma; e

IV - o acesso à Internet para propósitos particulares ou estranhos às atividades do INSS poderá ser bloqueado, sem prévia comunicação ao usuário e sem prejuízo das demais sanções aplicáveis.

Art. 4º O acesso aos sítios da Internet para todos os usuários será realizado mediante a atribuição de perfis de acesso, distribuídos nos seguintes níveis:

I - Perfil 1: Perfil Restrito, inicialmente atribuído a usuários com maior restrição de acesso à Internet, permitindo acesso somente a sítios governamentais, instituições bancárias e sítios considerados de interesse do INSS;

II - Perfil 2: Perfil Básico, inicialmente atribuído a estagiários, recepcionistas e usuários externos, permitindo acesso a todos os sítios permitidos pelo Perfil 1 e a sítios de provedores de e-mail pessoal e instituições de ensino;

III - Perfil 3: Perfil Padrão para os servidores do quadro do Instituto, permitindo acesso a todos os sítios da Internet, exceto aqueles que contêm veiculação de material em áudio e vídeo; e

IV - Perfil 4: Perfil Avançado, atribuído preferencialmente a servidores do quadro do Instituto e estagiários que desempenham funções relacionadas a Comunicação Social, Desenvolvimento de Pessoas e gestores, respeitado o princípio da necessidade de conhecer e demandando designação dos Autorizadores deste Perfil. Permite acesso todos os sítios da Internet, incluindo sítios que veiculam material em áudio e vídeo (**streaming**), sítios de compartilhamento de vídeos, blogs e redes sociais.

§ 1º O perfil concedido a agentes externos será de caráter temporário, com validade equivalente à vigência do trabalho a ser executado.

§ 2º Os processos de alteração, bloqueio, liberação e categorização de sítios, assim como a criação e/ou alterações de perfis de acesso descritos nesta Norma, quando necessários, serão definidos pela Diretoria de Tecnologia da Informação – DTI, e publicados no Portal do INSS na Intranet.

§ 3º Os novos usuários que não tiverem um perfil de acesso atribuído deverão ser direcionados para uma página da Intranet contendo orientações e normas relacionadas ao acesso à Internet no INSS, definidas pela DTI.

Art. 5º O acesso à Intranet e Internet a partir da rede de dados corporativa nas dependências do INSS e aos demais órgãos da Administração Pública Direta e Indireta, de qualquer das esferas de governo, será concedido exclusivamente a servidores e empregados públicos, efetivos ou ocupantes de cargo em comissão.

§ 1º O acesso de usuários externos das entidades que compõem o Poder Público será concedido mediante o estabelecimento em convênio, contrato, acordo de cooperação técnica ou instrumento congênere, especificamente firmados com o INSS para este fim.

§ 2º O gestor ou Coordenador-Geral da área responsável pelo convênio, contrato, acordo de cooperação técnica ou instrumento congênere assumirá o papel de Autorizador do serviço de acesso à Internet para os usuários externos, e deverá fundamentar as solicitações com base no instrumento.

§ 3º Poderão ser concedidos acessos temporários para auditores de controle interno e externo, vinculados à Controladoria-Geral da União – CGU ou do Tribunal de Contas da União - TCU, no uso de suas atribuições.

Art. 6º O acesso à Internet por terceirizados deverá ser provido pela empresa contratada.

Parágrafo único. Em caráter de exceção, poderá ser concedido o acesso aos terceirizados a partir da infraestrutura de rede do INSS, desde que preenchidos os seguintes requisitos:

I - o contrato de prestação de serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

II - a empresa contratada deverá manter com seus funcionários Termo de Confidencialidade;

III - o contrato de prestação de serviços deverá prever a necessidade de acesso à Internet a partir das dependências do INSS; e

IV - o Autorizador, que para estes fins será o gestor do contrato ou o responsável pela área requisitante do serviço, deverá fundamentar as necessidades de acesso dos empregados da contratada, definindo os recursos que serão disponibilizados, endereços da Intranet e Internet necessários para o desenvolvimento das atividades e eventuais restrições a dias e horários para realização do acesso.

Art. 7º A conexão de equipamentos pessoais de visitantes à rede do INSS, quando necessária e motivada pelo interesse da Administração, deverá ser previamente autorizada pelo gestor da unidade onde o equipamento será utilizado.

Parágrafo único. Só será permitida a utilização da rede local por visitantes caso seus equipamentos atendam a todos os requisitos estabelecidos pela DTI e o acesso se dará, exclusivamente, à Internet, sendo vedado o acesso ao conteúdo disponibilizado na Intranet.

Art. 8º A todos os perfis de acesso descritos nesta Norma aplicam-se as restrições de acesso a sítios que:

I - contenham material pornográfico ou obsceno;

II - contenham material ilegal;

III - disponibilizem jogos, inclusive os da Internet (**on line**);

IV - contenham material impróprio, ofensivo, preconceituoso ou discriminatório, que façam apologia à violência, ao terrorismo e às drogas; e

V - contenha e/ou divulgue conteúdo de violação de direito autoral (pirataria) e/ou execução de quaisquer tipos ou formas de fraudes.

Art. 9º O processo de atribuição de acesso à Internet seguirá as seguintes diretrizes:

I - a atribuição dos perfis de acesso à Internet serão feitas pelos Autorizadores, de forma fundamentada e respeitando o princípio da necessidade de conhecer, de acordo com a tabela abaixo:

Perfil	Autorizador
Perfil 1, 2 e 3	Gerente de Agência da Previdência Social - APS, Gerente-Executivo, Superintendentes-Regionais, Procuradores -Regionais, Coordenadores-Gerais, Superintendentes-Regionais, Presidente do INSS, Auditor-Geral, Corregedor-Geral, Procurador-Geral da PFE-INSS, Diretores, Gestores ou Chefes da área responsável pelo Contrato ou ato administrativo similar no âmbito do INSS.
Perfil 4	Chefes de Assessoria de Comunicação Social nas Superintendências-Regionais, Assessor de Comunicação Social (Administração Central), Diretor de Tecnologia da Informação e Inovação, Diretor de Gestão de Pessoas e Administração e Presidente do INSS.

II - nos casos de novos usuários de rede (LDAP), criados por meio de registro de chamado técnico, quando o solicitante não indicar o perfil de acesso à internet, será atribuído o Perfil 1;

III - para fins de alteração do perfil de acesso, os usuários deverão preencher o “Formulário de Acesso à Internet” (Anexo II) e providenciar a assinatura pelo Autorizador do acesso; e

IV - ao registrar a solicitação, deve-se anexar o Formulário de Solicitação de Acesso à Internet devidamente preenchido e assinado (pelo solicitante e Autorizador), conforme documento nato digital ou digitalizado no formato PDF.

Art. 10. A solicitação para perfis de acesso em caráter temporário deverá conter, no Formulário de Solicitação de Acesso à Internet, a motivação da necessidade e a data de início e de expiração do acesso.

Art. 11. Das responsabilidades:

I - O usuário deverá:

a) preencher os requisitos e termos estabelecidos nesta Norma;

b) estar devidamente autorizado a utilizar a Internet nas formas estabelecidas nesta norma;

c) fazer uso da Internet de forma responsável e segura, utilizando o acesso exclusivamente em razão de trabalho, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal; e

d) impedir a divulgação e compartilhamento das chaves de segurança atribuídas, que são pessoais e intransferíveis.

II - o autorizador deverá:

a) conceder os perfis de acesso à Internet rigorosamente de acordo com as atribuições dos usuários de sua abrangência, observando os normativos do INSS;

b) verificar periodicamente o uso dos acessos concedidos e, sempre que necessário, solicitar alteração dos perfis de acesso dos usuários de sua abrangência; e

c) reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR-INSS;

III - a área responsável pela gestão de TI no INSS deverá:

a) monitorar os acessos à internet e sua utilização de acordo com as diretrizes estabelecidas nesta norma; e

b) identificar os casos de mau uso da Internet e adotar uma ou mais das seguintes providências:

1. alertar ao usuário, responsável pelo acesso, e ao Autorizador, responsável pela concessão, acerca do uso indevido da internet; e

2. nos casos de reincidência, solicitar a revogação do acesso à internet concedido ao usuário e encaminhar a documentação que comprova a má utilização do acesso concedido para a Corregedoria do INSS, para análise e adoção das medidas cabíveis.

Art. 12. Configura-se como uso indevido da Internet:

I - acessar a Internet disponibilizada pelo INSS sem estar devidamente autorizado, conforme estabelecido nesta Norma;

II - não manifestar concordância com as regras estabelecidas nesta norma e nas demais aplicáveis;

III - fazer uso dos recursos de Internet disponibilizados pelo INSS para fins alheios ao trabalho, em discordância com os procedimentos dispostos nesta Norma, sem prejuízo de demais normatizações vigentes na Administração Pública Federal;

IV - utilizar os serviços extrapolando os privilégios do perfil de acesso que lhe foi designado;

V - divulgar e/ou compartilhar as chaves de segurança, que são pessoais e intransferíveis, permitindo a utilização por terceiros do perfil que lhe foi atribuído;

VI - praticar atos de comercialização de produtos e serviços, em proveito próprio ou de terceiros, que não atendam os interesses do INSS;

VII - utilizar recursos ou dispositivos para acesso a computadores ou redes externas ao INSS com o objetivo de obter informações não autorizadas ou provocar a interrupção de serviços de rede;

VIII - utilizar modem ou dispositivo de rede que interligue a rede interna do INSS a outras redes ou à Internet;

IX - expor, armazenar, distribuir, editar, gravar ou compartilhar, através do uso dos recursos computacionais e de comunicação do INSS, arquivos estranhos às atividades do INSS e não autorizados pela chefia imediata;

X - realizar qualquer atividade que apoie ou facilite o vazamento de dados;

XI - baixar arquivos ou programas da Internet que contrariem as diretrizes da Política de Segurança da Informação - POSIN vigente; e

XII - utilizar **proxy** não disponibilizado pelo INSS.

Art. 13. O acesso à Internet é passível de registro e monitoração, incluindo quaisquer dados transmitidos pela rede do INSS.

§ 1º Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a ETIR-INSS deverá ser imediatamente acionada, para tomar as providências necessárias a fim de sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação do INSS;

§ 2º As ocorrências de mau uso do acesso à Internet não previstas nesta norma, assim como os casos de dúvidas em relação à aplicação das disposições aqui estabelecidas, deverão ser encaminhadas à DTI para registro, análise e avaliação da necessidade de alterações de acordo com o processo de governança em vigência no INSS;

§ 3º O descumprimento desta Norma poderá acarretar ao usuário as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei, responsabilidade administrativa, civil e criminal.

Art. 14. Esta Norma deverá ser atualizada periodicamente, não excedendo o prazo máximo de 3 (três) anos.



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 9/CEGOV/INSS, DE 1 DE SETEMBRO DE 2020

Atualiza a
Política de
Segurança
da
Informação
do Instituto
Nacional
do Seguro
Social –
POSIN-
INSS.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do Processo Administrativo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Instituir, no âmbito do INSS, e nos termos do Anexo a esta Resolução, a Política de Segurança da Informação POSIN-INSS.

Art. 2º Fica revogada a Resolução nº 672/PRES/INSS, de 27 de dezembro de 2018, publicada no Diário Oficial da União nº 250, de 31 de dezembro de 2018, Seção 1, pág. 151.

Art. 3º Esta Resolução entra em vigor sete dias após a data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

**ALESSANDRO ROOSEVELT SILVA
RIBEIRO**
Diretor de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração



Documento assinado eletronicamente por **ALEXINALDO MESSIAS CERQUEIRA**, **Chefe de Serviço**, em 28/08/2020, às 19:00, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1592201** e o código CRC **A6962901**.

ANEXO I

RESOLUÇÃO Nº 9/CEGOV/INSS, DE DE AGOSTO DE 2020

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO INSTITUTO NACIONAL DO SEGURO SOCIAL – POSIN-INSS.

Art. 1º A POSIN-INSS tem por objetivo estabelecer e difundir diretrizes e princípios de Segurança da Informação – SI, com vistas à orientação para uso e proteção adequados das informações produzidas e custodiadas pelo Instituto, preservando sua disponibilidade, integridade, confidencialidade e autenticidade.

Parágrafo único. A Política de que trata o **caput** e suas normas complementares aplicam-se a todos os agentes públicos que têm vínculo direto e/ou indireto com o Instituto.

Art. 2º Para os efeitos da POSIN-INSS, entende-se:

I - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta;

II - atividades críticas: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade, de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo;

III - ativos de informação: meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV - dados processados: dados submetidos a qualquer operação ou tratamento, por meio de

processamento eletrônico ou automatizado, com o emprego de tecnologia da informação;

V - gestor de Segurança da Informação: é o responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da Administração Pública Federal;

VI - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

VII - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

VIII - necessidade de conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

IX - riscos de segurança da informação: potencial associado à exploração de uma ou mais vulnerabilidades nos ativos de informação, em razão de ameaças, com impacto negativo às atividades do Instituto;

X - Segurança da Informação – SI: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e autenticidades das informações;

XI - vínculo direto: agentes públicos contratados diretamente pelo INSS; e

XII - vínculo indireto: agentes privados ou públicos pertencentes a órgãos ou unidades da Administração Pública Federal, Estadual ou Municipal que mantenham contrato, convênio, acordo de cooperação técnica ou instrumento congênere com o INSS.

Art. 3º Esta POSIN-INSS foi elaborada com base nos seguintes normativos:

I - Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;

II - Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto na Constituição Federal;

III - Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

IV - Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais;

V - Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

VI - Decreto nº 7.724, de 16 de maio de 2012, regulamenta a Lei nº 12.527, de 18 de novembro de 2011;

VII - Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

VIII - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

IX - Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

X - Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que disciplina a gestão de segurança da informação na Administração Pública Federal, direta e indireta, e dá outras providências;

XI - instruções normativas relacionadas à segurança da informação, publicadas pelo Gabinete de Segurança Institucional da Presidência da República;

XII - Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação; e

XIII - NBR ISO/IEC 27002:2013, que institui código de melhores práticas para a Gestão de Segurança da Informação.

Art. 4º Esta POSIN-INSS foi elaborada com base nos seguintes princípios:

I - a preservação da imagem do Instituto e de seus agentes públicos;

II - a salvaguarda das informações do cidadão;

III - ações de segurança orientadas pela gestão de riscos;

IV - continuidade assegurada dos serviços ao cidadão;

V - o alinhamento com a missão institucional e seu planejamento estratégico; e

VI - respeito à natureza e finalidade de cada área do Instituto.

Art. 5º São diretrizes gerais da POSIN-INSS:

I - tratamento da informação:

a) toda informação produzida pelos agentes públicos, no exercício de suas atividades, é de propriedade do INSS e deve ser protegida;

b) informações produzidas, armazenadas e tratadas pelo Instituto, especialmente as informações pessoais e custodiadas, devem receber o devido tratamento para assegurar sua proteção durante todo o ciclo de vida; e

c) somente os canais de comunicação disponibilizados pelo INSS devem ser utilizados para trafegar informações institucionais;

II - tratamento de incidentes de SI: todo incidente de segurança da informação deve ser imediatamente relatado à área responsável pela gestão de segurança da informação de Tecnologia da Informação – TI, observando-se a apropriada coleta de evidências;

III - gestão de riscos de segurança:

a) os riscos de segurança da informação devem ser identificados e tratados; e

b) os critérios para a gestão de risco devem ser definidos e comunicados à toda Instituição;

IV - gestão de continuidade:

a) os ativos de informação que suportam as atividades críticas do Instituto devem ser suportados por ambiente de alta disponibilidade e ter capacidade de recuperação em prazos e condições previamente definidos para situações de contingência, em conformidade com o processo de continuidade; e

b) a continuidade das operações e serviços de TI deve estar prevista nos contratos, assim como os prazos e condições devem estar formalmente estabelecidos;

V - controles de acesso:

a) todo acesso à informação deve ser motivado pela necessidade de conhecer;

b) os sistemas de informação e as instalações físicas devem ter capacidade de controlar os acessos, com fins de responsabilização pelo seu uso; e

c) as autorizações de acesso às informações, sistemas e instalações físicas devem ter critérios de acesso definidos e divulgados a todos da Instituição;

VI - recursos computacionais:

a) correio eletrônico:

1. o correio eletrônico, e-mail, é uma forma de comunicação oficial e deve ser utilizado exclusivamente no desempenho das atividades funcionais; e

2. ao produzir, responder ou encaminhar mensagem em caixa de correio eletrônico institucional, o servidor deverá se identificar, subscrevendo, ao menos, seu nome, cargo e telefone de contato institucional;

b) acesso à Internet:

1. o acesso à Internet, por meio da rede de dados do INSS, é uma concessão e deve ter seu uso orientado para a execução das atividades do Instituto; e

2. os acessos serão liberados de acordo com perfis previamente definidos pelo órgão responsável pelos serviços de TI;

c) gestão de mudanças de TI:

1. toda mudança nos sistemas de informação do INSS deve ser previamente e formalmente autorizada; e

2. a gestão de mudanças deve prever, no mínimo, a guarda dos registros, realização de testes e a possibilidade de recuperação do ambiente;

d) computação em nuvem:

1. o ambiente de computação em nuvem, sua infraestrutura e canal de comunicação devem estar aderentes às diretrizes e normas de SI, estabelecidas pelo Instituto, e às legislações vigentes; e

2. o contrato de prestação de serviço, quando for o caso, deverá conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço;

VII - educação e conscientização:

a) esta Política e seus normativos complementares devem ser periodicamente divulgados a todos os agentes públicos do Instituto;

b) o Instituto deve manter programa contínuo de conscientização dos agentes públicos em

SI; e

c) deve ser mantido plano de capacitação especializado aos profissionais que atuam na gestão de SI;

VIII - auditoria e conformidade:

a) o cumprimento desta Política e de suas normas complementares deve ser avaliado periodicamente, por meio de verificações de conformidade; e

b) o uso dos recursos de TI disponibilizados pelo Instituto é passível de monitoramento e auditoria;

IX - responsabilidade pela gestão das informações:

a) os responsáveis pela gestão dos ativos da informação e sistemas corporativos devem descrever os requisitos de segurança; e

b) os sistemas de informação devem ser concebidos possibilitando a segregação de funções;

X - segurança física e do ambiente:

a) as instalações em que as informações críticas ou sensíveis serão processadas deverão ser mantidas em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção física; e

b) os ativos da organização devem ser protegidos contra acesso físico não autorizado, danos, perdas, furto e interferência. As proteções devem estar alinhadas aos riscos identificados;

XI - gestão de ativos da informação:

a) os ativos de informação devem:

1. ser inventariados e protegidos;

2. ter identificados os seus proprietários e custodiantes;

3. ter a sua entrada e saída nas dependências do Instituto autorizadas e registradas por autoridade competente; e

4. ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 6º A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas, cíveis e penais, previstas na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), no Código Penal, no Código Civil, e, ainda, em legislação que regule ou venha regular a matéria.

Art. 7º Competências e responsabilidades:

I - cabe ao Gestor de SI:

- a) promover cultura de segurança da informação;
- b) acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
- c) propor os recursos necessários à implementação das ações de SI;
- d) coordenar o Comitê de Segurança da Informação - CSI ou estrutura equivalente;
- e) acompanhar os trabalhos e a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR-INSS;
- f) propor o detalhamento das diretrizes desta Política, por meio de normas e procedimentos, e acompanhar sua implementação;
- g) assessorar a alta administração na implementação da Política de SI;
- h) estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à SI;
- i) promover a divulgação da política e das normas internas de SI do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no INSS;
- j) incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à SI;
- k) verificar os resultados dos trabalhos de auditoria sobre a gestão da SI;
- l) acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da SI; e
- m) manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à SI;

II - cabe ao Presidente do INSS nomear o Gestor de SI;

III - caso o Gestor de SI não seja nomeado, as atribuições relacionadas no inciso I do art. 7º serão desempenhadas pelo Diretor de Tecnologia da Informação e Inovação;

IV - a ETIR-INSS deve analisar e propor respostas a notificações e atividades relacionadas a incidentes de SI, no âmbito do Instituto;

V - é responsabilidade de todos os agentes públicos, diretos e indiretos, conhecer e cumprir as diretrizes desta Política e demais normas e procedimentos complementares de SI;

VI - compete ao Comitê Estratégico de Governança - CEGOV deliberar sobre políticas e normas de segurança da informação, assessorado pelo Comitê Temático de Governança Digital, tendo em vista o Sistema de Governança do INSS, instituído pela Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019.

Parágrafo único. O Comitê Temático de Gestão da Informação é responsável pela aprovação de procedimentos e de normas internas que orientem o compartilhamento de dados sob gestão do INSS e pela aprovação da categorização dos níveis de compartilhamento de dados com outras entidades públicas (federais ou de outras esferas e poderes) da sociedade civil, nos termos do art. 6º do anexo à Portaria nº 3.213/PRES/INSS, de 2019.

Art. 8º Esta Política e seus normativos devem ser revisados sempre que necessário, não excedendo o período máximo de 3 (três) anos.



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 10/CEGOV/INSS, DE 1 DE SETEMBRO DE 2020

Define as regras para emissão de credenciais de acesso lógico.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do Processo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Instituir, na forma do Anexo I, a Norma de Controle de Acesso Lógico - NCAL do INSS, e aprovar os Anexos II e III.

Art. 2º Fica revogada a Resolução nº 413/PRES/INSS, de 20 de maio de 2014, publicada no Diário Oficial da União nº 95, de 21 de maio de 2014, Seção 1, pág. 43/44.

Art. 3º Esta Resolução entra em vigor sete dias após a data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

**ALESSANDRO ROOSEVELT SILVA
RIBEIRO**
Diretor de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e
Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **ALEXINALDO MESSIAS CERQUEIRA, Chefe de Serviço**, em 28/08/2020, às 19:01, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1592240** e o código CRC **1421F40E**.

ANEXO I

RESOLUÇÃO Nº 10/CEGOV/INSS, DE 1 DE SETEMBRO DE 2020

NORMA DE CONTROLE DE ACESSO LÓGICO – INSS

Art. 1º Os termos definidos nesta norma aplicam-se a todos os agentes públicos e privados com vínculo direto ou indireto, permanente ou temporário com o INSS.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Federais vinculados à Advocacia-Geral da União – AGU, que atuarem na consultoria e no assessoramento jurídico, e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta Norma de Controle de Acesso Lógico, são estabelecidos os seguintes conceitos e definições:

I - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

II - administrador de domínio: usuário responsável pela administração de um domínio por meio da aplicação de políticas globais, criação, edição e exclusão de usuários e grupos, e instalação de programas em um grande número de estações de trabalho;

III - administrador local: usuário responsável pela administração de partes de um domínio (geralmente restrito a um setor ou abrangência), por meio de políticas locais, edição de grupos e usuários locais, e instalação de programas em estações de trabalho limitadas a um setor ou abrangência;

IV - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta;

V - ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VI - contas de serviço: contas de acesso à rede corporativa de computadores, necessárias para a execução de procedimentos automáticos (aplicação, **script**, etc.), sem qualquer intervenção humana no seu uso;

VII - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais;

VIII - credenciamento: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer;

IX - necessidade de conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

X - credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física, como crachá, cartão e selo ou lógica como identificação usuário e senha;

XI - dado: é um elemento informativo concreto e sua forma plural expressa uma informação, é o registro do atributo de um ente objeto ou fenômeno onde registro indica o ato de registrar, ou seja, é a gravação ou a impressão de caracteres ou símbolos que tenham um significado em algum documento ou suporte físico;

XII - domínio: agrupamento lógico de computadores em rede que compartilham recursos em um banco de dados de segurança, comum, onde a administração e autenticação são centralizadas. Desta forma um usuário precisa de uma conta para ter acesso ao domínio e aos recursos compartilhados;

XIII - endereço IP (**Internet Protocol**): conjunto de elementos numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores. Sequência de números associada a cada computador conectado à Internet. No caso de IPv4, o endereço IP é dividido em quatro grupos, separados por "." e compostos por números entre 0 e 255. No caso de IPv6, o endereço IP é dividido em até oito grupos, separados por ":" e compostos por números hexadecimais (números e letras de "A" a "F") entre 0 e FFFF;

XIV - entidade externa: organização governamental, não governamental ou privada, amparada por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica ou instrumento congênere com o INSS;

XV - e-SIC: Sistema Eletrônico do Serviço de Informações ao Cidadão, aplicação disponibilizada na internet, que centraliza todos os pedidos de informações dirigidos ao Poder Executivo Federal;

XVI - estagiário: educando que esteja frequentando o ensino regular, em instituições de educação superior, de educação profissional, de ensino médio, de educação especial e dos anos finais do ensino fundamental, na modalidade profissional da educação de jovens e adultos, que desenvolve as atividades relacionadas à sua área de formação profissional junto as pessoas Jurídicas de Direito Privado, órgãos da Administração Pública e Instituições de Ensino, que tenham condições de proporcionar experiência prática na sua linha de formação;

XVII - estágio supervisionado: ato educativo escolar supervisionado, desenvolvido no ambiente de trabalho, que visa a preparação para o trabalho produtivo de educandos;

XVIII - ferramenta de gestão de acessos: **software** que possibilita a gestão integrada de papéis e permissões de acesso dos usuários nos sistemas corporativos;

XIX - gestor da informação: usuário que gerou a informação, que responde pelo seu conteúdo ou que foi formalmente designado para definir, alterar a sua classificação nos graus de sigilo e perfil de acesso dos demais usuários e processos;

XX - gestão de identidades: combinação de sistemas técnicos, regras e procedimentos que definem a posse, utilização e segurança de uma identidade. Seu objetivo primário é estabelecer a confiança na associação de atributos a uma identidade digital e conectar esta identidade com uma entidade individual;

XXI - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXII - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

XXIII - **log** ou registro de auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional;

XXIV - perfil de acesso do usuário: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

XXV - recursos de rede: dispositivos (impressoras, **scanners**, multifuncionais, etc) ou serviços (sistemas, portais, etc) disponibilizados para os usuários por meio de uma rede de dados;

XXVI - serviço de diretório: serviço que armazena e organiza informações relativas a recursos disponíveis e usuários de uma rede de dados. Permite que o administrador da rede gerencie o acesso de usuários e sistemas aos recursos disponíveis;

XXVII - sistemas corporativos: sistemas de operação, ou finalísticos, que se coadunam com os fins da Previdência Social. Assim, entende-se que este conceito comporta o conjunto de sistemas e subsistemas que garantem a operação dos Regimes Geral e Próprio de Previdência Social, inclusive de previdência complementar;

XXVIII - sistemas legados: compreendem o conjunto de aplicações desenvolvidas com tecnologias obsoletas que permanecem em operação no INSS;

XXIX - usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal, formalizada por meio da

assinatura do Termo de Responsabilidade;

XXX - usuário interno: servidor do quadro do INSS lotado em uma Unidade Orgânica – UO, que se utiliza dos sistemas corporativos do Instituto; e

XXXI - usuário externo: usuários vinculados a uma Entidade Externa, que se utiliza dos sistemas corporativos do Instituto por meio de um perfil de acesso concedido por um Gestor de Acesso Externo.

Art. 3º São diretrizes desta NCAL-INSS:

I - o acesso à rede e aos sistemas corporativos do INSS dar-se-á por meio de autenticação integrada de domínio baseado em serviço de diretório, administrado por meio de uma ferramenta de gestão de identidades;

II - as concessões de acesso à rede de dados e aos sistemas corporativos são distintas. Sendo assim, o usuário pode obter permissão de acesso apenas à rede de dados, ou apenas a determinado (s) sistema (s) corporativo (s);

III - as credenciais de acesso a rede de dados e aos sistemas corporativos do INSS são conferidas aos usuários com base na necessidade de conhecer, para viabilizar o exercício de suas atribuições funcionais e atividades a serem desenvolvidas no âmbito do INSS; e

IV - o uso indevido de informações dos sistemas corporativos do INSS sujeitará o agente às penalidades previstas na legislação.

Art. 4º Base Cadastral é a base de dados do Serviço de Diretórios (acesso à rede de dados), do Sistema de Gestão de Acessos (sistemas corporativos) e dos sistemas legados, que devem ser alimentadas por informações disponibilizadas pelo INSS. Para tanto, a área responsável pela gestão de pessoas do INSS disponibilizará semanalmente as informações extraídas do Sistema Integrado de Administração de Recursos Humanos – SIAPE para a empresa prestadora de serviços tecnológicos contratada pelo Instituto, com a supervisão da área de gestão de TI do INSS, contendo, minimamente, os seguintes dados:

Tabela 1: Informações Usuários

ITEM	INFORMAÇÃO	CAMPO	DESCRIÇÃO
1	GR-MATRICULA	N 0012	GRUPO NUMÉRICO COMPOSTO DE NÚMERO DO ÓRGÃO (N0005) E NÚMERO DE MATRÍCULA DO SERVIDOR (N0007)
2	IT-NU-IDEN-SERV-ORIGEM	A 0008	NÚMERO DE IDENTIFICAÇÃO DO SERVIDOR NA ORIGEM - NÚMERO VINCULADO AO CARGO EFETIVO OU EM COMISSÃO
3	IT-NO-SERVIDOR	A 0060	NOME

4	IT-DA-NASCIMENTO	N 0008	DATA DE NASCIMENTO
5	IT-NU-CPF	N 0011	NÚMERO DO CPF
6	IT-NU-PIS-PASEP	N 0011	NÚMERO DO PIS
7	IT-IN-SUPRESSAO-PAGAMENTO	A 0001	INDICATIVO DE SUPRESSÃO DE PAGAMENTO
8	IT-CO-SITUACAO-SERVIDOR	N 0002	CÓDIGO DE SITUAÇÃO FUNCIONAL DO SERVIDOR
9	IT-CO-GRUPO-OCOR-AFASTAMENTO	N 0002	CÓDIGO DE OCORRÊNCIA DE AFASTAMENTO
10	IT-DA-INICIO-OCOR-AFASTAMENTO	N 0008	DATA DO INÍCIO DA OCORRÊNCIA DE AFASTAMENTO
11	IT-DA-TERMINO-OCOR-AFASTAMENTO	N 0008	DATA DE TÉRMINO DA OCORRÊNCIA DE AFASTAMENTO
12	IT-CO-GRUPO-OCOR-EXCLUSAO	N 0002	CÓDIGO DE OCORRÊNCIA DE EXCLUSÃO
13	IT-CO-UORG-LOTACAO-SERVIDOR	N 0009	CÓDIGO DA UORG DE LOTAÇÃO DO SERVIDOR
14	IT-CO-ORGAO-REQUISITANTE	N 0005	CÓDIGO DO ÓRGÃO REQUISITANTE

Parágrafo único. A Diretoria de Tecnologia da Informação e Inovação procederá com a atualização das bases cadastrais do serviço de diretórios e dos sistemas corporativos, bem como realizará a validação das informações disponibilizados pelo INSS por meio de outras bases, na periodicidade do envio das informações, e a área responsável pela gestão de pessoas do INSS poderá acordar, com a área responsável pela gestão de TI do INSS, a revisão das informações necessárias à administração de contas de usuários.

Art. 5º Sobre credenciais e perfis de acesso, verifica-se que a emissão de uma credencial permite ao usuário acessar a rede de dados corporativa do INSS. Para que o mesmo obtenha acesso aos sistemas corporativos, a credencial deve ser associada a um perfil de acesso, e o o processo de credenciamento de usuário aos ativos de informação deve ser feito observando os seguintes critérios:

I - a credencial de acesso concedida para acesso à rede de dados e sistemas corporativos do INSS é de caráter pessoal e intransferível;

II - as credenciais de acesso devem ser concedidas após a data de contratação ou entrada em exercício do usuário; e

III - as mesmas credenciais de acesso devem ser utilizadas para o acesso à rede de dados e aos sistemas corporativos do INSS, mediante autenticação que permita ao usuário acessar vários sistemas, por meio de ferramenta de gestão de identidades e acessos.

§ 1º A área responsável pela gestão de pessoas do INSS deverá utilizar os canais de atendimento disponibilizados pela empresa prestadora de serviços tecnológicos contratada pelo Instituto, ou outro canal informado pela DTI, para solicitar:

I - o credenciamento de usuários do quadro de pessoal do INSS na data do ato administrativo de retorno ou ingresso no órgão, para acesso à rede, e de estagiários, após assinatura do contrato de prestação de serviço, para acesso à rede;

II - a revogação de credenciais de acesso de servidores do quadro de pessoal do INSS cedidos a outros órgãos;

III - a desativação de usuários do quadro de pessoal do INSS na data do ato administrativo ou de ocorrências que ensejem desligamento para fins de acesso lógico; e

IV - a desativação do acesso de usuários do quadro de pessoal em atividade do INSS afastados ou com licença programada de suas funções por mais de sessenta dias ininterruptos.

§ 2º Quanto ao processo de formação das credenciais de acesso fica estabelecido que o nome do usuário será composto de acordo com os padrões estabelecidos no Guia de Interoperabilidade do Governo Eletrônico – e-Ping, mais especificamente no documento “Caixas Individuais-Fundacionais no Governo Federal” (Rede do Governo, 2010) que define regras de formação de nomes para a composição de endereços eletrônicos.

§ 3º Com relação às senhas de acesso, deve se observar que:

I - deverão ter no mínimo oito caracteres e conter, obrigatoriamente, caracteres alfanuméricos (combinação de letras e números). O usuário poderá acrescentar caracteres especiais (espaços em branco, símbolos, sinais de pontuação, etc.);

II - é vedada a reutilização das últimas quatro senhas utilizadas pelo usuário;

III - podem ser alteradas sempre que preciso ou quando o usuário achar necessário;

IV - o prazo de validade não deve ultrapassar 90 (noventa) dias; e

V - o usuário receberá, por meio de comunicado direto (via interface do sistema ou por mensagem no correio eletrônico), a informação do prazo próximo de vencimento da senha, quando esta estiver a 15 (quinze) dias da sua data de expiração.

§ 4º Os perfis de acesso aos sistemas corporativos deverão contemplar um conjunto de permissões e ações vinculadas às atividades desenvolvidas pelo usuário, sendo que:

I - caberá à área responsável pela gestão de TI do INSS estabelecer, em conjunto com as áreas responsáveis pela gestão dos sistemas corporativos, a norma de criação dos perfis de acesso;

II - as áreas responsáveis pela gestão dos sistemas corporativos são responsáveis pelas permissões, transações e ações que devem compor cada perfil de acesso; e

III - os perfis de acesso e de gestão concedidos para usuários internos e externos deverão ser objeto de revisão contínua pelos gestores responsáveis, não podendo ultrapassar o prazo máximo de 30 (trinta) meses.

§ 5º Quanto à utilização das credenciais e perfis de acesso, o usuário:

I - deve ter conhecimento prévio desta Norma de Controle de Acesso Lógico e preencher os requisitos estabelecidos na mesma;

II - deve estar devidamente autorizado a utilizar a rede corporativa e/ou os sistemas corporativos, de acordo com os requisitos estabelecidos nesta Norma;

III - deve utilizar os serviços e as informações obtidas, por meio do perfil de acesso, única e exclusivamente em razão do exercício da função pública e para os fins que lhe foi designado, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal;

IV - não pode divulgar, nem mesmo compartilhar, os códigos de segurança que lhe forem atribuídos (credenciais de acesso), os quais são pessoais e intransferíveis;

V - não pode utilizar as credenciais para acessar os recursos disponíveis em mais de uma estação de trabalho simultaneamente;

VI - não pode fazer uso das credenciais de acesso de outros usuários;

VII - deve fornecer informações acessadas nos sistemas e na rede de dados corporativos do INSS somente mediante demanda formalizada de quem tenha competência para tal;

VIII - deve comunicar à chefia imediata ou responsável pela administração do sistema ou rede corporativa quaisquer violações ou incidentes referentes à proteção do equipamento utilizado, do **software** ou de outros ativos da informação;

IX - deve, sempre que for necessário, afastar-se da estação de trabalho, certificar-se de que a sessão de rede ou acesso ao sistema corporativo esteja encerrado ou bloqueado;

X - deverá, obrigatoriamente, efetuar processo de alteração da sua senha em seu primeiro acesso à rede de dados corporativa; e

XI - no ato do primeiro acesso, bem como após cada atualização desta Norma, o usuário deverá manifestar concordância com os termos dispostos na mesma.

§ 6º O processo de autenticação de usuários deve ser definido pela área responsável pela gestão de Tecnologia da Informação do Instituto e poderá ser baseada em autenticação simples (nome de usuário e senha) agregada a autenticação multifator (certificação digital ou outros meios disponíveis).

§ 7º O credenciamento de usuários internos se dá pelo cadastro de novos servidores ou ocupantes de cargo em comissão, no âmbito do Instituto, pode ser solicitado por servidor vinculado à área responsável pela gestão de pessoas ou pela chefia imediata do usuário.

§ 8º O cadastro de que trata o § 7º deve ser solicitado por meio dos canais de atendimento disponibilizados pela prestadora de serviços tecnológicos contratada pelo Instituto ou outro informado pela DTI.

§ 9º O credenciamento de estagiários, se dará com a emissão de credencial de acesso, tendo como requisito as seguintes condições:

I - a empresa que atuar como agente de integração do estágio supervisionado deve manter contrato com o INSS;

II - o contrato de estágio supervisionado deverá conter cláusula de confidencialidade e sigilo de informações preestabelecidos com a Administração Pública;

III - a criação de perfis específicos e restritos às atividades do estagiário pelos gestores dos sistemas corporativos para o acesso dos estagiários;

IV - é vedada a concessão de perfis de acesso aos sistemas corporativos para estagiários com permissão de alteração das bases de dados institucionais;

V - o acesso será concedido mediante solicitação expressa de servidor do quadro do INSS, responsável pela supervisão do estágio, que deverá avaliar os riscos de utilização indevida de informações institucionais e as eventuais restrições referentes aos dias e horários para a realização dos acessos;

VI - o acesso será precedido da assinatura do Termo de Confidencialidade e de Manutenção de Sigilo – TCMS, Anexo II, o qual deverá ser firmado pelo estagiário ou pelo estagiário e seu responsável legal, no caso de se tratar de estagiário menor de 18 (dezoito) anos;

VII - as solicitações de acesso à rede para estagiários devem ser procedidas por meio dos canais remotos de atendimento disponibilizados pela empresa prestadora de serviços tecnológicos contratada pelo Instituto ou outro canal informado pela DTI, pela unidade de gestão de pessoas, pela chefia imediata do educando ou pelo responsável por sua supervisão;

VIII - os gestores de sistemas devem criar perfis diferenciados para estagiários de nível médio e nível superior;

IX - o supervisor do estagiário deverá, periodicamente, orientá-lo quanto ao uso responsável e adequado do acesso aos sistemas corporativos; e

X - o acesso do estagiário limitar-se-á à data final do contrato ou imediatamente cessado na hipótese de rescisão antecipada do estágio, cabendo ao supervisor do estagiário, em quaisquer dos casos, adotar as providências necessárias ao bloqueio do acesso, tão logo finde a contratação.

§ 10. O credenciamento de usuários externos, obedecerá as seguintes diretrizes:

I - as credenciais de acesso para usuários externos devem ser emitidas tendo em vista o interesse do INSS, devidamente justificadas e previstas no convênio, acordo de cooperação técnica ou instrumento congênere;

II - as solicitações de emissão de credenciais de acesso à rede corporativa para usuários amparados por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica, contrato ou instrumento congênere devem:

a) ser feitas pelo gestor da unidade/área responsável pela gestão do instrumento legal; e

b) ser atendidas somente após validação das credenciais do gestor solicitante do Instituto, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700);

III - a emissão de credenciais de acesso à rede corporativa para prestadores de serviço terceirizados ou equiparados nas dependências do INSS, quando necessária, será provida unicamente pelo interesse do INSS, devendo ser atendidos os seguintes requisitos:

a) a organização a qual o usuário é vinculado deve manter contrato, acordo de cooperação, convênio ou instrumento congênere vigente com o INSS;

b) instrumento deve conter cláusulas prevendo:

1. a necessidade e justificativa para acesso à rede corporativa;

2. a confidencialidade e sigilo de informações preestabelecidas junto ao Instituto; e

3. a obrigatoriedade da organização ou do ente contratado informar previamente ao representante legal do INSS, responsável pela gestão do contrato, quaisquer alterações em seu corpo de colaboradores que impacte na emissão/exclusão das contas de acesso;

c) a organização ou ente contratado também deverá manter com seus colaboradores Termo

de Confidencialidade de Manutenção de Sigilo – TCMS; e

d) o gestor do contrato pelo INSS deve fundamentar a necessidade do acesso à rede para prestadores de serviço terceirizados ou equiparados, definindo os recursos que devem ser disponibilizados e eventuais restrições a dias e horas para realização do acesso à rede;

IV - os TCMS deverão ser arquivados junto aos instrumentos assinados com o INSS e uma cópia ou **link** eletrônico deverá ser encaminhada ao Gestor do Contrato. O mesmo deve ocorrer para quaisquer alterações ocorridas na vigência dos contratos, acordos ou convênios;

V - caso os Termos sejam gerados de forma eletrônica, deverá ser disponibilizado o arquivo correspondente, atendendo aos requisitos necessários para garantia de integridade e disponibilidade de acesso, assim como os requisitos específicos previstos em contrato; e

VI - a emissão de credenciais de acesso poderá ser feita pelo gestor do contrato, representante legal do INSS, ou pelo gestor da unidade responsável pela gestão do contrato, convênio, acordo de cooperação técnica ou instrumento congênere e serão atendidas somente após validação das credenciais do solicitante, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700).

§ 11. O acesso aos prestadores de serviço vinculados à Central de Atendimento 135 se dará observando as seguintes condições:

I - a empresa deve manter contrato com o INSS;

II - o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

III - a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade - TCMS;

IV - o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte do INSS, definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;

V - os acessos deverão ser realizados única e exclusivamente por necessidade de serviço;

VI - os contratos de prestação de serviços de teleatendimento devem conter documento a ser utilizado para formalização das indicações de gestores de acesso aos sistemas corporativos do Instituto; e

VII - o INSS pode disponibilizar, de forma restrita, às centrais 135, uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

§ 12. Nos casos referentes a prestadores de serviço vinculados à Ouvidoria do Ministério da Economia, o acesso se dará observando-se as seguintes condições:

I - a empresa deve manter contrato direto com a Ouvidoria do Ministério da Economia;

II - o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

III - a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade;

IV - o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte da Ouvidoria do Ministério da Economia, definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;

V - os acessos deverão ser realizados única e exclusivamente por necessidade de serviço; e

VI - o INSS pode disponibilizar, de forma restrita, à Ouvidoria do Ministério da Economia, uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

§ 13. O acesso à rede corporativa por servidores vinculados a órgãos de controle externo, envolvidos em ações de auditoria no âmbito do INSS, será concedido mediante apresentação da equipe de auditoria por meio de documento formal que conste:

I - dados necessários ao cadastro de usuários externos;

II - informações acerca dos objetivos dos trabalhos a serem executados;

III - os prazos envolvidos; e

IV - informações complementares.

§ 14. O tipo de acesso de que trata o § 12 deverá observar:

I - as parcerias institucionalmente estabelecidas entres esses órgãos e o INSS no que tange à cobertura/previsão de acesso à rede corporativa do Instituto;

II - o atendimento de pedido de solicitação de informações advindo de pessoas físicas ou jurídicas externas, respeitadas as restrições de acesso às informações previstas na Lei nº 12.527, de 18 de novembro de 2011, serão analisadas pela área designada para responder as demandas dos cidadãos por meio do e-SIC; e

III - os procedimentos referentes às solicitações de inclusão, exclusão, inativação e suspensão de contas de acesso de usuários devem ser executados tendo como premissa a preservação dos registros para efeito de auditoria.

§ 15. O bloqueio administrativo se dará da seguinte forma:

I - o responsável pela Corregedoria-Geral do INSS, quando necessário, poderá solicitar a suspensão, bloqueio ou inativação imediata de contas de acesso de usuários que estiverem envolvidos em inquérito penal, em Processo Administrativo Disciplinar – PAD ou em Sindicância, decorrente de infrações cometidas no exercício das atribuições do cargo, quando o usuário estiver na seguinte situação:

a) afastado temporariamente do cargo ou função pública em razão de ato que se encontra sob apuração;

b) indiciado em processo administrativo disciplinar, por incursão nos incisos IX, XI, XII, XV, XVI e XVII do art. 117 e arts. 130 e 132 da Lei nº 8.112, de 11 de dezembro de 1990, ou cuja proposta pela Comissão Processante, no relatório final, seja pela aplicação de penalidade a partir de suspensão de 30 (trinta) dias; e

c) submetido à prisão em flagrante, temporária ou preventiva decorrente do cometimento de infração no exercício das atribuições do cargo, enquanto estiver em apuração de inquérito policial ou pelo Ministério Público Federal;

II - as solicitações de que tratam o inciso I deverão ser efetuadas mediante comunicação formal da Corregedoria-Geral para a prestadora de serviços tecnológicos contratada pelo Instituto, ou outro canal informado pela DTI, a qual procederá a imediata implementação da mudança;

III - o bloqueio de acessos tratados nas situações do inciso I serão efetivados no âmbito da ferramenta de gestão de acessos nas seguintes situações:

a) usuário afastado temporariamente do cargo ou função, enquanto durar o afastamento; e

b) usuário indiciado nos termos da alínea "c" do inciso I do § 15, até o efetivo cumprimento da penalidade porventura aplicada ou, em caso de não aplicação de penalidade, enquanto durar o processo.

Art. 6º A Rede de Dados Corporativa compõe a infraestrutura de rede, que é disponibilizada para uso institucional, logo, apenas equipamentos de propriedade do Instituto são autorizados e devem ser conectados à rede corporativa.

§ 1º Em casos excepcionais, a conexão de equipamentos particulares à rede corporativa deve ser feita em razão do interesse do Instituto e sob prévia autorização do responsável pela gestão da unidade em que o equipamento estiver localizado.

§ 2º O INSS poderá disponibilizar o acesso à rede de dados corporativa por meio de tecnologia **Wireless** (sem fio). Para tanto os seguintes critérios deverão ser adotados:

I - os projetos que envolvam a utilização de pontos de acesso sem fio à rede corporativa no âmbito do Instituto deverão ser devidamente registrados e aprovados pela área responsável pela gestão de TI do INSS;

II - os pontos de acesso à rede de dados corporativa sem fio poderão ser objeto de testes periódicos de penetração e de auditoria a critério da área responsável pela gestão de TI no INSS; e

III - as conexões à rede sem fio serão avaliadas pela área responsável pela gestão de TI do INSS em relação aos requisitos de segurança e deverão atender ao princípio do privilégio mínimo.

§ 3º A área responsável pela gestão de TI do INSS poderá disponibilizar rede sem fio com regras específicas de acesso para visitantes nas diversas unidades do Instituto.

§ 4º Os dispositivos conectados à rede do INSS por meio de conexão sem fio deverão suportar configurações de criptografia estabelecidas pela área responsável pela gestão de TI no âmbito do INSS;

§ 5º Qualquer tecnologia de acesso sem fio implementada no INSS deverá suportar autenticação forte, com possibilidade de efetuar checagens em bancos de dados externos, e a área responsável pela gestão de TI do INSS deve dispor de mecanismos automáticos que possibilitem:

I - a detecção e bloqueio de equipamentos externos conectados à rede corporativa; e

II - a identificação e rastreamento dos endereços IP de origem e destino, bem como os serviços utilizados na rede corporativa inclusive nos acessos remotos.

§ 6º A administração da rede corporativa trata da operacionalização da rede do INSS, que é realizada por empresa prestadora de serviços tecnológicos contratada pelo Instituto e seguem as seguintes premissas:

I - prover, gerenciar e operacionalizar os ativos, acessos e serviços que compõem a rede de dados corporativa do INSS; e

II - submeter-se ao monitoramento de serviços de tecnologia contratados pelo Instituto, seguindo as regras desta Norma.

§ 7º Quanto ao processo de geração de contas de serviço, fica estabelecido que:

I - os critérios para a emissão de contas de serviços serão vinculados a um processo formal estabelecido pela área responsável pela gestão de TI do INSS;

II - a concessão de contas de serviços deve ser feita conforme a necessidade de uso de acordo com os critérios estabelecidos nesta Norma;

III - o direito de acesso privilegiado, por meio de contas de serviços, associado a sistemas

ou processos, deve ser identificado;

IV - deve ser viabilizada ferramenta que possibilite a gestão das contas de serviço de forma automatizada, possibilitando o registro e verificação de todos os privilégios concedidos;

V - as contas de serviço fornecidas devem ser utilizadas exclusivamente para os fins aos quais foram concedidas;

VI - as contas de serviço emitidas devem ser revalidadas periodicamente com base na função exercida e na área de atuação do servidor; e

VII - as contas de serviço com credenciais de acesso de uso compartilhado devem ter suas senhas alteradas periodicamente, conforme estabelecido nesta Norma de Controle de Acesso Lógico, ou sempre que ocorrerem mudanças no grupo de usuários que utilizam as mesmas.

§ 8º É vedado o uso da rede corporativa para:

I - acesso por meio de equipamento não homologado ou não autorizado pelo INSS;

II - fazer download, instalar e/ou utilizar sistemas ou aplicativos não homologados pela área responsável pela gestão de TI do INSS nos equipamentos de propriedade do Instituto;

III - a utilização de **softwares** particulares em equipamentos do INSS sem autorização expressa;

IV - a instalação e conexão de equipamentos particulares à rede corporativa do Instituto sem a prévia autorização do gestor responsável pela unidade ou da área responsável pela gestão de TI do INSS;

V - o uso dos recursos de rede para fins particulares ou de terceiros alheios aos interesses do INSS, em especial, quando tal procedimento prejudique o tráfego da rede de dados;

VI - o uso para fins de divulgação ou distribuição de material que não possua vínculo com as atividades desenvolvidas pelo Instituto;

VII - a instalação ou utilização de ferramentas de monitoramento de rede sem a anuência e autorização expressa da área responsável pela gestão de TI no Instituto;

VIII - a instalação de dispositivos de comunicação ou de compartilhamento de dados sem fio, particulares, à rede corporativa do Instituto, sem autorização expressa da área responsável pela gestão de TI do INSS; e

IX - burlar as regras de acesso a internet configuradas em **proxy** ou ferramenta similar de gerenciamento de conteúdo **web**.

§ 9º Cabe à área responsável pela gestão de TI no âmbito do INSS definir os aspectos relacionados à plataforma tecnológica, gestão operacional, forma de autenticação e sustentação do domínio de rede do INSS.

Art. 7º A Gestão do Acesso aos Sistemas Corporativos seguirá as seguintes premissas:

I - sistemas legados:

a) as regras estabelecidas nesta norma devem ser aplicadas, guardando-se as devidas limitações tecnológicas, aos sistemas legados; e

b) o controle de acesso aos sistemas legados é efetuado por base própria;

II - sistemas de apoio à administração:

a) os ambientes de hospedagem desses sistemas são suportados por terceiros;

b) o ambiente deverá ser gerenciado e operacionalizado pela área de gestão de TI do INSS;

c) o acesso pelos usuários a esses sistemas deverá ser autenticado pelo serviço de diretório utilizado pelo Instituto; e

d) as regras de hospedagem de sistemas serão definidas, em ato próprio, pela área de gestão de TI do INSS;

III - armazenamento de registros **logs**:

a) as áreas responsáveis pela gestão de sistemas corporativos e demais aplicações devem definir, em conjunto com a área responsável pela gestão de TI, a temporalidade de registro dos **logs** de acesso e transações, e quais registros devem ser armazenados por um período maior que o estipulado no **caput** do art. 8º;

b) o INSS poderá alterar a temporalidade destes dados em norma específica; e

c) os **logs** de acesso devem contemplar minimamente os registros relacionados no Anexo III;

IV - administração da ferramenta de gestão de acesso:

a) com o objetivo de operacionalizar a gestão dos acessos aos sistemas corporativos no âmbito do INSS, serão criados os seguintes papéis:

1. administrador de sistema INSS: servidor do quadro, lotado na área responsável pela gestão de TI, designado por meio de Portaria do Diretor de Tecnologia da Informação e Inovação, a ser publicada em Boletim de Serviço – BS, responsável pela administração da ferramenta de gestão de acesso aos sistemas corporativos no âmbito do INSS;

2. gestor de sistema: servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em BS, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedoria-Geral e Procuradoria Federal Especializada junto ao INSS - PFE-INSS. É responsável pela implementação de sistemas corporativos no âmbito do INSS;

3. gestor de acesso central: servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em BS, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedoria-Geral e PFE-INSS. É responsável pela manutenção dos perfis de gestão dos usuários nas áreas que compõem a Administração Central e, quando necessário, dos gestores de acesso das Superintendências-Regionais - SR;

4. gestor de acesso interno: servidor do quadro, lotado na Administração Central, SR, Gerência-Executiva - GEX, Agência da Previdência Social - APS, indicado pelo Gestor de Acesso Central ou por um Gestor de Acesso, responsável pela atribuição do perfil de acesso e de gestão dos usuários no INSS; e

5. gestor de acesso externo: pessoa formalmente indicada, por documento previsto no instrumento legal que firmou a parceria ou por meio de Ofício de lavra do representante máximo de uma Entidade Externa, responsável pelo cadastro de usuários externos e a gestão dos acessos aos sistemas corporativos do Instituto;

b) os perfis de acesso serão atribuídos de acordo com a necessidade do fluxo de operação definido para cada sistema corporativo;

c) a indicação e o processo de substituição dos responsáveis pela gestão dos acessos aos sistemas corporativos no âmbito do INSS poderá ser procedida das seguintes formas:

1. a autoridade responsável pela indicação do gestor de acessos pode indicar opcionalmente o substituto;

2. o próprio gestor de acessos pode designar, a qualquer momento, por meio da ferramenta de gestão de acessos um substituto;

3. quando não houver um gestor responsável, ou substituto, por uma unidade devidamente designado, a gestão dos usuários será transferida, preferencialmente de forma automática, para o responsável pela área da abrangência daquela unidade e assim subsequentemente; e

4. o Gestor de Acesso é corresponsável com os perfis de gestão ou acesso que ele atribuir aos usuários;

d) ao usuário interno cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Norma de Controle de Acesso Lógico e suas normas complementares;

2. solicitar, ao Gestor de Acesso responsável pela gestão da unidade de lotação a qual é vinculado, a suspensão do seu perfil de acesso nos períodos de afastamento do serviço por mais de 30 (trinta) dias consecutivos;

3. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e

4. ter conhecimento e estar de acordo com o disposto nesta Norma;

e) ao usuário externo cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Norma de Controle de Acesso Lógico;

2. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e

3. ter conhecimento e estar de acordo com o disposto nesta Norma;

f) ao administrador do sistema INSS cabe:

1. criar os sistemas e subsistemas, devidamente homologados pela área de negócio responsável, no ambiente de produção, por meio de ferramenta de gestão de acesso;

2. mediante apresentação de Portaria de designação para Gestores de Acesso Central, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores quanto à atribuição dos perfis de gestão; e

3. mediante apresentação de Portaria de designação para Gestores de Sistema, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores acerca do processo de implementação dos sistemas corporativos no âmbito do INSS;

g) ao gestor de sistema cabe:

1. efetuar os procedimentos de importação, inclusão, alteração e exclusão de papéis e permissões nos sistemas corporativos em ambiente de produção; e

2. atuar, em conjunto com o Administrador do Sistema INSS e a prestadora de serviços tecnológicos contratada pelo Instituto, no planejamento e execução do processo de implementação dos sistemas corporativos dos quais for designado responsável;

h) ao gestor de acesso central cabe:

1. efetuar o credenciamento, suspensão ou exclusão de perfis de gestão dos sistemas corporativos aos Gestores de Acesso na Administração Central e, quando necessário, dos Gestores de Acesso da SR, GEX, APS e demais usuários de sua abrangência; e

2. orientar os usuários de sua abrangência e os gestores da Administração Central e SR, GEX e APS acerca das regras para o acesso aos sistemas corporativos do INSS;

i) ao gestor de acesso interno cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários da Administração Central, SR, GEX, APS;

2. atribuir, alterar ou excluir os perfis de acesso aos usuários da Administração Central, SR, GEX, APS; e

3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS;

j) ao gestor de acesso externo cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários do seu Órgão/Entidade;

2. atribuir, alterar ou excluir os perfis de acesso aos usuários do seu Órgão/Entidade; e

3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS;

V - configura-se mau uso, sujeito a responsabilidade penal, civil e disciplinar:

a) a divulgação, sem autorização expressa da chefia imediata ou do gestor de acesso de sua abrangência, de informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS;

b) acessar sistemas corporativos sem autorização prévia, de acordo com os requisitos estabelecidos nesta Norma;

c) utilizar-se das informações obtidas por meio de acesso concedido em desacordo com os procedimentos dispostos nesta Norma e demais normas vigentes na Administração Pública Federal;

d) compartilhar ou fazer uso das credenciais de acesso, aos sistemas corporativos, de outros usuários; e

e) a instalação de sistemas corporativos em equipamentos particulares.

VI - em casos excepcionais, a área responsável pela gestão de TI do INSS, mediante ato formal, poderá autorizar a adoção das medidas descritas no § 2º do art.8º.

Art. 8º Todo acesso à rede de dados e aos sistemas corporativos deve ser registrado e monitorado de modo que permita a rastreabilidade, a identificação e o bloqueio de usuários e equipamentos não autorizados. Estas informações devem ser armazenadas por um período de, no mínimo, doze (12) meses, observando o disposto no inciso III do art. 7º.

§ 1º As ocorrências de mau uso do acesso aos recursos disponíveis na rede e sistemas corporativos não previstas nesta norma e os casos omissos serão encaminhados para a área responsável pela gestão de TI no âmbito do INSS para análise e pronunciamento.

§ 2º Identificada irregularidade de mau uso dos recursos de rede poderá ocorrer o bloqueio preventivo do acesso pela DTI, o encaminhamento de dossiê com as informações para a Corregedoria-Geral do INSS ou Corregedorias-Regionais, nas suas áreas de abrangências, a fim de que seja realizada a análise no âmbito disciplinar.

§ 3º O descumprimento dessa Norma poderá resultar em sanções administrativas, civis e criminais.

Art. 9º Esta norma deve ser revisada num período máximo de 3 (três) anos.

ANEXO II

RESOLUÇÃO Nº 10/CEGOV/INSS, DE 1 DE SETEMBRO DE 2020

TERMO DE RESPONSABILIDADE

Pelo _____, presente _____, instrumento, _____ eu
identidade nº _____, CPF nº _____, documento de
_____ expedida pelo _____, em _____, e lotado no(a)
_____do Instituto Nacional do Seguro Social –
INSS, DECLARO, sob pena das sanções cabíveis nos termos da Política de Segurança da Informação -
POSIN do INSS que assumo a responsabilidade por:

I - tratar o(s) ativo(s) de informação como patrimônio do Instituto Nacional do Seguro Social;

II - utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do INSS;

III - contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que disciplina a gestão de segurança da informação na Administração Pública Federal, direta e indireta, e dá outras providências;

IV - utilizar as credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do INSS;

V - responder, perante o INSS, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

_____, ____ de _____ de _____

Nome e assinatura do usuário:	Unidade de Lotação:
Nome e assinatura da Autoridade Responsável pela Autorização do Acesso:	

ANEXO III

RESOLUÇÃO Nº 10/CEGOV/INSS, DE 1 DE SETEMBRO DE 2020

REGISTROS DE LOGS

1. Relação dos campos de registros de logs do GERID
 - 1.1. Dados Gerais
 - 1.1.1. Data
 - 1.1.2. Sistema
 - 1.1.3. Ambiente
 - 1.1.4. IP destino
 - 1.1.5. IP origem
 - 1.1.6. CPF usuário

- 1.1.7. URL de origem
- 2. Ações:
 - 2.1. CAS (autenticação): Central **Authentication Service** - Serviço Central de Autenticação
 - 2.1.1. Criação de **service ticket** (ST)
 - 2.1.2. Criação de **ticket granting ticket** (TGT)
 - 2.1.3. validação de ST
 - 2.1.4. Exclusão de **ticket** TGT
 - 2.1.5. Autenticação com sucesso (**login+password**)
 - 2.1.6. Autenticação com sucesso (certificado digital)
 - 2.1.7. Autenticação com falha
 - 2.2. GPA: Gerenciamento de Permissão de Acesso
 - 2.2.1. Início de sessão
 - 2.2.2. Dados do usuário em sessão (CPF, NOME, PAPEL)
 - 2.2.3. Requisição de **logout**
 - 2.2.4. Dados de credenciais
 - 2.2.5. Concessão de credenciais
 - 2.2.6. Alteração de Credenciais
 - 2.2.7. Dados de receptor (CPF, NOME, Lotação)
 - 2.2.8. Inserção de credencial no usuário
 - 2.2.9. Revogação de Credenciais
 - 2.2.10. Pesquisa de credenciais
 - 2.2.11. Pesquisa de usuários
 - 2.2.12. Substituição de gestor



INSTITUTO NACIONAL DO SEGURO SOCIAL
RESOLUÇÃO Nº 11/CEGOV/INSS, DE 1 DE SETEMBRO DE 2020

MINUTA DE RESOLUÇÃO

Institui a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR do Instituto Nacional do Seguro Social.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do Processo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Instituir, no âmbito do INSS, e nos termos do Anexo a esta Resolução, a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR-INSS.

Art. 2º Esta Resolução complementa Política de Segurança da Informação POSIN-INSS vigente.

Art. 3º Esta Resolução entra em vigor sete dias após a data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

**ALESSANDRO ROOSEVELT SILVA
RIBEIRO**
Diretor de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **ALEXINALDO MESSIAS CERQUEIRA, Chefe de Serviço**, em 28/08/2020, às 19:01, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1592323** e o código CRC **1136F948**.

ANEXO

RESOLUÇÃO Nº 11/CEGOV/INSS, DE 1 DE SETEMBRO DE 2020

EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS - ETIR-INSS

Art. 1º A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR-INSS tem por objetivo agir proativamente, receber, analisar, monitorar, coordenar e propor respostas a notificações e atividades relacionadas a incidentes de segurança da informação e comunicações no âmbito do INSS.

Art. 2º As atividades pertinentes à ETIR-INSS englobam os usuários dos serviços de Tecnologia da Informação - TI e os sistemas de informação do INSS e serão realizadas com intercâmbio de informações e em cooperação com as seguintes instâncias:

I - o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR GOV;

II - a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR de empresas prestadoras de serviços de tecnologia contratadas pelo INSS;

III - as ETIRs ou estrutura equivalente dos demais órgãos, entidades e empresas, públicas ou privadas, que tenham contratos, acordos, convênios ou instrumentos congêneres com o INSS; e

IV - o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República – GSI/PR.

Art. 3º Para os efeitos desta Resolução ficam estabelecidos os seguintes conceitos e definições:

I - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR: equipe de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

II - CTIR GOV: Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI;

III - agente responsável: servidor público ocupante de cargo efetivo de órgão ou entidade da Administração Pública Federal, direta ou indireta ou militar de carreira incumbido de chefiar e gerenciar uma ETIR;

IV - artefato malicioso: qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

V - Comunidade ou Público Alvo: conjunto de pessoas, setores, órgãos ou entidades atendidas por uma ETIR ou estrutura equivalente;

VI - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VII - serviço: conjunto de procedimentos, estruturados em processo definido, oferecido à comunidade pela ETIR;

VIII - Tratamento de Incidentes de Segurança em Redes Computacionais: serviço consistente em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

IX - usuário: pessoas que fazem uso de serviços de TI e sistemas de informação de propriedade do INSS, independentemente do cargo ocupado (contratados, consultores, conselheiros, servidores, temporários e etc.); e

X - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que possam resultar em risco para um sistema ou por uma organização, e que possam ser evitados por uma ação interna de segurança da informação.

Art. 4º A implementação e o funcionamento da ETIR-INSS seguirão metodologia definida pelo GSI/PR e as seguintes diretrizes:

I - basear-se no “Modelo 1 – Utilizando a equipe de Tecnologia da Informação”, conforme definido pelo GSI/PR;

II - os integrantes da Equipe deverão ser profissionais da área de Tecnologia da Informação, servidores públicos efetivos, lotados na Diretoria de Tecnologia da Informação e Inovação – DTI do INSS, sem prejuízo de suas atribuições típicas do cargo, com experiência e conhecimentos técnicos compatíveis com a importância da missão da ETIR-INSS;

III - a ETIR-INSS ficará vinculada tecnicamente à Coordenação-Geral de Infraestrutura e Operações – CGIN da DTI;

IV - o Coordenador da ETIR-INSS será nomeado por ato do Diretor de Tecnologia da

V - na ausência de Coordenador formalmente nomeado, as atribuições relacionadas à coordenação da equipe serão desempenhadas pelo Coordenador-Geral de Infraestrutura e Operações.

Art. 5º A ETIR-INSS será composta por membros:

I - permanentes, que efetivamente atuarão em todos os incidentes registrados;

II - colaboradores, que atuarão, de forma esporádica, no tratamento de incidentes relacionados às suas áreas de atuação; e

III - opcionais, servidores das unidades descentralizadas do INSS sob supervisão da DTI.

§ 1º Os membros da ETIR-INSS serão designados por meio de ato do Diretor de Tecnologia da Informação e Inovação.

§ 2º A distribuição dos membros da ETIR-INSS se dará da seguinte forma:

I - 2 (dois) servidores permanentes, oriundos do Serviço de Segurança de TIC;

II - 2 (dois) servidores colaboradores, oriundos da CGIN;

III - 2 (dois) servidores colaboradores, oriundos da Coordenação-Geral de Projetos e Soluções Digitais da DTI; e

IV - 2 (dois) servidores opcionais, oriundos das unidades descentralizadas do INSS.

Art. 6º A ETIR-INSS terá autonomia limitada para o tratamento de incidentes de Segurança da Informação, devendo implementar ações que possam impactar outras áreas do Instituto somente com anuência do Diretor de Tecnologia da Informação e Inovação e do Gestor responsável pela área/sistema afetada, e poderá, ainda, gerar relatórios técnicos sugerindo a adoção de medidas para resolução de incidentes.

Art. 7º A ETIR-INSS fornecerá o serviço de Tratamento de Incidentes de Segurança em Redes Computacionais, que compreende as seguintes ações:

I - recepção de solicitações e alertas diversos, utilizando como canal de comunicação a caixa postal etir@inss.gov.br, a ser disponibilizada pelo INSS;

II - filtragem de todo conteúdo direcionado à ETIR-INSS, para fins de verificação quanto à necessidade de tratamento pela Equipe e, caso não se trate de incidente de segurança em redes computacionais, encaminhar para a área competente;

III - catalogação dos incidentes detectados em ferramenta a ser indicada pela DTI, com nível de acesso restrito;

IV - classificação dos incidentes detectados quanto ao nível de severidade e impacto;

V - tratamento do incidente com medidas corretivas e indicação de formas de se evitar que ocorra novamente;

VI - resposta às solicitações e alertas encaminhados para a ETIR; e

VII - monitoramento da aplicação do tratamento dos incidentes indicados.

§ 1º A ETIR-INSS deverá analisar os incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências; e

§ 2º O detalhamento dos serviços prestados pela ETIR-INSS deverá ser publicado em página específica da Intranet do INSS, no prazo de 30 (trinta) dias a partir da publicação desta Resolução.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações

DESPACHO

Coordenação-Geral De Infraestrutura e Operações, em 29/08/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

A s s . : Minutas de
Resolução de políticas e
normas de segurança da
informação do Instituto
Nacional do Seguro Social
- INSS.

1. Trata-se dos normativos para instituição de políticas e normas de segurança da informação do Instituto Nacional do Seguro Social - INSS.
2. Atendidos os itens dispostos no Despacho CSG 1548091 e Despacho CEGOV 1571869, conforme Despacho SSEG 1585512, encaminha-se ao Comitê Estratégico de Governança - CEGOV - para publicação dos normativos em 01/09/2020.

CLAUDIO AUGUSTO NOVAIS FERRAZ

Coordenador-Geral de Infraestrutura e Operações



Documento assinado eletronicamente por **Claudio Augusto Novais Ferraz, Coordenador(a) Geral**, em 29/08/2020, às 14:53, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site
https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1593846** e o código CRC **CCF89613**.



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria De Integridade, Governança e Gerenciamento De Riscos
Comitê Estratégico de Governança

DESPACHO

Comitê Estratégico de Governança, em 31/08/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO, COMITÊ
ESTRATÉGICO DE
GOVERNANÇA

A s s . : Minuta de
Resolução de políticas e
normas de segurança da
informação do Instituto
Nacional do Seguro Social
- INSS.

1. Trata-se dos normativos para instituição de políticas e normas de segurança da informação do Instituto Nacional do Seguro Social - INSS que foram discutidos na 6ª Reunião Ordinária do Comitê Estratégico de Governança - CEGOV, realizada no dia 22/07/2020 (Processo SEI nº 35014.164930/2020-78).
2. Em resposta ao Despacho CSG nº 1548091, a Diretoria de Tecnologia da Informação e Inovação revisou as normas, incluiu o anexo faltante, e ajustou a data proposta para início da vigência das normas, em consonância com o Decreto nº 10.139/2019. As minutas finais constam dos documentos SEI nº 1586319, 1592201, 1592240 e 1592323.
3. Feitas as considerações, retornam-se os autos à Coordenação de Suporte ao Gabinete - CSG, para elaboração das Resoluções finais e sua disponibilização em bloco de assinatura para os membros do Comitê Estratégico de Governança.
4. Após o feito, solicita-se que o processo seja retornado ao CEGOV, para publicação das normas no Site do INSS.

CIBELLE CESAR DO AMARAL BRASIL
Coordenadora-Geral de Governança
Secretaria-Executiva do Comitê Estratégico de Governança



Documento assinado eletronicamente por **CIBELLE CESAR DO AMARAL BRASIL**,
Coordenador(a) Geral, em 31/08/2020, às 10:43, conforme horário oficial de Brasília, com fundamento
no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1599626** e o código CRC **D910F974**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1599626



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Gabinete
Coordenação de Suporte ao Gabinete

DESPACHO

Coordenação de Suporte ao Gabinete, em 31/8/2020.

Ref.: Processo nº
35014.047735/2020-84.

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO, COMITÊ
ESTRATÉGICO DE
GOVERNANÇA.

A s s . : Minutas de
Resolução de políticas e
normas de segurança da
informação do Instituto
Nacional do Seguro Social
- INSS.

1. Cuidam-se de propostas de Resoluções com vistas à instituição de políticas e normas de segurança da informação no âmbito do INSS, as quais foram discutidas na 6ª Reunião Ordinária do Comitê Estratégico de Governança - CEGOV, realizada no dia 22 de julho de 2020 (Processo SEI nº 35014.164930/2020-78).

2. Em continuidade ao nosso Despacho SEI nº 1548091, restitua-se os autos à Diretoria de Tecnologia da Informação e Inovação para inclusão do Anexo II, citado no inciso III do art. 9º do Anexo I da minuta de Resolução SEI nº 1586319, no corpo da mesma minuta, em meio editável, com posterior retorno dos autos a esta Coordenação.

DIOGO FREITAS FIGUEIREDO

Coordenador de Suporte ao Gabinete



Documento assinado eletronicamente por **DIOGO FREITAS FIGUEIREDO, Coordenador(a)**, em 31/08/2020, às 13:49, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1603022** e o código CRC **C6B52C9F**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

DESPACHO

Diretoria De Tecnologia da Informação e Inovação, em 31/08/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

A s s . : Minutas de
Resolução de políticas e
normas de segurança da
informação do Instituto
Nacional do Seguro Social
- INSS.

1. Ciente.
2. Encaminhe-se ao Serviço de Segurança em TIC, com trâmite pela CGIN, para as tratativas necessárias na forma do despacho SEI CSG 1603022.

RENATA CESÁRIO DE OLIVEIRA GOMES

Analista em Tecnologia da Informação



Documento assinado eletronicamente por **RENATA CESARIO DE OLIVEIRA GOMES, Analista em Tecnologia da Informação**, em 31/08/2020, às 15:28, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site
https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1607692** e o código CRC **FD79A447**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1607692



INSTITUTO NACIONAL DO SEGURO SOCIAL
RESOLUÇÃO Nº 12/CEGOV/INSS, DE 1 DE SETEMBRO DE 2020
MINUTA DE RESOLUÇÃO

Disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso à Internet, competências e conteúdo de acesso para cada perfil.

O **COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS**, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do Processo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Estabelecer, nos termos do Anexo I a esta Resolução, os critérios para o uso da Internet no âmbito do INSS e aprovar o Anexo II.

Art. 2º Esta Resolução complementa a Política de Segurança da Informação POSIN-INSS vigente.

Art. 3º Esta Resolução entra em vigor sete dias após a data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES Presidente	ALESSANDRO ROOSEVELT SILVA RIBEIRO Diretor de Benefícios
JOBSON DE PAIVA SILVEIRA SALES Diretor de Atendimento	HELDER CALADO DE ARAÚJO Diretor de Gestão de Pessoas e Administração
CLÓVIS DE CASTRO JÚNIOR Diretor de Integridade, Governança e Gerenciamento de Riscos	FLÁVIO FERREIRA DOS SANTOS Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **ALEXINALDO MESSIAS CERQUEIRA**, **Chefe de Serviço**, em 31/08/2020, às 16:00, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1605875** e o código CRC **24531A6F**.

ANEXO I
RESOLUÇÃO Nº 12/CEGOV/INSS, DE 1 DE SETEMBRO DE 2020
NORMAS DE USO DA INTERNET

Art. 1º Esta norma se aplica a todos os servidores e colaboradores, vinculados direta ou indiretamente ao INSS, bem como a servidores e empregados de entidades e órgãos da Administração Pública ou privados que necessitem ou estejam autorizados a acessar a Internet a partir da rede corporativa do Instituto.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União – AGU que atuarem na consultoria, assessoramento jurídico e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta norma, ficam estabelecidos os seguintes conceitos e definições:

I - autorizador: ocupantes de cargo responsáveis pela autorização da concessão de perfis de acesso para usuários finais de sua área de abrangência;

II - Internet: rede mundial que interliga computadores de diferentes tipos e dimensões e permite a comunicação entre pessoas e organizações,

independentemente da localização geográfica;

III - Intranet: rede de computadores administrada pelo INSS, que utiliza os mesmos serviços e tecnologias disponíveis na rede mundial;

IV - perfil de acesso: atributo que estabelece as categorias de sítios acessíveis e tipos de arquivos que podem ser recebidos ou transmitidos pelos usuários;

V - **proxy**: ferramenta que desempenha a função de conexão do computador local à rede externa (Internet);

VI - sítio: conjunto de informações ou serviços disponíveis na Internet ou na Intranet, organizados em páginas eletrônicas e acessíveis por meio de endereços que identificam, de forma padronizada, sua origem e conteúdo;

VII - usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal-APF, formalizada por meio da assinatura do Termo de Responsabilidade; e

VIII - VPN: Rede Privada Virtual (**Virtual Private Network**) construída sobre a infraestrutura de uma rede pública, possibilitando a conexão de dois computadores por meio de uma rede pública.

Art. 3º O acesso pelos usuários à Internet disponibilizado pelo INSS deverá pautar-se pelas seguintes diretrizes:

I - seu uso se dará exclusivamente em razão de trabalho e de acordo com os procedimentos dispostos nesta Norma;

II - os recursos disponibilizados pelo INSS não poderão ser usados para quaisquer propósitos ilegais ou proibidos, que possam danificar, desativar, sobrecarregar ou prejudicar qualquer área, serviço ou conteúdo, ou interferir no uso e execução das atividades laborais de outros usuários;

III - o volume de tráfego de Internet e os endereços **web** visitados poderão ser monitorados, visando assegurar o cumprimento desta norma; e

IV - o acesso à Internet para propósitos particulares ou estranhos às atividades do INSS poderá ser bloqueado, sem prévia comunicação ao usuário e sem prejuízo das demais sanções aplicáveis.

Art. 4º O acesso aos sítios da Internet para todos os usuários será realizado mediante a atribuição de perfis de acesso, distribuídos nos seguintes níveis:

I - Perfil 1: Perfil Restrito, inicialmente atribuído a usuários com maior restrição de acesso à Internet, permitindo acesso somente a sítios governamentais, instituições bancárias e sítios considerados de interesse do INSS;

II - Perfil 2: Perfil Básico, inicialmente atribuído a estagiários, recepcionistas e usuários externos, permitindo acesso a todos os sítios permitidos pelo Perfil 1 e a sítios de provedores de e-mail pessoal e instituições de ensino;

III - Perfil 3: Perfil Padrão para os servidores do quadro do Instituto, permitindo acesso a todos os sítios da Internet, exceto aqueles que contêm veiculação de material em áudio e vídeo; e

IV - Perfil 4: Perfil Avançado, atribuído preferencialmente a servidores do quadro do Instituto e estagiários que desempenham funções relacionadas a Comunicação Social, Desenvolvimento de Pessoas e gestores, respeitado o princípio da necessidade de conhecer e demandando designação dos Autorizadores deste Perfil. Permite acesso todos os sítios da Internet, incluindo sítios que veiculam material em áudio e vídeo (**streaming**), sítios de compartilhamento de vídeos, blogs e redes sociais.

§ 1º O perfil concedido a agentes externos será de caráter temporário, com validade equivalente à vigência do trabalho a ser executado.

§ 2º Os processos de alteração, bloqueio, liberação e categorização de sítios, assim como a criação e/ou alterações de perfis de acesso descritos nesta Norma, quando necessários, serão definidos pela Diretoria de Tecnologia da Informação e Inovação – DTI, e publicados no Portal do INSS na Intranet.

§ 3º Os novos usuários que não tiverem um perfil de acesso atribuído deverão ser direcionados para uma página da Intranet contendo orientações e normas relacionadas ao acesso à Internet no INSS, definidas pela DTI.

Art. 5º O acesso à Intranet e Internet a partir da rede de dados corporativa nas dependências do INSS e aos demais órgãos da Administração Pública Direta e Indireta, de qualquer das esferas de governo, será concedido exclusivamente a servidores e empregados públicos, efetivos ou ocupantes de cargo em comissão.

§ 1º O acesso de usuários externos das entidades que compõem o Poder Público será concedido mediante o estabelecimento em convênio, contrato, acordo de cooperação técnica ou instrumento congênere, especificamente firmados com o INSS para este fim.

§ 2º O gestor ou Coordenador-Geral da área responsável pelo convênio, contrato, acordo de cooperação técnica ou instrumento congênere assumirá o papel de Autorizador do serviço de acesso à Internet para os usuários externos, e deverá fundamentar as solicitações com base no

instrumento.

§ 3º Poderão ser concedidos acessos temporários para auditores de controle interno e externo, vinculados à Controladoria-Geral da União – CGU ou do Tribunal de Contas da União - TCU, no uso de suas atribuições.

Art. 6º O acesso à Internet por terceirizados deverá ser provido pela empresa contratada.

Parágrafo único. Em caráter de exceção, poderá ser concedido o acesso aos terceirizados a partir da infraestrutura de rede do INSS, desde que preenchidos os seguintes requisitos:

I - o contrato de prestação de serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

II - a empresa contratada deverá manter com seus funcionários Termo de Confidencialidade;

III - o contrato de prestação de serviços deverá prever a necessidade de acesso à Internet a partir das dependências do INSS; e

IV - o Autorizador, que para estes fins será o gestor do contrato ou o responsável pela área requisitante do serviço, deverá fundamentar as necessidades de acesso dos empregados da contratada, definindo os recursos que serão disponibilizados, endereços da Intranet e Internet necessários para o desenvolvimento das atividades e eventuais restrições a dias e horários para realização do acesso.

Art. 7º A conexão de equipamentos pessoais de visitantes à rede do INSS, quando necessária e motivada pelo interesse da Administração, deverá ser previamente autorizada pelo gestor da unidade onde o equipamento será utilizado.

Parágrafo único. Só será permitida a utilização da rede local por visitantes caso seus equipamentos atendam a todos os requisitos estabelecidos pela DTI e o acesso se dará, exclusivamente, à Internet, sendo vedado o acesso ao conteúdo disponibilizado na Intranet.

Art. 8º A todos os perfis de acesso descritos nesta Norma aplicam-se as restrições de acesso a sítios que:

I - contenham material pornográfico ou obsceno;

II - contenham material ilegal;

III - disponibilizem jogos, inclusive os da Internet (**on line**);

IV - contenham material impróprio, ofensivo, preconceituoso ou discriminatório, que façam apologia à violência, ao terrorismo e às drogas; e

V - contenha e/ou divulgue conteúdo de violação de direito autoral (pirataria) e/ou execução de quaisquer tipos ou formas de fraudes.

Art. 9º O processo de atribuição de acesso à Internet seguirá as seguintes diretrizes:

I - a atribuição dos perfis de acesso à Internet serão feitas pelos Autorizadores, de forma fundamentada e respeitando o princípio da necessidade de conhecer, de acordo com a tabela abaixo:

Perfil	Autorizador
Perfil 1, 2 e 3	Gerente de Agência da Previdência Social - APS, Gerente-Executivo, Superintendentes-Regionais, Procuradores-Regionais, Coordenadores-Gerais, Superintendentes-Regionais, Presidente do INSS, Auditor-Geral, Corregedor-Geral, Procurador-Geral da PFE-INSS, Diretores, Gestores ou Chefes da área responsável pelo Contrato ou ato administrativo similar no âmbito do INSS.
Perfil 4	Chefes de Assessoria de Comunicação Social nas Superintendências-Regionais, Assessor de Comunicação Social (Administração Central), Diretor de Tecnologia da Informação e Inovação, Diretor de Gestão de Pessoas e Administração e Presidente do INSS.

II - nos casos de novos usuários de rede (LDAP), criados por meio de registro de chamado técnico, quando o solicitante não indicar o perfil de acesso à internet, será atribuído o Perfil 1;

III - para fins de alteração do perfil de acesso, os usuários deverão preencher o “Formulário de Acesso à Internet” (Anexo II) e providenciar a assinatura pelo Autorizador do acesso; e

IV - ao registrar a solicitação, deve-se anexar o Formulário de Solicitação de Acesso à Internet devidamente preenchido e assinado (pelo solicitante e Autorizador), conforme documento nato digital ou digitalizado no formato PDF.

Art. 10. A solicitação para perfis de acesso em caráter temporário deverá conter, no Formulário de Solicitação de Acesso à Internet, a motivação da necessidade e a data de início e de expiração do acesso.

Art. 11. Das responsabilidades:

I - O usuário deverá:

- a) preencher os requisitos e termos estabelecidos nesta Norma;
- b) estar devidamente autorizado a utilizar a Internet nas formas estabelecidas nesta norma;
- c) fazer uso da Internet de forma responsável e segura, utilizando o acesso exclusivamente em razão de trabalho, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal; e
- d) impedir a divulgação e compartilhamento das chaves de segurança atribuídas, que são pessoais e intransferíveis.

II - o autorizador deverá:

- a) conceder os perfis de acesso à Internet rigorosamente de acordo com as atribuições dos usuários de sua abrangência, observando os normativos do INSS;
- b) verificar periodicamente o uso dos acessos concedidos e, sempre que necessário, solicitar alteração dos perfis de acesso dos usuários de sua abrangência; e
- c) reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR-INSS;

III - a área responsável pela gestão de TI no INSS deverá:

- a) monitorar os acessos à internet e sua utilização de acordo com as diretrizes estabelecidas nesta norma; e
- b) identificar os casos de mau uso da Internet e adotar uma ou mais das seguintes providências:
 - 1. alertar ao usuário, responsável pelo acesso, e ao Autorizador, responsável pela concessão, acerca do uso indevido da internet; e
 - 2. nos casos de reincidência, solicitar a revogação do acesso à internet concedido ao usuário e encaminhar a documentação que comprova a má utilização do acesso concedido para a Corregedoria do INSS, para análise e adoção das medidas cabíveis.

Art. 12. Configura-se como uso indevido da Internet:

- I - acessar a Internet disponibilizada pelo INSS sem estar devidamente autorizado, conforme estabelecido nesta Norma;
- II - não manifestar concordância com as regras estabelecidas nesta norma e nas demais aplicáveis;
- III - fazer uso dos recursos de Internet disponibilizados pelo INSS para fins alheios ao trabalho, em discordância com os procedimentos dispostos nesta Norma, sem prejuízo de demais normatizações vigentes na Administração Pública Federal;
- IV - utilizar os serviços extrapolando os privilégios do perfil de acesso que lhe foi designado;
- V - divulgar e/ou compartilhar as chaves de segurança, que são pessoais e intransferíveis, permitindo a utilização por terceiros do perfil que lhe foi atribuído;
- VI - praticar atos de comercialização de produtos e serviços, em proveito próprio ou de terceiros, que não atendam os interesses do INSS;
- VII - utilizar recursos ou dispositivos para acesso a computadores ou redes externas ao INSS com o objetivo de obter informações não autorizadas ou provocar a interrupção de serviços de rede;
- VIII - utilizar modem ou dispositivo de rede que interligue a rede interna do INSS a outras redes ou à Internet;

IX - expor, armazenar, distribuir, editar, gravar ou compartilhar, através do uso dos recursos computacionais e de comunicação do INSS, arquivos estranhos às atividades do INSS e não autorizados pela chefia imediata;

X - realizar qualquer atividade que apoie ou facilite o vazamento de dados;

XI - baixar arquivos ou programas da Internet que contrariem as diretrizes da Política de Segurança da Informação - POSIN vigente; e

XII - utilizar **proxy** não disponibilizado pelo INSS.

Art. 13. O acesso à Internet é passível de registro e monitoração, incluindo quaisquer dados transmitidos pela rede do INSS.

§ 1º Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a ETIR-INSS deverá ser imediatamente acionada, para tomar as providências necessárias a fim de sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação do INSS;

§ 2º As ocorrências de mau uso do acesso à Internet não previstas nesta norma, assim como os casos de dúvidas em relação à aplicação das disposições aqui estabelecidas, deverão ser encaminhadas à DTI para registro, análise e avaliação da necessidade de alterações de acordo com o processo de governança em vigência no INSS;

§ 3º O descumprimento desta Norma poderá acarretar ao usuário as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei, responsabilidade administrativa, civil e criminal.

Art. 14. Esta Norma deverá ser atualizada periodicamente, não excedendo o prazo máximo de 3 (três) anos.

ANEXO II

RESOLUÇÃO Nº 12/CEGOV/INSS, DE 1 DE SETEMBRO DE 2020

FORMULÁRIO DE SOLICITAÇÃO DE ACESSO À INTERNET

Informações do Usuário		
Nome:	Login de Rede:	
Matrícula:	CPF:	
Lotação:	Código do Setor:	
Telefone: ()	E-mail:	_____@inss.gov.br
		_____@agu.gov.br

☐	Perfil 1	data de expiração:	
☐	Perfil 2		
☐	Perfil 3		
☐	Perfil 4		
☐	Terceirizados	Contrato Nº ou Convênio	data de expiração

Descreva abaixo a justificativa e quais páginas devem ser acessadas pelo usuário terceirizado:

Declaro ter conhecimento e estar de acordo com as regras estabelecidas na Norma de Uso da internet do INSS (Resolução nº 12/CEGOV/INSS, de 1 de setembro de 2020) e demais normas aplicáveis.

_____, ____ de _____ de _____.

Local e Data

Informações do Autorizante		
Nome:		
Lotação:	Código do Setor:	
Telefone: ()	E-mail:	_____@inss.gov.br
		_____@agu.gov.br

Assinatura e Carimbo do Solicitante

Autorizo a concessão de Acesso Internet

_____, ____ de _____ de _____.

Local e Data



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações

DESPACHO

Coordenação-Geral De Infraestrutura e Operações, em 31/08/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

A s s . : Minutas de
Resolução de políticas e
normas de segurança da
informação do Instituto
Nacional do Seguro Social
- INSS.

1. Considerando a solicitação do Despacho CSG (SEI 1603022) foram realizados os ajustes na minuta de Resolução SEI nº 1605875.
2. Encaminha-se à CSG para prosseguimento do processo.

CLAUDIO AUGUSTO NOVAIS FERRAZ

Coordenador-Geral de Infraestrutura e Operações



Documento assinado eletronicamente por **Claudio Augusto Novais Ferraz, Coordenador(a) Geral**, em 31/08/2020, às 16:08, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1608847** e o código CRC **8638C93F**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

RESOLUÇÃO Nº 9/CEGOV/INSS, DE 31 DE AGOSTO DE 2020

Atualiza a Política de Segurança da Informação do Instituto Nacional do Seguro Social – POSIN-INSS.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do Processo Administrativo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Instituir, no âmbito do INSS, e nos termos do Anexo a esta Resolução, a Política de Segurança da Informação – POSIN-INSS.

Art. 2º Fica revogada a Resolução nº 672/PRES/INSS, de 27 de dezembro de 2018, publicada no Diário Oficial da União nº 250, de 31 de dezembro de 2018, Seção 1, pág. 151.

Art. 3º Esta Resolução entra em vigor sete dias após a data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

**ALESSANDRO ROOSEVELT SILVA
RIBEIRO**
Diretor de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **FLAVIO FERREIRA DOS SANTOS, Diretor(a) de Tecnologia da Informação e Inovação**, em 31/08/2020, às 18:21, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **JOBSON DE PAIVA SILVEIRA SALES, Diretor(a)**, em 31/08/2020, às 18:41, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **CLOVIS DE CASTRO JUNIOR, Diretor(a) de Integridade, Governança e Gerenciamento de Riscos**, em 31/08/2020, às 18:58, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **HELDER CALADO DE ARAUJO, Diretor(a)**, em 31/08/2020, às 19:39, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **ALESSANDRO ROOSEVELT SILVA RIBEIRO, Diretor(a)**, em 01/09/2020, às 17:35, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **LEONARDO JOSE ROLIM GUIMARAES, Presidente**, em 01/09/2020, às 19:43, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1610115** e o código CRC **145DAB3B**.

ANEXO I

RESOLUÇÃO Nº 9/CEGOV/INSS, DE 31 DE AGOSTO DE 2020

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO INSTITUTO NACIONAL DO SEGURO SOCIAL – POSIN–INSS.

Art. 1º A POSIN-INSS tem por objetivo estabelecer e difundir diretrizes e princípios de Segurança da Informação – SI, com vistas à orientação para uso e proteção adequados das informações produzidas e custodiadas pelo Instituto, preservando sua disponibilidade, integridade, confidencialidade e autenticidade.

Parágrafo único. A Política de que trata o **caput** e suas normas complementares aplicam-se a todos os agentes públicos que têm vínculo direto e/ou indireto com o Instituto.

Art. 2º Para os efeitos da POSIN-INSS, entende-se:

I - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta;

II - atividades críticas: atividades que devem ser executadas de forma a garantir a

consecução dos produtos e serviços fundamentais do órgão ou entidade, de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo;

III - ativos de informação: meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV - dados processados: dados submetidos a qualquer operação ou tratamento, por meio de processamento eletrônico ou automatizado, com o emprego de tecnologia da informação;

V - gestor de Segurança da Informação: é o responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da Administração Pública Federal;

VI - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

VII - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

VIII - necessidade de conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

IX - riscos de segurança da informação: potencial associado à exploração de uma ou mais vulnerabilidades nos ativos de informação, em razão de ameaças, com impacto negativo às atividades do Instituto;

X - Segurança da Informação – SI: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e autenticidades das informações;

XI - vínculo direto: agentes públicos contratados diretamente pelo INSS; e

XII - vínculo indireto: agentes privados ou públicos pertencentes a órgãos ou unidades da Administração Pública Federal, Estadual ou Municipal que mantenham contrato, convênio, acordo de cooperação técnica ou instrumento congênere com o INSS.

Art. 3º Esta POSIN-INSS foi elaborada com base nos seguintes normativos:

I - Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;

II - Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto

na Constituição Federal;

III - Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

IV - Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais;

V - Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

VI - Decreto nº 7.724, de 16 de maio de 2012, regulamenta a Lei nº 12.527, de 18 de novembro de 2011;

VII - Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

VIII - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

IX - Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

X - Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que disciplina a gestão de segurança da informação na Administração Pública Federal, direta e indireta, e dá outras providências;

XI - instruções normativas relacionadas à segurança da informação, publicadas pelo Gabinete de Segurança Institucional da Presidência da República;

XII - Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação; e

XIII - NBR ISO/IEC 27002:2013, que institui código de melhores práticas para a Gestão de Segurança da Informação.

Art. 4º Esta POSIN-INSS foi elaborada com base nos seguintes princípios:

I - a preservação da imagem do Instituto e de seus agentes públicos;

II - a salvaguarda das informações do cidadão;

III - ações de segurança orientadas pela gestão de riscos;

IV - continuidade assegurada dos serviços ao cidadão;

V - o alinhamento com a missão institucional e seu planejamento estratégico; e

VI - respeito à natureza e finalidade de cada área do Instituto.

Art. 5º São diretrizes gerais da POSIN-INSS:

I - tratamento da informação:

a) toda informação produzida pelos agentes públicos, no exercício de suas atividades, é de propriedade do INSS e deve ser protegida;

b) informações produzidas, armazenadas e tratadas pelo Instituto, especialmente as informações pessoais e custodiadas, devem receber o devido tratamento para assegurar sua proteção durante todo o ciclo de vida; e

c) somente os canais de comunicação disponibilizados pelo INSS devem ser utilizados para trafegar informações institucionais;

II - tratamento de incidentes de SI: todo incidente de segurança da informação deve ser imediatamente relatado à área responsável pela gestão de segurança da informação de Tecnologia da Informação – TI, observando-se a apropriada coleta de evidências;

III - gestão de riscos de segurança:

a) os riscos de segurança da informação devem ser identificados e tratados; e

b) os critérios para a gestão de risco devem ser definidos e comunicados à toda Instituição;

IV - gestão de continuidade:

a) os ativos de informação que suportam as atividades críticas do Instituto devem ser suportados por ambiente de alta disponibilidade e ter capacidade de recuperação em prazos e condições previamente definidos para situações de contingência, em conformidade com o processo de continuidade; e

b) a continuidade das operações e serviços de TI deve estar prevista nos contratos, assim como os prazos e condições devem estar formalmente estabelecidos;

V - controles de acesso:

a) todo acesso à informação deve ser motivado pela necessidade de conhecer;

b) os sistemas de informação e as instalações físicas devem ter capacidade de controlar os acessos, com fins de responsabilização pelo seu uso; e

c) as autorizações de acesso às informações, sistemas e instalações físicas devem ter critérios de acesso definidos e divulgados a todos da Instituição;

VI - recursos computacionais:

a) correio eletrônico:

1. o correio eletrônico, e-mail, é uma forma de comunicação oficial e deve ser utilizado exclusivamente no desempenho das atividades funcionais; e

2. ao produzir, responder ou encaminhar mensagem em caixa de correio eletrônico institucional, o servidor deverá se identificar, inscrevendo, ao menos, seu nome, cargo e telefone de contato institucional;

b) acesso à Internet:

1. o acesso à Internet, por meio da rede de dados do INSS, é uma concessão e deve ter seu uso orientado para a execução das atividades do Instituto; e

2. os acessos serão liberados de acordo com perfis previamente definidos pelo órgão responsável pelos serviços de TI;

c) gestão de mudanças de TI:

1. toda mudança nos sistemas de informação do INSS deve ser previamente e formalmente autorizada; e

2. a gestão de mudanças deve prever, no mínimo, a guarda dos registros, realização de testes e a possibilidade de recuperação do ambiente;

d) computação em nuvem:

1. o ambiente de computação em nuvem, sua infraestrutura e canal de comunicação devem estar aderentes às diretrizes e normas de SI, estabelecidas pelo Instituto, e às legislações vigentes; e

2. o contrato de prestação de serviço, quando for o caso, deverá conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço;

VII - educação e conscientização:

- a) esta Política e seus normativos complementares devem ser periodicamente divulgados a todos os agentes públicos do Instituto;
- b) o Instituto deve manter programa contínuo de conscientização dos agentes públicos em SI; e
- c) deve ser mantido plano de capacitação especializado aos profissionais que atuam na gestão de SI;

VIII - auditoria e conformidade:

- a) o cumprimento desta Política e de suas normas complementares deve ser avaliado periodicamente, por meio de verificações de conformidade; e
- b) o uso dos recursos de TI disponibilizados pelo Instituto é passível de monitoramento e auditoria;

IX - responsabilidade pela gestão das informações:

- a) os responsáveis pela gestão dos ativos da informação e sistemas corporativos devem descrever os requisitos de segurança; e
- b) os sistemas de informação devem ser concebidos possibilitando a segregação de funções;

X - segurança física e do ambiente:

- a) as instalações em que as informações críticas ou sensíveis serão processadas deverão ser mantidas em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção física; e
- b) os ativos da organização devem ser protegidos contra acesso físico não autorizado, danos, perdas, furto e interferência. As proteções devem estar alinhadas aos riscos identificados;

XI - gestão de ativos da informação, os ativos de informação devem:

- a) ser inventariados e protegidos;
- b) ter identificados os seus proprietários e custodiantes;
- c) ter a sua entrada e saída nas dependências do Instituto autorizadas e registradas por

autoridade competente; e

d) ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 6º A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas, cíveis e penais, previstas na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), no Código Penal, no Código Civil, e, ainda, em legislação que regule ou venha regular a matéria.

Art. 7º Competências e responsabilidades:

I - cabe ao Gestor de SI:

- a) promover cultura de segurança da informação;
- b) acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
- c) propor os recursos necessários à implementação das ações de SI;
- d) coordenar o Comitê de Segurança da Informação - CSI ou estrutura equivalente;
- e) acompanhar os trabalhos e a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR-INSS;
- f) propor o detalhamento das diretrizes desta Política, por meio de normas e procedimentos, e acompanhar sua implementação;
- g) assessorar a alta administração na implementação da Política de SI;
- h) estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à SI;
- i) promover a divulgação da política e das normas internas de SI do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no INSS;
- j) incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à SI;
- k) verificar os resultados dos trabalhos de auditoria sobre a gestão da SI;

l) acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da SI; e

m) manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à SI;

II - cabe ao Presidente do INSS nomear o Gestor de SI;

III - caso o Gestor de SI não seja nomeado, as atribuições relacionadas no inciso I do art. 7º serão desempenhadas pelo Diretor de Tecnologia da Informação e Inovação;

IV - a ETIR-INSS deve analisar e propor respostas a notificações e atividades relacionadas a incidentes de SI, no âmbito do Instituto;

V - é responsabilidade de todos os agentes públicos, diretos e indiretos, conhecer e cumprir as diretrizes desta Política e demais normas e procedimentos complementares de SI; e

VI - compete ao Comitê Estratégico de Governança - CEGOV deliberar sobre políticas e normas de segurança da informação, assessorado pelo Comitê Temático de Governança Digital, tendo em vista o Sistema de Governança do INSS, instituído pela Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019.

Parágrafo único. O Comitê Temático de Gestão da Informação é responsável pela aprovação de procedimentos e de normas internas que orientem o compartilhamento de dados sob gestão do INSS e pela aprovação da categorização dos níveis de compartilhamento de dados com outras entidades públicas (federais ou de outras esferas e poderes) da sociedade civil, nos termos do art. 6º do anexo à Portaria nº 3.213/PRES/INSS, de 2019.

Art. 8º Esta Política e seus normativos devem ser revisados sempre que necessário, não excedendo o período máximo de 3 (três) anos.



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE RESOLUÇÃO

RESOLUÇÃO Nº 10/CEGOV/INSS, DE 31 DE AGOSTO DE 2020

Define as regras para emissão de credenciais de acesso lógico.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do Processo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Instituir, na forma do Anexo I, a Norma de Controle de Acesso Lógico - NCAL do INSS, e aprovar os Anexos II e III.

Art. 2º Fica revogada a Resolução nº 413/PRES/INSS, de 20 de maio de 2014, publicada no Diário Oficial da União nº 95, de 21 de maio de 2014, Seção 1, págs. 43/44.

Art. 3º Esta Resolução entra em vigor sete dias após a data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

**ALESSANDRO ROOSEVELT SILVA
RIBEIRO**
Diretor de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e
Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **FLAVIO FERREIRA DOS SANTOS, Diretor(a) de Tecnologia da Informação e Inovação**, em 31/08/2020, às 18:21, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **JOBSON DE PAIVA SILVEIRA SALES, Diretor(a)**, em 31/08/2020, às 18:41, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **CLOVIS DE CASTRO JUNIOR, Diretor(a) de Integridade, Governança e Gerenciamento de Riscos**, em 31/08/2020, às 18:58, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **HELDER CALADO DE ARAUJO, Diretor(a)**, em 31/08/2020, às 19:40, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **ALESSANDRO ROOSEVELT SILVA RIBEIRO, Diretor(a)**, em 01/09/2020, às 17:35, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **LEONARDO JOSE ROLIM GUIMARAES, Presidente**, em 01/09/2020, às 19:43, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site

[https://sei.inss.gov.br/sei/controlador_externo.php?](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)

[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **1610700** e o código CRC **B2C42439**.

ANEXO I

RESOLUÇÃO Nº 10/CEGOV/INSS, DE 31 DE AGOSTO DE 2020

NORMA DE CONTROLE DE ACESSO LÓGICO – INSS

Art. 1º Os termos definidos nesta norma aplicam-se a todos os agentes públicos e privados com vínculo direto ou indireto, permanente ou temporário com o INSS.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Federais vinculados à Advocacia-Geral da União – AGU, que atuarem na consultoria e no assessoramento jurídico, e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta Norma de Controle de Acesso Lógico, são estabelecidos os seguintes conceitos e definições:

I - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

II - administrador de domínio: usuário responsável pela administração de um domínio por meio da aplicação de políticas globais, criação, edição e exclusão de usuários e grupos, e instalação de programas em um grande número de estações de trabalho;

III - administrador local: usuário responsável pela administração de partes de um domínio (geralmente restrito a um setor ou abrangência), por meio de políticas locais, edição de grupos e usuários locais, e instalação de programas em estações de trabalho limitadas a um setor ou abrangência;

IV - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta;

V - ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VI - contas de serviço: contas de acesso à rede corporativa de computadores, necessárias para a execução de procedimentos automáticos (aplicação, **script**, etc.), sem qualquer intervenção humana no seu uso;

VII - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais;

VIII - credenciamento: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer;

IX - necessidade de conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

X - credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física, como crachá, cartão e selo ou lógica como identificação usuário e senha;

XI - dado: é um elemento informativo concreto e sua forma plural expressa uma informação, é o registro do atributo de um ente objeto ou fenômeno onde registro indica o ato de registrar, ou seja, é a gravação ou a impressão de caracteres ou símbolos que tenham um significado em algum documento ou suporte físico;

XII - domínio: agrupamento lógico de computadores em rede que compartilham recursos em um banco de dados de segurança, comum, onde a administração e autenticação são centralizadas. Desta forma um usuário precisa de uma conta para ter acesso ao domínio e aos recursos compartilhados;

XIII - endereço IP (**Internet Protocol**): conjunto de elementos numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores. Sequência de números associada a cada computador conectado à Internet. No caso de IPv4, o endereço IP é dividido em quatro grupos, separados por " . " e compostos por números entre 0 e 255. No caso de IPv6, o endereço IP é dividido em

até oito grupos, separados por ":" e compostos por números hexadecimais (números e letras de "A" a "F") entre 0 e FFFF;

XIV - entidade externa: organização governamental, não governamental ou privada, amparada por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica ou instrumento congênere com o INSS;

XV - e-SIC: Sistema Eletrônico do Serviço de Informações ao Cidadão, aplicação disponibilizada na internet, que centraliza todos os pedidos de informações dirigidos ao Poder Executivo Federal;

XVI - estagiário: educando que esteja frequentando o ensino regular, em instituições de educação superior, de educação profissional, de ensino médio, de educação especial e dos anos finais do ensino fundamental, na modalidade profissional da educação de jovens e adultos, que desenvolve as atividades relacionadas à sua área de formação profissional junto as pessoas Jurídicas de Direito Privado, órgãos da Administração Pública e Instituições de Ensino, que tenham condições de proporcionar experiência prática na sua linha de formação;

XVII - estágio supervisionado: ato educativo escolar supervisionado, desenvolvido no ambiente de trabalho, que visa a preparação para o trabalho produtivo de educandos;

XVIII - ferramenta de gestão de acessos: **software** que possibilita a gestão integrada de papéis e permissões de acesso dos usuários nos sistemas corporativos;

XIX - gestor da informação: usuário que gerou a informação, que responde pelo seu conteúdo ou que foi formalmente designado para definir, alterar a sua classificação nos graus de sigilo e perfil de acesso dos demais usuários e processos;

XX - gestão de identidades: combinação de sistemas técnicos, regras e procedimentos que definem a posse, utilização e segurança de uma identidade. Seu objetivo primário é estabelecer a confiança na associação de atributos a uma identidade digital e conectar esta identidade com uma entidade individual;

XXI - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXII - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

XXIII - **log** ou registro de auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional;

XXIV - perfil de acesso do usuário: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

XXV - recursos de rede: dispositivos (impressoras, **scanners**, multifuncionais, etc) ou

serviços (sistemas, portais, etc) disponibilizados para os usuários por meio de uma rede de dados;

XXVI - serviço de diretório: serviço que armazena e organiza informações relativas a recursos disponíveis e usuários de uma rede de dados. Permite que o administrador da rede gerencie o acesso de usuários e sistemas aos recursos disponíveis;

XXVII - sistemas corporativos: sistemas de operação, ou finalísticos, que se coadunam com os fins da Previdência Social. Assim, entende-se que este conceito comporta o conjunto de sistemas e subsistemas que garantem a operação dos Regimes Geral e Próprio de Previdência Social, inclusive de previdência complementar;

XXVIII - sistemas legados: compreendem o conjunto de aplicações desenvolvidas com tecnologias obsoletas que permanecem em operação no INSS;

XXIX - usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal, formalizada por meio da assinatura do Termo de Responsabilidade;

XXX - usuário interno: servidor do quadro do INSS lotado em uma Unidade Orgânica – UO, que se utiliza dos sistemas corporativos do Instituto; e

XXXI - usuário externo: usuários vinculados a uma Entidade Externa, que se utiliza dos sistemas corporativos do Instituto por meio de um perfil de acesso concedido por um Gestor de Acesso Externo.

Art. 3º São diretrizes desta NCAL-INSS:

I - o acesso à rede e aos sistemas corporativos do INSS dar-se-á por meio de autenticação integrada de domínio baseado em serviço de diretório, administrado por meio de uma ferramenta de gestão de identidades;

II - as concessões de acesso à rede de dados e aos sistemas corporativos são distintas. Sendo assim, o usuário pode obter permissão de acesso apenas à rede de dados, ou apenas a determinado (s) sistema (s) corporativo (s);

III - as credenciais de acesso a rede de dados e aos sistemas corporativos do INSS são conferidas aos usuários com base na necessidade de conhecer, para viabilizar o exercício de suas atribuições funcionais e atividades a serem desenvolvidas no âmbito do INSS; e

IV - o uso indevido de informações dos sistemas corporativos do INSS sujeitará o agente às penalidades previstas na legislação.

Art. 4º Base Cadastral é a base de dados do Serviço de Diretórios (acesso à rede de dados), do Sistema de Gestão de Acessos (sistemas corporativos) e dos sistemas legados, que devem ser alimentadas por informações disponibilizadas pelo INSS. Para tanto, a área responsável pela gestão de

peças do INSS disponibilizará semanalmente as informações extraídas do Sistema Integrado de Administração de Recursos Humanos – SIAPE para a empresa prestadora de serviços tecnológicos contratada pelo Instituto, com a supervisão da área de gestão de TI do INSS, contendo, minimamente, os seguintes dados:

Tabela 1: Informações Usuários

ITEM	INFORMAÇÃO	CAMPO	DESCRIÇÃO
1	GR-MATRICULA	N 0012	GRUPO NUMÉRICO COMPOSTO DE NÚMERO DO ÓRGÃO (N0005) E NÚMERO DE MATRÍCULA DO SERVIDOR (N0007)
2	IT-NU-IDEN-SERV-ORIGEM	A 0008	NÚMERO DE IDENTIFICAÇÃO DO SERVIDOR NA ORIGEM - NÚMERO VINCULADO AO CARGO EFETIVO OU EM COMISSÃO
3	IT-NO-SERVIDOR	A 0060	NOME
4	IT-DA-NASCIMENTO	N 0008	DATA DE NASCIMENTO
5	IT-NU-CPF	N 0011	NÚMERO DO CPF
6	IT-NU-PIS-PASEP	N 0011	NÚMERO DO PIS
7	IT-IN-SUPRESSAO-PAGAMENTO	A 0001	INDICATIVO DE SUPRESSÃO DE PAGAMENTO
8	IT-CO-SITUACAO-SERVIDOR	N 0002	CÓDIGO DE SITUAÇÃO FUNCIONAL DO SERVIDOR
9	IT-CO-GRUPO-OCOR-AFASTAMENTO	N 0002	CÓDIGO DE OCORRÊNCIA DE AFASTAMENTO
10	IT-DA-INICIO-OCOR-AFASTAMENTO	N 0008	DATA DO INÍCIO DA OCORRÊNCIA DE AFASTAMENTO
11	IT-DA-TERMINO-OCOR-AFASTAMENTO	N 0008	DATA DE TÉRMINO DA OCORRÊNCIA DE AFASTAMENTO
12	IT-CO-GRUPO-OCOR-EXCLUSAO	N 0002	CÓDIGO DE OCORRÊNCIA DE EXCLUSÃO
13	IT-CO-UORG-LOTACAO-SERVIDOR	N 0009	CÓDIGO DA UORG DE LOTAÇÃO DO SERVIDOR
14	IT-CO-ORGAO-REQUISITANTE	N 0005	CÓDIGO DO ÓRGÃO REQUISITANTE

Parágrafo único. A Diretoria de Tecnologia da Informação e Inovação procederá com a atualização das bases cadastrais do serviço de diretórios e dos sistemas corporativos, bem como realizará a validação das informações disponibilizados pelo INSS por meio de outras bases, na periodicidade do envio das informações, e a área responsável pela gestão de pessoas do INSS poderá acordar, com a área responsável pela gestão de TI do INSS, a revisão das informações necessárias à administração de contas de usuários.

Art. 5º Sobre credenciais e perfis de acesso, verifica-se que a emissão de uma credencial permite ao usuário acessar a rede de dados corporativa do INSS. Para que o mesmo obtenha acesso aos sistemas corporativos, a credencial deve ser associada a um perfil de acesso, e o o processo de credenciamento de usuário aos ativos de informação deve ser feito observando os seguintes critérios:

I - a credencial de acesso concedida para acesso à rede de dados e sistemas corporativos do INSS é de caráter pessoal e intransferível;

II - as credenciais de acesso devem ser concedidas após a data de contratação ou entrada em exercício do usuário; e

III - as mesmas credenciais de acesso devem ser utilizadas para o acesso à rede de dados e aos sistemas corporativos do INSS, mediante autenticação que permita ao usuário acessar vários sistemas, por meio de ferramenta de gestão de identidades e acessos.

§ 1º A área responsável pela gestão de pessoas do INSS deverá utilizar os canais de atendimento disponibilizados pela empresa prestadora de serviços tecnológicos contratada pelo Instituto, ou outro canal informado pela DTI, para solicitar:

I - o credenciamento de usuários do quadro de pessoal do INSS na data do ato administrativo de retorno ou ingresso no órgão, para acesso à rede, e de estagiários, após assinatura do contrato de prestação de serviço, para acesso à rede;

II - a revogação de credenciais de acesso de servidores do quadro de pessoal do INSS cedidos a outros órgãos;

III - a desativação de usuários do quadro de pessoal do INSS na data do ato administrativo ou de ocorrências que ensejem desligamento para fins de acesso lógico; e

IV - a desativação do acesso de usuários do quadro de pessoal em atividade do INSS afastados ou com licença programada de suas funções por mais de sessenta dias ininterruptos.

§ 2º Quanto ao processo de formação das credenciais de acesso fica estabelecido que o nome do usuário será composto de acordo com os padrões estabelecidos no Guia de Interoperabilidade do Governo Eletrônico – e-Ping, mais especificamente no documento “Caixas Individuais-Fundacionais no Governo Federal” (Rede do Governo, 2010) que define regras de formação de nomes para a composição de endereços eletrônicos.

§ 3º Com relação às senhas de acesso, deve se observar que:

I - deverão ter no mínimo oito caracteres e conter, obrigatoriamente, caracteres alfanuméricos (combinação de letras e números). O usuário poderá acrescentar caracteres especiais (espaços em branco, símbolos, sinais de pontuação, etc.);

II - é vedada a reutilização das últimas quatro senhas utilizadas pelo usuário;

III - podem ser alteradas sempre que preciso ou quando o usuário achar necessário;

IV - o prazo de validade não deve ultrapassar 90 (noventa) dias; e

V - o usuário receberá, por meio de comunicado direto (via interface do sistema ou por mensagem no correio eletrônico), a informação do prazo próximo de vencimento da senha, quando esta estiver a 15 (quinze) dias da sua data de expiração.

§ 4º Os perfis de acesso aos sistemas corporativos deverão contemplar um conjunto de permissões e ações vinculadas às atividades desenvolvidas pelo usuário, sendo que:

I - caberá à área responsável pela gestão de TI do INSS estabelecer, em conjunto com as áreas responsáveis pela gestão dos sistemas corporativos, a norma de criação dos perfis de acesso;

II - as áreas responsáveis pela gestão dos sistemas corporativos são responsáveis pelas permissões, transações e ações que devem compor cada perfil de acesso; e

III - os perfis de acesso e de gestão concedidos para usuários internos e externos deverão ser objeto de revisão contínua pelos gestores responsáveis, não podendo ultrapassar o prazo máximo de 30 (trinta) meses.

§ 5º Quanto à utilização das credenciais e perfis de acesso, o usuário:

I - deve ter conhecimento prévio desta Norma de Controle de Acesso Lógico e preencher os requisitos estabelecidos na mesma;

II - deve estar devidamente autorizado a utilizar a rede corporativa e/ou os sistemas corporativos, de acordo com os requisitos estabelecidos nesta Norma;

III - deve utilizar os serviços e as informações obtidas, por meio do perfil de acesso, única e exclusivamente em razão do exercício da função pública e para os fins que lhe foi designado, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal;

IV - não pode divulgar, nem mesmo compartilhar, os códigos de segurança que lhe forem atribuídos (credenciais de acesso), os quais são pessoais e intransferíveis;

V - não pode utilizar as credenciais para acessar os recursos disponíveis em mais de uma estação de trabalho simultaneamente;

VI - não pode fazer uso das credenciais de acesso de outros usuários;

VII - deve fornecer informações acessadas nos sistemas e na rede de dados corporativos do INSS somente mediante demanda formalizada de quem tenha competência para tal;

VIII - deve comunicar à chefia imediata ou responsável pela administração do sistema ou rede corporativa quaisquer violações ou incidentes referentes à proteção do equipamento utilizado, do **software** ou de outros ativos da informação;

IX - deve, sempre que for necessário, afastar-se da estação de trabalho, certificar-se de que a sessão de rede ou acesso ao sistema corporativo esteja encerrado ou bloqueado;

X - deverá, obrigatoriamente, efetuar processo de alteração da sua senha em seu primeiro acesso à rede de dados corporativa; e

XI - no ato do primeiro acesso, bem como após cada atualização desta Norma, o usuário deverá manifestar concordância com os termos dispostos na mesma.

§ 6º O processo de autenticação de usuários deve ser definido pela área responsável pela gestão de Tecnologia da Informação do Instituto e poderá ser baseada em autenticação simples (nome de usuário e senha) agregada a autenticação multifator (certificação digital ou outros meios disponíveis).

§ 7º O credenciamento de usuários internos se dá pelo cadastro de novos servidores ou ocupantes de cargo em comissão, no âmbito do Instituto, pode ser solicitado por servidor vinculado à área responsável pela gestão de pessoas ou pela chefia imediata do usuário.

§ 8º O cadastro de que trata o § 7º deve ser solicitado por meio dos canais de atendimento disponibilizados pela prestadora de serviços tecnológicos contratada pelo Instituto ou outro informado pela DTI.

§ 9º O credenciamento de estagiários, se dará com a emissão de credencial de acesso, tendo como requisito as seguintes condições:

I - a empresa que atuar como agente de integração do estágio supervisionado deve manter contrato com o INSS;

II - o contrato de estágio supervisionado deverá conter cláusula de confidencialidade e sigilo de informações preestabelecidos com a Administração Pública;

III - a criação de perfis específicos e restritos às atividades do estagiário pelos gestores dos sistemas corporativos para o acesso dos estagiários;

IV - é vedada a concessão de perfis de acesso aos sistemas corporativos para estagiários com permissão de alteração das bases de dados institucionais;

V - o acesso será concedido mediante solicitação expressa de servidor do quadro do INSS, responsável pela supervisão do estágio, que deverá avaliar os riscos de utilização indevida de informações institucionais e as eventuais restrições referentes aos dias e horários para a realização dos acessos;

VI - o acesso será precedido da assinatura do Termo de Confidencialidade e de Manutenção de Sigilo – TCMS, Anexo II, o qual deverá ser firmado pelo estagiário ou pelo estagiário e seu responsável legal, no caso de se tratar de estagiário menor de 18 (dezoito) anos;

VII - as solicitações de acesso à rede para estagiários devem ser procedidas por meio dos canais remotos de atendimento disponibilizados pela empresa prestadora de serviços tecnológicos contratada pelo Instituto ou outro canal informado pela DTI, pela unidade de gestão de pessoas, pela chefia imediata do educando ou pelo responsável por sua supervisão;

VIII - os gestores de sistemas devem criar perfis diferenciados para estagiários de nível médio e nível superior;

IX - o supervisor do estagiário deverá, periodicamente, orientá-lo quanto ao uso responsável e adequado do acesso aos sistemas corporativos; e

X - o acesso do estagiário limitar-se-á à data final do contrato ou imediatamente cessado na hipótese de rescisão antecipada do estágio, cabendo ao supervisor do estagiário, em quaisquer dos casos, adotar as providências necessárias ao bloqueio do acesso, tão logo finde a contratação.

§ 10. O credenciamento de usuários externos, obedecerá as seguintes diretrizes:

I - as credenciais de acesso para usuários externos devem ser emitidas tendo em vista o interesse do INSS, devidamente justificadas e previstas no convênio, acordo de cooperação técnica ou instrumento congênere;

II - as solicitações de emissão de credenciais de acesso à rede corporativa para usuários amparados por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica, contrato ou instrumento congênere devem:

a) ser feitas pelo gestor da unidade/área responsável pela gestão do instrumento legal; e

b) ser atendidas somente após validação das credenciais do gestor solicitante do Instituto, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700);

III - a emissão de credenciais de acesso à rede corporativa para prestadores de serviço terceirizados ou equiparados nas dependências do INSS, quando necessária, será provida unicamente pelo interesse do INSS, devendo ser atendidos os seguintes requisitos:

a) a organização a qual o usuário é vinculado deve manter contrato, acordo de cooperação, convênio ou instrumento congênere vigente com o INSS;

b) instrumento deve conter cláusulas prevendo:

1. a necessidade e justificativa para acesso à rede corporativa;

2. a confidencialidade e sigilo de informações preestabelecidas junto ao Instituto; e

3. a obrigatoriedade da organização ou do ente contratado informar previamente ao representante legal do INSS, responsável pela gestão do contrato, quaisquer alterações em seu corpo de colaboradores que impacte na emissão/exclusão das contas de acesso;

c) a organização ou ente contratado também deverá manter com seus colaboradores Termo de Confidencialidade de Manutenção de Sigilo – TCMS; e

d) o gestor do contrato pelo INSS deve fundamentar a necessidade do acesso à rede para prestadores de serviço terceirizados ou equiparados, definindo os recursos que devem ser disponibilizados e eventuais restrições a dias e horas para realização do acesso à rede;

IV - os TCMS deverão ser arquivados junto aos instrumentos assinados com o INSS e uma cópia ou **link** eletrônico deverá ser encaminhada ao Gestor do Contrato. O mesmo deve ocorrer para quaisquer alterações ocorridas na vigência dos contratos, acordos ou convênios;

V - caso os Termos sejam gerados de forma eletrônica, deverá ser disponibilizado o arquivo correspondente, atendendo aos requisitos necessários para garantia de integridade e disponibilidade de acesso, assim como os requisitos específicos previstos em contrato; e

VI - a emissão de credenciais de acesso poderá ser feita pelo gestor do contrato, representante legal do INSS, ou pelo gestor da unidade responsável pela gestão do contrato, convênio, acordo de cooperação técnica ou instrumento congênere e serão atendidas somente após validação das credenciais do solicitante, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700).

§ 11. O acesso aos prestadores de serviço vinculados à Central de Atendimento 135 se dará observando as seguintes condições:

I - a empresa deve manter contrato com o INSS;

II - o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

III - a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade - TCMS;

IV - o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte do INSS, definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;

V - os acessos deverão ser realizados única e exclusivamente por necessidade de serviço;

VI - os contratos de prestação de serviços de teleatendimento devem conter documento a ser utilizado para formalização das indicações de gestores de acesso aos sistemas corporativos do Instituto; e

VII - o INSS pode disponibilizar, de forma restrita, às centrais 135, uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

§ 12. Nos casos referentes a prestadores de serviço vinculados à Ouvidoria do Ministério da Economia, o acesso se dará observando-se as seguintes condições:

I - a empresa deve manter contrato direto com a Ouvidoria do Ministério da Economia;

II - o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

III - a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade;

IV - o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte da Ouvidoria do Ministério da Economia, definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;

V - os acessos deverão ser realizados única e exclusivamente por necessidade de serviço; e

VI - o INSS pode disponibilizar, de forma restrita, à Ouvidoria do Ministério da Economia, uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

§ 13. O acesso à rede corporativa por servidores vinculados a órgãos de controle externo, envolvidos em ações de auditoria no âmbito do INSS, será concedido mediante apresentação da equipe de auditoria por meio de documento formal que conste:

I - dados necessários ao cadastro de usuários externos;

II - informações acerca dos objetivos dos trabalhos a serem executados;

III - os prazos envolvidos; e

IV - informações complementares.

§ 14. O tipo de acesso de que trata o § 12 deverá observar:

I - as parcerias institucionalmente estabelecidas entre esses órgãos e o INSS no que tange à cobertura/previsão de acesso à rede corporativa do Instituto;

II - o atendimento de pedido de solicitação de informações advindo de pessoas físicas ou jurídicas externas, respeitadas as restrições de acesso às informações previstas na Lei nº 12.527, de 18 de novembro de 2011, serão analisadas pela área designada para responder as demandas dos cidadãos por meio do e-SIC; e

III - os procedimentos referentes às solicitações de inclusão, exclusão, inativação e suspensão de contas de acesso de usuários devem ser executados tendo como premissa a preservação dos registros para efeito de auditoria.

§ 15. O bloqueio administrativo se dará da seguinte forma:

I - o responsável pela Corregedoria-Geral do INSS, quando necessário, poderá solicitar a suspensão, bloqueio ou inativação imediata de contas de acesso de usuários que estiverem envolvidos em inquérito penal, em Processo Administrativo Disciplinar – PAD ou em Sindicância, decorrente de infrações cometidas no exercício das atribuições do cargo, quando o usuário estiver na seguinte situação:

a) afastado temporariamente do cargo ou função pública em razão de ato que se encontra sob apuração;

b) indiciado em processo administrativo disciplinar, por incursão nos incisos IX, XI, XII, XV, XVI e XVII do art. 117 e arts. 130 e 132 da Lei nº 8.112, de 11 de dezembro de 1990, ou cuja proposta pela Comissão Processante, no relatório final, seja pela aplicação de penalidade a partir de suspensão de 30 (trinta) dias; e

c) submetido à prisão em flagrante, temporária ou preventiva decorrente do cometimento de infração no exercício das atribuições do cargo, enquanto estiver em apuração de inquérito policial ou pelo Ministério Público Federal;

II - as solicitações de que tratam o inciso I deverão ser efetuadas mediante comunicação formal da Corregedoria-Geral para a prestadora de serviços tecnológicos contratada pelo Instituto, ou outro canal informado pela DTI, a qual procederá a imediata implementação da mudança;

III - o bloqueio de acessos tratados nas situações do inciso I serão efetivados no âmbito da ferramenta de gestão de acessos nas seguintes situações:

a) usuário afastado temporariamente do cargo ou função, enquanto durar o afastamento; e

b) usuário indiciado nos termos da alínea "c" do inciso I do § 15, até o efetivo cumprimento da penalidade porventura aplicada ou, em caso de não aplicação de penalidade, enquanto durar o processo.

Art. 6º A Rede de Dados Corporativa compõe a infraestrutura de rede, que é disponibilizada para uso institucional, logo, apenas equipamentos de propriedade do Instituto são autorizados e devem ser conectados à rede corporativa.

§ 1º Em casos excepcionais, a conexão de equipamentos particulares à rede corporativa deve ser feita em razão do interesse do Instituto e sob prévia autorização do responsável pela gestão da unidade em que o equipamento estiver localizado.

§ 2º O INSS poderá disponibilizar o acesso à rede de dados corporativa por meio de tecnologia **Wireless** (sem fio). Para tanto os seguintes critérios deverão ser adotados:

I - os projetos que envolvam a utilização de pontos de acesso sem fio à rede corporativa no âmbito do Instituto deverão ser devidamente registrados e aprovados pela área responsável pela gestão de TI do INSS;

II - os pontos de acesso à rede de dados corporativa sem fio poderão ser objeto de testes periódicos de penetração e de auditoria a critério da área responsável pela gestão de TI no INSS; e

III - as conexões à rede sem fio serão avaliadas pela área responsável pela gestão de TI do INSS em relação aos requisitos de segurança e deverão atender ao princípio do privilégio mínimo.

§ 3º A área responsável pela gestão de TI do INSS poderá disponibilizar rede sem fio com regras específicas de acesso para visitantes nas diversas unidades do Instituto.

§ 4º Os dispositivos conectados à rede do INSS por meio de conexão sem fio deverão suportar configurações de criptografia estabelecidas pela área responsável pela gestão de TI no âmbito do INSS;

§ 5º Qualquer tecnologia de acesso sem fio implementada no INSS deverá suportar autenticação forte, com possibilidade de efetuar checagens em bancos de dados externos, e a área responsável pela gestão de TI do INSS deve dispor de mecanismos automáticos que possibilitem:

I - a detecção e bloqueio de equipamentos externos conectados à rede corporativa; e

II - a identificação e rastreamento dos endereços IP de origem e destino, bem como os serviços utilizados na rede corporativa inclusive nos acessos remotos.

§ 6º A administração da rede corporativa trata da operacionalização da rede do INSS, que é realizada por empresa prestadora de serviços tecnológicos contratada pelo Instituto e seguem as seguintes premissas:

I - prover, gerenciar e operacionalizar os ativos, acessos e serviços que compõem a rede de dados corporativa do INSS; e

II - submeter-se ao monitoramento de serviços de tecnologia contratados pelo Instituto, seguindo as regras desta Norma.

§ 7º Quanto ao processo de geração de contas de serviço, fica estabelecido que:

I - os critérios para a emissão de contas de serviços serão vinculados a um processo formal estabelecido pela área responsável pela gestão de TI do INSS;

II - a concessão de contas de serviços deve ser feita conforme a necessidade de uso de acordo com os critérios estabelecidos nesta Norma;

III - o direito de acesso privilegiado, por meio de contas de serviços, associado a sistemas ou processos, deve ser identificado;

IV - deve ser viabilizada ferramenta que possibilite a gestão das contas de serviço de forma automatizada, possibilitando o registro e verificação de todos os privilégios concedidos;

V - as contas de serviço fornecidas devem ser utilizadas exclusivamente para os fins aos quais foram concedidas;

VI - as contas de serviço emitidas devem ser revalidadas periodicamente com base na função exercida e na área de atuação do servidor; e

VII - as contas de serviço com credenciais de acesso de uso compartilhado devem ter suas senhas alteradas periodicamente, conforme estabelecido nesta Norma de Controle de Acesso Lógico, ou sempre que ocorrerem mudanças no grupo de usuários que utilizam as mesmas.

§ 8º É vedado o uso da rede corporativa para:

I - acesso por meio de equipamento não homologado ou não autorizado pelo INSS;

II - fazer download, instalar e/ou utilizar sistemas ou aplicativos não homologados pela área responsável pela gestão de TI do INSS nos equipamentos de propriedade do Instituto;

III - a utilização de **softwares** particulares em equipamentos do INSS sem autorização expressa;

IV - a instalação e conexão de equipamentos particulares à rede corporativa do Instituto sem a prévia autorização do gestor responsável pela unidade ou da área responsável pela gestão de TI do INSS;

V - o uso dos recursos de rede para fins particulares ou de terceiros alheios aos interesses do INSS, em especial, quando tal procedimento prejudique o tráfego da rede de dados;

VI - o uso para fins de divulgação ou distribuição de material que não possua vínculo com as atividades desenvolvidas pelo Instituto;

VII - a instalação ou utilização de ferramentas de monitoramento de rede sem a anuência e autorização expressa da área responsável pela gestão de TI no Instituto;

VIII - a instalação de dispositivos de comunicação ou de compartilhamento de dados sem fio, particulares, à rede corporativa do Instituto, sem autorização expressa da área responsável pela gestão de TI do INSS; e

IX - burlar as regras de acesso a internet configuradas em **proxy** ou ferramenta similar de gerenciamento de conteúdo **web**.

§ 9º Cabe à área responsável pela gestão de TI no âmbito do INSS definir os aspectos relacionados à plataforma tecnológica, gestão operacional, forma de autenticação e sustentação do domínio de rede do INSS.

Art. 7º A Gestão do Acesso aos Sistemas Corporativos seguirá as seguintes premissas:

I - sistemas legados:

a) as regras estabelecidas nesta norma devem ser aplicadas, guardando-se as devidas limitações tecnológicas, aos sistemas legados; e

b) o controle de acesso aos sistemas legados é efetuado por base própria;

II - sistemas de apoio à administração:

a) os ambientes de hospedagem desses sistemas são suportados por terceiros;

b) o ambiente deverá ser gerenciado e operacionalizado pela área de gestão de TI do INSS;

c) o acesso pelos usuários a esses sistemas deverá ser autenticado pelo serviço de diretório utilizado pelo Instituto; e

d) as regras de hospedagem de sistemas serão definidas, em ato próprio, pela área de gestão de TI do INSS;

III - armazenamento de registros **logs**:

a) as áreas responsáveis pela gestão de sistemas corporativos e demais aplicações devem definir, em conjunto com a área responsável pela gestão de TI, a temporalidade de registro dos **logs** de acesso e transações, e quais registros devem ser armazenados por um período maior que o estipulado no **caput** do art. 8º;

b) o INSS poderá alterar a temporalidade destes dados em norma específica; e

c) os **logs** de acesso devem contemplar minimamente os registros relacionados no Anexo III;

IV - administração da ferramenta de gestão de acesso:

a) com o objetivo de operacionalizar a gestão dos acessos aos sistemas corporativos no âmbito do INSS, serão criados os seguintes papéis:

1. administrador de sistema INSS: servidor do quadro, lotado na área responsável pela gestão de TI, designado por meio de Portaria do Diretor de Tecnologia da Informação e Inovação, a ser publicada em Boletim de Serviço – BS, responsável pela administração da ferramenta de gestão de acesso aos sistemas corporativos no âmbito do INSS;

2. gestor de sistema: servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em BS, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedoria-Geral e Procuradoria Federal Especializada junto ao INSS - PFE-INSS. É responsável pela implementação de sistemas corporativos no âmbito do INSS;

3. gestor de acesso central: servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em BS, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedoria-Geral e PFE-INSS. É responsável pela manutenção dos perfis de gestão dos usuários nas áreas que compõem a Administração Central e, quando necessário, dos gestores de acesso das Superintendências-Regionais - SR;

4. gestor de acesso interno: servidor do quadro, lotado na Administração Central, SR, Gerência-Executiva - GEX, Agência da Previdência Social - APS, indicado pelo Gestor de Acesso Central ou por um Gestor de Acesso, responsável pela atribuição do perfil de acesso e de gestão dos usuários no INSS; e

5. gestor de acesso externo: pessoa formalmente indicada, por documento previsto no instrumento legal que firmou a parceria ou por meio de Ofício de lavra do representante máximo de uma Entidade Externa, responsável pelo cadastro de usuários externos e a gestão dos acessos aos sistemas corporativos do Instituto;

b) os perfis de acesso serão atribuídos de acordo com a necessidade do fluxo de operação definido para cada sistema corporativo;

c) a indicação e o processo de substituição dos responsáveis pela gestão dos acessos aos sistemas corporativos no âmbito do INSS poderá ser procedida das seguintes formas:

1. a autoridade responsável pela indicação do gestor de acessos pode indicar opcionalmente o substituto;

2. o próprio gestor de acessos pode designar, a qualquer momento, por meio da ferramenta de gestão de acessos um substituto;

3. quando não houver um gestor responsável, ou substituto, por uma unidade devidamente designado, a gestão dos usuários será transferida, preferencialmente de forma automática, para o responsável pela área da abrangência daquela unidade e assim subsequentemente; e

4. o Gestor de Acesso é corresponsável com os perfis de gestão ou acesso que ele atribuir aos usuários;

d) ao usuário interno cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Norma de Controle de Acesso Lógico e suas normas complementares;

2. solicitar, ao Gestor de Acesso responsável pela gestão da unidade de lotação a qual é vinculado, a suspensão do seu perfil de acesso nos períodos de afastamento do serviço por mais de 30 (trinta) dias consecutivos;

3. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e

4. ter conhecimento e estar de acordo com o disposto nesta Norma;

e) ao usuário externo cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Norma de Controle de Acesso Lógico;

2. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e

3. ter conhecimento e estar de acordo com o disposto nesta Norma;

f) ao administrador do sistema INSS cabe:

1. criar os sistemas e subsistemas, devidamente homologados pela área de negócio responsável, no ambiente de produção, por meio de ferramenta de gestão de acesso;

2. mediante apresentação de Portaria de designação para Gestores de Acesso Central, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores quanto à atribuição dos perfis de gestão; e

3. mediante apresentação de Portaria de designação para Gestores de Sistema, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores acerca do processo de implementação dos sistemas corporativos no âmbito do INSS;

g) ao gestor de sistema cabe:

1. efetuar os procedimentos de importação, inclusão, alteração e exclusão de papéis e permissões nos sistemas corporativos em ambiente de produção; e

2. atuar, em conjunto com o Administrador do Sistema INSS e a prestadora de serviços tecnológicos contratada pelo Instituto, no planejamento e execução do processo de implementação dos sistemas corporativos dos quais for designado responsável;

h) ao gestor de acesso central cabe:

1. efetuar o credenciamento, suspensão ou exclusão de perfis de gestão dos sistemas corporativos aos Gestores de Acesso na Administração Central e, quando necessário, dos Gestores de Acesso da SR, GEX, APS e demais usuários de sua abrangência; e

2. orientar os usuários de sua abrangência e os gestores da Administração Central e SR, GEX e APS acerca das regras para o acesso aos sistemas corporativos do INSS;

i) ao gestor de acesso interno cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários da Administração Central, SR, GEX, APS;

2. atribuir, alterar ou excluir os perfis de acesso aos usuários da Administração Central, SR, GEX, APS; e

3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS;

j) ao gestor de acesso externo cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários do seu Órgão/Entidade;

2. atribuir, alterar ou excluir os perfis de acesso aos usuários do seu Órgão/Entidade; e

3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS;

V - configura-se mau uso, sujeito a responsabilidade penal, civil e disciplinar:

a) a divulgação, sem autorização expressa da chefia imediata ou do gestor de acesso de sua abrangência, de informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS;

b) acessar sistemas corporativos sem autorização prévia, de acordo com os requisitos estabelecidos nesta Norma;

c) utilizar-se das informações obtidas por meio de acesso concedido em desacordo com os procedimentos dispostos nesta Norma e demais normas vigentes na Administração Pública Federal;

d) compartilhar ou fazer uso das credenciais de acesso, aos sistemas corporativos, de outros usuários; e

e) a instalação de sistemas corporativos em equipamentos particulares;

VI - em casos excepcionais, a área responsável pela gestão de TI do INSS, mediante ato formal, poderá autorizar a adoção das medidas descritas no § 2º do art.8º.

Art. 8º Todo acesso à rede de dados e aos sistemas corporativos deve ser registrado e monitorado de modo que permita a rastreabilidade, a identificação e o bloqueio de usuários e equipamentos não autorizados. Estas informações devem ser armazenadas por um período de, no mínimo, doze (12) meses, observando o disposto no inciso III do art. 7º.

§ 1º As ocorrências de mau uso do acesso aos recursos disponíveis na rede e sistemas corporativos não previstas nesta norma e os casos omissos serão encaminhados para a área responsável pela gestão de TI no âmbito do INSS para análise e pronunciamento.

§ 2º Identificada irregularidade de mau uso dos recursos de rede poderá ocorrer o bloqueio preventivo do acesso pela DTI, o encaminhamento de dossiê com as informações para a Corregedoria-Geral do INSS ou Corregedorias-Regionais, nas suas áreas de abrangências, a fim de que seja realizada a análise no âmbito disciplinar.

§ 3º O descumprimento dessa Norma poderá resultar em sanções administrativas, civis e criminais.

Art. 9º Esta norma deve ser revisada num período máximo de 3 (três) anos.

ANEXO II

RESOLUÇÃO Nº 10/CEGOV/INSS, DE 31 DE AGOSTO DE 2020

TERMO DE RESPONSABILIDADE

Pelo _____ presente _____ instrumento, _____ eu
identidade nº _____, CPF nº _____, documento de
_____ expedida pelo _____, em _____, e lotado no(a)
_____ do Instituto Nacional do Seguro Social –
INSS, DECLARO, sob pena das sanções cabíveis nos termos da Política de Segurança da Informação -
POSIN do INSS que assumo a responsabilidade por:

I - tratar o(s) ativo(s) de informação como patrimônio do Instituto Nacional do Seguro Social;

II - utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do INSS;

III - contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que disciplina a gestão de segurança da informação na Administração Pública Federal, direta e indireta, e dá outras providências;

IV - utilizar as credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do INSS;

V - responder, perante o INSS, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

_____, _____ de _____ de _____

Nome e assinatura do usuário:	Unidade de Lotação:
Nome e assinatura da Autoridade Responsável pela Autorização do Acesso:	

ANEXO III

RESOLUÇÃO Nº 10/CEGOV/INSS, DE 31 DE AGOSTO DE 2020

REGISTROS DE LOGS

1. Relação dos campos de registros de logs do GERID
 - 1.1. Dados Gerais
 - 1.1.1. Data
 - 1.1.2. Sistema
 - 1.1.3. Ambiente
 - 1.1.4. IP destino
 - 1.1.5. IP origem
 - 1.1.6. CPF usuário
 - 1.1.7. URL de origem
2. Ações:
 - 2.1. CAS (autenticação): Central **Authentication Service** - Serviço Central de Autenticação
 - 2.1.1. Criação de **service ticket** (ST)
 - 2.1.2. Criação de **ticket granting ticket** (TGT)
 - 2.1.3. validação de ST
 - 2.1.4. Exclusão de **ticket** TGT
 - 2.1.5. Autenticação com sucesso (**login+password**)
 - 2.1.6. Autenticação com sucesso (certificado digital)
 - 2.1.7. Autenticação com falha
 - 2.2. GPA: Gerenciamento de Permissão de Acesso
 - 2.2.1. Início de sessão
 - 2.2.2. Dados do usuário em sessão (CPF, NOME, PAPEL)
 - 2.2.3. Requisição de **logout**
 - 2.2.4. Dados de credenciais
 - 2.2.5. Concessão de credenciais
 - 2.2.6. Alteração de Credenciais
 - 2.2.7. Dados de receptor (CPF, NOME, Lotação)
 - 2.2.8. Inserção de credencial no usuário
 - 2.2.9. Revogação de Credenciais
 - 2.2.10. Pesquisa de credenciais
 - 2.2.11. Pesquisa de usuários
 - 2.2.12. Substituição de gestor



INSTITUTO NACIONAL DO SEGURO SOCIAL

RESOLUÇÃO Nº 11/CEGOV/INSS, DE 31 DE AGOSTO DE 2020

Institui a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR do Instituto Nacional do Seguro Social.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do Processo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Instituir, no âmbito do INSS, e nos termos do Anexo a esta Resolução, a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR-INSS.

Art. 2º Esta Resolução complementa Política de Segurança da Informação POSIN-INSS vigente e entra em vigor sete dias após a data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

**ALESSANDRO ROOSEVELT SILVA
RIBEIRO**
Diretor de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **FLAVIO FERREIRA DOS SANTOS, Diretor(a) de Tecnologia da Informação e Inovação**, em 31/08/2020, às 18:21, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **JOBSON DE PAIVA SILVEIRA SALES, Diretor(a)**, em 31/08/2020, às 18:41, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **CLOVIS DE CASTRO JUNIOR, Diretor(a) de Integridade, Governança e Gerenciamento de Riscos**, em 31/08/2020, às 18:59, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **HELDER CALADO DE ARAUJO, Diretor(a)**, em 31/08/2020, às 19:40, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **ALESSANDRO ROOSEVELT SILVA RIBEIRO, Diretor(a)**, em 01/09/2020, às 17:35, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **LEONARDO JOSE ROLIM GUIMARAES, Presidente**, em 01/09/2020, às 19:43, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1611085** e o código CRC **47A32CAE**.

ANEXO

RESOLUÇÃO Nº 11/CEGOV/INSS, DE 31 DE AGOSTO DE 2020

EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS - ETIR-INSS

Art. 1º A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR-INSS tem por objetivo agir proativamente, receber, analisar, monitorar, coordenar e propor respostas a notificações e atividades relacionadas a incidentes de segurança da informação e comunicações no âmbito do INSS.

Art. 2º As atividades pertinentes à ETIR-INSS englobam os usuários dos serviços de Tecnologia da Informação - TI e os sistemas de informação do INSS e serão realizadas com intercâmbio de informações e em cooperação com as seguintes instâncias:

I - o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR GOV;

II - a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR de empresas prestadoras de serviços de tecnologia contratadas pelo INSS;

III - as ETIRs ou estrutura equivalente dos demais órgãos, entidades e empresas, públicas ou privadas, que tenham contratos, acordos, convênios ou instrumentos congêneres com o INSS; e

IV - o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República – GSI/PR.

Art. 3º Para os efeitos desta Resolução ficam estabelecidos os seguintes conceitos e definições:

I - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR: equipe de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

II - CTIR GOV: Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI;

III - agente responsável: servidor público ocupante de cargo efetivo de órgão ou entidade da Administração Pública Federal, direta ou indireta ou militar de carreira incumbido de chefiar e gerenciar uma ETIR;

IV - artefato malicioso: qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

V - Comunidade ou Público Alvo: conjunto de pessoas, setores, órgãos ou entidades atendidas por uma ETIR ou estrutura equivalente;

VI - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VII - serviço: conjunto de procedimentos, estruturados em processo definido, oferecido à comunidade pela ETIR;

VIII - Tratamento de Incidentes de Segurança em Redes Computacionais: serviço consistente em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

IX - usuário: pessoas que fazem uso de serviços de TI e sistemas de informação de propriedade do INSS, independentemente do cargo ocupado (contratados, consultores, conselheiros, servidores, temporários e etc.); e

X - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que possam resultar em risco para um sistema ou por uma organização, e que possam ser evitados por uma ação interna de segurança da informação.

Art. 4º A implementação e o funcionamento da ETIR-INSS seguirão metodologia definida pelo GSI/PR e as seguintes diretrizes:

I - basear-se no “Modelo 1 – Utilizando a equipe de Tecnologia da Informação”, conforme definido pelo GSI/PR;

II - os integrantes da Equipe deverão ser profissionais da área de Tecnologia da Informação, servidores públicos efetivos, lotados na Diretoria de Tecnologia da Informação e Inovação – DTI do INSS, sem prejuízo de suas atribuições típicas do cargo, com experiência e conhecimentos técnicos compatíveis com a importância da missão da ETIR-INSS;

III - a ETIR-INSS ficará vinculada tecnicamente à Coordenação-Geral de Infraestrutura e Operações – CGIN da DTI;

IV - o Coordenador da ETIR-INSS será nomeado por ato do Diretor de Tecnologia da Informação e Inovação; e

V - na ausência de Coordenador formalmente nomeado, as atribuições relacionadas à coordenação da equipe serão desempenhadas pelo Coordenador-Geral de Infraestrutura e Operações.

Art. 5º A ETIR-INSS será composta por membros:

I - permanentes, que efetivamente atuarão em todos os incidentes registrados;

II - colaboradores, que atuarão, de forma esporádica, no tratamento de incidentes relacionados às suas áreas de atuação; e

III - opcionais, servidores das unidades descentralizadas do INSS sob supervisão da DTI.

§ 1º Os membros da ETIR-INSS serão designados por meio de ato do Diretor de Tecnologia da Informação e Inovação.

§ 2º A distribuição dos membros da ETIR-INSS se dará da seguinte forma:

I - 2 (dois) servidores permanentes, oriundos do Serviço de Segurança de TIC;

II - 2 (dois) servidores colaboradores, oriundos da CGIN;

III - 2 (dois) servidores colaboradores, oriundos da Coordenação-Geral de Projetos e Soluções Digitais da DTI; e

IV - 2 (dois) servidores opcionais, oriundos das unidades descentralizadas do INSS.

Art. 6º A ETIR-INSS terá autonomia limitada para o tratamento de incidentes de Segurança da Informação, devendo implementar ações que possam impactar outras áreas do Instituto somente com anuência do Diretor de Tecnologia da Informação e Inovação e do Gestor responsável pela área/sistema afetada, e poderá, ainda, gerar relatórios técnicos sugerindo a adoção de medidas para resolução de incidentes.

Art. 7º A ETIR-INSS fornecerá o serviço de Tratamento de Incidentes de Segurança em Redes Computacionais, que compreende as seguintes ações:

I - recepção de solicitações e alertas diversos, utilizando como canal de comunicação a caixa postal etir@inss.gov.br, a ser disponibilizada pelo INSS;

II - filtragem de todo conteúdo direcionado à ETIR-INSS, para fins de verificação quanto à necessidade de tratamento pela Equipe e, caso não se trate de incidente de segurança em redes computacionais, encaminhar para a área competente;

III - catalogação dos incidentes detectados em ferramenta a ser indicada pela DTI, com nível de acesso restrito;

IV - classificação dos incidentes detectados quanto ao nível de severidade e impacto;

V - tratamento do incidente com medidas corretivas e indicação de formas de se evitar que ocorra novamente;

VI - resposta às solicitações e alertas encaminhados para a ETIR; e

VII - monitoramento da aplicação do tratamento dos incidentes indicados.

§ 1º A ETIR-INSS deverá analisar os incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências; e

§ 2º O detalhamento dos serviços prestados pela ETIR-INSS deverá ser publicado em página específica da Intranet do INSS, no prazo de 30 (trinta) dias a partir da publicação desta Resolução.



INSTITUTO NACIONAL DO SEGURO SOCIAL

RESOLUÇÃO Nº 12/CEGOV/INSS, DE 31 DE AGOSTO DE 2020

Disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.

O **COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS**, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante do Processo Administrativo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Estabelecer, nos termos do Anexo I, os critérios para o uso da Internet no âmbito do INSS e aprovar o Formulário de Solicitação de Acesso à Internet, constante do Anexo II.

Art. 2º Esta Resolução complementa Política de Segurança da Informação POSIN-INSS vigente e entra em vigor sete dias após a data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES
Presidente

ALESSANDRO ROOSEVELT SILVA RIBEIRO
Diretor de Benefícios

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Atendimento

HELDER CALADO DE ARAÚJO
Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR
Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **FLAVIO FERREIRA DOS SANTOS, Diretor(a) de Tecnologia da Informação e Inovação**, em 31/08/2020, às 18:21, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **JOBSON DE PAIVA SILVEIRA SALES, Diretor(a)**, em 31/08/2020, às 18:41, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **CLOVIS DE CASTRO JUNIOR, Diretor(a) de Integridade, Governança e Gerenciamento de Riscos**, em 31/08/2020, às 18:59, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **HELDER CALADO DE ARAUJO, Diretor(a)**, em 31/08/2020, às 19:40, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **ALESSANDRO ROOSEVELT SILVA RIBEIRO, Diretor(a)**, em 01/09/2020, às 17:35, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1609867** e o código CRC **B6502F8C**.

ANEXO I

RESOLUÇÃO Nº 12/CEGOV/INSS, DE 31 DE AGOSTO DE 2020

NORMAS DE USO DA INTERNET

Art. 1º Esta norma se aplica a todos os servidores e colaboradores, vinculados direta ou indiretamente ao INSS, bem como a servidores e empregados de entidades e órgãos da Administração Pública ou privados que necessitem ou estejam autorizados a acessar a Internet a partir da rede corporativa do Instituto.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União – AGU que atuarem na consultoria, assessoramento jurídico e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta norma, ficam estabelecidos os seguintes conceitos e definições:

I - autorizador: ocupantes de cargo responsáveis pela autorização da concessão de perfis de acesso para usuários finais de sua área de abrangência;

II - Internet: rede mundial que interliga computadores de diferentes tipos e dimensões e permite a comunicação entre pessoas e organizações, independentemente da localização geográfica;

III - Intranet: rede de computadores administrada pelo INSS, que utiliza os mesmos serviços e tecnologias disponíveis na rede mundial;

IV - perfil de acesso: atributo que estabelece as categorias de sítios acessíveis e tipos de arquivos que podem ser recebidos ou transmitidos pelos usuários;

V - **proxy**: ferramenta que desempenha a função de conexão do computador local à rede externa (Internet);

VI - sítio: conjunto de informações ou serviços disponíveis na Internet ou na Intranet, organizados em páginas eletrônicas e acessíveis por meio de endereços que identificam, de forma padronizada, sua origem e conteúdo;

VII - usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal - APF, formalizada por meio da assinatura do Termo de Responsabilidade; e

VIII - VPN: Rede Privada Virtual (**Virtual Private Network**) construída sobre a infraestrutura de uma rede pública, possibilitando a conexão de dois computadores por meio de uma rede pública.

Art. 3º O acesso pelos usuários à Internet disponibilizado pelo INSS deverá pautar-se pelas seguintes diretrizes:

I - seu uso se dará exclusivamente em razão de trabalho e de acordo com os procedimentos dispostos nesta Norma;

II - os recursos disponibilizados pelo INSS não poderão ser usados para quaisquer propósitos ilegais ou proibidos, que possam danificar, desativar, sobrecarregar ou prejudicar qualquer área, serviço ou conteúdo, ou interferir no uso e execução

das atividades laborais de outros usuários;

III - o volume de tráfego de Internet e os endereços **web** visitados poderão ser monitorados, visando assegurar o cumprimento desta norma; e

IV - o acesso à Internet para propósitos particulares ou estranhos às atividades do INSS poderá ser bloqueado, sem prévia comunicação ao usuário e sem prejuízo das demais sanções aplicáveis.

Art. 4º O acesso aos sítios da Internet para todos os usuários será realizado mediante a atribuição de perfis de acesso, distribuídos nos seguintes níveis:

I - Perfil 1: Perfil Restrito, inicialmente atribuído a usuários com maior restrição de acesso à Internet, permitindo acesso somente a sítios governamentais, instituições bancárias e sítios considerados de interesse do INSS;

II - Perfil 2: Perfil Básico, inicialmente atribuído a estagiários, recepcionistas e usuários externos, permitindo acesso a todos os sítios permitidos pelo Perfil 1 e a sítios de provedores de e-mail pessoal e instituições de ensino;

III - Perfil 3: Perfil Padrão, para os servidores do quadro do Instituto, permitindo acesso a todos os sítios da Internet, exceto aqueles que contêm veiculação de material em áudio e vídeo; e

IV - Perfil 4: Perfil Avançado, atribuído preferencialmente a servidores do quadro do Instituto e estagiários que desempenham funções relacionadas a Comunicação Social, Desenvolvimento de Pessoas e gestores, respeitado o princípio da necessidade de conhecer e demandando designação dos Autorizadores deste Perfil, permitindo o acesso a todos os sítios da Internet, incluindo sítios que veiculam material em áudio e vídeo (**streaming**), sítios de compartilhamento de vídeos, blogs e redes sociais.

§ 1º O perfil concedido a agentes externos será de caráter temporário, com validade equivalente à vigência do trabalho a ser executado.

§ 2º Os processos de alteração, bloqueio, liberação e categorização de sítios, assim como a criação e/ou alterações de perfis de acesso descritos nesta Norma, quando necessários, serão definidos pela Diretoria de Tecnologia da Informação e Inovação – DTI, e publicados no Portal do INSS na Intranet.

§ 3º Os novos usuários que não tiverem um perfil de acesso atribuído deverão ser direcionados para uma página da Intranet contendo orientações e normas relacionadas ao acesso à Internet no INSS, definidas pela DTI.

Art. 5º O acesso à Intranet e Internet a partir da rede de dados corporativa nas dependências do INSS e aos demais órgãos da Administração Pública Direta e Indireta, de qualquer das esferas de governo, será concedido exclusivamente a servidores e empregados públicos, efetivos ou ocupantes de cargo em comissão.

§ 1º O acesso de usuários externos das entidades que compõem o Poder Público será concedido mediante o estabelecimento em convênio, contrato, acordo de cooperação técnica ou instrumento congênere, especificamente firmados com o INSS para este fim.

§ 2º O gestor ou Coordenador-Geral da área responsável pelo convênio, contrato, acordo de cooperação técnica ou instrumento congênere assumirá o papel de Autorizador do serviço de acesso à Internet para os usuários externos, e deverá fundamentar as solicitações com base no instrumento.

§ 3º Poderão ser concedidos acessos temporários para auditores de controle interno e externo, vinculados à Controladoria-Geral da União – CGU ou ao Tribunal de Contas da União - TCU, no uso de suas atribuições.

Art. 6º O acesso à Internet por terceirizados deverá ser provido pela empresa contratada.

Parágrafo único. Em caráter de exceção, poderá ser concedido o acesso aos terceirizados a partir da infraestrutura de rede do INSS, desde que preenchidos os seguintes requisitos:

I - o contrato de prestação de serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

II - a empresa contratada deverá manter com seus funcionários Termo de Confidencialidade;

III - o contrato de prestação de serviços deverá prever a necessidade de acesso à Internet a partir das dependências do INSS; e

IV - o Autorizador, que para estes fins será o gestor do contrato ou o responsável pela área requisitante do serviço, deverá fundamentar as necessidades de acesso dos empregados da contratada, definindo os recursos que serão disponibilizados, endereços da Intranet e Internet necessários para o desenvolvimento das atividades e eventuais restrições a dias e horários para realização do acesso.

Art. 7º A conexão de equipamentos pessoais de visitantes à rede do INSS, quando necessária e motivada pelo interesse da Administração, deverá ser previamente autorizada pelo gestor da unidade onde o equipamento será utilizado.

Parágrafo único. Só será permitida a utilização da rede local por visitantes, caso seus equipamentos atendam a todos os requisitos estabelecidos pela DTI e o acesso se dará, exclusivamente, à Internet, sendo vedado o acesso ao conteúdo disponibilizado na Intranet.

Art. 8º A todos os perfis de acesso descritos nesta Norma aplicam-se as restrições de acesso a sítios que:

I - contenham material pornográfico ou obsceno;

II - contenham material ilegal;

III - disponibilizem jogos, inclusive os da Internet (**on line**);

IV - contenham material impróprio, ofensivo, preconceituoso ou discriminatório, que façam apologia à violência, ao terrorismo e às drogas; e

V - contenha e/ou divulgue conteúdo de violação de direito autoral (pirataria) e/ou execução de quaisquer tipos ou formas de fraudes.

Art. 9º O processo de atribuição de acesso à Internet seguirá as seguintes diretrizes:

I - a atribuição dos perfis de acesso à Internet será feita pelos Autorizadores, de forma fundamentada e respeitando o princípio da necessidade de conhecer, de acordo com a tabela abaixo:

Perfil	Autorizador
Perfil 1, 2 e 3	Gerente de Agência da Previdência Social - APS, Gerente-Executivo, Superintendentes-Regionais, Procuradores-Regionais, Coordenadores-Gerais, Superintendentes-Regionais, Presidente do INSS, Auditor-Geral, Corregedor-Geral, Procurador-Geral da PFE-INSS, Diretores, Gestores ou Chefes da área responsável pelo Contrato ou ato administrativo similar no âmbito do INSS.
Perfil 4	Chefes de Assessoria de Comunicação Social nas Superintendências-Regionais, Assessor de Comunicação Social (Administração Central), Diretor de Tecnologia da Informação e Inovação, Diretor de Gestão de Pessoas e Administração e Presidente do INSS.

II - nos casos de novos usuários de rede (LDAP), criados por meio de registro de chamado técnico, quando o solicitante não indicar o perfil de acesso à internet, será atribuído o Perfil 1;

III - para fins de alteração do perfil de acesso, os usuários deverão preencher o Formulário de Solicitação de Acesso à Internet (Anexo II) e providenciar a assinatura pelo Autorizador do acesso; e

IV - ao registrar a solicitação, deve-se anexar o Formulário de Solicitação de Acesso à Internet (Anexo II) devidamente preenchido e assinado (pelo solicitante e Autorizador), conforme documento nato digital ou digitalizado no formato PDF.

Art. 10. A solicitação para perfis de acesso em caráter temporário, realizada mediante o Formulário de Solicitação de Acesso à Internet (Anexo II), deverá conter a motivação da necessidade e a data de início e de expiração do acesso.

Art. 11. As responsabilidades ficam estabelecidas na seguinte forma:

I - o usuário deverá:

- a) preencher os requisitos e termos estabelecidos nesta Norma;
- b) estar devidamente autorizado a utilizar a Internet nas formas estabelecidas nesta Norma;
- c) fazer uso da Internet de forma responsável e segura, utilizando o acesso exclusivamente em razão de trabalho, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal; e
- d) impedir a divulgação e compartilhamento das chaves de segurança atribuídas, que são pessoais e intransferíveis;

II - o autorizador deverá:

- a) conceder os perfis de acesso à Internet rigorosamente de acordo com as atribuições dos usuários de sua abrangência, observando os normativos do INSS;
- b) verificar periodicamente o uso dos acessos concedidos e, sempre que necessário, solicitar alteração dos perfis de acesso dos usuários de sua abrangência; e
- c) reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR-INSS;

III - a área responsável pela gestão de TI no INSS deverá:

- a) monitorar os acessos à internet e sua utilização de acordo com as diretrizes estabelecidas nesta Norma; e
- b) identificar os casos de mau uso da Internet e adotar uma ou mais das seguintes providências:
 - 1. alertar o usuário, responsável pelo acesso, e o Autorizador, responsável pela concessão, acerca do uso indevido da internet; e
 - 2. nos casos de reincidência, solicitar a revogação do acesso à internet concedido ao usuário e encaminhar a documentação que comprova a má utilização do acesso concedido à Corregedoria do INSS, para análise e adoção das medidas cabíveis.

Art. 12. Configura-se como uso indevido da Internet:

- I - acessar a Internet disponibilizada pelo INSS sem estar devidamente autorizado, conforme estabelecido nesta

Norma;

II - não manifestar concordância com as regras estabelecidas nesta Norma e nas demais aplicáveis;

III - fazer uso dos recursos de Internet disponibilizados pelo INSS para fins alheios ao trabalho, em discordância com os procedimentos dispostos nesta Norma, sem prejuízo de demais normatizações vigentes na Administração Pública Federal;

IV - utilizar os serviços extrapolando os privilégios do perfil de acesso que lhe foi designado;

V - divulgar e/ou compartilhar as chaves de segurança, que são pessoais e intransferíveis, permitindo a utilização por terceiros do perfil que lhe foi atribuído;

VI - praticar atos de comercialização de produtos e serviços, em proveito próprio ou de terceiros, que não atendam os interesses do INSS;

VII - utilizar recursos ou dispositivos para acesso a computadores ou redes externas ao INSS com o objetivo de obter informações não autorizadas ou provocar a interrupção de serviços de rede;

VIII - utilizar modem ou dispositivo de rede que interligue a rede interna do INSS a outras redes ou à Internet;

IX - expor, armazenar, distribuir, editar, gravar ou compartilhar, através do uso dos recursos computacionais e de comunicação do INSS, arquivos estranhos às atividades do INSS e não autorizados pela chefia imediata;

X - realizar qualquer atividade que apoie ou facilite o vazamento de dados;

XI - baixar arquivos ou programas da Internet que contrariem as diretrizes da POSIN vigente; e

XII - utilizar **proxy** não disponibilizado pelo INSS.

Art. 13. O acesso à Internet é passível de registro e monitoração, incluindo quaisquer dados transmitidos pela rede do INSS.

§ 1º Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a ETIR-INSS deverá ser imediatamente acionada, para tomar as providências necessárias a fim de sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação do INSS;

§ 2º As ocorrências de mau uso do acesso à Internet não previstas nesta norma, assim como os casos de dúvidas em relação à aplicação das disposições aqui estabelecidas, deverão ser encaminhadas à DTI para registro, análise e avaliação da necessidade de alterações de acordo com o processo de governança em vigência no INSS;

§ 3º O descumprimento desta Norma poderá acarretar ao usuário as penalidades previstas nas políticas e procedimentos internos e/ou, na forma da lei, responsabilidade administrativa, civil e criminal.

Art. 14. Esta Norma deverá ser atualizada periodicamente, não excedendo o prazo máximo de 3 (três) anos.

ANEXO II

RESOLUÇÃO Nº 12/CEGOV/INSS, DE 31 DE AGOSTO DE 2020

FORMULÁRIO DE SOLICITAÇÃO DE ACESSO À INTERNET

Informações do Usuário		
Nome:	Login de Rede:	
Matrícula:	CPF:	
Lotação:	Código do Setor:	
Telefone: ()	E-mail:	_____@inss.gov.br
		_____@agu.gov.br

☐	Perfil 1	Data de expiração:	
☐	Perfil 2		
☐	Perfil 3		
☐	Perfil 4		
☐	Terceirizados	Contrato nº ou Convênio	Data de expiração

Descreva abaixo a justificativa e quais páginas devem ser acessadas pelo usuário terceirizado:

Declaro ter conhecimento e estar de acordo com as regras estabelecidas na Norma de Uso da internet do INSS (Resolução nº 12/CEGOV/INSS, de 1 de setembro de 2020) e demais normas aplicáveis.

_____, ____ de _____ de _____.

Local e Data

Informações do Autorizante		
Nome:		
Lotação:	Código do Setor:	
Telefone: ()	E-mail:	_____@inss.gov.br
		_____@agu.gov.br

Assinatura e Carimbo do Solicitante

Autorizo a concessão de Acesso Internet

_____, ____ de _____ de ____.

Local e Data

Referência: Processo nº 35014.047735/2020-84

SEI nº 1609867



INSTITUTO NACIONAL DO SEGURO SOCIAL
GABINETE DA PRESIDÊNCIA
Serviço Técnico Administrativo

DESPACHO

Serviço Técnico Administrativo do Gabinete, em 02/09/2020

Ref.: Processo nº
35014.047735/2020-84

I n t . : COMITÊ
ESTRATÉGICO DE
GOVERNANÇA
DO INSTITUTO
NACIONAL DO
SEGURO
SOCIAL – INSS

A s s . : Publicação de
Resoluções

Assinada as Resoluções nºs 9 a 12/CEGON/INSS, de 31 de agosto de 2020, de ordem,
encaminhe-se:

1. ao Serviço de Publicidade Legal para publicação no Diário Oficial da União (DOU);
e
2. à Divisão de Comunicação Administrativa para divulgação no Portal.

RAIMUNDO RODRIGUES

Servidor



Documento assinado eletronicamente por **RAIMUNDO NONATO RODRIGUES DA SILVA**,
Servidor(a), em 02/09/2020, às 07:38, conforme horário oficial de Brasília, com fundamento no art. 6º,
§ 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site

[https://sei.inss.gov.br/sei/controlador_externo.php?](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)

[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **1632372** e o código CRC **D7CAE9E1**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1632372



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Assessoria De Comunicação Social
Coordenação De Comunicação Social
Serviço De Publicidade Legal

DESPACHO

Serviço De Publicidade Legal, em 02/09/2020.

1. As Resoluções nºs 9 a 12 foram encaminhadas para o DOU do dia 03.09.2020.
2. Restitua-se para as devidas providências.

DANIELA MIRANDA DA SILVA OLIVEIRA

Chefe do Serviço de Publicidade Legal do INSS - Substituta



Documento assinado eletronicamente por **DANIELA MIRANDA DA SILVA OLIVEIRA**, **Chefe de Serviço Substituto(a)**, em 02/09/2020, às 12:11, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1637101** e o código CRC **0F9871DD**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1637101

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 03/09/2020 | Edição: 170 | Seção: 1 | Página: 50

Órgão: Ministério da Economia/Instituto Nacional do Seguro Social/Presidência

COMITÊ ESTRATÉGICO DE GOVERNANÇA

RESOLUÇÃO Nº 9, DE 31 DE AGOSTO DE 2020

Atualiza a Política de Segurança da Informação do Instituto Nacional do Seguro Social - POSIN-INSS.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do Processo Administrativo nº 35014.047735/2020-84, resolve:

Art. 1º Instituir, no âmbito do INSS, e nos termos do Anexo a esta Resolução, a Política de Segurança da Informação - POSIN-INSS.

Art. 2º Fica revogada a Resolução nº 672/PRES/INSS, de 27 de dezembro de 2018, publicada no Diário Oficial da União nº 250, de 31 de dezembro de 2018, Seção 1, pág. 151.

Art. 3º Esta Resolução entra em vigor sete dias após a data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES

Presidente do Comitê

ALESSANDRO ROOSEVELT SILVA RIBEIRO

Diretor de Benefícios

JOBSON DE PAIVA SILVEIRA SALES

Diretor de Atendimento

HELDER CALADO DE ARAÚJO

Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR

Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS

Diretor de Tecnologia da Informação e Inovação

ANEXO I

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO INSTITUTO NACIONAL DO SEGURO SOCIAL - POSIN-INSS.

Art. 1º A POSIN-INSS tem por objetivo estabelecer e difundir diretrizes e princípios de Segurança da Informação - SI, com vistas à orientação para uso e proteção adequados das informações produzidas e custodiadas pelo Instituto, preservando sua disponibilidade, integridade, confidencialidade e autenticidade.

Parágrafo único. A Política de que trata o caput e suas normas complementares aplicam-se a todos os agentes públicos que têm vínculo direto e/ou indireto com o Instituto.

Art. 2º Para os efeitos da POSIN-INSS, entende-se:

I - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta;

II - atividades críticas: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade, de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo;

III - ativos de informação: meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV - dados processados: dados submetidos a qualquer operação ou tratamento, por meio de processamento eletrônico ou automatizado, com o emprego de tecnologia da informação;

V - gestor de Segurança da Informação: é o responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da Administração Pública Federal;

VI - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

VII - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

VIII - necessidade de conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

IX - riscos de segurança da informação: potencial associado à exploração de uma ou mais vulnerabilidades nos ativos de informação, em razão de ameaças, com impacto negativo às atividades do Instituto;

X - Segurança da Informação - SI: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e autenticidades das informações;

XI - vínculo direto: agentes públicos contratados diretamente pelo INSS; e

XII - vínculo indireto: agentes privados ou públicos pertencentes a órgãos ou unidades da Administração Pública Federal, Estadual ou Municipal que mantenham contrato, convênio, acordo de cooperação técnica ou instrumento congênere com o INSS.

Art. 3º Esta POSIN-INSS foi elaborada com base nos seguintes normativos:

I - Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;

II - Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto na Constituição Federal;

III - Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

IV - Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais;

V - Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

VI - Decreto nº 7.724, de 16 de maio de 2012, regulamenta a Lei nº 12.527, de 18 de novembro de 2011;

VII - Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

VIII - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

IX - Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

X - Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que disciplina a gestão de segurança da informação na Administração Pública Federal, direta e indireta, e dá outras providências;

XI - instruções normativas relacionadas à segurança da informação, publicadas pelo Gabinete de Segurança Institucional da Presidência da República;

XII - Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação; e

XIII - NBR ISO/IEC 27002:2013, que institui código de melhores práticas para a Gestão de Segurança da Informação.

Art. 4º Esta POSIN-INSS foi elaborada com base nos seguintes princípios:

I - a preservação da imagem do Instituto e de seus agentes públicos;

II - a salvaguarda das informações do cidadão;

III - ações de segurança orientadas pela gestão de riscos;

IV - continuidade assegurada dos serviços ao cidadão;

V - o alinhamento com a missão institucional e seu planejamento estratégico; e

VI - respeito à natureza e finalidade de cada área do Instituto.

Art. 5º São diretrizes gerais da POSIN-INSS:

I - tratamento da informação:

a) toda informação produzida pelos agentes públicos, no exercício de suas atividades, é de propriedade do INSS e deve ser protegida;

b) informações produzidas, armazenadas e tratadas pelo Instituto, especialmente as informações pessoais e custodiadas, devem receber o devido tratamento para assegurar sua proteção durante todo o ciclo de vida; e

c) somente os canais de comunicação disponibilizados pelo INSS devem ser utilizados para trafegar informações institucionais;

II - tratamento de incidentes de SI: todo incidente de segurança da informação deve ser imediatamente relatado à área responsável pela gestão de segurança da informação de Tecnologia da Informação - TI, observando-se a apropriada coleta de evidências;

III - gestão de riscos de segurança:

a) os riscos de segurança da informação devem ser identificados e tratados; e

b) os critérios para a gestão de risco devem ser definidos e comunicados à toda Instituição;

IV - gestão de continuidade:

a) os ativos de informação que suportam as atividades críticas do Instituto devem ser suportados por ambiente de alta disponibilidade e ter capacidade de recuperação em prazos e condições previamente definidos para situações de contingência, em conformidade com o processo de continuidade; e

b) a continuidade das operações e serviços de TI deve estar prevista nos contratos, assim como os prazos e condições devem estar formalmente estabelecidos;

V - controles de acesso:

a) todo acesso à informação deve ser motivado pela necessidade de conhecer;

b) os sistemas de informação e as instalações físicas devem ter capacidade de controlar os acessos, com fins de responsabilização pelo seu uso; e

c) as autorizações de acesso às informações, sistemas e instalações físicas devem ter critérios de acesso definidos e divulgados a todos da Instituição;

VI - recursos computacionais:

a) correio eletrônico:

1. o correio eletrônico, e-mail, é uma forma de comunicação oficial e deve ser utilizado exclusivamente no desempenho das atividades funcionais; e

2. ao produzir, responder ou encaminhar mensagem em caixa de correio eletrônico institucional, o servidor deverá se identificar, subscrevendo, ao menos, seu nome, cargo e telefone de contato institucional;

b) acesso à Internet:

1. o acesso à Internet, por meio da rede de dados do INSS, é uma concessão e deve ter seu uso orientado para a execução das atividades do Instituto; e

2. os acessos serão liberados de acordo com perfis previamente definidos pelo órgão responsável pelos serviços de TI;

c) gestão de mudanças de TI:

1. toda mudança nos sistemas de informação do INSS deve ser previamente e formalmente autorizada; e

2. a gestão de mudanças deve prever, no mínimo, a guarda dos registros, realização de testes e a possibilidade de recuperação do ambiente;

d) computação em nuvem:

1. o ambiente de computação em nuvem, sua infraestrutura e canal de comunicação devem estar aderentes às diretrizes e normas de SI, estabelecidas pelo Instituto, e às legislações vigentes; e

2. o contrato de prestação de serviço, quando for o caso, deverá conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço;

VII - educação e conscientização:

a) esta Política e seus normativos complementares devem ser periodicamente divulgados a todos os agentes públicos do Instituto;

b) o Instituto deve manter programa contínuo de conscientização dos agentes públicos em SI; e

c) deve ser mantido plano de capacitação especializado aos profissionais que atuam na gestão de SI;

VIII - auditoria e conformidade:

a) o cumprimento desta Política e de suas normas complementares deve ser avaliado periodicamente, por meio de verificações de conformidade; e

b) o uso dos recursos de TI disponibilizados pelo Instituto é passível de monitoramento e auditoria;

IX - responsabilidade pela gestão das informações:

a) os responsáveis pela gestão dos ativos da informação e sistemas corporativos devem descrever os requisitos de segurança; e

b) os sistemas de informação devem ser concebidos possibilitando a segregação de funções;

X - segurança física e do ambiente:

a) as instalações em que as informações críticas ou sensíveis serão processadas deverão ser mantidas em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção física; e

b) os ativos da organização devem ser protegidos contra acesso físico não autorizado, danos, perdas, furto e interferência. As proteções devem estar alinhadas aos riscos identificados;

XI - gestão de ativos da informação, os ativos de informação devem:

a) ser inventariados e protegidos;

b) ter identificados os seus proprietários e custodiantes;

c) ter a sua entrada e saída nas dependências do Instituto autorizadas e registradas por autoridade competente; e

d) ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 6º A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas, cíveis e penais, previstas na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), no Código Penal, no Código Civil, e, ainda, em legislação que regule ou venha regular a matéria.

Art. 7º Competências e responsabilidades:

I - cabe ao Gestor de SI:

- a) promover cultura de segurança da informação;
- b) acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
- c) propor os recursos necessários à implementação das ações de SI;
- d) coordenar o Comitê de Segurança da Informação - CSI ou estrutura equivalente;
- e) acompanhar os trabalhos e a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR-INSS;
- f) propor o detalhamento das diretrizes desta Política, por meio de normas e procedimentos, e acompanhar sua implementação;
- g) assessorar a alta administração na implementação da Política de SI;
- h) estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à SI;
- i) promover a divulgação da política e das normas internas de SI do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no INSS;
- j) incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à SI;
- k) verificar os resultados dos trabalhos de auditoria sobre a gestão da SI;
- l) acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da SI; e

m) manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à SI;

II - cabe ao Presidente do INSS nomear o Gestor de SI;

III - caso o Gestor de SI não seja nomeado, as atribuições relacionadas no inciso I do art. 7º serão desempenhadas pelo Diretor de Tecnologia da Informação e Inovação;

IV - a ETIR-INSS deve analisar e propor respostas a notificações e atividades relacionadas a incidentes de SI, no âmbito do Instituto;

V - é responsabilidade de todos os agentes públicos, diretos e indiretos, conhecer e cumprir as diretrizes desta Política e demais normas e procedimentos complementares de SI; e

VI - compete ao Comitê Estratégico de Governança - CEGOV deliberar sobre políticas e normas de segurança da informação, assessorado pelo Comitê Temático de Governança Digital, tendo em vista o Sistema de Governança do INSS, instituído pela Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019.

Parágrafo único. O Comitê Temático de Gestão da Informação é responsável pela aprovação de procedimentos e de normas internas que orientem o compartilhamento de dados sob gestão do INSS e pela aprovação da categorização dos níveis de compartilhamento de dados com outras entidades públicas (federais ou de outras esferas e poderes) da sociedade civil, nos termos do art. 6º do anexo à Portaria nº 3.213/PRES/INSS, de 2019.

Art. 8º Esta Política e seus normativos devem ser revisados sempre que necessário, não excedendo o período máximo de 3 (três) anos.

Este conteúdo não substitui o publicado na versão certificada.

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 03/09/2020 | Edição: 170 | Seção: 1 | Página: 51

Órgão: Ministério da Economia/Instituto Nacional do Seguro Social/Presidência

RESOLUÇÃO Nº 10, DE 31 DE AGOSTO DE 2020

Define as regras para emissão de credenciais de acesso lógico.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do Processo nº 35014.047735/2020-84, resolve:

Art. 1º Instituir, na forma do Anexo I, a Norma de Controle de Acesso Lógico - NCAL do INSS, e aprovar os Anexos II e III.

Art. 2º Fica revogada a Resolução nº 413/PRES/INSS, de 20 de maio de 2014, publicada no Diário Oficial da União nº 95, de 21 de maio de 2014, Seção 1, págs. 43/44.

Art. 3º Esta Resolução entra em vigor sete dias após a data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES

Presidente do Comitê

ALESSANDRO ROOSEVELT SILVA RIBEIRO

Diretor de Benefícios

JOBSON DE PAIVA SILVEIRA SALES

Diretor de Atendimento

HELDER CALADO DE ARAÚJO

Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR

Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS

Diretor de Tecnologia da Informação e Inovação

ANEXO I

NORMA DE CONTROLE DE ACESSO LÓGICO - INSS

Art. 1º Os termos definidos nesta norma aplicam-se a todos os agentes públicos e privados com vínculo direto ou indireto, permanente ou temporário com o INSS.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Federais vinculados à Advocacia-Geral da União - AGU, que atuarem na consultoria e no assessoramento jurídico, e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta Norma de Controle de Acesso Lógico, são estabelecidos os seguintes conceitos e definições:

I - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

II - administrador de domínio: usuário responsável pela administração de um domínio por meio da aplicação de políticas globais, criação, edição e exclusão de usuários e grupos, e instalação de programas em um grande número de estações de trabalho;

III - administrador local: usuário responsável pela administração de partes de um domínio (geralmente restrito a um setor ou abrangência), por meio de políticas locais, edição de grupos e usuários locais, e instalação de programas em estações de trabalho limitadas a um setor ou abrangência;

IV - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta;

V - ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VI - contas de serviço: contas de acesso à rede corporativa de computadores, necessárias para a execução de procedimentos automáticos (aplicação, script, etc.), sem qualquer intervenção humana no seu uso;

VII - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais;

VIII - credenciamento: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer;

IX - necessidade de conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

X - credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física, como crachá, cartão e selo ou lógica como identificação usuário e senha;

XI - dado: é um elemento informativo concreto e sua forma plural expressa uma informação, é o registro do atributo de um ente objeto ou fenômeno onde registro indica o ato de registrar, ou seja, é a gravação ou a impressão de caracteres ou símbolos que tenham um significado em algum documento ou suporte físico;

XII - domínio: agrupamento lógico de computadores em rede que compartilham recursos em um banco de dados de segurança, comum, onde a administração e autenticação são centralizadas. Desta forma um usuário precisa de uma conta para ter acesso ao domínio e aos recursos compartilhados;

XIII - endereço IP (Internet Protocol): conjunto de elementos numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores. Sequência de números associada a cada computador conectado à Internet. No caso de IPv4, o endereço IP é dividido em quatro grupos, separados por "." e compostos por números entre 0 e 255. No caso de IPv6, o endereço IP é dividido em até oito grupos, separados por ":" e compostos por números hexadecimais (números e letras de "A" a "F") entre 0 e FFFF;

XIV - entidade externa: organização governamental, não governamental ou privada, amparada por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica ou instrumento congênere com o INSS;

XV - e-SIC: Sistema Eletrônico do Serviço de Informações ao Cidadão, aplicação disponibilizada na internet, que centraliza todos os pedidos de informações dirigidos ao Poder Executivo Federal;

XVI - estagiário: educando que esteja frequentando o ensino regular, em instituições de educação superior, de educação profissional, de ensino médio, de educação especial e dos anos finais do ensino fundamental, na modalidade profissional da educação de jovens e adultos, que desenvolve as atividades relacionadas à sua área de formação profissional junto as pessoas Jurídicas de Direito Privado, órgãos da Administração Pública e Instituições de Ensino, que tenham condições de proporcionar experiência prática na sua linha de formação;

XVII - estágio supervisionado: ato educativo escolar supervisionado, desenvolvido no ambiente de trabalho, que visa a preparação para o trabalho produtivo de educandos;

XVIII - ferramenta de gestão de acessos: software que possibilita a gestão integrada de papéis e permissões de acesso dos usuários nos sistemas corporativos;

XIX - gestor da informação: usuário que gerou a informação, que responde pelo seu conteúdo ou que foi formalmente designado para definir, alterar a sua classificação nos graus de sigilo e perfil de acesso dos demais usuários e processos;

XX - gestão de identidades: combinação de sistemas técnicos, regras e procedimentos que definem a posse, utilização e segurança de uma identidade. Seu objetivo primário é estabelecer a confiança na associação de atributos a uma identidade digital e conectar esta identidade com uma entidade individual;

XXI - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXII - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

XXIII - log ou registro de auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional;

XXIV - perfil de acesso do usuário: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

XXV - recursos de rede: dispositivos (impressoras, scanners, multifuncionais, etc) ou serviços (sistemas, portais, etc) disponibilizados para os usuários por meio de uma rede de dados;

XXVI - serviço de diretório: serviço que armazena e organiza informações relativas a recursos disponíveis e usuários de uma rede de dados. Permite que o administrador da rede gerencie o acesso de usuários e sistemas aos recursos disponíveis;

XXVII - sistemas corporativos: sistemas de operação, ou finalísticos, que se coadunam com os fins da Previdência Social. Assim, entende-se que este conceito comporta o conjunto de sistemas e subsistemas que garantem a operação dos Regimes Geral e Próprio de Previdência Social, inclusive de previdência complementar;

XXVIII - sistemas legados: compreendem o conjunto de aplicações desenvolvidas com tecnologias obsoletas que permanecem em operação no INSS;

XXIX - usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal, formalizada por meio da assinatura do Termo de Responsabilidade;

XXX - usuário interno: servidor do quadro do INSS lotado em uma Unidade Orgânica - UO, que se utiliza dos sistemas corporativos do Instituto; e

XXXI - usuário externo: usuários vinculados a uma Entidade Externa, que se utiliza dos sistemas corporativos do Instituto por meio de um perfil de acesso concedido por um Gestor de Acesso Externo.

Art. 3º São diretrizes desta NCAL-INSS:

I - o acesso à rede e aos sistemas corporativos do INSS dar-se-á por meio de autenticação integrada de domínio baseado em serviço de diretório, administrado por meio de uma ferramenta de gestão de identidades;

II - as concessões de acesso à rede de dados e aos sistemas corporativos são distintas. Sendo assim, o usuário pode obter permissão de acesso apenas à rede de dados, ou apenas a determinado (s) sistema (s) corporativo (s);

III - as credenciais de acesso a rede de dados e aos sistemas corporativos do INSS são conferidas aos usuários com base na necessidade de conhecer, para viabilizar o exercício de suas atribuições funcionais e atividades a serem desenvolvidas no âmbito do INSS; e

IV - o uso indevido de informações dos sistemas corporativos do INSS sujeitará o agente às penalidades previstas na legislação.

Art. 4º Base Cadastral é a base de dados do Serviço de Diretórios (acesso à rede de dados), do Sistema de Gestão de Acessos (sistemas corporativos) e dos sistemas legados, que devem ser alimentadas por informações disponibilizadas pelo INSS. Para tanto, a área responsável pela gestão de pessoas do INSS disponibilizará semanalmente as informações extraídas do Sistema Integrado de Administração de Recursos Humanos - SIAPE para a empresa prestadora de serviços tecnológicos contratada pelo Instituto, com a supervisão da área de gestão de TI do INSS, contendo, minimamente, os seguintes dados:

Tabela 1: Informações Usuários

ITEM	INFORMAÇÃO	CAMPO	DESCRIÇÃO
1	GR-MATRICULA	N 0012	GRUPO NUMÉRICO COMPOSTO DE NÚMERO DO ÓRGÃO (N0005) E NÚMERO DE MATRICULA DO SERVIDOR (N0007)
2	IT-NU-IDEN-SERV-ORIGEM	A 0008	NÚMERO DE IDENTIFICAÇÃO DO SERVIDOR NA ORIGEM - NÚMERO VINCULADO AO CARGO EFETIVO OU EM COMISSÃO
3	IT-NO-SERVIDOR	A 0060	NOME
4	IT-DA-NASCIMENTO	N 0008	DATA DE NASCIMENTO
5	IT-NU-CPF	N 0011	NÚMERO DO CPF
6	IT-NU-PIS-PASEP	N 0011	NÚMERO DO PIS
7	IT-IN-SUPRESSAO-PAGAMENTO	A 0001	INDICATIVO DE SUPRESSÃO DE PAGAMENTO
8	IT-CO-SITUACAO-SERVIDOR	N 0002	CÓDIGO DE SITUAÇÃO FUNCIONAL DO SERVIDOR
9	IT-CO-GRUPO-OCOR-AFASTAMENTO	N 0002	CÓDIGO DE OCORRÊNCIA DE AFASTAMENTO
10	IT-DA-INICIO-OCOR-AFASTAMENTO	N 0008	DATA DO INÍCIO DA OCORRÊNCIA DE AFASTAMENTO
11	IT-DA-TERMINO-OCOR-AFASTAMENTO	N 0008	DATA DE TÉRMINO DA OCORRÊNCIA DE AFASTAMENTO
12	IT-CO-GRUPO-OCOR-EXCLUSAO	N 0002	CÓDIGO DE OCORRÊNCIA DE EXCLUSÃO
13	IT-CO-UORG-LOTACAO-SERVIDOR	N 0009	CÓDIGO DA UORG DE LOTAÇÃO DO SERVIDOR
14	IT-CO-ORGAO-REQUISITANTE	N 0005	CÓDIGO DO ÓRGÃO REQUISITANTE

Parágrafo único. A Diretoria de Tecnologia da Informação e Inovação procederá com a atualização das bases cadastrais do serviço de diretórios e dos sistemas corporativos, bem como realizará a validação das informações disponibilizados pelo INSS por meio de outras bases, na periodicidade do envio das informações, e a área responsável pela gestão de pessoas do INSS poderá acordar, com a área responsável pela gestão de TI do INSS, a revisão das informações necessárias à administração de contas de usuários.

Art. 5º Sobre credenciais e perfis de acesso, verifica-se que a emissão de uma credencial permite ao usuário acessar a rede de dados corporativa do INSS. Para que o mesmo obtenha acesso aos sistemas corporativos, a credencial deve ser associada a um perfil de acesso, e o o processo de credenciamento de usuário aos ativos de informação deve ser feito observando os seguintes critérios:

I - a credencial de acesso concedida para acesso à rede de dados e sistemas corporativos do INSS é de caráter pessoal e intransferível;

II - as credenciais de acesso devem ser concedidas após a data de contratação ou entrada em exercício do usuário; e

III - as mesmas credenciais de acesso devem ser utilizadas para o acesso à rede de dados e aos sistemas corporativos do INSS, mediante autenticação que permita ao usuário acessar vários sistemas, por meio de ferramenta de gestão de identidades e acessos.

§ 1º A área responsável pela gestão de pessoas do INSS deverá utilizar os canais de atendimento disponibilizados pela empresa prestadora de serviços tecnológicos contratada pelo Instituto, ou outro canal informado pela DTI, para solicitar:

I - o credenciamento de usuários do quadro de pessoal do INSS na data do ato administrativo de retorno ou ingresso no órgão, para acesso à rede, e de estagiários, após assinatura do contrato de prestação de serviço, para acesso à rede;

II - a revogação de credenciais de acesso de servidores do quadro de pessoal do INSS cedidos a outros órgãos;

III - a desativação de usuários do quadro de pessoal do INSS na data do ato administrativo ou de ocorrências que ensejem desligamento para fins de acesso lógico; e

IV - a desativação do acesso de usuários do quadro de pessoal em atividade do INSS afastados ou com licença programada de suas funções por mais de sessenta dias ininterruptos.

§ 2º Quanto ao processo de formação das credenciais de acesso fica estabelecido que o nome do usuário será composto de acordo com os padrões estabelecidos no Guia de Interoperabilidade do Governo Eletrônico - e-Ping, mais especificamente no documento "Caixas Individuais-Fundacionais no Governo Federal" (Rede do Governo, 2010) que define regras de formação de nomes para a composição de endereços eletrônicos.

§ 3º Com relação às senhas de acesso, deve se observar que:

I - deverão ter no mínimo oito caracteres e conter, obrigatoriamente, caracteres alfanuméricos (combinação de letras e números). O usuário poderá acrescentar caracteres especiais (espaços em branco, símbolos, sinais de pontuação, etc.);

II - é vedada a reutilização das últimas quatro senhas utilizadas pelo usuário;

III - podem ser alteradas sempre que preciso ou quando o usuário achar necessário;

IV - o prazo de validade não deve ultrapassar 90 (noventa) dias; e

V - o usuário receberá, por meio de comunicado direto (via interface do sistema ou por mensagem no correio eletrônico), a informação do prazo próximo de vencimento da senha, quando esta estiver a 15 (quinze) dias da sua data de expiração.

§ 4º Os perfis de acesso aos sistemas corporativos deverão contemplar um conjunto de permissões e ações vinculadas às atividades desenvolvidas pelo usuário, sendo que:

I - caberá à área responsável pela gestão de TI do INSS estabelecer, em conjunto com as áreas responsáveis pela gestão dos sistemas corporativos, a norma de criação dos perfis de acesso;

II - as áreas responsáveis pela gestão dos sistemas corporativos são responsáveis pelas permissões, transações e ações que devem compor cada perfil de acesso; e

III - os perfis de acesso e de gestão concedidos para usuários internos e externos deverão ser objeto de revisão contínua pelos gestores responsáveis, não podendo ultrapassar o prazo máximo de 30 (trinta) meses.

§ 5º Quanto à utilização das credenciais e perfis de acesso, o usuário:

I - deve ter conhecimento prévio desta Norma de Controle de Acesso Lógico e preencher os requisitos estabelecidos na mesma;

II - deve estar devidamente autorizado a utilizar a rede corporativa e/ou os sistemas corporativos, de acordo com os requisitos estabelecidos nesta Norma;

III - deve utilizar os serviços e as informações obtidas, por meio do perfil de acesso, única e exclusivamente em razão do exercício da função pública e para os fins que lhe foi designado, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal;

IV - não pode divulgar, nem mesmo compartilhar, os códigos de segurança que lhe forem atribuídos (credenciais de acesso), os quais são pessoais e intransferíveis;

V - não pode utilizar as credenciais para acessar os recursos disponíveis em mais de uma estação de trabalho simultaneamente;

VI - não pode fazer uso das credenciais de acesso de outros usuários;

VII - deve fornecer informações acessadas nos sistemas e na rede de dados corporativos do INSS somente mediante demanda formalizada de quem tenha competência para tal;

VIII - deve comunicar à chefia imediata ou responsável pela administração do sistema ou rede corporativa quaisquer violações ou incidentes referentes à proteção do equipamento utilizado, do software ou de outros ativos da informação;

IX - deve, sempre que for necessário, afastar-se da estação de trabalho, certificar-se de que a sessão de rede ou acesso ao sistema corporativo esteja encerrado ou bloqueado;

X - deverá, obrigatoriamente, efetuar processo de alteração da sua senha em seu primeiro acesso à rede de dados corporativa; e

XI - no ato do primeiro acesso, bem como após cada atualização desta Norma, o usuário deverá manifestar concordância com os termos dispostos na mesma.

§ 6º O processo de autenticação de usuários deve ser definido pela área responsável pela gestão de Tecnologia da Informação do Instituto e poderá ser baseada em autenticação simples (nome de usuário e senha) agregada a autenticação multifator (certificação digital ou outros meios disponíveis).

§ 7º O credenciamento de usuários internos se dá pelo cadastro de novos servidores ou ocupantes de cargo em comissão, no âmbito do Instituto, pode ser solicitado por servidor vinculado à área responsável pela gestão de pessoas ou pela chefia imediata do usuário.

§ 8º O cadastro de que trata o § 7º deve ser solicitado por meio dos canais de atendimento disponibilizados pela prestadora de serviços tecnológicos contratada pelo Instituto ou outro informado pela DTI.

§ 9º O credenciamento de estagiários, se dará com a emissão de credencial de acesso, tendo como requisito as seguintes condições:

I - a empresa que atuar como agente de integração do estágio supervisionado deve manter contrato com o INSS;

II - o contrato de estágio supervisionado deverá conter cláusula de confidencialidade e sigilo de informações preestabelecidos com a Administração Pública;

III - a criação de perfis específicos e restritos às atividades do estagiário pelos gestores dos sistemas corporativos para o acesso dos estagiários;

IV - é vedada a concessão de perfis de acesso aos sistemas corporativos para estagiários com permissão de alteração das bases de dados institucionais;

V - o acesso será concedido mediante solicitação expressa de servidor do quadro do INSS, responsável pela supervisão do estágio, que deverá avaliar os riscos de utilização indevida de informações institucionais e as eventuais restrições referentes aos dias e horários para a realização dos acessos;

VI - o acesso será precedido da assinatura do Termo de Confidencialidade e de Manutenção de Sigilo - TCMS, Anexo II, o qual deverá ser firmado pelo estagiário ou pelo estagiário e seu responsável legal, no caso de se tratar de estagiário menor de 18 (dezoito) anos;

VII - as solicitações de acesso à rede para estagiários devem ser procedidas por meio dos canais remotos de atendimento disponibilizados pela empresa prestadora de serviços tecnológicos contratada pelo Instituto ou outro canal informado pela DTI, pela unidade de gestão de pessoas, pela chefia imediata do educando ou pelo responsável por sua supervisão;

VIII - os gestores de sistemas devem criar perfis diferenciados para estagiários de nível médio e nível superior;

IX - o supervisor do estagiário deverá, periodicamente, orientá-lo quanto ao uso responsável e adequado do acesso aos sistemas corporativos; e

X - o acesso do estagiário limitar-se-á à data final do contrato ou imediatamente cessado na hipótese de rescisão antecipada do estágio, cabendo ao supervisor do estagiário, em quaisquer dos casos, adotar as providências necessárias ao bloqueio do acesso, tão logo finde a contratação.

§ 10. O credenciamento de usuários externos, obedecerá as seguintes diretrizes:

I - as credenciais de acesso para usuários externos devem ser emitidas tendo em vista o interesse do INSS, devidamente justificadas e previstas no convênio, acordo de cooperação técnica ou instrumento congênere;

II - as solicitações de emissão de credenciais de acesso à rede corporativa para usuários amparados por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica, contrato ou instrumento congênere devem:

a) ser feitas pelo gestor da unidade/área responsável pela gestão do instrumento legal; e

b) ser atendidas somente após validação das credenciais do gestor solicitante do Instituto, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700);

III - a emissão de credenciais de acesso à rede corporativa para prestadores de serviço terceirizados ou equiparados nas dependências do INSS, quando necessária, será provida unicamente pelo interesse do INSS, devendo ser atendidos os seguintes requisitos:

a) a organização a qual o usuário é vinculado deve manter contrato, acordo de cooperação, convênio ou instrumento congênere vigente com o INSS;

b) instrumento deve conter cláusulas prevendo:

1. a necessidade e justificativa para acesso à rede corporativa;

2. a confidencialidade e sigilo de informações preestabelecidas junto ao Instituto; e

3. a obrigatoriedade da organização ou do ente contratado informar previamente ao representante legal do INSS, responsável pela gestão do contrato, quaisquer alterações em seu corpo de colaboradores que impacte na emissão/exclusão das contas de acesso;

c) a organização ou ente contratado também deverá manter com seus colaboradores Termo de Confidencialidade de Manutenção de Sigilo - TCMS; e

d) o gestor do contrato pelo INSS deve fundamentar a necessidade do acesso à rede para prestadores de serviço terceirizados ou equiparados, definindo os recursos que devem ser disponibilizados e eventuais restrições a dias e horas para realização do acesso à rede;

IV - os TCMS deverão ser arquivados junto aos instrumentos assinados com o INSS e uma cópia ou link eletrônico deverá ser encaminhada ao Gestor do Contrato. O mesmo deve ocorrer para quaisquer alterações ocorridas na vigência dos contratos, acordos ou convênios;

V - caso os Termos sejam gerados de forma eletrônica, deverá ser disponibilizado o arquivo correspondente, atendendo aos requisitos necessários para garantia de integridade e disponibilidade de acesso, assim como os requisitos específicos previstos em contrato; e

VI - a emissão de credenciais de acesso poderá ser feita pelo gestor do contrato, representante legal do INSS, ou pelo gestor da unidade responsável pela gestão do contrato, convênio, acordo de cooperação técnica ou instrumento congênere e serão atendidas somente após validação das credenciais do solicitante, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700).

§ 11. O acesso aos prestadores de serviço vinculados à Central de Atendimento 135 se dará observando as seguintes condições:

I - a empresa deve manter contrato com o INSS;

II - o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

III - a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade - TCMS;

IV - o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte do INSS, definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;

V - os acessos deverão ser realizados única e exclusivamente por necessidade de serviço;

VI - os contratos de prestação de serviços de teleatendimento devem conter documento a ser utilizado para formalização das indicações de gestores de acesso aos sistemas corporativos do Instituto; e

VII - o INSS pode disponibilizar, de forma restrita, às centrais 135, uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

§ 12. Nos casos referentes a prestadores de serviço vinculados à Ouvidoria do Ministério da Economia, o acesso se dará observando-se as seguintes condições:

I - a empresa deve manter contrato direto com a Ouvidoria do Ministério da Economia;

II - o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

III - a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade;

IV - o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte da Ouvidoria do Ministério da Economia, definindo quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;

V - os acessos deverão ser realizados única e exclusivamente por necessidade de serviço; e

VI - o INSS pode disponibilizar, de forma restrita, à Ouvidoria do Ministério da Economia, uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias para correto desempenho de suas funções.

§ 13. O acesso à rede corporativa por servidores vinculados a órgãos de controle externo, envolvidos em ações de auditoria no âmbito do INSS, será concedido mediante apresentação da equipe de auditoria por meio de documento formal que conste:

I - dados necessários ao cadastro de usuários externos;

II - informações acerca dos objetivos dos trabalhos a serem executados;

III - os prazos envolvidos; e

IV - informações complementares.

§ 14. O tipo de acesso de que trata o § 12 deverá observar:

I - as parcerias institucionalmente estabelecidas entres esses órgãos e o INSS no que tange à cobertura/previsão de acesso à rede corporativa do Instituto;

II - o atendimento de pedido de solicitação de informações advindo de pessoas físicas ou jurídicas externas, respeitadas as restrições de acesso às informações previstas na Lei nº 12.527, de 18 de novembro de 2011, serão analisadas pela área designada para responder as demandas dos cidadãos por meio do e-SIC; e

III - os procedimentos referentes às solicitações de inclusão, exclusão, inativação e suspensão de contas de acesso de usuários devem ser executados tendo como premissa a preservação dos registros para efeito de auditoria.

§ 15. O bloqueio administrativo se dará da seguinte forma:

I - o responsável pela Corregedoria-Geral do INSS, quando necessário, poderá solicitar a suspensão, bloqueio ou inativação imediata de contas de acesso de usuários que estiverem envolvidos em inquérito penal, em Processo Administrativo Disciplinar - PAD ou em Sindicância, decorrente de infrações cometidas no exercício das atribuições do cargo, quando o usuário estiver na seguinte situação:

a) afastado temporariamente do cargo ou função pública em razão de ato que se encontra sob apuração;

b) indiciado em processo administrativo disciplinar, por incursão nos incisos IX, XI, XII, XV, XVI e XVII do art. 117 e arts. 130 e 132 da Lei nº 8.112, de 11 de dezembro de 1990, ou cuja proposta pela Comissão Processante, no relatório final, seja pela aplicação de penalidade a partir de suspensão de 30 (trinta) dias; e

c) submetido à prisão em flagrante, temporária ou preventiva decorrente do cometimento de infração no exercício das atribuições do cargo, enquanto estiver em apuração de inquérito policial ou pelo Ministério Público Federal;

II - as solicitações de que tratam o inciso I deverão ser efetuadas mediante comunicação formal da Corregedoria-Geral para a prestadora de serviços tecnológicos contratada pelo Instituto, ou outro canal informado pela DTI, a qual procederá a imediata implementação da mudança;

III - o bloqueio de acessos tratados nas situações do inciso I serão efetivados no âmbito da ferramenta de gestão de acessos nas seguintes situações:

a) usuário afastado temporariamente do cargo ou função, enquanto durar o afastamento; e

b) usuário indiciado nos termos da alínea "c" do inciso I do § 15, até o efetivo cumprimento da penalidade porventura aplicada ou, em caso de não aplicação de penalidade, enquanto durar o processo.

Art. 6º A Rede de Dados Corporativa compõe a infraestrutura de rede, que é disponibilizada para uso institucional, logo, apenas equipamentos de propriedade do Instituto são autorizados e devem ser conectados à rede corporativa.

§ 1º Em casos excepcionais, a conexão de equipamentos particulares à rede corporativa deve ser feita em razão do interesse do Instituto e sob prévia autorização do responsável pela gestão da unidade em que o equipamento estiver localizado.

§ 2º O INSS poderá disponibilizar o acesso à rede de dados corporativa por meio de tecnologia Wirelles (sem fio). Para tanto os seguintes critérios deverão ser adotados:

I - os projetos que envolvam a utilização de pontos de acesso sem fio à rede corporativa no âmbito do Instituto deverão ser devidamente registrados e aprovados pela área responsável pela gestão de TI do INSS;

II - os pontos de acesso à rede de dados corporativa sem fio poderão ser objeto de testes periódicos de penetração e de auditoria a critério da área responsável pela gestão de TI no INSS; e

III - as conexões à rede sem fio serão avaliadas pela área responsável pela gestão de TI do INSS em relação aos requisitos de segurança e deverão atender ao princípio do privilégio mínimo.

§ 3º A área responsável pela gestão de TI do INSS poderá disponibilizar rede sem fio com regras específicas de acesso para visitantes nas diversas unidades do Instituto.

§ 4º Os dispositivos conectados à rede do INSS por meio de conexão sem fio deverão suportar configurações de criptografia estabelecidas pela área responsável pela gestão de TI no âmbito do INSS;

§ 5º Qualquer tecnologia de acesso sem fio implementada no INSS deverá suportar autenticação forte, com possibilidade de efetuar checagens em bancos de dados externos, e a área responsável pela gestão de TI do INSS deve dispor de mecanismos automáticos que possibilitem:

I - a detecção e bloqueio de equipamentos externos conectados à rede corporativa; e

II - a identificação e rastreamento dos endereços IP de origem e destino, bem como os serviços utilizados na rede corporativa inclusive nos acessos remotos.

§ 6º A administração da rede corporativa trata da operacionalização da rede do INSS, que é realizada por empresa prestadora de serviços tecnológicos contratada pelo Instituto e seguem as seguintes premissas:

I - prover, gerenciar e operacionalizar os ativos, acessos e serviços que compõem a rede de dados corporativa do INSS; e

II - submeter-se ao monitoramento de serviços de tecnologia contratados pelo Instituto, seguindo as regras desta Norma.

§ 7º Quanto ao processo de geração de contas de serviço, fica estabelecido que:

I - os critérios para a emissão de contas de serviços serão vinculados a um processo formal estabelecido pela área responsável pela gestão de TI do INSS;

II - a concessão de contas de serviços deve ser feita conforme a necessidade de uso de acordo com os critérios estabelecidos nesta Norma;

III - o direito de acesso privilegiado, por meio de contas de serviços, associado a sistemas ou processos, deve ser identificado;

IV - deve ser viabilizada ferramenta que possibilite a gestão das contas de serviço de forma automatizada, possibilitando o registro e verificação de todos os privilégios concedidos;

V - as contas de serviço fornecidas devem ser utilizadas exclusivamente para os fins aos quais foram concedidas;

VI - as contas de serviço emitidas devem ser revalidadas periodicamente com base na função exercida e na área de atuação do servidor; e

VII - as contas de serviço com credenciais de acesso de uso compartilhado devem ter suas senhas alteradas periodicamente, conforme estabelecido nesta Norma de Controle de Acesso Lógico, ou sempre que ocorrerem mudanças no grupo de usuários que utilizam as mesmas.

§ 8º É vedado o uso da rede corporativa para:

I - acesso por meio de equipamento não homologado ou não autorizado pelo INSS;

II - fazer download, instalar e/ou utilizar sistemas ou aplicativos não homologados pela área responsável pela gestão de TI do INSS nos equipamentos de propriedade do Instituto;

III - a utilização de softwares particulares em equipamentos do INSS sem autorização expressa;

IV - a instalação e conexão de equipamentos particulares à rede corporativa do Instituto sem a prévia autorização do gestor responsável pela unidade ou da área responsável pela gestão de TI do INSS;

V - o uso dos recursos de rede para fins particulares ou de terceiros alheios aos interesses do INSS, em especial, quando tal procedimento prejudique o tráfego da rede de dados;

VI - o uso para fins de divulgação ou distribuição de material que não possua vínculo com as atividades desenvolvidas pelo Instituto;

VII - a instalação ou utilização de ferramentas de monitoramento de rede sem a anuência e autorização expressa da área responsável pela gestão de TI no Instituto;

VIII - a instalação de dispositivos de comunicação ou de compartilhamento de dados sem fio, particulares, à rede corporativa do Instituto, sem autorização expressa da área responsável pela gestão de TI do INSS; e

IX - burlar as regras de acesso a internet configuradas em proxy ou ferramenta similar de gerenciamento de conteúdo web.

§ 9º Cabe à área responsável pela gestão de TI no âmbito do INSS definir os aspectos relacionados à plataforma tecnológica, gestão operacional, forma de autenticação e sustentação do domínio de rede do INSS.

Art. 7º A Gestão do Acesso aos Sistemas Corporativos seguirá as seguintes premissas:

I - sistemas legados:

a) as regras estabelecidas nesta norma devem ser aplicadas, guardando-se as devidas limitações tecnológicas, aos sistemas legados; e

b) o controle de acesso aos sistemas legados é efetuado por base própria;

II - sistemas de apoio à administração:

a) os ambientes de hospedagem desses sistemas são suportados por terceiros;

b) o ambiente deverá ser gerenciado e operacionalizado pela área de gestão de TI do INSS;

c) o acesso pelos usuários a esses sistemas deverá ser autenticado pelo serviço de diretório utilizado pelo Instituto; e

d) as regras de hospedagem de sistemas serão definidas, em ato próprio, pela área de gestão de TI do INSS;

III - armazenamento de registros logs:

a) as áreas responsáveis pela gestão de sistemas corporativos e demais aplicações devem definir, em conjunto com a área responsável pela gestão de TI, a temporalidade de registro dos logs de acesso e transações, e quais registros devem ser armazenados por um período maior que o estipulado no

caput do art. 8º;

b) o INSS poderá alterar a temporalidade destes dados em norma específica; e

c) os logs de acesso devem contemplar minimamente os registros relacionados no Anexo III;

IV - administração da ferramenta de gestão de acesso:

a) com o objetivo de operacionalizar a gestão dos acessos aos sistemas corporativos no âmbito do INSS, serão criados os seguintes papéis:

1. administrador de sistema INSS: servidor do quadro, lotado na área responsável pela gestão de TI, designado por meio de Portaria do Diretor de Tecnologia da Informação e Inovação, a ser publicada em Boletim de Serviço - BS, responsável pela administração da ferramenta de gestão de acesso aos sistemas corporativos no âmbito do INSS;

2. gestor de sistema: servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em BS, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedoria-Geral e Procuradoria Federal Especializada junto ao INSS - PFE-INSS. É responsável pela implementação de sistemas corporativos no âmbito do INSS;

3. gestor de acesso central: servidor do quadro, lotado na Administração Central, indicado e designado, por meio de Portaria a ser publicada em BS, pelo titular de cada área: Presidência e suas Coordenações-Gerais, Diretorias, Auditoria-Geral, Corregedoria-Geral e PFE-INSS. É responsável pela manutenção dos perfis de gestão dos usuários nas áreas que compõem a Administração Central e, quando necessário, dos gestores de acesso das Superintendências-Regionais - SR;

4. gestor de acesso interno: servidor do quadro, lotado na Administração Central, SR, Gerência-Executiva - GEX, Agência da Previdência Social - APS, indicado pelo Gestor de Acesso Central ou por um Gestor de Acesso, responsável pela atribuição do perfil de acesso e de gestão dos usuários no INSS; e

5. gestor de acesso externo: pessoa formalmente indicada, por documento previsto no instrumento legal que firmou a parceria ou por meio de Ofício de lavra do representante máximo de uma Entidade Externa, responsável pelo cadastro de usuários externos e a gestão dos acessos aos sistemas corporativos do Instituto;

b) os perfis de acesso serão atribuídos de acordo com a necessidade do fluxo de operação definido para cada sistema corporativo;

c) a indicação e o processo de substituição dos responsáveis pela gestão dos acessos aos sistemas corporativos no âmbito do INSS poderá ser procedida das seguintes formas:

1. a autoridade responsável pela indicação do gestor de acessos pode indicar opcionalmente o substituto;

2. o próprio gestor de acessos pode designar, a qualquer momento, por meio da ferramenta de gestão de acessos um substituto;

3. quando não houver um gestor responsável, ou substituto, por uma unidade devidamente designado, a gestão dos usuários será transferida, preferencialmente de forma automática, para o responsável pela área da abrangência daquela unidade e assim subsequentemente; e

4. o Gestor de Acesso é corresponsável com os perfis de gestão ou acesso que ele atribuir aos usuários;

d) ao usuário interno cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Norma de Controle de Acesso Lógico e suas normas complementares;

2. solicitar, ao Gestor de Acesso responsável pela gestão da unidade de lotação a qual é vinculado, a suspensão do seu perfil de acesso nos períodos de afastamento do serviço por mais de 30 (trinta) dias consecutivos;

3. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e

4. ter conhecimento e estar de acordo com o disposto nesta Norma;

e) ao usuário externo cabe:

1. fazer uso dos perfis de acesso atribuídos aos sistemas corporativos, de acordo com as regras e requisitos estabelecidos nesta Norma de Controle de Acesso Lógico;
2. manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e
3. ter conhecimento e estar de acordo com o disposto nesta Norma;

f) ao administrador do sistema INSS cabe:

1. criar os sistemas e subsistemas, devidamente homologados pela área de negócio responsável, no ambiente de produção, por meio de ferramenta de gestão de acesso;
2. mediante apresentação de Portaria de designação para Gestores de Acesso Central, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores quanto à atribuição dos perfis de gestão; e
3. mediante apresentação de Portaria de designação para Gestores de Sistema, efetuar a atribuição ou alteração dos perfis de gestão, por meio de ferramenta de gestão de acessos e orientar os gestores acerca do processo de implementação dos sistemas corporativos no âmbito do INSS;

g) ao gestor de sistema cabe:

1. efetuar os procedimentos de importação, inclusão, alteração e exclusão de papéis e permissões nos sistemas corporativos em ambiente de produção; e
2. atuar, em conjunto com o Administrador do Sistema INSS e a prestadora de serviços tecnológicos contratada pelo Instituto, no planejamento e execução do processo de implementação dos sistemas corporativos dos quais for designado responsável;

h) ao gestor de acesso central cabe:

1. efetuar o credenciamento, suspensão ou exclusão de perfis de gestão dos sistemas corporativos aos Gestores de Acesso na Administração Central e, quando necessário, dos Gestores de Acesso da SR, GEX, APS e demais usuários de sua abrangência; e
2. orientar os usuários de sua abrangência e os gestores da Administração Central e SR, GEX e APS acerca das regras para o acesso aos sistemas corporativos do INSS;

i) ao gestor de acesso interno cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários da Administração Central, SR, GEX, APS;
2. atribuir, alterar ou excluir os perfis de acesso aos usuários da Administração Central, SR, GEX, APS; e
3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS;

j) ao gestor de acesso externo cabe:

1. efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos aos usuários do seu Órgão/Entidade;
2. atribuir, alterar ou excluir os perfis de acesso aos usuários do seu Órgão/Entidade; e
3. orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS;

V - configura-se mau uso, sujeito a responsabilidade penal, civil e disciplinar:

- a) a divulgação, sem autorização expressa da chefia imediata ou do gestor de acesso de sua abrangência, de informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS;
- b) acessar sistemas corporativos sem autorização prévia, de acordo com os requisitos estabelecidos nesta Norma;
- c) utilizar-se das informações obtidas por meio de acesso concedido em desacordo com os procedimentos dispostos nesta Norma e demais normas vigentes na Administração Pública Federal;

d) compartilhar ou fazer uso das credenciais de acesso, aos sistemas corporativos, de outros usuários; e

e) a instalação de sistemas corporativos em equipamentos particulares;

VI - em casos excepcionais, a área responsável pela gestão de TI do INSS, mediante ato formal, poderá autorizar a adoção das medidas descritas no § 2º do art.8º.

Art. 8º Todo acesso à rede de dados e aos sistemas corporativos deve ser registrado e monitorado de modo que permita a rastreabilidade, a identificação e o bloqueio de usuários e equipamentos não autorizados. Estas informações devem ser armazenadas por um período de, no mínimo, doze (12) meses, observando o disposto no inciso III do art. 7º.

§ 1º As ocorrências de mau uso do acesso aos recursos disponíveis na rede e sistemas corporativos não previstas nesta norma e os casos omissos serão encaminhados para a área responsável pela gestão de TI no âmbito do INSS para análise e pronunciamento.

§ 2º Identificada irregularidade de mau uso dos recursos de rede poderá ocorrer o bloqueio preventivo do acesso pela DTI, o encaminhamento de dossiê com as informações para a Corregedoria-Geral do INSS ou Corregedorias-Regionais, nas suas áreas de abrangências, a fim de que seja realizada a análise no âmbito disciplinar.

§ 3º O descumprimento dessa Norma poderá resultar em sanções administrativas, civis e criminais.

Art. 9º Esta norma deve ser revisada num período máximo de 3 (três) anos.

ANEXO II

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF nº _____, documento de identidade nº _____, expedida pelo _____, em _____, e lotado no(a) _____do Instituto Nacional do Seguro Social - INSS, DECLARO, sob pena das sanções cabíveis nos termos da Política de Segurança da Informação - POSIN do INSS que assumo a responsabilidade por:

I - tratar o(s) ativo(s) de informação como patrimônio do Instituto Nacional do Seguro Social;

II - utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do INSS;

III - contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que disciplina a gestão de segurança da informação na Administração Pública Federal, direta e indireta, e dá outras providências;

IV - utilizar as credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do INSS;

V - responder, perante o INSS, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

_____, _____de _____de _____

Nome e assinatura do usuário:	Unidade de Lotação:
Nome e assinatura da Autoridade Responsável pela Autorização do Acesso:	

ANEXO III

REGISTROS DE LOGS

1. Relação dos campos de registros de logs do GERID

1.1. Dados Gerais

1.1.1. Data

1.1.2. Sistema

1.1.3. Ambiente

1.1.4. IP destino

1.1.5. IP origem

1.1.6. CPF usuário

1.1.7. URL de origem

2. Ações:

2.1. CAS (autenticação): Central Authentication Service - Serviço Central de Autenticação

2.1.1. Criação de service ticket (ST)

2.1.2. Criação de ticket granting ticket (TGT)

2.1.3. validação de ST

2.1.4. Exclusão de ticket TGT

2.1.5. Autenticação com sucesso (login+password)

2.1.6. Autenticação com sucesso (certificado digital)

2.1.7. Autenticação com falha

2.2. GPA: Gerenciamento de Permissão de Acesso

2.2.1. Início de sessão

2.2.2. Dados do usuário em sessão (CPF, NOME, PAPEL)

2.2.3. Requisição de logout

2.2.4. Dados de credenciais

2.2.5. Concessão de credenciais

2.2.6. Alteração de Credenciais

2.2.7. Dados de receptor (CPF, NOME, Lotação)

2.2.8. Inserção de credencial no usuário

2.2.9. Revogação de Credenciais

2.2.10. Pesquisa de credenciais

2.2.11. Pesquisa de usuários

2.2.12. Substituição de gestor

Este conteúdo não substitui o publicado na versão certificada.

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 03/09/2020 | Edição: 170 | Seção: 1 | Página: 54

Órgão: Ministério da Economia/Instituto Nacional do Seguro Social/Presidência

RESOLUÇÃO Nº 11, DE 31 DE AGOSTO DE 2020

Institui a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR do Instituto Nacional do Seguro Social.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do Processo nº 35014.047735/2020-84, resolve:

Art. 1º Instituir, no âmbito do INSS, e nos termos do Anexo a esta Resolução, a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR-INSS.

Art. 2º Esta Resolução complementa Política de Segurança da Informação POSIN-INSS vigente e entra em vigor sete dias após a data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES

Presidente do Comitê

ALESSANDRO ROOSEVELT SILVA RIBEIRO

Diretor de Benefícios

JOBSON DE PAIVA SILVEIRA SALES

Diretor de Atendimento

HELDER CALADO DE ARAÚJO

Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR

Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS

Diretor de Tecnologia da Informação e Inovação

ANEXO

EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS - ETIR-INSS

Art. 1º A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR-INSS tem por objetivo agir proativamente, receber, analisar, monitorar, coordenar e propor respostas a notificações e atividades relacionadas a incidentes de segurança da informação e comunicações no âmbito do INSS.

Art. 2º As atividades pertinentes à ETIR-INSS englobam os usuários dos serviços de Tecnologia da Informação - TI e os sistemas de informação do INSS e serão realizadas com intercâmbio de informações e em cooperação com as seguintes instâncias:

I - o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR GOV;

II - a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR de empresas prestadoras de serviços de tecnologia contratadas pelo INSS;

III - as ETIRs ou estrutura equivalente dos demais órgãos, entidades e empresas, públicas ou privadas, que tenham contratos, acordos, convênios ou instrumentos congêneres com o INSS; e

IV - o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República - GSI/PR.

Art. 3º Para os efeitos desta Resolução ficam estabelecidos os seguintes conceitos e definições:

I - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR: equipe de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

II - CTIR GOV: Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança de Informação e Comunicações - DSIC do Gabinete de Segurança Institucional da Presidência da República - GSI;

III - agente responsável: servidor público ocupante de cargo efetivo de órgão ou entidade da Administração Pública Federal, direta ou indireta ou militar de carreira incumbido de chefiar e gerenciar uma ETIR;

IV - artefato malicioso: qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

V - Comunidade ou Público Alvo: conjunto de pessoas, setores, órgãos ou entidades atendidas por uma ETIR ou estrutura equivalente;

VI - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VII - serviço: conjunto de procedimentos, estruturados em processo definido, oferecido à comunidade pela ETIR;

VIII - Tratamento de Incidentes de Segurança em Redes Computacionais: serviço consistente em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

IX - usuário: pessoas que fazem uso de serviços de TI e sistemas de informação de propriedade do INSS, independentemente do cargo ocupado (contratados, consultores, conselheiros, servidores, temporários e etc.); e

X - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que possam resultar em risco para um sistema ou por uma organização, e que possam ser evitados por uma ação interna de segurança da informação.

Art. 4º A implementação e o funcionamento da ETIR-INSS seguirão metodologia definida pelo GSI/PR e as seguintes diretrizes:

I - basear-se no "Modelo 1 - Utilizando a equipe de Tecnologia da Informação", conforme definido pelo GSI/PR;

II - os integrantes da Equipe deverão ser profissionais da área de Tecnologia da Informação, servidores públicos efetivos, lotados na Diretoria de Tecnologia da Informação e Inovação - DTI do INSS, sem prejuízo de suas atribuições típicas do cargo, com experiência e conhecimentos técnicos compatíveis com a importância da missão da ETIR-INSS;

III - a ETIR-INSS ficará vinculada tecnicamente à Coordenação-Geral de Infraestrutura e Operações - CGIN da DTI;

IV - o Coordenador da ETIR-INSS será nomeado por ato do Diretor de Tecnologia da Informação e Inovação; e

V - na ausência de Coordenador formalmente nomeado, as atribuições relacionadas à coordenação da equipe serão desempenhadas pelo Coordenador-Geral de Infraestrutura e Operações.

Art. 5º A ETIR-INSS será composta por membros:

I - permanentes, que efetivamente atuarão em todos os incidentes registrados;

II - colaboradores, que atuarão, de forma esporádica, no tratamento de incidentes relacionados às suas áreas de atuação; e

III - opcionais, servidores das unidades descentralizadas do INSS sob supervisão da DTI.

§ 1º Os membros da ETIR-INSS serão designados por meio de ato do Diretor de Tecnologia da Informação e Inovação.

§ 2º A distribuição dos membros da ETIR-INSS se dará da seguinte forma:

I - 2 (dois) servidores permanentes, oriundos do Serviço de Segurança de TIC;

II - 2 (dois) servidores colaboradores, oriundos da CGIN;

III - 2 (dois) servidores colaboradores, oriundos da Coordenação-Geral de Projetos e Soluções Digitais da DTI; e

IV - 2 (dois) servidores opcionais, oriundos das unidades descentralizadas do INSS.

Art. 6º A ETIR-INSS terá autonomia limitada para o tratamento de incidentes de Segurança da Informação, devendo implementar ações que possam impactar outras áreas do Instituto somente com anuência do Diretor de Tecnologia da Informação e Inovação e do Gestor responsável pela área/sistema afetada, e poderá, ainda, gerar relatórios técnicos sugerindo a adoção de medidas para resolução de incidentes.

Art. 7º A ETIR-INSS fornecerá o serviço de Tratamento de Incidentes de Segurança em Redes Computacionais, que compreende as seguintes ações:

I - recepção de solicitações e alertas diversos, utilizando como canal de comunicação a caixa postal etir@inss.gov.br, a ser disponibilizada pelo INSS;

II - filtragem de todo conteúdo direcionado à ETIR-INSS, para fins de verificação quanto à necessidade de tratamento pela Equipe e, caso não se trate de incidente de segurança em redes computacionais, encaminhar para a área competente;

III - catalogação dos incidentes detectados em ferramenta a ser indicada pela DTI, com nível de acesso restrito;

IV - classificação dos incidentes detectados quanto ao nível de severidade e impacto;

V - tratamento do incidente com medidas corretivas e indicação de formas de se evitar que ocorra novamente;

VI - resposta às solicitações e alertas encaminhados para a ETIR; e

VII - monitoramento da aplicação do tratamento dos incidentes indicados.

§ 1º A ETIR-INSS deverá analisar os incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências; e

§ 2º O detalhamento dos serviços prestados pela ETIR-INSS deverá ser publicado em página específica da Intranet do INSS, no prazo de 30 (trinta) dias a partir da publicação desta Resolução.

Este conteúdo não substitui o publicado na versão certificada.

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 03/09/2020 | Edição: 170 | Seção: 1 | Página: 55

Órgão: Ministério da Economia/Instituto Nacional do Seguro Social/Presidência

RESOLUÇÃO Nº 12, DE 31 DE AGOSTO DE 2020

Disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante do Processo Administrativo nº 35014.047735/2020-84, resolve:

Art. 1º Estabelecer, nos termos do Anexo I, os critérios para o uso da Internet no âmbito do INSS e aprovar o Formulário de Solicitação de Acesso à Internet, constante do Anexo II.

Art. 2º Esta Resolução complementa Política de Segurança da Informação POSIN-INSS vigente e entra em vigor sete dias após a data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES

Presidente do Comitê

ALESSANDRO ROOSEVELT SILVA RIBEIRO

Diretor de Benefícios

JOBSON DE PAIVA SILVEIRA SALES

Diretor de Atendimento

HELDER CALADO DE ARAÚJO

Diretor de Gestão de Pessoas e Administração

CLÓVIS DE CASTRO JÚNIOR

Diretor de Integridade, Governança e Gerenciamento de Riscos

FLÁVIO FERREIRA DOS SANTOS

Diretor de Tecnologia da Informação e Inovação

ANEXO I

NORMAS DE USO DA INTERNET

Art. 1º Esta norma se aplica a todos os servidores e colaboradores, vinculados direta ou indiretamente ao INSS, bem como a servidores e empregados de entidades e órgãos da Administração Pública ou privados que necessitem ou estejam autorizados a acessar a Internet a partir da rede corporativa do Instituto.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União - AGU que atuarem na consultoria, assessoramento jurídico e na representação judicial e extrajudicial do INSS.

Art. 2º Para os efeitos desta norma, ficam estabelecidos os seguintes conceitos e definições:

I - autorizador: ocupantes de cargo responsáveis pela autorização da concessão de perfis de acesso para usuários finais de sua área de abrangência;

II - Internet: rede mundial que interliga computadores de diferentes tipos e dimensões e permite a comunicação entre pessoas e organizações, independentemente da localização geográfica;

III - Intranet: rede de computadores administrada pelo INSS, que utiliza os mesmos serviços e tecnologias disponíveis na rede mundial;

IV - perfil de acesso: atributo que estabelece as categorias de sítios acessíveis e tipos de arquivos que podem ser recebidos ou transmitidos pelos usuários;

V - proxy: ferramenta que desempenha a função de conexão do computador local à rede externa (Internet);

VI - sítio: conjunto de informações ou serviços disponíveis na Internet ou na Intranet, organizados em páginas eletrônicas e acessíveis por meio de endereços que identificam, de forma padronizada, sua origem e conteúdo;

VII - usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal - APF, formalizada por meio da assinatura do Termo de Responsabilidade; e

VIII - VPN: Rede Privada Virtual (Virtual Private Network) construída sobre a infraestrutura de uma rede pública, possibilitando a conexão de dois computadores por meio de uma rede pública.

Art. 3º O acesso pelos usuários à Internet disponibilizado pelo INSS deverá pautar-se pelas seguintes diretrizes:

I - seu uso se dará exclusivamente em razão de trabalho e de acordo com os procedimentos dispostos nesta Norma;

II - os recursos disponibilizados pelo INSS não poderão ser usados para quaisquer propósitos ilegais ou proibidos, que possam danificar, desativar, sobrecarregar ou prejudicar qualquer área, serviço ou conteúdo, ou interferir no uso e execução das atividades laborais de outros usuários;

III - o volume de tráfego de Internet e os endereços web visitados poderão ser monitorados, visando assegurar o cumprimento desta norma; e

IV - o acesso à Internet para propósitos particulares ou estranhos às atividades do INSS poderá ser bloqueado, sem prévia comunicação ao usuário e sem prejuízo das demais sanções aplicáveis.

Art. 4º O acesso aos sítios da Internet para todos os usuários será realizado mediante a atribuição de perfis de acesso, distribuídos nos seguintes níveis:

I - Perfil 1: Perfil Restrito, inicialmente atribuído a usuários com maior restrição de acesso à Internet, permitindo acesso somente a sítios governamentais, instituições bancárias e sítios considerados de interesse do INSS;

II - Perfil 2: Perfil Básico, inicialmente atribuído a estagiários, recepcionistas e usuários externos, permitindo acesso a todos os sítios permitidos pelo Perfil 1 e a sítios de provedores de e-mail pessoal e instituições de ensino;

III - Perfil 3: Perfil Padrão, para os servidores do quadro do Instituto, permitindo acesso a todos os sítios da Internet, exceto aqueles que contêm veiculação de material em áudio e vídeo; e

IV - Perfil 4: Perfil Avançado, atribuído preferencialmente a servidores do quadro do Instituto e estagiários que desempenham funções relacionadas a Comunicação Social, Desenvolvimento de Pessoas e gestores, respeitado o princípio da necessidade de conhecer e demandando designação dos Autorizadores deste Perfil, permitindo o acesso a todos os sítios da Internet, incluindo sítios que veiculam material em áudio e vídeo (streaming), sítios de compartilhamento de vídeos, blogs e redes sociais.

§ 1º O perfil concedido a agentes externos será de caráter temporário, com validade equivalente à vigência do trabalho a ser executado.

§ 2º Os processos de alteração, bloqueio, liberação e categorização de sítios, assim como a criação e/ou alterações de perfis de acesso descritos nesta Norma, quando necessários, serão definidos pela Diretoria de Tecnologia da Informação e Inovação - DTI, e publicados no Portal do INSS na Intranet.

§ 3º Os novos usuários que não tiverem um perfil de acesso atribuído deverão ser direcionados para uma página da Intranet contendo orientações e normas relacionadas ao acesso à Internet no INSS, definidas pela DTI.

Art. 5º O acesso à Intranet e Internet a partir da rede de dados corporativa nas dependências do INSS e aos demais órgãos da Administração Pública Direta e Indireta, de qualquer das esferas de governo, será concedido exclusivamente a servidores e empregados públicos, efetivos ou ocupantes de cargo em comissão.

§ 1º O acesso de usuários externos das entidades que compõem o Poder Público será concedido mediante o estabelecimento em convênio, contrato, acordo de cooperação técnica ou instrumento congênere, especificamente firmados com o INSS para este fim.

§ 2º O gestor ou Coordenador-Geral da área responsável pelo convênio, contrato, acordo de cooperação técnica ou instrumento congênere assumirá o papel de Autorizador do serviço de acesso à Internet para os usuários externos, e deverá fundamentar as solicitações com base no instrumento.

§ 3º Poderão ser concedidos acessos temporários para auditores de controle interno e externo, vinculados à Controladoria-Geral da União - CGU ou ao Tribunal de Contas da União - TCU, no uso de suas atribuições.

Art. 6º O acesso à Internet por terceirizados deverá ser provido pela empresa contratada.

Parágrafo único. Em caráter de exceção, poderá ser concedido o acesso aos terceirizados a partir da infraestrutura de rede do INSS, desde que preenchidos os seguintes requisitos:

I - o contrato de prestação de serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

II - a empresa contratada deverá manter com seus funcionários Termo de Confidencialidade;

III - o contrato de prestação de serviços deverá prever a necessidade de acesso à Internet a partir das dependências do INSS; e

IV - o Autorizador, que para estes fins será o gestor do contrato ou o responsável pela área requisitante do serviço, deverá fundamentar as necessidades de acesso dos empregados da contratada, definindo os recursos que serão disponibilizados, endereços da Intranet e Internet necessários para o desenvolvimento das atividades e eventuais restrições a dias e horários para realização do acesso.

Art. 7º A conexão de equipamentos pessoais de visitantes à rede do INSS, quando necessária e motivada pelo interesse da Administração, deverá ser previamente autorizada pelo gestor da unidade onde o equipamento será utilizado.

Parágrafo único. Só será permitida a utilização da rede local por visitantes, caso seus equipamentos atendam a todos os requisitos estabelecidos pela DTI e o acesso se dará, exclusivamente, à Internet, sendo vedado o acesso ao conteúdo disponibilizado na Intranet.

Art. 8º A todos os perfis de acesso descritos nesta Norma aplicam-se as restrições de acesso a sítios que:

I - contenham material pornográfico ou obsceno;

II - contenham material ilegal;

III - disponibilizem jogos, inclusive os da Internet (on line);

IV - contenham material impróprio, ofensivo, preconceituoso ou discriminatório, que façam apologia à violência, ao terrorismo e às drogas; e

V - contenha e/ou divulgue conteúdo de violação de direito autoral (pirataria) e/ou execução de quaisquer tipos ou formas de fraudes.

Art. 9º O processo de atribuição de acesso à Internet seguirá as seguintes diretrizes:

I - a atribuição dos perfis de acesso à Internet será feita pelos Autorizadores, de forma fundamentada e respeitando o princípio da necessidade de conhecer, de acordo com a tabela abaixo:

Perfil	Autorizador
Perfil 1, 2 e 3	Gerente de Agência da Previdência Social - APS, Gerente-Executivo, Superintendentes-Regionais, Procuradores-Regionais, Coordenadores-Gerais, Superintendentes-Regionais, Presidente do INSS, Auditor-Geral, Corregedor-Geral, Procurador-Geral da PFE-INSS, Diretores, Gestores ou Chefes da área responsável pelo Contrato ou ato administrativo similar no âmbito do INSS.

Perfil 4	Chefes de Assessoria de Comunicação Social nas Superintendências-Regionais, Assessor de Comunicação Social (Administração Central), Diretor de Tecnologia da Informação e Inovação, Diretor de Gestão de Pessoas e Administração e Presidente do INSS.

II - nos casos de novos usuários de rede (LDAP), criados por meio de registro de chamado técnico, quando o solicitante não indicar o perfil de acesso à internet, será atribuído o Perfil 1;

III - para fins de alteração do perfil de acesso, os usuários deverão preencher o Formulário de Solicitação de Acesso à Internet (Anexo II) e providenciar a assinatura pelo Autorizador do acesso; e

IV - ao registrar a solicitação, deve-se anexar o Formulário de Solicitação de Acesso à Internet (Anexo II) devidamente preenchido e assinado (pelo solicitante e Autorizador), conforme documento nato digital ou digitalizado no formato PDF.

Art. 10. A solicitação para perfis de acesso em caráter temporário, realizada mediante o Formulário de Solicitação de Acesso à Internet (Anexo II), deverá conter a motivação da necessidade e a data de início e de expiração do acesso.

Art. 11. As responsabilidades ficam estabelecidas na seguinte forma:

I - o usuário deverá:

- a) preencher os requisitos e termos estabelecidos nesta Norma;
- b) estar devidamente autorizado a utilizar a Internet nas formas estabelecidas nesta Norma;
- c) fazer uso da Internet de forma responsável e segura, utilizando o acesso exclusivamente em razão de trabalho, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal; e
- d) impedir a divulgação e compartilhamento das chaves de segurança atribuídas, que são pessoais e intransferíveis;

II - o autorizador deverá:

- a) conceder os perfis de acesso à Internet rigorosamente de acordo com as atribuições dos usuários de sua abrangência, observando os normativos do INSS;
- b) verificar periodicamente o uso dos acessos concedidos e, sempre que necessário, solicitar alteração dos perfis de acesso dos usuários de sua abrangência; e
- c) reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR-INSS;

III - a área responsável pela gestão de TI no INSS deverá:

- a) monitorar os acessos à internet e sua utilização de acordo com as diretrizes estabelecidas nesta Norma; e
- b) identificar os casos de mau uso da Internet e adotar uma ou mais das seguintes providências:
 - 1. alertar o usuário, responsável pelo acesso, e o Autorizador, responsável pela concessão, acerca do uso indevido da internet; e
 - 2. nos casos de reincidência, solicitar a revogação do acesso à internet concedido ao usuário e encaminhar a documentação que comprova a má utilização do acesso concedido à Corregedoria do INSS, para análise e adoção das medidas cabíveis.

Art. 12. Configura-se como uso indevido da Internet:

I - acessar a Internet disponibilizada pelo INSS sem estar devidamente autorizado, conforme estabelecido nesta Norma;

II - não manifestar concordância com as regras estabelecidas nesta Norma e nas demais aplicáveis;

III - fazer uso dos recursos de Internet disponibilizados pelo INSS para fins alheios ao trabalho, em discordância com os procedimentos dispostos nesta Norma, sem prejuízo de demais normatizações vigentes na Administração Pública Federal;

IV - utilizar os serviços extrapolando os privilégios do perfil de acesso que lhe foi designado;

V - divulgar e/ou compartilhar as chaves de segurança, que são pessoais e intransferíveis, permitindo a utilização por terceiros do perfil que lhe foi atribuído;

VI - praticar atos de comercialização de produtos e serviços, em proveito próprio ou de terceiros, que não atendam os interesses do INSS;

VII - utilizar recursos ou dispositivos para acesso a computadores ou redes externas ao INSS com o objetivo de obter informações não autorizadas ou provocar a interrupção de serviços de rede;

VIII - utilizar modem ou dispositivo de rede que interligue a rede interna do INSS a outras redes ou à Internet;

IX - expor, armazenar, distribuir, editar, gravar ou compartilhar, através do uso dos recursos computacionais e de comunicação do INSS, arquivos estranhos às atividades do INSS e não autorizados pela chefia imediata;

X - realizar qualquer atividade que apoie ou facilite o vazamento de dados;

XI - baixar arquivos ou programas da Internet que contrariem as diretrizes da POSIN vigente; e

XII - utilizar proxy não disponibilizado pelo INSS.

Art. 13. O acesso à Internet é passível de registro e monitoração, incluindo quaisquer dados transmitidos pela rede do INSS.

§ 1º Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a ETIR-INSS deverá ser imediatamente acionada, para tomar as providências necessárias a fim de sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação do INSS;

§ 2º As ocorrências de mau uso do acesso à Internet não previstas nesta norma, assim como os casos de dúvidas em relação à aplicação das disposições aqui estabelecidas, deverão ser encaminhadas à DTI para registro, análise e avaliação da necessidade de alterações de acordo com o processo de governança em vigência no INSS;

§ 3º O descumprimento desta Norma poderá acarretar ao usuário as penalidades previstas nas políticas e procedimentos internos e/ou, na forma da lei, responsabilidade administrativa, civil e criminal.

Art. 14. Esta Norma deverá ser atualizada periodicamente, não excedendo o prazo máximo de 3 (três) anos.

ANEXO II

FORMULÁRIO DE SOLICITAÇÃO DE ACESSO À INTERNET

Informações do Usuário		
Nome:	Login de Rede:	
Matrícula:	CPF:	
Lotação:	Código do Setor:	
Telefone: ()	E-mail:	_____@inss.gov.br
		_____@agu.gov.br

☐	Perfil 1	Data de expiração:	
☐	Perfil 2		
☐	Perfil 3		
☐	Perfil 4		
☐	Terceirizados	Contrato nº ou Convênio	Data de expiração

Descreva abaixo a justificativa e quais páginas devem ser acessadas pelo usuário terceirizado:

Declaro ter conhecimento e estar de acordo com as regras estabelecidas na Norma de Uso da internet do INSS (Resolução nº 12/CEGOV/INSS, de 1 de setembro de 2020) e demais normas aplicáveis.

-----, ____ de ----- de -----.

Local e Data

Informações do Autorizante		
Nome:		
Lotação:	Código do Setor:	
Telefone: ()	E-mail:	-----@inss.gov.br
		-----@agu.gov.br

Assinatura e Carimbo do Solicitante

Autorizo a concessão de Acesso Internet

-----, ____ de ----- de -----.

Local e Data

Este conteúdo não substitui o publicado na versão certificada.



INSTITUTO NACIONAL DO SEGURO SOCIAL
GABINETE DA PRESIDÊNCIA
Serviço Técnico Administrativo

DESPACHO

Serviço Técnico Administrativo do Gabinete, em 03/09/2020

Ref.: Processo nº
35014.047735/2020-84

Int.: CEGOV

A s s . : Resoluções do CEGOV para instituição de normas de segurança da informação e comunicação, em atendimento ao Decreto nº 9.637, de 26 de dezembro de 2018, que trata da Política Nacional de Segurança da Informação do Poder Executivo Federal

Restituir para o Comitê Estratégico de Governança - CEGOV, de ordem, após publicação das Resoluções nºs 9 a 12/CEGOV/INSS, de 31 de agosto de 2020, no DOU nº 170, de 3 de setembro de 2020, Seção 1, para as providências cabíveis.

RAIMUNDO RODRIGUES

Servidor



Documento assinado eletronicamente por **RAIMUNDO NONATO RODRIGUES DA SILVA**, **Servidor(a)**, em 03/09/2020, às 08:21, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1644386** e o código CRC **DB44DE36**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Assessoria De Comunicação Social
Coordenação De Comunicação Social
Divisão De Comunicação Administrativa

DESPACHO

Divisão de Comunicação Administrativa, em 03/09/2020

Ref.: Processo nº
35014.047735/2020-84

Int.: Serviço Técnico
Administrativo do
Gabinete da Presidência

A s s . : Publicação de
Resoluções

1. Trata-se da publicação e divulgação das Resoluções nºs 9 a 12 /CEGOV/INSS, de 31 de agosto de 2020.
2. Informamos que os referidos atos, foram publicados no DOU nº 170, de 3 de setembro de 2020, Seção 1, págs. 50/56 e no Portal-INSS, na intraprev.
3. Ao Comitê Estratégico de Governança - CEGOV, para conhecimento e providências julgadas necessárias.

ALDAMIR GERALDO DE LISBÔA LIMA

Chefe da Divisão de Comunicação Administrativa - DIVCA



Documento assinado eletronicamente por **ALDAMIR GERALDO DE LISBOA LIMA**, **Chefe de Divisão**, em 03/09/2020, às 10:45, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site
https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1644616** e o código CRC **3877ECA2**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1644616



INSTITUTO NACIONAL DO SEGURO SOCIAL

Comitê Estratégico de Governança

DESPACHO

Comitê Estratégico de Governança, em 04/09/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Encaminha para a
CGGOV para
conhecimento.

1. Uma vez publicadas as normas de segurança da informação tratadas no presente processo, encaminham-se os autos para a Coordenação-Geral de Governança, para registro em processos correlatos à temática, decorrentes de ação de auditoria da CGU.

CIBELLE CESAR DO AMARAL BRASIL

Coordenadora-Geral de Governança

Secretaria-Executiva do Comitê Estratégico de Governança



Documento assinado eletronicamente por **CIBELLE CESAR DO AMARAL BRASIL**,
Coordenador(a) Geral, em 04/09/2020, às 15:09, conforme horário oficial de Brasília, com fundamento
no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site
[https://sei.inss.gov.br/sei/controlador_externo.php?](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)
[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **1661234** e o
código CRC **748125CD**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 1661234



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

NOTA TÉCNICA Nº 10/2020/DTI

PROCESSO Nº 35014.047735/2020-84

INTERESSADO: DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO

**Designação de
Gestor da
Segurança da
Informação do
INSS.**

1. Trata-se de nota técnica de apresentação da minuta de portaria (SEI 2292658) que propõe a designação do Gestor de Segurança da Informação e seu substituto.

2. Sobre o tema tratado, informa-se que este Instituto tem trabalhado ativamente na melhoria da segurança da informação preconizada pelo Gabinete de Segurança Institucional - GSI tendo, inclusive, aprovado as Normas de Segurança da Informação no CEGOV (processo SEI nº 35014.047735/2020-84), conforme abaixo:

- Política de Segurança da Informação (POSIN) - RESOLUÇÃO Nº 9 /CEGOV/INSS, DE 31 DE AGOSTO DE 2020;
- Política de Controle de Acesso Lógico (PCAL) - RESOLUÇÃO Nº 10 /CEGOV/INSS, DE 31 DE AGOSTO DE 202;
- Norma de Uso da Internet - RESOLUÇÃO Nº 12 /CEGOV/INSS, DE 31 DE AGOSTO DE 2020;
- Norma de instituição da ETIR - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - RESOLUÇÃO Nº 11 /CEGOV/INSS, DE 31 DE AGOSTO DE 2020.

3. A minuta de portaria apresentada atende ao disposto no Art. 7, incisos II e III da Resolução nº 9, de 31 de agosto de 2020, que instituiu Política de Segurança da Informação - POSIN-INSS:

II - cabe ao Presidente do INSS nomear o Gestor de SI;

III - caso o Gestor de SI não seja nomeado, as atribuições relacionadas no inciso I do art. 7º serão desempenhadas pelo Diretor de Tecnologia da Informação e Inovação;

4. Observa-se o atendimento também ao disposto no art. 15, inciso I, da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020 do Gabinete de Segurança Institucional da Presidência da República:

Art. 15. Além das obrigações já dispostas nesta Instrução Normativa, compete aos órgãos e às entidades da administração pública federal, direta e indireta, em seu âmbito de atuação:

I - designar um gestor de segurança da informação interno, indicado pela alta administração do órgão ou da entidade;

5. Diante do exposto, propõe-se o encaminhamento da minuta de Portaria constante do documento SEI nº 2292658 à Coordenação de Suporte ao Gabinete para avaliação, conforme Art. 14 da Resolução nº 708/PRES/INSS, de 6 de novembro de 2019.

Brasília, 26 de novembro de 2020.

FLÁVIO FERREIRA DOS SANTOS

Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **FLAVIO FERREIRA DOS SANTOS, Diretor(a) de Tecnologia da Informação e Inovação**, em 26/11/2020, às 11:16, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site

[https://sei.inss.gov.br/sei/controlador_externo.php?](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)

[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **2292739** e o código CRC **5F5F3E42**.

Referência: Processo nº 35014.047735/2020-84

SEI nº 2292739



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria De Tecnologia da Informação e Inovação

MINUTA DE PORTARIA

Designa o Gestor de Segurança da Informação e o Gestor de Segurança da Informação Substituto.

O PRESIDENTE DO INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS, no uso das atribuições que lhe confere o Decreto nº 9.746, de 8 de abril de 2019, e considerando o que consta no Processo Administrativo nº 35014.047735/2020-84 e no disposto no art. 15, inciso I, da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020 do Gabinete de Segurança Institucional da Presidência da República, resolve:

Art. 1º Designar Claudio Augusto Novais Ferraz, matrícula SIAPE nº. 1.148.338, como Gestor de Segurança da Informação.

Art. 2º Designar João Rodrigues da Silva Filho, matrícula nº 1.561.845, como Gestor de Segurança da Informação Substituto.

Art. 3º São competências do Gestor de Segurança da Informação do Instituto Nacional do Seguro Social, observado o disposto no art. 19 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020:

- I - coordenar o Comitê de Segurança da Informação ou estrutura equivalente;
- II - coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do órgão, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;
- III - assessorar a alta administração na implementação da Política de Segurança da Informação;
- IV - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;
- V - promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade;
- VI - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;
- VII - propor recursos necessários às ações de segurança da informação;
- VIII - acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes Cibernéticos;
- IX - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;
- X - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e
- XI - manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Art. 4º A gestão da Segurança da Informação é considerada serviço de natureza relevante e não ensejará qualquer tipo de remuneração.

Art. 5º Esta Portaria entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES

Presidente



Documento assinado eletronicamente por **FLAVIO FERREIRA DOS SANTOS, Diretor(a) de Tecnologia da Informação e Inovação**, em 26/11/2020, às 11:16, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2292658** e o código CRC **BC2D4D59**.

Referência: Processo nº 35014.047735/2020-84

SEI nº 2292658



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

DESPACHO

Diretoria De Tecnologia da Informação e Inovação, em 26/11/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

A s s . : Nomear o
Coordenador da Equipe de
Equipe de Prevenção,
Tratamento e Resposta a
Incidentes Cibernéticos –
ETIR

1. Trata-se de minuta de portaria de nomeação do Coordenador da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR. conforme Resolução nº 11, de 31 de agosto de 2020, artigo 4º, inciso IV:

IV - o Coordenador da ETIR-INSS será nomeado por ato do Diretor de Tecnologia da Informação e Inovação

2. Encaminhe-se ao Serviço de Acompanhamento Técnico Operacional para análise da minuta de portaria.

FLÁVIO FERREIRA DOS SANTOS

Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **FLAVIO FERREIRA DOS SANTOS, Diretor(a) de Tecnologia da Informação e Inovação**, em 26/11/2020, às 11:17, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site
https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2294381** e o código CRC **E387202E**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 2294381



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria De Tecnologia da Informação e Inovação

MINUTA DE PORTARIA

Nomear o Coordenador da Equipe de
Equipe de Prevenção, Tratamento e
Resposta a Incidentes Cibernéticos – ETIR

O DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO DO INSTITUTO NACIONAL DO SEGURO SOCIAL- INSS, no uso das atribuições que lhe confere o Decreto nº 9.746 de 8 de Abril de 2019 e considerando o que consta no Processo Administrativo nº 35014.047735/2020-84, resolve:

Art. 1º Designar João Rodrigues da Silva Filho, matrícula nº 1.561.845, como Coordenador da Equipe de Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR deste Instituto.

Art. 2º A coordenação da Equipe de Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos é considerada serviço de natureza relevante e não ensejará qualquer tipo de remuneração.

FLÁVIO FERREIRA DOS SANTOS

Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **FLAVIO FERREIRA DOS SANTOS, Diretor(a) de Tecnologia da Informação e Inovação**, em 26/11/2020, às 11:17, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2293631** e o código CRC **A19A9E68**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Gestão De Pessoas e Administração
Coordenação-Geral De Gestão De Pessoas
Serviço De Acompanhamento Técnico Operacional

DESPACHO

Serviço De Acompanhamento Técnico Operacional, em 26/11/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

A s s . : Nomear o
Coordenador da Equipe de
Equipe de Prevenção,
Tratamento e Resposta a
Incidentes Cibernéticos –
ETIR

1. Trata-se de minuta de portaria de nomeação do Coordenador da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR.
2. Registra-se, por oportuno, que a este Serviço compete a confecção de minutas e análise para instrução processual dos processos que contenham indicações para nomeação, designação, exoneração e dispensa de cargos em comissão, de funções comissionadas e de funções gratificadas.
3. No caso em tela, se trata de nomeação de Coordenador de Equipe, não cabendo, portanto, a esse Serviço se manifestar sobre a matéria.
4. Feitas as considerações, restitua-se à Diretoria de Tecnologia da Informação e Inovação.

FÁTIMA OLIVEIRA DA SILVA

Chefe do Serviço de Acompanhamento Técnico Operacional



Documento assinado eletronicamente por **FATIMA OLIVEIRA DA SILVA**, **Chefe de Serviço**, em 26/11/2020, às 12:26, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2298110** e o código CRC **1540191E**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 2298110



INSTITUTO NACIONAL DO SEGURO SOCIAL

PORTARIA Nº 44/DTI/INSS, DE 26 DE NOVEMBRO DE 2020

O DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO DO INSTITUTO NACIONAL DO SEGURO SOCIAL- INSS, no uso das atribuições que lhe confere o Decreto nº 9.746 de 8 de Abril de 2019 e considerando o que consta no Processo Administrativo nº 35014.047735/2020-84, resolve:

Art. 1º Designar João Rodrigues da Silva Filho, matrícula nº 1.561.845, como Coordenador da Equipe de Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR deste Instituto.

Art. 2º A coordenação da Equipe de Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos é considerada serviço de natureza relevante e não ensejará qualquer tipo de remuneração.

FLÁVIO FERREIRA DOS SANTOS

Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **FLAVIO FERREIRA DOS SANTOS, Diretor(a) de Tecnologia da Informação e Inovação**, em 26/11/2020, às 15:10, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site

[https://sei.inss.gov.br/sei/controlador_externo.php?](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)

[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **2299795** e o código CRC **4FF90A44**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

DESPACHO

Diretoria De Tecnologia da Informação e Inovação, em 26/11/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Publicação Portaria

1. Trata-se de publicação, em boletim de serviço, da Portaria Nº 44/DTI/INSS, DE 26 de novembro de 2020 (SEI 2299652).

2. De ordem do Diretor desta DTI, encaminhe-se:

1.1 à Divisão de Comunicação Administrativa para divulgação no Portal;

1.2 ao Serviço de Publicidade Legal para publicação no próximo Boletim de Serviço - BS.

RENATA CESÁRIO DE OLIVEIRA GOMES

Analista em Tecnologia da Informação



Documento assinado eletronicamente por **RENATA CESARIO DE OLIVEIRA GOMES, Analista em Tecnologia da Informação**, em 26/11/2020, às 15:19, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site

[https://sei.inss.gov.br/sei/controlador_externo.php?](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)

[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **2299652** e o código CRC **2CBBF024**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 2299652



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Assessoria De Comunicação Social
Coordenação De Comunicação Social
Serviço De Publicidade Legal

DESPACHO

Serviço De Publicidade Legal, em 26/11/2020.

1. A Portaria nº 44/DTI/INSS será publicada no Boletim de Serviço nº 226, de 26/11/2020.
2. Restitua-se para as devidas providências.

DANIELA MIRANDA DA SILVA OLIVEIRA

Chefe do Serviço de Publicidade Legal do INSS - Substituta



Documento assinado eletronicamente por **DANIELA MIRANDA DA SILVA OLIVEIRA**, Técnico do Seguro Social, em 26/11/2020, às 17:10, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2303167** e o código CRC **22232D48**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 2303167



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Assessoria De Comunicação Social
Coordenação De Comunicação Social
Divisão De Comunicação Administrativa

DESPACHO

Divisão de Comunicação Administrativa, em 27/11/2020

Ref.: Processo
nº 35014.047735/2020-84

Int.: Diretoria de
Tecnologia da Informação
e Inovação

A s s . : Publicação de
Portaria

1. Trata-se de publicação e divulgação da Portaria nº 44 /DTI/INSS, de 26 de novembro de 2020.
2. Informo que o referido ato, foi publicado no BS nº 226 de 26 de novembro de 2020 e no Portal-INSS, na intraprev.
3. Encaminhe-se à Diretoria de Tecnologia da Informação e Inovação, para conhecimento e providências julgadas necessárias.

GISÉLIA M. P. VIEIRA DE SOUZA

Chefe da Divisão de Comunicação Administrativa - DIVCA
Substituta



Documento assinado eletronicamente por **GISELIA MARIA PINTO VIEIRA DE SOUZA**, Técnico do Seguro Social, em 27/11/2020, às 11:22, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2309646** e o código CRC **01B497DE**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 2309646



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência

Gabinete

Coordenação De Suporte ao Gabinete

MINUTA DE PORTARIA

Designa o Gestor de Segurança da Informação e o Gestor de Segurança da Informação Substituto.

O PRESIDENTE DO INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS, no uso das atribuições que lhe confere o Decreto nº 9.746, de 8 de abril de 2019, e considerando o que consta no Processo Administrativo nº 35014.047735/2020-84 e no que dispõe o art. 15, inciso I, da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República,

RESOLVE:

Art. 1º Designar CLAUDIO AUGUSTO NOVAIS FERRAZ, matrícula nº 1.148.338, como Gestor de Segurança da Informação do INSS.

Parágrafo único. O servidor designado no **caput** será substituído pelo servidor JOÃO RODRIGUES DA SILVA FILHO, matrícula nº 1.561.845, em suas ausências e afastamentos legais.

Art. 2º São competências do Gestor de Segurança da Informação do INSS, de acordo com o disposto no art. 19 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020:

I - coordenar o Comitê de Segurança da Informação ou estrutura equivalente;

II - coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do órgão, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

III - assessorar a alta administração na implementação da Política de Segurança da Informação;

IV - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

V - promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade;

VI - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

VII - propor recursos necessários às ações de segurança da informação;

VIII - acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes Cibernéticos;

IX - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

X - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

XI - manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Art. 3º A gestão da Segurança da Informação é considerada serviço de natureza relevante e não ensejará qualquer tipo de remuneração adicional.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES

Presidente



Documento assinado eletronicamente por **DIOGO FREITAS FIGUEIREDO, Coordenador(a)**, em 30/11/2020, às 10:24, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **CINTHYA DE AVILA OLIVEIRA TROJAN REPISO, Chefe da Divisão**, em 30/11/2020, às 10:49, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2302485** e o código CRC **4254D5A5**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Gabinete
Coordenação De Suporte ao Gabinete

DESPACHO

Coordenação De Suporte ao Gabinete, em 26/11/2020.

Ref.: Processo
nº 35014.047735/2020-84.

Int.: Diretoria de
Tecnologia da Informação
e Inovação.

A s s . : Designação de
Gestor da Segurança da
Informação do INSS.

1. Trata-se de minuta de Portaria, oriunda da Diretoria de Tecnologia da Informação e Inovação, para fins de designação do Gestor de Segurança da Informação e seu substituto no âmbito do INSS.

2. Para justificar e fundamentar a edição dos atos em questão, foi expedida a Nota Técnica nº 10/2020/DTI/INSS (2292739).

3. Sobre a adequação do ato em comento, dispõe a alínea "e" do inciso I do art. 20 da Resolução nº 708/PRES/INSS, de 6 de novembro de 2019, que versa sobre a elaboração, redação e alteração dos atos administrativos no âmbito do INSS:

Art. 20. Consideram-se atos constitutivos:

I - Portaria: é o ato administrativo de autoridade competente, no âmbito de suas atribuições regimentais, que:

...

e) efetiva nomeações, exonerações, **designações** dispensas, punições, delegação e subdelegação; ou (grifo nosso)

4. Logo, está adequada a modalidade de ato escolhida, pois trata da designação do Gestor de Segurança da Informação e seu substituto no âmbito do INSS.

5. Sobre as regras para elaboração, articulação e redação da minuta de Portaria, consigna-se a adequação com as regras estabelecidas na Lei Complementar nº 95, de 26 de fevereiro de 1998, no Decreto nº 9.191, de 1º de novembro de 2017, e na Resolução nº 708/PRES/INSS, de 2019, sendo analisadas e formatadas por esta Coordenação.

6. Ante o exposto, encaminhe-se à Procuradoria Federal Especializada junto ao INSS para manifestação quanto à regularidade jurídico-formal da proposta, cuja versão final consta do Documento SEI nº 2302485.

**CINTHYA DE ÁVILA O. TROJAN
REPISO**

Chefe da Divisão de Normas e Acordos

DIOGO FREITAS FIGUEIREDO

Coordenador de Suporte ao Gabinete



Documento assinado eletronicamente por **DIOGO FREITAS FIGUEIREDO, Coordenador(a)**, em 30/11/2020, às 10:26, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **CINTHYA DE AVILA OLIVEIRA TROJAN REPISO, Chefe da Divisão**, em 30/11/2020, às 10:49, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2302805** e o código CRC **8C231F61**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 2302805



ADVOCACIA-GERAL DA UNIÃO
PROCURADORIA-GERAL FEDERAL
PROCURADORIA FEDERAL ESPECIALIZADA JUNTO AO INSTITUTO NACIONAL DO SEGURO SOCIAL -
PFE/INSS - SEDE
DIVISÃO DE PESSOAL
SETOR DE AUTARQUIAS SUL QUADRA 2 BLOCO O 3º ANDAR

PARECER n. 00112/2020/DPES/PFE-INSS-SEDE/PGF/AGU

NUP: 35014.047735/2020-84

INTERESSADOS: DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO

ASSUNTOS: DIREITO ADMINISTRATIVO E OUTRAS MATÉRIAS DE DIREITO PÚBLICO

EMENTA: Direito administrativo. Análise prévia. Minuta de portaria que altera a Resolução Nº 675 /PRES/INSS, de 21 de fevereiro de 2019.

II – Regularidade de seu conteúdo jurídico-formal. Recomendações. Aprovação condicionada.

Sr. Coordenador-Geral de Matéria Administrativa,

1. RELATÓRIO

1. Trata-se de processo que contém os atos relativos a edição das Resoluções do CEGOV para instituição de normas de segurança da informação e comunicação, em atendimento ao Decreto nº 9.637, de 26 de dezembro de 2018, que trata da Política Nacional de Segurança da Informação do Poder Executivo Federal e, no presente caso, foram encaminhados para análise jurídico-formal de minuta de portaria a ser expedida pelo Presidente do INSS e que visa a designação de Gestor da Segurança da Informação do INSS.

2. Instruem os autos os seguintes documentos considerados relevantes para a presente análise (Seq. Sapiens 43-51):

- a. NOTA TÉCNICA Nº 10/2020/DTI (SEI/INSS 2292739) - da Diretoria de Tecnologia da Informação e Inovação, em que se apresenta a primeira versão de minuta de portaria, assim como as justificativas para emissão do ato;
- b. Minuta de portaria (SEI/INSS - 2292658);
- c. Segunda versão da Minuta de portaria (SEI/INSS - 2302485);
- d. Manifestação da Coordenação de Suporte ao Gabinete (SEI/INSS 2302805) que entende pela adequação formal do ato, encaminhando os autos a esta PFE/INSS para manifestação quanto à regularidade jurídico-formal da proposta, cuja versão final consta do Documento SEI nº 2302485;

3. Com efeito, o procedimento veio para análise desta PFE-INSS por força do art. 10 da Lei nº 10.480/2002 c/c o art. 10 da Instrução Normativa Conjunta PGF/INSS nº 01/2010, do art. 15, §4º, da Resolução nº 708/INSS/PRES.

4. É o relatório. Passe-se ao exame.

2. FUNDAMENTAÇÃO

5. Vale ressaltar que é competência desta Coordenação-Geral de Matéria Administrativa, nos termos do art. 46 do Regimento Interno do INSS aprovado pela Portaria MDS n. 414, de 29 de setembro de 2017, dentre outras coisas, manifestar-se previamente à edição de atos normativos e interpretativos do INSS, relacionados à matéria administrativa, analisando os aspectos legais e formais adotados na sua elaboração.

6. A presente manifestação toma por base, exclusivamente, os elementos constantes do Sistema Sapiens até a presente data (que conta até o sequencial 51), e que, em face do que dispõe o art. 131 da Constituição Federal de 1988 – CF/88, o artigo 11 da Lei Complementar nº 73, de 10 de fevereiro de 1993, e o artigo 10 da Lei nº 10.480, de 2 de julho de 2002, incumbe a este órgão de execução consultivo manifestação sob o prisma estritamente jurídico, não lhe competindo adentrar na análise de aspectos de conveniência e oportunidade, nem analisar elementos de natureza eminentemente técnica, administrativa ou financeira.

7. Em relação ao ato ora em exame, **quanto a sua forma**, o art. 20 da Resolução nº 708 /PRES/INSS, de 6 de novembro de 2019, que efetiva nomeações, exonerações, designações, dispensas, punições, delegação e subdelegação no âmbito do INSS, dispõe:

Art. 20. Considera-se ato constitutivo:

I - Portaria: é o ato administrativo de autoridade competente, no âmbito de suas atribuições regimentais, que:

- a) contém recomendações de caráter técnico e específico;
- b) define, cria e institui normas de execução de serviço e procedimentais;
- c) constitui grupos de trabalho, comitês e comissão;
- d) aprova manuais, guias, cartilhas e minutas padrão;
- e) efetiva nomeações, exonerações, designações, dispensas, punições, delegação e subdelegação; ou**
- f) dispõe sobre qualquer outra matéria relativa à gestão administrativa e ao funcionamento das unidades e Diretorias do INSS;**

8. O Decreto 10.139, de 28 de novembro de 2019, que dispõe sobre a revisão e a consolidação dos atos normativos inferiores a decreto, cuja vigência se inicia em 03 de fevereiro de 2020, destaca:

Art. 2º A partir da entrada em vigor deste Decreto os atos normativos inferiores a decreto serão editados sob a forma de:

I - portarias - atos normativos editados por uma ou mais autoridades singulares;

II - resoluções - atos normativos editados por colegiados; ou

III - instruções normativas - atos normativos que, sem inovar, orientem a execução das normas vigentes pelos agentes públicos.

Parágrafo único. O disposto no **caput** não afasta a possibilidade de:

- I - uso excepcional de outras denominações de atos normativos por força de exigência legal; e
- II - edição de portarias ou resoluções conjuntas.

9. A partir do conceito supramencionado, constata-se que a minuta proposta está adequada, no tocante à **forma**, posto que o normativo será utilizado para instituir normas de execução de serviço e relativas ao funcionamento de unidades do INSS.

10. Quanto à **competência** para edição do ato, verifica-se que o Presidente do INSS, nos termos do inciso I do art. 17 do Anexo I da Estrutura Regimental aprovada pelo Decreto nº 9.746/2019, compete ao Presidente do INSS exercer a direção superior e o comando hierárquico deste instituto INSS.

11. Ainda, em relação ao ato em si, o Art. 7º, incisos II e III da Resolução nº 9, de 31 de agosto de 2020, que instituiu a Política de Segurança da Informação - POSIN-INSS, assim estabelece:

Art. 7º Competências e responsabilidades:

(...)

II - cabe ao Presidente do INSS nomear o Gestor de SI;

III - caso o Gestor de SI não seja nomeado, as atribuições relacionadas no inciso I do art. 7º serão desempenhadas pelo Diretor de Tecnologia da Informação e Inovação;

12. Observa-se também o atendimento ao disposto no art. 15, inciso I, da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020 do Gabinete de Segurança Institucional da Presidência da República:

Art. 15. Além das obrigações já dispostas nesta Instrução Normativa, compete aos órgãos e às entidades da administração pública federal, direta e indireta, em seu âmbito de atuação:

I - designar um gestor de segurança da informação interno, indicado pela alta administração do órgão ou da entidade;

13. Neste sentido o Presidente do INSS é, por força dos dispositivos retromencionados, a autoridade competente para designar o Gestor de Segurança de Informação no âmbito do INSS.

14. No que se refere à **motivação e à finalidade**, a NOTA TÉCNICA Nº 10/2020/DTI (SEI/INSS 2292739), emitida pela Diretoria de Tecnologia da Informação e Inovação é o documento que nestes autos demonstra a motivação e a finalidade do ato.

15. Sobre este ponto, registro que não cabe a este órgão de assessoramento jurídico, com relação às justificativas, aos estudos e opções apresentadas, adentrar em aspectos relativos à conveniência e à oportunidade da prática dos atos administrativos, que estão reservados à esfera discricionária do administrador público legalmente competente, apenas destacando-se necessidade das informações e dos dados serem fidedignos e que justifiquem tecnicamente a proposição, inclusive sejam suficientes para responder a eventuais indagações de órgãos de controle a respeito das medidas adotadas.

16. No tocante ao **conteúdo da norma em si**, registra-se que o parágrafo único do artigo 1º não prevê o exercício da substituição em situações de impedimento legal do Gestor de Segurança da Informação, devendo a administração avaliar a inclusão do impedimento legal como causa de substituição, além das previstas em razão de ausências e afastamentos legais.

17. Não existem outras considerações a serem apresentadas, eis que o ato encontra-se em seus termos em consonância com o que dispõe a Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020 do Gabinete de Segurança Institucional da Presidência da República.

18. Quanto à data de início de vigência da norma, deve ser destacado que o art. 4º do Decreto nº 10.139, de 2019, assim estabelece:

"Art. 4º Os atos normativos estabelecerão data certa para a sua entrada em vigor e para a sua produção de efeitos:

I - de, no mínimo, uma semana após a data de sua publicação; e

II - sempre no primeiro dia do mês ou em seu primeiro dia útil. Parágrafo único. O disposto neste artigo não se aplica às hipóteses de urgência justificada no expediente administrativo".

19. Assim sendo, a minuta deverá atender às regras do Decreto nº 10.139, de 2019, cabendo à Administração estabelecer uma data certa para a entrada em vigor do dispositivo em questão, data esta que deverá estar, simultaneamente, no mínimo, uma semana após a data de sua publicação e sempre no primeiro dia do mês ou em seu primeiro dia útil, ressalvando que **tal regramento não se aplicará nas hipóteses de urgência justificada da Administração, que deverão estar expressa e devidamente demonstradas no processo administrativo - o que não se localizou no presente caso, até o momento.**

20. Assim, *se for o caso*, é preciso que haja um ato formal da Administração reconhecendo que as medidas afiguram-se urgentes, para que sua entrada em vigor ocorra fora da regra geral do Decreto nº 10.139, de 2019.

21. Neste sentido, depreende-se que as minuta de portaria remetida à análise encontram o devido amparo jurídico, sob o aspecto formal.

22. São essas as considerações feitas por força do art. 131, caput, da Constituição Federal de 1988 c/c o art. 10 da Lei nº 10.480/2002 e com o art. 11 da Lei Complementar nº 73/93.

3. CONCLUSÃO

23. Com base nos fundamentos anteriormente expostos, opina-se pela regularidade jurídico-formal da minuta apresentada, desde que atendida as recomendações contidas nos itens 16, 19 e 20 da presente manifestação.

24. À consideração superior, sugerindo-se o seu retorno à Diretoria de Atendimento em prosseguimento para conhecimento e providências cabíveis.

Brasília, 10 de dezembro de 2020.

ALEX DA COSTA GRAÇANO
PROCURADOR FEDERAL
CHEFE DA DIVISÃO DE PESSOAL

De acordo com a manifestação jurídica supra, por seus próprios e jurídicos fundamentos.

Remetam-se à consideração do Exmo. Sr. Procurador-Geral da Procuradoria Federal Especializada junto ao INSS, para apreciação nos termos do art. 7º da Portaria AGU nº 1.399, de 5 de outubro de 2009 combinado com art. 13 da Portaria PGF nº 526, de 26 de agosto de 2013.

(assinado eletronicamente)
ANDRÉ CAMARGO HORTA DE MACEDO
PROCURADOR FEDERAL
COORDENADOR-GERAL DE MATÉRIA ADMINISTRATIVA SUBSTITUTO

Atenção, a consulta ao processo eletrônico está disponível em <http://sapiens.agu.gov.br> mediante o fornecimento do Número Único de Protocolo (NUP) 35014047735202084 e da chave de acesso bd3f7ef1

Documento assinado eletronicamente por ANDRE CAMARGO HORTA DE MACEDO, de acordo com os normativos legais aplicáveis. A conferência da autenticidade do documento está disponível com o código 549880377 no endereço eletrônico <http://sapiens.agu.gov.br>. Informações adicionais: Signatário (a): ANDRE CAMARGO HORTA DE MACEDO. Data e Hora: 11-12-2020 14:06. Número de Série: 17100539. Emissor: Autoridade Certificadora SERPRORFBv5.

Documento assinado eletronicamente por ALEX DA COSTA GRACANO, de acordo com os normativos legais aplicáveis. A conferência da autenticidade do documento está disponível com o código 549880377 no endereço eletrônico <http://sapiens.agu.gov.br>. Informações adicionais: Signatário (a): ALEX DA COSTA GRACANO. Data e Hora: 11-12-2020 13:50. Número de Série: 11959186519222134530093840898. Emissor: Autoridade Certificadora SERPRORFBv5.



ADVOCACIA-GERAL DA UNIÃO
PROCURADORIA-GERAL FEDERAL
PROCURADORIA FEDERAL ESPECIALIZADA JUNTO AO INSTITUTO NACIONAL DO SEGURO SOCIAL -
PFE/INSS - SEDE
GABINETE DO PROCURADOR-GERAL
SETOR DE AUTARQUIAS SUL QUADRA 2 BLOCO O 3º ANDAR

DESPACHO n. 00422/2020/GAB/PFE-INSS-SEDE/PGF/AGU

NUP: 35014.047735/2020-84

INTERESSADOS: DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO

ASSUNTOS: DIREITO ADMINISTRATIVO E OUTRAS MATÉRIAS DE DIREITO PÚBLICO

1. Aprovo, com ressalva, o **PARECER n. 00112/2020/DPES/PFE-INSS-SEDE/PGF/AGU.**
2. A minuta de portaria submetida à análise desta Procuradoria não veicula ato normativo, de modo que não há a incidência do art. 4º do Decreto nº 10.139, de 2019. Com efeito, embora o art. 3º da minuta disponha sobre as competências do Gestor de Segurança da Informação do INSS (como se ato normativo fosse), a redação é mera repetição do que consta do art. 19 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, razão pela qual a portaria analisada enquadra-se na definição de ato constitutivo, conforme art. 20, I, "e", da Resolução nº 708, de 6 de novembro de 2019, do Presidente do INSS (parcialmente prejudicado, mas não nessa parte, pelo citado Decreto nº 10.139, de 2019).
3. Dessa forma, a administração deverá observar apenas a recomendação contida no item 16 da manifestação jurídica mencionada acima (avaliar a inclusão do *impedimento legal* como causa de substituição, além das previstas em razão de ausências e afastamentos legais).
4. Encaminhe-se, diretamente, ao Gabinete da Presidência, para ciência e adoção das providências que entender cabíveis.

Brasília, 11 de dezembro de 2020.

FLÁVIO CHIARELLI VICENTE DE AZEVEDO
PROCURADOR-GERAL SUBSTITUTO

Atenção, a consulta ao processo eletrônico está disponível em <http://sapiens.agu.gov.br> mediante o fornecimento do Número Único de Protocolo (NUP) 35014047735202084 e da chave de acesso bd3f7ef1

Documento assinado eletronicamente por FLAVIO CHIARELLI VICENTE DE AZEVEDO, de acordo com os normativos legais aplicáveis. A conferência da autenticidade do documento está disponível com o código 550516009 no endereço eletrônico <http://sapiens.agu.gov.br>. Informações adicionais: Signatário (a): FLAVIO CHIARELLI VICENTE DE AZEVEDO. Data e Hora: 11-12-2020 18:05. Número de Série: 13968459. Emissor: Autoridade Certificadora SERPRORFBv4.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Gabinete
Coordenação De Suporte ao Gabinete

DESPACHO

Coordenação De Suporte ao Gabinete, em 14/12/2020.

Ref.: Processo
nº 35014.047735/2020-84.

Int.: Diretoria de
Tecnologia da Informação
e Inovação.

A s s . : Designação de
Gestor da Segurança da
Informação do INSS.

1. Trata-se de minuta de Portaria, oriunda da Diretoria de Tecnologia da Informação e Inovação - DTI, para fins de designação do Gestor de Segurança da Informação e seu substituto no âmbito do INSS.
2. No que concerne ao disposto no § 4º do art. 15 da Resolução nº 708/PRES/INSS, de 6 de novembro de 2019, a Procuradoria Federal Especializada junto ao INSS – PFE-INSS emitiu o Parecer nº 00112/2020/DPES/PFE-INSS-SEDE/PGF/AGU, (Sei nº 2442246), opinando “(...) *pela regularidade jurídico-formal da minuta apresentada, desde que atendida as recomendações contidas nos itens 16, 19 e 20 da presente manifestação.*”.
3. Ante o exposto, encaminhem-se os autos à DTI para cumprimento/justificativa quanto às recomendações exaradas pela PFE-INSS e posterior retorno à esta Coordenação.

CINTHYA DE ÁVILA O. TROJAN REPISO

Analista do Seguro Social

DIOGO FREITAS FIGUEIREDO

Coordenador de Suporte ao Gabinete



Documento assinado eletronicamente por **DIOGO FREITAS FIGUEIREDO**, Coordenador(a), em 14/12/2020, às 10:31, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **CINTHYA DE AVILA OLIVEIRA TROJAN REPISO**, **Chefe da Divisão**, em 14/12/2020, às 11:32, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2444765** e o código CRC **562B8949**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 2444765



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

DESPACHO

Diretoria De Tecnologia da Informação e Inovação, em 14/12/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

A s s . : Designação de
Gestor da Segurança da
Informação do INSS.

1. Ciente do despacho SEI 2444765.
2. Sobre o DESPACHO n. 00422/2020/GAB/PFE-INSS-SEDE/PGF/AGU (SEI 2442252) esta DTI vem tratar do item 16, conforme apontando no referido despacho:

Dessa forma, a administração deverá observar apenas a recomendação contida no item 16 da manifestação jurídica mencionada acima (avaliar a inclusão do impedimento legal como causa de substituição, além das previstas em razão de ausências e afastamentos legais).

3. Dessa forma, sugere-se que o parágrafo único do artigo 1º seja readequado da seguinte forma:

Parágrafo único. O servidor designado no **caput** será substituído pelo servidor JOÃO RODRIGUES DA SILVA FILHO, matrícula nº 1.561.845, em suas impedimentos legais, ausências e afastamentos.

4. Restitua-se o processo à Coordenação de Suporte ao Gabinete para avaliação e, se de acordo, encaminhamento para assinatura e publicação.

FLÁVIO FERREIRA DOS SANTOS

Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **FLAVIO FERREIRA DOS SANTOS, Diretor(a) de Tecnologia da Informação e Inovação**, em 14/12/2020, às 16:20, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2450628** e o código CRC **4F2AAFFF**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Gabinete
Coordenação De Suporte ao Gabinete

DESPACHO

Coordenação De Suporte ao Gabinete, em 15/12/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

A s s . : Designação de
Gestor da Segurança da
Informação do INSS.

1. Ciente quanto ao despacho da Diretoria de Tecnologia da Informação e Inovação- DTI, SEI nº 2450628.
2. Entretanto, carecem os autos de manifestação quanto às recomendações constantes dos itens 19 e 20 do Parecer nº 00112/2020/DPES/PFE-INSS-SEDE/PGF/AGU.
3. Restitua-se à DTI para saneamento e posterior devolução a esta Coordenação.

CINTHYA DE ÁVILA O. TROJAN REPISO

Analista do Seguro Social

DIOGO FREITAS FIGUEIREDO

Coordenador de Suporte ao Gabinete



Documento assinado eletronicamente por **DIOGO FREITAS FIGUEIREDO, Coordenador(a)**, em 15/12/2020, às 15:17, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **CINTHYA DE AVILA OLIVEIRA TROJAN REPISO, Chefe da Divisão**, em 15/12/2020, às 15:39, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site

[https://sei.inss.gov.br/sei/controlador_externo.php?](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)

[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **2462031** e o código CRC **F981E18A**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 2462031



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

DESPACHO

Diretoria De Tecnologia da Informação e Inovação, em 17/12/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

A s s . : Designação de
Gestor da Segurança da
Informação do INSS.

1. Em resposta ao Despacho CSG 2450628, fazemos referência ao DESPACHO n. 00422/2020/GAB/PFE-INSS-SEDE/PGF/AGU (2442252), que traz a aprovação, com ressalva sobre o PARECER n. 00112/2020/DPES/PFE-INSS-SEDE/PGF/AGU (2442246).

2. Entende-se, dessa forma, que o despacho do Procurador-Geral Substituto solicita atendimento apenas da recomendação do item 16, conforme abaixo:

Dessa forma, a administração *deverá observar apenas a recomendação contida no item 16 da manifestação jurídica mencionada acima* (avaliar a inclusão do impedimento legal como causa de substituição, além das previstas em razão de ausências e afastamentos legais).

3. No contexto apresentado, tendo a DTI observado a recomendação do item 16, restitua-se o processo à CSG para continuidade.

FLÁVIO FERREIRA DOS SANTOS

Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **FLAVIO FERREIRA DOS SANTOS, Diretor(a) de Tecnologia da Informação e Inovação**, em 17/12/2020, às 11:31, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site
https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2482356** e o código CRC **8B2A6738**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

MINUTA DE PORTARIA

Designa o Gestor de Segurança da Informação e o Gestor de Segurança da Informação Substituto.

O PRESIDENTE SUBSTITUTO DO INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS, no uso das atribuições que lhe confere o Decreto nº 9.746, de 8 de abril de 2019, e considerando o que dispõe o art. 15, inciso I, da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, bem como o que consta no Processo Administrativo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Designar CLAUDIO AUGUSTO NOVAIS FERRAZ, matrícula nº 1.148.338, como Gestor de Segurança da Informação do INSS.

Parágrafo único. O servidor designado no **caput** será substituído pelo servidor JOÃO RODRIGUES DA SILVA FILHO, matrícula nº 1.561.845, em suas ausências e afastamentos legais.

Art. 2º São competências do Gestor de Segurança da Informação do INSS, de acordo com o disposto no art. 19 da Instrução Normativa GSI/PR nº 1, de 2020:

- I - coordenar o Comitê de Segurança da Informação ou estrutura equivalente;
- II - coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do órgão, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;
- III - assessorar a alta administração na implementação da Política de Segurança da Informação;
- IV - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;
- V - promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade;

VI - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

VII - propor recursos necessários às ações de segurança da informação;

VIII - acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes Cibernéticos;

IX - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

X - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

XI - manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Art. 3º A gestão da Segurança da Informação é considerada serviço de natureza relevante e não ensejará qualquer tipo de remuneração adicional.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

ALESSANDRO ROOSEVELT SILVA RIBEIRO

Presidente Substituto



Documento assinado eletronicamente por **DIOGO FREITAS FIGUEIREDO, Coordenador(a)**, em 17/12/2020, às 19:06, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **CINTHYA DE AVILA OLIVEIRA TROJAN REPISO, Chefe da Divisão**, em 18/12/2020, às 08:35, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2486822** e o código CRC **C83CD8DF**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Gabinete
Coordenação De Suporte ao Gabinete

DESPACHO

Coordenação De Suporte ao Gabinete, em 17/12/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

A s s . : Designação de
Gestor da Segurança da
Informação do INSS.

1. Trata-se de minuta de Portaria, oriunda da Diretoria de Tecnologia da Informação e Inovação - DTI, para fins de designação do Gestor de Segurança da Informação e seu substituto no âmbito do INSS.

2. Retornam os autos da Procuradoria Federal Especializada junto ao INSS - PFE/INSS, a qual emitiu o Parecer nº 00112/2020/DPES/PFE-INSS-SEDE/PGF/AGU (2309779), opinando pela “(...) *pela regularidade jurídico-formal da minuta apresentada, desde que atendida as recomendações contidas nos itens 16, 19 e 20 da presente manifestação.*”, aprovado, com ressalva, pelo Despacho n. 00422/2020/GAB/PFE-INSS-SEDE/PGF/AGU, que recomendou apenas o cumprimento do item 16 do referido Parecer.

3. Consigna-se o atendimento da citada recomendação por meio da alteração da redação do parágrafo único do art. 1º, que passou a ser:

Parágrafo único. O servidor designado no **caput** será substituído pelo servidor JOÃO RODRIGUES DA SILVA FILHO, matrícula nº 1.561.845, em suas impedimentos legais, ausências e afastamentos.

4. Ante o exposto, encaminhe-se ao Gabinete da Presidência, não havendo óbice à assinatura do ato em questão, cuja última versão consta do Documento SEI nº 2486822.

CINTHYA DE ÁVILA O. TROJAN REPISO

DIOGO FREITAS FIGUEIREDO

Coordenador de Suporte ao Gabinete



Documento assinado eletronicamente por **DIOGO FREITAS FIGUEIREDO, Coordenador(a)**, em 17/12/2020, às 19:06, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



Documento assinado eletronicamente por **CINTHYA DE AVILA OLIVEIRA TROJAN REPISO, Chefe da Divisão**, em 18/12/2020, às 08:35, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2486636** e o código CRC **555468A5**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 2486636



INSTITUTO NACIONAL DO SEGURO SOCIAL

PORTARIA Nº 1.246/PRES/INSS, DE 18 DE DEZEMBRO DE 2020

Designa o Gestor de Segurança da Informação e o Gestor de Segurança da Informação Substituto.

O **PRESIDENTE DO INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS**, no uso das atribuições que lhe confere o Decreto nº 9.746, de 8 de abril de 2019, e considerando o que dispõe o art. 15, inciso I, da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, bem como o que consta no Processo Administrativo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Designar CLAUDIO AUGUSTO NOVAIS FERRAZ, matrícula nº 1.148.338, como Gestor de Segurança da Informação do INSS.

Parágrafo único. O servidor designado no **caput** será substituído pelo servidor JOÃO RODRIGUES DA SILVA FILHO, matrícula nº 1.561.845, em suas ausências e afastamentos legais.

Art. 2º São competências do Gestor de Segurança da Informação do INSS, de acordo com o disposto no art. 19 da Instrução Normativa GSI/PR nº 1, de 2020:

- I - coordenar o Comitê de Segurança da Informação ou estrutura equivalente;
- II - coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do órgão, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;
- III - assessorar a alta administração na implementação da Política de Segurança da Informação;
- IV - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;
- V - promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade;

VI - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

VII - propor recursos necessários às ações de segurança da informação;

VIII - acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes Cibernéticos;

IX - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

X - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

XI - manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Art. 3º A gestão da Segurança da Informação é considerada serviço de natureza relevante e não ensejará qualquer tipo de remuneração adicional.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES

Presidente



Documento assinado eletronicamente por **LEONARDO JOSE ROLIM GUIMARAES**, **Presidente**, em 18/12/2020, às 13:57, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2489775** e o código CRC **89DE4D6C**.



INSTITUTO NACIONAL DO SEGURO SOCIAL
GABINETE DA PRESIDÊNCIA
Serviço Técnico Administrativo

DESPACHO

Serviço Técnico Administrativo do Gabinete, em 18/12/2020

Ref.: Processo nº
35014.047735/2020-84

Int.:
DTI/PRESIDÊNCIA

Ass.: Designa o Gestor de
Segurança da Informação
e o Gestor de Segurança
da Informação Substituto

Assinada a Portaria nº 1.246/PRES/INSS, de 18 de dezembro de 2020, de ordem,
encaminhe-se:

1. ao Serviço de Publicidade Legal para publicação no Boletim de Serviço (BS); e
2. à Divisão de Comunicação Administrativa para divulgação no Portal.

RAIMUNDO RODRIGUES

Servidor



Documento assinado eletronicamente por **RAIMUNDO NONATO RODRIGUES DA SILVA**,
Servidor(a), em 18/12/2020, às 15:12, conforme horário oficial de Brasília, com fundamento no art. 6º,
§ 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site
[https://sei.inss.gov.br/sei/controlador_externo.php?](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)
[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **2496627** e o
código CRC **35BE4507**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Assessoria De Comunicação Social
Coordenação De Comunicação Social
Serviço De Publicidade Legal

DESPACHO

Serviço De Publicidade Legal, em 18/12/2020.

1. A Portaria nº 1.246/PRES/INSS será publicada no Boletim de Serviço nº 242, de 18/12/2020.
2. Restitua-se para as devidas providências.

DANIELA MIRANDA DA SILVA OLIVEIRA

Chefe do Serviço de Publicidade Legal do INSS - Substituta



Documento assinado eletronicamente por **DANIELA MIRANDA DA SILVA OLIVEIRA**, Técnico do Seguro Social, em 18/12/2020, às 17:35, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2498546** e o código CRC **A02406DE**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 2498546



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Assessoria De Comunicação Social
Coordenação De Comunicação Social
Divisão De Comunicação Administrativa

DESPACHO

Divisão De Comunicação Administrativa, em 18/12/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

A s s . : Publicação de
Portaria

1. Trata-se da publicação e divulgação da Portaria nº 1.246 /PRES/INSS, de 18 de dezembro de 2020.
2. Informamos que o referido ato, foi publicado no BS nº 242, de 18 de dezembro de 2020 e no Portal-INSS, na intraprev.
3. Ao Serviço Técnico Administrativo do Gabinete da Presidência, para conhecimento e providências julgadas necessárias.

ALDAMIR GERALDO DE LISBÔA LIMA

Chefe da Divisão de Comunicação Administrativa - DIVCA



Documento assinado eletronicamente por **ALDAMIR GERALDO DE LISBOA LIMA, Chefe da Divisão**, em 18/12/2020, às 17:49, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site
https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2498643** e o código CRC **D06FF9AD**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 2498643



INSTITUTO NACIONAL DO SEGURO SOCIAL
GABINETE DA PRESIDÊNCIA
Serviço Técnico Administrativo

DESPACHO

Serviço Técnico Administrativo do Gabinete, em 18/12/2020

Ref.: Processo nº
35014.047735/2020-84

Int.:
DTI/PRESIDÊNCIA

Ass.: Designa o Gestor de
Segurança da Informação
e o Gestor de Segurança
da Informação Substituto

Restituir para a Diretoria de Tecnologia da Informação e Inovação, de ordem, após publicação da Portaria nº 1.246/PRES/INSS, de 18 de dezembro de 2020, no Boletim de Serviço nº 242, de 18 de dezembro de 2020.

RAIMUNDO RODRIGUES

Servidor



Documento assinado eletronicamente por **RAIMUNDO NONATO RODRIGUES DA SILVA**, **Servidor(a)**, em 18/12/2020, às 18:08, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site
https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2498729** e o código CRC **55B70818**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 2498729



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

DESPACHO

Diretoria De Tecnologia da Informação e Inovação, em 21/12/2020.

Ref.: Processo
nº 35014.047735/2020-84

Int.: DIRETORIA DE
TECNOLOGIA DA
INFORMAÇÃO E
INOVAÇÃO

Ass.: Designa o Gestor de
Segurança da Informação
e o Gestor de Segurança
da Informação Substituto

1. Trata-se da publicação e divulgação da Portaria nº 1.246 /PRES/INSS, de 18 de dezembro de 2020 que designa o Gestor de Segurança da Informação e o Gestor de Segurança da Informação Substituto.
2. De ordem do Diretor desta DTI, encaminhe-se à CGIN para ciência dos designados.

RENATA CESÁRIO DE OLIVEIRA GOMES

Analista em Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **RENATA CESARIO DE OLIVEIRA GOMES, Analista em Tecnologia da Informação**, em 21/12/2020, às 10:39, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2503645** e o código CRC **F7316B6B**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 2503645



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

DESPACHO

Diretoria De Tecnologia da Informação e Inovação, em 15/08/2021

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria De Tecnologia da Informação e Inovação.

Ass.: Solicita indicação para alteração do Gestor de Segurança da Informação e seu Substituto e propõe alteração da NCAL

1. Trata-se de necessidade de revisão da Resolução Nº 12/CEGOV/INSS, de 31 de Agosto de 2020 que disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil e da Portaria 1.246/PRES/INSS, de 18 de Dezembro de 2020.

2. A Resolução Nº 12/CEGOV/INSS, de 31 de Agosto de 2020, indica o Diretor de Tecnologia da Informação e Inovação como responsável por autorizar pedidos para o Perfil 4, que não sejam de servidores da Assessoria de Comunicação Social ou da Diretoria de Gestão de Pessoas e Administração.

3. Esta diretoria proporá ao Comitê Temático de Governança Digital - CTGD que tal papel seja atribuído ao Gestor de Segurança da Informação que poderá avaliar com mais critério os pedidos recebidos nesta unidade. Para isso, será elaborada Nota Técnica para deliberação na próxima reunião do comitê com a proposta de redação abaixo - alteração em negrito:

Art. 9º O processo de atribuição de acesso à Internet seguirá as seguintes diretrizes:

I - a atribuição dos perfis de acesso à Internet será feita pelos Autorizadores, de forma fundamentada e respeitando o princípio da necessidade de conhecer, de acordo com a tabela abaixo:

<i>Perfil</i>	<i>Autorizador</i>
<i>Perfil 1, 2 e 3</i>	<i>Gerente de Agência da Previdência Social - APS, Gerente-Executivo, Superintendentes-Regionais, Procuradores-Regionais, Coordenadores-Gerais, Superintendentes-Regionais, Presidente do INSS, Auditor-Geral, Corregedor-Geral, Procurador-Geral da PFE-INSS, Diretores, Gestores ou Chefes da área responsável pelo Contrato ou ato administrativo similar no âmbito do INSS.</i>

<i>Perfil</i>	<i>Autorizador</i>
Perfil 4	<i>Chefes de Assessoria de Comunicação Social nas Superintendências-Regionais, Assessor de Comunicação Social (Administração Central), Gestor de Segurança da Informação, Diretor de Gestão de Pessoas e Administração e Presidente do INSS.</i>

4. Além disso, é necessário a atualização dos servidores designados na Portaria 1.246/PRES/INSS, de 18 de Dezembro de 2020 para os papéis de Gestor de Segurança da Informação e seu substituto.

5. De ordem do diretor, encaminhe-se à CGIN para indicação do Gestor de Segurança da Informação e seu substituto e à CGOV para elaboração de Nota Técnica para alteração da NCAL.

MARCELO GENU BESERRA

Coordenador de Governança e Planejamento de TIC



Documento assinado eletronicamente por **MARCELO GENU BESERRA**, Técnico do Seguro Social, em 15/08/2021, às 09:43, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4576764** e o código CRC **73FCFC1C**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 4576764



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

Coordenação De Governança e Planejamento De Tecnologia da Informação e Comunicação

NOTA TÉCNICA Nº 8/2021/CGOV/DTI-INSS

PROCESSO Nº 35014.047735/2020-84

INTERESSADO: DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO

Proposta de alteração da Resolução Nº 12/CEGOV/INSS, de 31 de Agosto de 2020

1. Esta nota técnica trata da atualização da Resolução Nº 12/CEGOV/INSS, de 31 de Agosto de 2020 que disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.

2. Abaixo segue mudança solicitada:

Art. 9º O processo de atribuição de acesso à Internet seguirá as seguintes diretrizes:

I - a atribuição dos perfis de acesso à Internet será feita pelos Autorizadores, de forma fundamentada e respeitando o princípio da necessidade de conhecer, de acordo com a tabela abaixo:

<i>Perfil</i>	<i>Autorizador</i>
<i>Perfil 1, 2 e 3</i>	<i>Gerente de Agência da Previdência Social - APS, Gerente-Executivo, Superintendentes-Regionais, Procuradores-Regionais, Coordenadores-Gerais, Superintendentes-Regionais, Presidente do INSS, Auditor-Geral, Corregedor-Geral, Procurador-Geral da PFE-INSS, Diretores, Gestores ou Chefes da área responsável pelo Contrato ou ato administrativo similar no âmbito do INSS.</i>
<i>Perfil 4</i>	<i>Chefes de Assessoria de Comunicação Social nas Superintendências-Regionais, Assessor de Comunicação Social (Administração Central), Gestor de Segurança da Informação, Diretor de Gestão de Pessoas e Administração e Presidente do INSS.</i>

3. Diante do exposto solicita-se a atualização da Resolução Nº 12/CEGOV/INSS, de 31 de Agosto de 2020.

4. Encaminhe-se ao CTGD para avaliação e Deliberação.

Brasília/DF, 15 de agosto de 2021.

MARCELO GENU BESERRA

Coordenador de Governança e Planejamento de TIC



Documento assinado eletronicamente por **MARCELO GENU BESERRA**, **Coordenador(a) de Governança e Planejamento de Tecnologia da Informação e Comunicação**, em 25/08/2021, às 16:55, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4576774** e o código CRC **80ACF6EC**.

Referência: Processo nº 35014.047735/2020-84

SEI nº 4576774



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações

DESPACHO

Coordenação-Geral De Infraestrutura e Operações, em 17/08/2021

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria De Tecnologia da Informação e Inovação.

Ass.: Solicita indicação para alteração do Gestor de Segurança da Informação e seu Substituto e propõe alteração da NCAL.

1. Trata-se de necessidade de revisão da Resolução Nº 12/CEGOV/INSS, de 31 de Agosto de 2020 que disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil e da Portaria 1.246/PRES/INSS, de 18 de Dezembro de 2020.
2. Em atenção ao Despacho DTI 4576764, opinamos pela indicação de **JOÃO RODRIGUES DA SILVA FILHO**, matrícula nº 1561845, como Gestor de Segurança da Informação do INSS e **LUZIVAN DE MOURA GOIS**, matrícula nº 1784525, para substituí-lo em suas ausências e afastamentos legais.
3. Isto posto, encaminhe-se à DTI, em resposta.

JOÃO RODRIGUES DA SILVA FILHO

Coordenador-Geral de Infraestrutura e Operações



Documento assinado eletronicamente por **JOAO RODRIGUES DA SILVA FILHO**, **Coordenador(a) Geral**, em 17/08/2021, às 19:55, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4597718** e o código CRC **F4BA6D61**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

MINUTA DE PORTARIA DTI/INSS Nº 5389493, DE 28 DE OUTUBRO DE 2021



Documento assinado eletronicamente por **MARCELO GENU BESERRA**, Técnico do Seguro Social, em 03/11/2021, às 16:41, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5389493** e o código CRC **08EB2E7F**.

MINUTA DE PORTARIA

Designa o Gestor de Segurança da Informação e o Gestor de Segurança da Informação Substituto.

O PRESIDENTE DO INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS, no uso das atribuições que lhe confere o Decreto nº 9.746, de 8 de abril de 2019, e considerando o que consta no Processo Administrativo nº 35014.047735/2020-84 e no que dispõe o art. 15, inciso I, da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República,

RESOLVE:

Art. 1º Designar JOÃO RODRIGUES DA SILVA FILHO, matrícula nº 1.561.845, como Gestor de Segurança da Informação do INSS.

Parágrafo único. O servidor designado no caput será substituído pelo servidor LUZIVAN DE MOURA GOIS, matrícula nº 1.784.525, em suas ausências e afastamentos legais.

Art. 2º São competências do Gestor de Segurança da Informação do INSS, de acordo com o disposto no art. 19 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020:

I - coordenar o Comitê de Segurança da Informação ou estrutura equivalente;

II - coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do órgão, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da

Presidência da República;

III - assessorar a alta administração na implementação da Política de Segurança da Informação;

IV - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

V - promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade;

VI - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

VII - propor recursos necessários às ações de segurança da informação;

VIII - acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes Cibernéticos;

IX - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

X - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

XI - manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Art. 3º A gestão da Segurança da Informação é considerada serviço de natureza relevante e não ensejará qualquer tipo de remuneração adicional.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

LEONARDO JOSÉ ROLIM GUIMARÃES

Presidente



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

DESPACHO

Diretoria De Tecnologia da Informação e Inovação, em 28/10/2021

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria De Tecnologia da Informação e Inovação.

Ass.: Indicação de Gestor e Substituto de Segurança da Informação do INSS - alteração de Portaria.

1. Trata-se de necessidade de revisão da Resolução Nº 12/CEGOV/INSS, de 31 de Agosto de 2020 que disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil e da Portaria 1.246/PRES/INSS, de 18 de Dezembro de 2020.
2. De acordo com a sugestão proposta pela Coordenação-Geral de Infraestrutura e Operações - CGIN, apresentamos a Minuta da Portaria (SEI nº 5389493) com a indicação de João Rodrigues da Silva Filho, Mat. 1561845, como Gestor de Segurança da Informação do INSS e Luzivan de Moura Gois, Mat. 1784525, para substituí-lo em suas ausências e afastamentos legais.
3. Encaminhe-se à Coordenação de Suporte ao Gabinete - CSG para as providências necessárias.

MARCELO GENU BESERRA

Coordenador de Governança e Planejamento de TI



Documento assinado eletronicamente por **MARCELO GENU BESERRA, Técnico do Seguro Social**, em 29/10/2021, às 15:32, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5389765** e o código CRC **185F3A8E**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Gabinete

DESPACHO

Gabinete, em 29/10/2021

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria De Tecnologia da Informação e Inovação.

Ass.: Indicação de Gestor e Substituto de Segurança da Informação do INSS - alteração de Portaria.

Restituam-se os autos à Diretoria de Tecnologia da Informação e Inovação para assinatura da minuta acostada ao documento SEI nº 5389493, bem como para manifestação de ciência e concordância por parte de seu titular quanto ao ato proposto.

EMANUEL DE ARAÚJO DANTAS

Chefe de Gabinete da Presidência



Documento assinado eletronicamente por **EMANUEL DE ARAUJO DANTAS, Chefe de Gabinete da Presidência**, em 29/10/2021, às 16:59, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5403901** e o código CRC **F82A0924**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 5403901



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

DESPACHO

Diretoria De Tecnologia da Informação e Inovação, em 03/11/2021

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria De Tecnologia da Informação e Inovação.

Ass.: Indicação de Gestor e Substituto de Segurança da Informação do INSS - alteração de Portaria.

1. Trata-se de necessidade de revisão da Resolução Nº 12/CEGOV/INSS, de 31 de Agosto de 2020 que disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil e da Portaria 1.246/PRES/INSS, de 18 de Dezembro de 2020.
2. Após assinatura da minuta e de acordo com a sugestão proposta pela Coordenação-Geral de Infraestrutura e Operações - CGIN, apresentamos a Minuta da Portaria (SEI nº 5389493) com a indicação de João Rodrigues da Silva Filho, Mat. 1561845, como Gestor de Segurança da Informação do INSS e Luzivan de Moura Gois, Mat. 1784525, para substituí-lo em suas ausências e afastamentos legais.
3. Encaminhe-se à Coordenação de Suporte ao Gabinete - CSG para as providências necessárias.

MARCELO GENU BESERRA

Coordenador de Governança e Planejamento de TI



Documento assinado eletronicamente por **MARCELO GENU BESERRA, Técnico do Seguro Social**, em 03/11/2021, às 16:43, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5422917** e o código CRC **153722A6**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 5422917



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Gabinete

DESPACHO

Gabinete, em 03/11/2021

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria De Tecnologia da Informação e Inovação.

Ass.: Indicação de Gestor e Substituto de Segurança da Informação do INSS - alteração de Portaria.

1. Ciente.
2. Conforme exposto no despacho deste Gabinete SEI nº 5403901, carecem os autos de manifestação de ciência e concordância **do Diretor de Tecnologia da Informação e Inovação** quanto aos termos da minuta ora proposta.
3. Restituam-se os autos para juntada da manifestação indicada.

EMANUEL DE ARAÚJO DANTAS

Chefe de Gabinete da Presidência



Documento assinado eletronicamente por **EMANUEL DE ARAUJO DANTAS, Chefe de Gabinete da Presidência**, em 03/11/2021, às 17:51, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5423561** e o código CRC **813CB757**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 5423561



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

DESPACHO

Diretoria De Tecnologia da Informação e Inovação, em 04/11/2021

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria De Tecnologia da Informação e Inovação.

Ass.: Indicação de Gestor e Substituto de Segurança da Informação do INSS - alteração de Portaria.

1. Ciente e de acordo com a minuta de portaria 5389493.
2. Encaminhe-se ao GABPRE em prosseguimento.

THIAGO WALTZ ALVES

Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **THIAGO WALTZ ALVES, Diretor(a) de Tecnologia da Informação e Inovação**, em 04/11/2021, às 17:16, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5427756** e o código CRC **5716B60B**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 5427756



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Gabinete
Coordenação De Suporte ao Gabinete

MINUTA DE PORTARIA

Altera a Portaria nº 1.246/PRES/INSS, de 18 de dezembro de 2020.

O PRESIDENTE DO INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS, no uso das atribuições que lhe confere o Decreto nº 9.746, de 8 de abril de 2019, e considerando o que consta no Processo Administrativo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º A Portaria nº 1.246/PRES/INSS, de 18 de dezembro de 2020, publicada no Boletim de Serviço nº 242, de 18 de dezembro de 2020, passa a vigorar com as seguintes alterações:

"Art. 1º Designar o servidor JOÃO RODRIGUES DA SILVA FILHO, matrícula nº 1.561.845, como Gestor de Segurança da Informação do INSS.

Parágrafo único. O servidor designado no **caput** será substituído pelo servidor LUZIVAN DE MOURA GOIS, matrícula nº 1.784.525, em suas ausências e afastamentos legais." (NR)

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

JOSÉ CARLOS OLIVEIRA

Presidente



Documento assinado eletronicamente por **DIOGO FREITAS FIGUEIREDO**, Coordenador(a), em 08/11/2021, às 10:53, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5439579** e o código CRC **8CA365C6**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Gabinete
Coordenação De Suporte ao Gabinete

DESPACHO

Coordenação De Suporte ao Gabinete, em 05/11/2021

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria de Tecnologia da Informação e Inovação.

Ass.: Altera a Portaria nº 1.246/PRES/INSS, de 18 de dezembro de 2020.

1. Trata-se de minuta de Portaria, oriunda da Diretoria de Tecnologia da Informação e Inovação, para fins de designação do Gestor de Segurança da Informação e seu substituto no âmbito do INSS.

2. Para justificar e fundamentar a edição dos atos em questão, foram expedidos os despachos SEI nºs 4576764 e 5389765, em lugar da Nota Técnica prevista no inciso III do art. 13 da Portaria PRES/INSS nº 1.313, de 17 de junho de 2021.

3. Cumpre aqui salientar que por tratar-se da designação do Gestor de Segurança da Informação e seu substituto, ensejando apenas a alteração do art. 1º da Portaria nº 1.246/PRES/INSS, de 2020, esta Coordenação optou pela alteração do referido ato, ao invés da publicação de novo ato, já que os demais dispositivos da portaria continuarão inalterados.

4. Sobre a adequação do ato em comento, dispõem o art. 9º e a alínea "a" do inciso I do art. 17 da Portaria PRES/INSS nº 1.313, de 2021, que versa sobre a elaboração, redação, alteração e revogação dos atos administrativos no âmbito do INSS:

Art. 9º A revogação e a alteração deverão ser procedidas por ato de mesma denominação e hierarquia, salvo disposição legal em contrário.

Art. 17. Portaria é o ato administrativo, editado por uma ou mais autoridades singulares competentes, no âmbito de suas atribuições regimentais, com caráter:

I - normativo, quando seu conteúdo for normativo, ou seja:

a) define, cria e institui normas e diretrizes gerais ou de execução e gestão de serviço, procedimentais e do funcionamento administrativo para fiel aplicação da política do Instituto;

5. Logo, está adequada a modalidade de ato constitutiva, pois trata de norma relativa à gestão administrativa e altera Portaria em vigor.

6. Sobre as regras para elaboração, articulação e redação da minuta de Portaria, consigna-se sua adequação com as regras estabelecidas na Lei Complementar nº 95, de 26 de fevereiro de 1998, no Decreto nº 9.191, de 1º de novembro de 2017, e na Portaria PRES/INSS nº 1.313, de 2021, tendo sido analisada por esta Coordenação, que propôs a nova redação.

7. Ante o exposto, considerando-se que a única alteração no texto da portaria refere-se à designação do Gestor de Segurança da Informação e seu substituto, entende-se por dispensável novo trâmite pela Procuradoria Federal Especializada junto ao INSS, motivo pelo qual encaminhamos os autos ao Gabinete da Presidência, não havendo óbice à assinatura do ato proposto, cuja versão final consta do Documento SEI nº 5439579.

CINTHYA DE ÁVILA O. TROJAN REPISO

Chefe da Divisão de Normas e Acordos

DIOGO FREITAS FIGUEIREDO

Coordenador de Suporte ao Gabinete



Documento assinado eletronicamente por **DIOGO FREITAS FIGUEIREDO, Coordenador(a)**, em 08/11/2021, às 11:03, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



Documento assinado eletronicamente por **CINTHYA DE AVILA OLIVEIRA TROJAN REPISO, Chefe da Divisão**, em 08/11/2021, às 11:05, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5444836** e o código CRC **AE18C9CA**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 5444836



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência

PORTARIA PRES/INSS Nº 1.377, DE 8 DE NOVEMBRO DE 2021.

Altera a Portaria nº 1.246/PRES/INSS, de 18 de dezembro de 2020.

O **PRESIDENTE DO INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS**, no uso das atribuições que lhe confere o Decreto nº 9.746, de 8 de abril de 2019, e considerando o que consta no Processo Administrativo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º A Portaria nº 1.246/PRES/INSS, de 18 de dezembro de 2020, publicada no Boletim de Serviço nº 242, de 18 de dezembro de 2020, passa a vigorar com as seguintes alterações:

"Art. 1º Designar o servidor JOÃO RODRIGUES DA SILVA FILHO, matrícula nº 1.561.845, como Gestor de Segurança da Informação do INSS.

Parágrafo único. O servidor designado no **caput** será substituído pelo servidor LUZIVAN DE MOURA GOIS, matrícula nº 1.784.525, em suas ausências e afastamentos legais." (NR)

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

JOSÉ CARLOS OLIVEIRA

Presidente



Documento assinado eletronicamente por **JOSE CARLOS OLIVEIRA, Presidente**, em 09/11/2021, às 08:49, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5463068** e o código CRC **9AEEBEAC**.



INSTITUTO NACIONAL DO SEGURO SOCIAL
GABINETE DA PRESIDÊNCIA
Serviço Técnico Administrativo

DESPACHO

SERVIÇO TÉCNICO ADMINISTRATIVO DO GABINETE, em 9/11/2021

Ref.: Processo nº
35014.047735/2020-84

Int.: Diretoria de
Tecnologia da Informação
e Inovação

Ass.: Altera a Portaria nº
1.246/PRES/INSS, de 18
de dezembro de 2020.

Restitua-se à Diretoria de Tecnologia da Informação e Inovação, de ordem, após publicação da Portaria PRES/INSS nº 1.377, de 8 de novembro de 2021, no BSE de 9 de novembro de 2021, para as providências decorrentes.

VINICIUS ROSA RODRIGUES

Chefe de Serviço Técnico Administrativo do Gabinete



Documento assinado eletronicamente por **VINICIUS ROSA RODRIGUES, Chefe de Serviço**, em 09/11/2021, às 09:41, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5477637** e o código CRC **ED9AF899**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 5477637



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Assessoria De Comunicação Social
Coordenação De Comunicação Social
Divisão De Comunicação Administrativa

DESPACHO

Divisão De Comunicação Administrativa, em 09/11/2021

Ref.: Processo nº 35014.047735/2020-84

Int.: Diretoria de Tecnologia da Informação e Inovação

Ass.: Publicação de Portaria

1. Trata-se da publicação e divulgação da Portaria PRES/INSS nº 1.377, de 8 de novembro de 2021.
2. Informamos que o referido ato, foi publicado no BSE, de 9 de novembro de 2021 e no Portal-INSS, na intraprev.
3. À Diretoria de Tecnologia da Informação e Inovação, para conhecimento e providências julgadas necessárias.

ALDAMIR GERALDO DE LISBÔA LIMA

Chefe da Divisão de Comunicação Administrativa - DIVCA



Documento assinado eletronicamente por **ALDAMIR GERALDO DE LISBOA LIMA, Chefe da Divisão**, em 09/11/2021, às 16:13, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5482039** e o código CRC **7F23723A**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 5482039



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

DESPACHO

Diretoria De Tecnologia da Informação e Inovação, em 09/11/2021

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria De Tecnologia da Informação e Inovação.

Ass.: Altera a Portaria nº 1.246/PRES/INSS, de 18 de dezembro de 2020.

1. Trata-se da PORTARIA PRES/INSS Nº 1.377, DE 8 DE NOVEMBRO DE 2021 que designa o Gestor de Segurança da Informação e seu substituto no âmbito do INSS.
2. De ordem do diretor, encaminhe-se à CGIN e DIOP para conhecimento.

MARCELO GENU BESERRA

Coordenador de Governança e Planejamento de TI



Documento assinado eletronicamente por **MARCELO GENU BESERRA, Técnico do Seguro Social**, em 09/11/2021, às 15:51, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5488360** e o código CRC **B0BA495C**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 5488360



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações
Coordenação De Suporte e Infraestrutura De Tecnologia da Informação e Comunicação
Divisão De Operações em Tecnologia da Informação e Comunicação

DESPACHO

Divisão De Operações em Tecnologia da Informação e Comunicação, em 12/11/2021

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria De Tecnologia da Informação e Inovação.

Ass.: Altera a Portaria nº 1.246/PRES/INSS, de 18 de dezembro de 2020.

1. Trata-se da PORTARIA PRES/INSS Nº 1.377, DE 8 DE NOVEMBRO DE 2021 que designa o Gestor de Segurança da Informação e seu substituto no âmbito do INSS.
2. Ciente da Portaria 1.377 (5463068).
3. Feitas as considerações, conclua-se o processo nesta unidade.

LUZIVAN DE MOURA GOIS

Chefe da Divisão de Operações de TIC



Documento assinado eletronicamente por **LUZIVAN DE MOURA GOIS, Chefe de Divisão de Operações em Tecnologia da Informação e Comunicação**, em 12/11/2021, às 11:36, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5530323** e o código CRC **542E48A5**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Comitê Estratégico de Governança

REGISTRO DE REUNIÃO

Reunião:	2ª Reunião Ordinária do Comitê Estratégico de Governança do INSS em 2022.
Data/hora:	23/02/2022, das 16h00 às 17h00
Local:	Gabinete da Presidência, Sala 1013
Processo SEI:	35014.072365/2022-85

1. Deliberações

DELIBERAÇÃO 1: Publicação de atos normativos e de gestão afetos à tecnologia da informação, escopo DTI e CEGOV	
Decisão:	
O Presidente Substituto do INSS apresentou a necessidade de revogação das seguintes normas: • Resolução nº 10/CEGOV/INSS, 31/08/2020 - Institui a Norma de Controle de Acesso Lógico - NCAL; • Resolução nº 11/CEGOV/INSS, 31/08/2020 - Institui a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR/INSS; • Resolução nº 12/CEGOV/INSS, 31/08/2020 - Institui a Disciplina o uso da internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil. A justificativa para a revogação das resoluções consta da Nota Técnica Nº 1/2022/CTGD-CEGOV/DIGOV-INSS, documento SEI nº (6587544). Foi deliberado que à Diretoria de Tecnologia da Informação e Inovação - DTI ficará responsável pela expedição dos atos normativos sobre os temas em questão.	
Votos a favor	Votos contrários
Decidido por unanimidade.	Não houve.

2. Informes

INFORME 1: Relatório de Verificação de Conformidade do Sistema de Governança SG-INSS 2021
O Relatório de Verificação de Conformidade do SG-INSS, foi apresentado pelo Coordenador-Geral de Governança e Cobrança Administrativa - CGGOV. O Relatório apresentado será encaminhado para as áreas do INSS e para os coordenadores dos comitês temáticos para ciência e adoção das medidas necessárias ao bom funcionamento dos comitês, via Processo SEI nº 35014.232683/2021-21.

INFORME 2: Lei Geral de Proteção de Dados - LGPD - Navegação Patrocinada.

O Encarregado pela LGPD no âmbito do INSS, Sr. Edson Alvarista informou que o processo de contratação de empresa para execução do serviço de Navegação Patrocinada necessita, urgentemente, de adequação do contrato celebrado entre o INSS e a prestadora do serviço de telefonia, por conter as seguintes fragilidades:

- necessidade de formalização do gestor do contrato por parte do INSS;
- ausência de cláusulas que versem sobre as regras de proteção dos dados, previstas na Lei nº 13.709.



Documento assinado eletronicamente por **ALEXANDRE GUIMARAES, Diretor(a) de Integridade, Governança e Gerenciamento de Riscos**, em 03/03/2022, às 16:21, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



Documento assinado eletronicamente por **JOBSON DE PAIVA SILVEIRA SALES, Diretor(a) de Atendimento**, em 03/03/2022, às 18:36, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



Documento assinado eletronicamente por **LARISSA ANDRADE MORA, Diretor(a) de Gestão de Pessoas e Administração**, em 04/03/2022, às 09:24, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



Documento assinado eletronicamente por **GUILHERME GASTALDELLO PINHEIRO SERRANO, Presidente, Substituto**, em 04/03/2022, às 10:12, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



Documento assinado eletronicamente por **SEBASTIAO FAUSTINO DE PAULA, Diretor(a)**, em 04/03/2022, às 14:02, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



Documento assinado eletronicamente por **VIRGILIO ANTONIO RIBEIRO DE OLIVEIRA FILHO, Procurador-Geral da PFE/INSS**, em 07/03/2022, às 15:54, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **6589827** e o código CRC **6F26561E**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações

NOTA TÉCNICA Nº 4/2022/CGIN/DTI-INSS

PROCESSO Nº 35014.047735/2020-84

INTERESSADO: DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO

Nota Técnica referente a Portaria que regulamenta e define conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil .

1. Trata-se de nota técnica de apresentação de minuta de portaria que regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil em atendimento a lei 12.965, de 23 de abril de 2014 que estabelece princípios, direitos e deveres da internet no Brasil.
2. O Decreto 9.203/2017 dispõe sobre a POLÍTICA DE GOVERNANÇA da administração pública federal direta, autárquica e fundacional.
3. O decreto conceitua Governança Pública como o conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade.
4. Os Princípios da Governança Pública são:
 - capacidade de resposta;
 - integridade;
 - confiabilidade;
 - melhoria regulatória;
 - prestação de contas e responsabilidade; e
 - Transparência.
5. Com Diretrizes o decreto destaca:
 - direcionar ações para a busca de resultados para a sociedade, encontrando soluções tempestivas e inovadoras para lidar com a limitação de recursos e com as mudanças de prioridades;

- promover a simplificação administrativa, a modernização da gestão pública e a integração dos serviços públicos, especialmente aqueles prestados por meio eletrônico;
- monitorar o desempenho e avaliar a concepção, a implementação e os resultados das políticas e das ações prioritárias para assegurar que as diretrizes estratégicas sejam observadas;
- articular instituições e coordenar processos para melhorar a integração entre os diferentes níveis e esferas do setor público, com vistas a gerar, preservar e entregar valor público;
- fazer incorporar padrões elevados de conduta pela alta administração para orientar o comportamento dos agentes públicos, em consonância com as funções e as atribuições de seus órgãos e de suas entidades;
- implementar controles internos fundamentados na gestão de risco, que privilegiará ações estratégicas de prevenção antes de processos sancionadores;
- avaliar as propostas de criação, expansão ou aperfeiçoamento de políticas públicas e de concessão de incentivos fiscais e aferir, sempre que possível, seus custos e benefícios;
- manter processo decisório orientado pelas evidências, pela conformidade legal, pela qualidade regulatória, pela desburocratização e pelo apoio à participação da sociedade;
- editar e revisar atos normativos, pautando-se pelas boas práticas regulatórias e pela legitimidade, estabilidade e coerência do ordenamento jurídico e realizando consultas públicas sempre que conveniente;
- definir formalmente as funções, as competências e as responsabilidades das estruturas e dos arranjos institucionais; e
- promover a comunicação aberta, voluntária e transparente das atividades e dos resultados da organização, de maneira a fortalecer o acesso público à informação.

6. Como Mecanismos para o exercício da governança pública, temos:

- Liderança, que compreende conjunto de práticas de natureza humana ou comportamental exercida nos principais cargos das organizações, para assegurar a existência das condições mínimas para o exercício da boa governança, quais sejam:
 1. integridade;
 2. competência;
 3. responsabilidade; e
 4. motivação;
- Estratégia, que compreende a definição de diretrizes, objetivos, planos e ações, além de critérios de priorização e alinhamento entre organizações e partes interessadas, para que os serviços e produtos de responsabilidade da organização alcancem o resultado pretendido; e
- Controle, que compreende processos estruturados para mitigar os possíveis riscos com vistas ao alcance dos objetivos institucionais e para garantir a execução ordenada, ética, econômica, eficiente e eficaz das atividades da organização, com preservação da legalidade e da economicidade no dispêndio de recursos públicos

7. Considerando que compete a DTI:

- propor políticas e diretrizes de tecnologia da informação e comunicação alinhadas à Política de Governança Digital;
- elaborar e propor o plano diretor de tecnologia da informação e comunicação do INSS;
- monitorar a execução do plano diretor de tecnologia da informação e comunicação do INSS;
- identificar e propor a priorização de projetos e contratações de tecnologia da informação e comunicação, por meio da composição dos interesses das diferentes áreas demandantes, de modo a compatibilizar a alocação de recursos às diretrizes estratégicas estabelecidas pelo INSS;
- assessorar na implementação das ações de segurança da informação necessárias ao cumprimento da Política Nacional de Segurança da Informação, nos termos do Decreto nº 9.637, de 26 de dezembro de 2018;
- propor e monitorar a política e os planos de segurança da informação e comunicações do INSS, nos termos do Decreto nº 9.637, de 2018; e
- propor e acompanhar indicadores de desempenho, planos e normas internas relativas à gestão de tecnologia da informação e comunicação.

8. O acesso a internet, por meio da rede dados do INSS, é uma concessão e deve ter seu uso orientado para a execução de atividades do Instituto e os acessos devem ser liberados com perfis previamente definidos pelo órgão responsável pelos serviços de TIC, cabendo a DTI através da área responsável pela gestão TIC no âmbito do INSS definir aspectos à plataforma tecnológica, gestão operacional, forma de autenticação e sustentação do domínio de rede do INSS.

9. Necessário se faz estabelecer regras de acesso e utilização da internet para todos os servidores e colaboradores, vinculados direta ou indiretamente ao INSS, servidores e empregados de entidades e órgãos da Administração Pública ou privados que necessitem ou estejam autorizados a acessar a Internet a partir da rede corporativa do Instituto, bem como definir os tipos de perfis de acesso e responsáveis pela autorização destes acessos. O processo de solicitação e autorização de acesso à internet compreenderá os seguintes perfis:

I - Perfil 1: Perfil Restrito, inicialmente atribuído a usuários com maior restrição de acesso à Internet, permitindo acesso somente a sítios governamentais, instituições bancárias e sítios considerados de interesse do INSS;

II - Perfil 2: Perfil Básico, inicialmente atribuído a estagiários, recepcionistas e usuários externos, permitindo acesso a todos os sítios permitidos pelo Perfil 1 e a sítios de provedores de e-mail pessoal e instituições de ensino;

III - Perfil 3: Perfil Padrão, para os servidores do quadro do Instituto, permitindo acesso a todos os sítios da Internet, exceto aqueles que contêm veiculação de material em áudio e vídeo; e

IV - Perfil 4: Perfil Avançado, atribuído preferencialmente a servidores do quadro do Instituto e estagiários que desempenham funções relacionadas a Comunicação Social, Desenvolvimento de Pessoas e gestores, respeitado o princípio da necessidade de conhecer e demandando designação dos Autorizadores deste Perfil, permitindo o acesso a todos os sítios da Internet, incluindo sítios que veiculam material em áudio e vídeo (streaming), sítios de compartilhamento de vídeos, blogs e redes sociais.

10. O acesso de usuários externos das entidades que compõem o Poder Público será concedido mediante o estabelecimento em convênio, contrato, acordo de cooperação técnica ou instrumento congênere, especificamente firmados com o INSS para este fim.

11. Cabe ainda definir em normativo quais são os deveres e responsabilidades do usuário interno ou

externo, inclusive sob as punições pela utilização indevida de seu acesso a internet no âmbito do INSS.

12. Sugere-se que a autorização para atribuição dos perfis de níveis 1 à 3 poderá ser dado pelo Presidente do INSS, Diretores, Coordenadores-Gerais, Chefes de Assessoria de Comunicação Social nas Superintendências-Regionais, Assessor de Comunicação Social (Administração Central), Auditor-Geral, Corregedor-Geral, Procuradores-Regionais, Procurador-Geral da PFE-INSS, Superintendentes-Regionais e Gerente-Executivo e Gerente de Agência da Previdência Social – APS, já o perfil de nível 4 poderá ser autorizado pelo Presidente do INSS, Diretores, Coordenadores-Gerais, Chefes de Assessoria de Comunicação Social nas Superintendências-Regionais, Assessor de Comunicação Social (Administração Central), Auditor-Geral, Corregedor-Geral, Procuradores-Regionais, Procurador-Geral da PFE-INSS, Superintendentes-Regionais e Gerente-Executivo.
13. Diante do exposto propomos a elaboração de Portaria que regulamente e defina o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.
14. Sugere-se o encaminhamento da presente Nota Técnica com a correspondente Minuta de Portaria à Coordenação de Governança em TIC desta Diretoria (CGOV).

Brasília/DF, 14 de março de 2022.

JOÃO RODRIGUES DA SILVA FILHO
Coordenador-Geral de Infraestrutura e Operações



Documento assinado eletronicamente por **JOAO RODRIGUES DA SILVA FILHO**, **Coordenador(a) Geral**, em 14/03/2022, às 12:31, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **6746748** e o código CRC **D09D3E8C**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações

MINUTA DE PORTARIA CGIN/INSS Nº 6747061, DE 14 DE MARÇO DE 2022

Disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.

O DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO - INSS, no uso da competência que lhe confere o Decreto nº 9.746, de 8 de abril de 2019, e tendo em vista o que consta no Processo Administrativo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Esta norma se aplica a todos os servidores e colaboradores, vinculados direta ou indiretamente ao INSS, bem como a servidores e empregados de entidades e órgãos da Administração Pública ou privados que necessitem ou estejam autorizados a acessar a Internet a partir da rede corporativa do Instituto.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União – AGU que atuem na consultoria, assessoramento jurídico e na representação judicial e extrajudicial do INSS e os servidores vinculados à Subsecretaria da Perícia Médica Federal.

Art. 2º Para os efeitos desta norma, ficam estabelecidos os seguintes conceitos e definições:

- I - Autorizador: ocupantes de cargo responsáveis pela autorização da concessão de perfis de acesso para usuários finais de sua área de abrangência;
- II - Internet: rede mundial que interliga computadores de diferentes tipos e dimensões e permite a comunicação entre pessoas e organizações, independentemente da localização geográfica;
- III - Intranet: rede de computadores administrada pelo INSS, que utiliza os mesmos serviços e tecnologias disponíveis na rede mundial;
- IV - Perfil de acesso: atributo que estabelece as categorias de sítios acessíveis e tipos de arquivos que podem ser recebidos ou transmitidos pelos usuários;
- V - Proxy: ferramenta que desempenha a função de conexão do computador local à rede externa (Internet);
- VI - Sítio: conjunto de informações ou serviços disponíveis na Internet ou na Intranet, organizados em páginas eletrônicas e acessíveis por meio de endereços que identificam, de forma padronizada, sua origem e conteúdo;
- VII - Usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal - APF, formalizada por meio da assinatura do Termo de Responsabilidade; e
- VIII - VPN: Rede Privada Virtual (Virtual Private Network) construída sobre a infraestrutura de uma rede pública, possibilitando a conexão de dois computadores por meio de uma rede pública.

Art. 3º O acesso pelos usuários à Internet disponibilizado pelo INSS deverá pautar-se pelas seguintes diretrizes:

- I - Seu uso se dará exclusivamente em razão de trabalho e de acordo com os procedimentos dispostos nesta Norma;
- II - Os recursos disponibilizados pelo INSS não poderão ser usados para quaisquer propósitos ilegais ou proibidos, que possam danificar, desativar, sobrecarregar ou prejudicar qualquer área, serviço ou conteúdo, ou interferir no uso e execução das atividades laborais de outros usuários;
- III - O volume de tráfego de Internet e os endereços web visitados poderão ser monitorados, visando assegurar o cumprimento desta norma; e
- IV - O acesso à Internet para propósitos particulares ou estranhos às atividades do INSS poderá ser bloqueado, sem prévia comunicação ao usuário e sem prejuízo das demais sanções aplicáveis.

Art. 4º O acesso aos sítios da Internet para todos os usuários será realizado mediante a atribuição de perfis de acesso, distribuídos nos seguintes níveis:

- I - Perfil 1: Perfil Restrito, inicialmente atribuído a usuários com maior restrição de acesso à Internet, permitindo acesso somente a sítios governamentais, instituições bancárias e sítios considerados de interesse do INSS;
- II - Perfil 2: Perfil Básico, inicialmente atribuído a estagiários, recepcionistas e usuários externos, permitindo acesso a todos os sítios permitidos pelo Perfil 1 e a sítios de provedores de e-mail pessoal e instituições de ensino;
- III - Perfil 3: Perfil Padrão, para os servidores do quadro do Instituto, permitindo acesso a todos os sítios da Internet, exceto redes sociais e aqueles que contêm veiculação de material em áudio e vídeo; e
- IV - Perfil 4: Perfil Avançado, atribuído preferencialmente a servidores, colaboradores e estagiários que desempenham funções relacionadas a Comunicação Social, Desenvolvimento de Pessoas e gestores, dentre outras situações específicas, respeitado o princípio da necessidade de conhecer e demandando designação dos Autorizadores deste Perfil, permitindo o acesso a todos os sítios da Internet, incluindo sítios que veiculam material em áudio e vídeo (streaming), sítios de compartilhamento de vídeos, blogs e redes sociais.

§ 1º O perfil concedido a agentes externos será de caráter temporário, com validade equivalente à vigência do trabalho a ser executado.

§ 2º Os processos de alteração, bloqueio, liberação e categorização de sítios, assim como a criação e/ou alterações de perfis de acesso descritos nesta Norma, quando necessários, serão definidos pela Diretoria de Tecnologia da Informação e Inovação – DTI.

§ 3º Os novos usuários que não tiverem um perfil de acesso atribuído deverão ser direcionados para uma página da Intranet contendo orientações e normas relacionadas ao acesso à Internet no INSS, definidas pela DTI.

Art. 5º O acesso à Intranet e Internet a partir da rede de dados corporativa nas dependências do INSS e aos demais órgãos da Administração Pública Direta e Indireta, de qualquer das esferas de governo, será concedido exclusivamente a servidores e empregados públicos, efetivos ou ocupantes de cargo em comissão.

§ 1º O acesso de usuários externos das entidades que compõem o Poder Público será concedido mediante o estabelecimento em convênio, contrato, acordo de cooperação técnica ou instrumento congênere, especificamente firmados com o INSS para este fim.

§ 2º O gestor ou Coordenador-Geral da área responsável pelo convênio, contrato, acordo de cooperação técnica ou instrumento congênere assumirá o papel de Autorizador do serviço de acesso à Internet para os usuários externos, e deverá fundamentar as solicitações com base no instrumento.

§ 3º Poderão ser concedidos acessos temporários para auditores de controle interno e externo, vinculados à Controladoria-Geral da União – CGU ou ao Tribunal de Contas da União - TCU, no uso de suas atribuições.

Art. 6º Nas situações em que a atividade necessitar, o acesso à Internet por terceirizados deverá ser concedido a partir da infraestrutura de rede do INSS, desde que preenchidos os seguintes requisitos:

I - O contrato de prestação de serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

II - A empresa contratada deverá manter com seus funcionários Termo de Confidencialidade;

III - O contrato de prestação de serviços deverá prever a necessidade de acesso à Internet a partir das dependências do INSS; e

IV - O Autorizador, que para estes fins será o gestor do contrato ou o responsável pela área requisitante do serviço, deverá fundamentar as necessidades de acesso dos empregados da contratada, definindo os recursos que serão disponibilizados, endereços da Intranet e Internet necessários para o desenvolvimento das atividades e eventuais restrições a dias e horários para realização do acesso.

Art. 7º A conexão de equipamentos pessoais de visitantes à rede do INSS, quando necessária e motivada pelo interesse da Administração, deverá ser previamente autorizada pelo gestor da unidade onde o equipamento será utilizado.

Parágrafo único. Só será permitida a utilização da rede local por visitantes, caso seus equipamentos atendam a todos os requisitos estabelecidos pela DTI e o acesso se dará, exclusivamente, à Internet, sendo vedado o acesso ao conteúdo disponibilizado na Intranet.

Art. 8º A todos os perfis de acesso descritos nesta Norma aplicam-se as restrições de acesso a sítios que:

I - Contenham material pornográfico ou obsceno;

II - Contenham material ilegal;

III - Disponibilizem jogos, inclusive os da Internet (on line);

IV - Contenham material impróprio, ofensivo, preconceituoso ou discriminatório, que façam apologia à violência, ao terrorismo e às drogas; e

V - Contenha e/ou divulgue conteúdo de violação de direito autoral (pirataria) e/ou execução de quaisquer tipos ou formas de fraudes.

Art. 9º O processo de atribuição de acesso à Internet seguirá as seguintes diretrizes:

I - A atribuição dos perfis de acesso à Internet será feita pelos Autorizadores, de forma fundamentada e respeitando o princípio da necessidade de conhecer, de acordo com a tabela abaixo:

Perfil	Autorizador
Perfil 1, 2, 3	Presidente do INSS, Diretores, Coordenadores-Gerais, Chefes de Assessoria de Comunicação Social nas Superintendências-Regionais, Assessor de Comunicação Social (Administração Central) Auditor-Geral, Corregedor-Geral, Procuradores-Regionais, Procurador-Geral da PFE-INSS, Superintendentes-Regionais, Gerente-Executivo e Gerente de Agência da Previdência Social - APS.
Perfil 4	Presidente do INSS, Diretores, Coordenadores-Gerais, Chefes de Assessoria de Comunicação Social nas Superintendências-Regionais, Assessor de Comunicação Social (Administração Central), Auditor-Geral, Corregedor-Geral, Procuradores-Regionais, Procurador-Geral da PFE-INSS, Superintendentes-Regionais e Gerentes-Executivos.

II - Nos casos de novos usuários de rede (LDAP), criados por meio de registro de chamado técnico, quando o solicitante não indicar o perfil de acesso à internet, será atribuído o Perfil 1;

III - Para fins de alteração do perfil de acesso, os usuários deverão preencher o Formulário de Solicitação de Acesso à Internet (Anexo II) e providenciar a assinatura no sistema SEI pelo Autorizador do acesso; e

IV - Ao registrar a solicitação, deve-se anexar o Formulário de Solicitação de Acesso à Internet (Anexo I) devidamente preenchido e assinado no sistema SEI (pelo solicitante e autorizador), conforme documento nato digital ou digitalizado no formato PDF.

Art. 10. A solicitação para perfis de acesso em caráter temporário, realizada mediante o Formulário de Solicitação de Acesso à Internet (Anexo II), deverá conter a motivação da necessidade e a data de início e de expiração do acesso.

Art. 11. As responsabilidades ficam estabelecidas na seguinte forma:

I - O usuário deverá:

a) Preencher os requisitos e termos estabelecidos nesta Norma;

b) Estar devidamente autorizado a utilizar a Internet nas formas estabelecidas nesta Norma;

c) Fazer uso da Internet de forma responsável e segura, utilizando o acesso exclusivamente em razão de trabalho, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal; e

d) Impedir a divulgação e compartilhamento das chaves de segurança atribuídas, que são pessoais e intransferíveis;

II - O autorizador deverá:

- a) Conceder os perfis de acesso à Internet rigorosamente de acordo com as atribuições dos usuários de sua abrangência, observando os normativos do INSS;
- b) Verificar periodicamente o uso dos acessos concedidos e, sempre que necessário, solicitar alteração dos perfis de acesso dos usuários de sua abrangência; e
- c) Reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR-INSS;

III - A área responsável pela gestão de TI no INSS deverá:

- a) Monitorar os acessos à internet e sua utilização de acordo com as diretrizes estabelecidas nesta Norma; e
- b) Identificar os casos de mau uso da Internet e adotar uma ou mais das seguintes providências:
 1. Alertar o usuário, responsável pelo acesso, e o Autorizador, responsável pela concessão, acerca do uso indevido da internet; e
 2. Nos casos de reincidência, solicitar a revogação do acesso à internet concedido ao usuário e encaminhar a documentação que comprova a má utilização do acesso concedido à Corregedoria do INSS, para análise e adoção das medidas cabíveis.

Art. 12. Configura-se como uso indevido da Internet:

- I - Acessar a Internet disponibilizada pelo INSS sem estar devidamente autorizado, conforme estabelecido nesta Norma;
- II - Não manifestar concordância com as regras estabelecidas nesta Norma e nas demais aplicáveis;
- III - Fazer uso dos recursos de Internet disponibilizados pelo INSS para fins alheios ao trabalho, em discordância com os procedimentos dispostos nesta Norma, sem prejuízo de demais normatizações vigentes na Administração Pública Federal;
- IV - Utilizar os serviços extrapolando os privilégios do perfil de acesso que lhe foi designado;
- V - Divulgar e/ou compartilhar as chaves de segurança, que são pessoais e intransferíveis, permitindo a utilização por terceiros do perfil que lhe foi atribuído;
- VI - Praticar atos de comercialização de produtos e serviços, em proveito próprio ou de terceiros, que não atendam os interesses do INSS;
- VII - utilizar recursos ou dispositivos para acesso a computadores ou redes externas ao INSS com o objetivo de obter informações não autorizadas ou provocar a interrupção de serviços de rede;
- VIII - utilizar modem ou dispositivo de rede que interligue a rede interna do INSS a outras redes ou à Internet;
- IX - Expor, armazenar, distribuir, editar, gravar ou compartilhar, através do uso dos recursos computacionais e de comunicação do INSS, arquivos estranhos às atividades do INSS e não autorizados pela chefia imediata;
- X - Realizar qualquer atividade que apoie ou facilite o vazamento de dados;
- XI - Baixar arquivos ou programas da Internet que contrariem as diretrizes da POSIN vigente; e
- XII - Utilizar proxy não disponibilizado pelo INSS.

Art. 13. O acesso à Internet é passível de registro e monitoração, incluindo quaisquer dados transmitidos pela rede do INSS.

§ 1º Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a ETIR-INSS deverá ser imediatamente acionada, para tomar as providências necessárias a fim de sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação do INSS;

§ 2º As ocorrências de mau uso do acesso à Internet não previstas nesta norma, assim como os casos de dúvidas em relação à aplicação das disposições aqui estabelecidas, deverão ser encaminhadas à DTI para registro, análise e avaliação da necessidade de alterações de acordo com o processo de governança em vigência no INSS;

§ 3º O descumprimento desta Norma poderá acarretar ao usuário as penalidades previstas nas políticas e procedimentos internos e/ou, na forma da lei, responsabilidade administrativa, civil e criminal.

Art. 14. Esta portaria entra em vigor em 1º de abril de 2022.

GUILHERME GASTALDELLO PINHEIRO SERRANO

Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **JOAO RODRIGUES DA SILVA FILHO**, **Coordenador(a) Geral**, em 14/03/2022, às 12:31, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **6747061** e o código CRC **2F7BCDC3**.

ANEXO I

PORTARIA Nº XX/DTI/INSS, DE XX DE XXXXXXXXX DE 2022

FORMULÁRIO DE SOLICITAÇÃO DE ACESSO À INTERNET

Informações do Usuário	
Nome:	Login de Rede:
Matrícula:	CPF:

Lotação:	Código do Setor:	
Telefone: ()	E-mail:	@inss.gov.br
		@agu.gov.br

☐	Perfil 1	
☐	Perfil 2	
☐	Perfil 3	
☐	Perfil 4	
☐	Terceirizados	Data de expiração:
	Contrato nº ou Convênio	Data de expiração

Descreva abaixo a justificativa e quais páginas devem ser acessadas pelo usuário terceirizado:

Declaro ter conhecimento e estar de acordo com as regras estabelecidas na Norma de Uso da internet do INSS (Resolução nº 12/CEGOV/INSS, de 1 de setembro de 2020) e demais normas aplicáveis.

, de de .
Local e Data

Informações do Autorizante		
Nome:		
Lotação:	Código do Setor:	
Telefone: ()	E-mail:	@inss.gov.br

Assinatura do Solicitante

Autorizo a concessão de Acesso Internet

, de de .
Local e Data

Assinatura do Autorizador



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Infraestrutura e Operações

DESPACHO

Coordenação-Geral De Infraestrutura e Operações, em 14/03/2022.

Ref.: Processo nº 35014.047735/2020-84.

Int.: Coordenação-Geral De Infraestrutura e Operações.

Ass.: Minuta de Portaria que regulamenta e define conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.

1. Trata-se de minuta de ato administrativo que regulamenta e define conjunto de perfis de acesso de internet, competências e conteúdo de acesso para cada perfil.
2. Encaminhamos Nota Técnica e Minuta de Portaria para avaliação da Coordenação de Governança e Planejamento de Tecnologia da Informação e Comunicação.
3. Feitas as considerações, encaminhe-se à CGOV.

Marcelo Vasques

Técnico do Seguro Social - Matrícula 1375892

Apoio DTI



Documento assinado eletronicamente por **MARCELO VASQUES, Técnico do Seguro Social**, em 14/03/2022, às 12:44, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **6750557** e o código CRC **AA59369F**.



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria De Tecnologia da Informação e Inovação
Coordenação De Governança e Planejamento De Tecnologia da Informação e Comunicação

MINUTA DE PORTARIA CGIN/INSS Nº 6747061, DE 14 DE MARÇO DE 2022

Disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.

O DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO - INSS, no uso da competência que lhe confere o Decreto nº 9.746, de 8 de abril de 2019, e tendo em vista o que consta no Processo Administrativo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Esta Norma se aplica a todos os servidores e colaboradores vinculados direta ou indiretamente ao INSS, bem como a servidores e empregados de entidades e órgãos da Administração Pública ou privados que necessitem ou estejam autorizados a acessar a Internet a partir da rede corporativa do Instituto.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União – AGU que atuarem na consultoria, assessoramento jurídico e na representação judicial e extrajudicial do INSS e os servidores vinculados à Subsecretaria da Perícia Médica Federal.

Art. 2º Para os efeitos desta Norma, ficam estabelecidos os seguintes conceitos e definições:

- I - Autorizador: ocupante de cargo responsável pela autorização da concessão de perfis de acesso para usuários finais de sua área de abrangência;
- II - Internet: rede mundial que interliga computadores de diferentes tipos e dimensões e permite a comunicação entre pessoas e organizações, independentemente da localização geográfica;
- III - Intranet: rede de computadores administrada pelo INSS, que utiliza os mesmos serviços e tecnologias disponíveis na rede mundial;
- IV - Perfil de acesso: atributo que estabelece as categorias de sítios acessíveis e tipos de arquivos que podem ser recebidos ou transmitidos pelos usuários;
- V - Proxy: ferramenta que desempenha a função de conexão do computador local à rede externa (Internet);
- VI - Sítio: conjunto de informações ou serviços disponíveis na Internet ou na Intranet, organizados em páginas eletrônicas e acessíveis por meio de endereços que identificam, de forma padronizada, sua origem e conteúdo;
- VII - Usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada, para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal - APF, formalizada por meio da assinatura do Termo de Responsabilidade; e
- VIII - VPN: Rede Privada Virtual (Virtual Private Network) construída sobre a infraestrutura de uma rede pública, possibilitando a conexão de dois computadores por meio de uma rede pública.

Art. 3º O acesso pelos usuários à Internet disponibilizado pelo INSS deverá pautar-se pelas seguintes diretrizes:

- I - Seu uso se dará exclusivamente em razão de trabalho e de acordo com os procedimentos dispostos nesta Norma;
- II - Os recursos disponibilizados pelo INSS não poderão ser usados para quaisquer propósitos ilegais ou proibidos, que possam danificar, desativar, sobrecarregar ou prejudicar qualquer área, serviço ou conteúdo, ou interferir no uso e execução das atividades laborais de outros usuários;
- III - O volume de tráfego de Internet e os endereços web visitados poderão ser monitorados, visando assegurar o cumprimento desta Norma; e
- IV - O acesso à Internet para propósitos particulares ou estranhos às atividades do INSS poderá ser bloqueado, sem prévia comunicação ao usuário e sem prejuízo das demais sanções aplicáveis.

Art. 4º O acesso aos sítios da Internet para todos os usuários será realizado mediante a atribuição de perfis de acesso, distribuídos nos seguintes níveis:

- I - Perfil 1: Perfil Restrito, inicialmente atribuído a usuários com maior restrição de acesso à Internet, permitindo acesso somente a sítios governamentais, instituições bancárias e sítios considerados de interesse do INSS;
- II - Perfil 2: Perfil Básico, inicialmente atribuído a estagiários, recepcionistas e usuários externos, permitindo acesso a todos os sítios permitidos pelo Perfil 1 e a sítios de provedores de e-mail pessoal e instituições de ensino;
- III - Perfil 3: Perfil Padrão, para os servidores do quadro do Instituto, permitindo acesso a todos os sítios da Internet, exceto redes sociais e aqueles que contêm veiculação de material em áudio e vídeo; e
- IV - Perfil 4: Perfil Avançado, atribuído preferencialmente a servidores, colaboradores e estagiários que desempenham funções relacionadas a Comunicação Social, Desenvolvimento de Pessoas e gestores, dentre outras situações específicas, respeitado o princípio da necessidade de conhecer e demandando designação dos Autorizadores deste Perfil, permitindo o acesso a todos os sítios da Internet, incluindo sítios que veiculam material em áudio e vídeo (streaming), sítios de compartilhamento de vídeos, blogs e redes sociais.

§ 1º O perfil concedido a agentes externos será de caráter temporário com validade equivalente à vigência do trabalho a ser executado.

§ 2º Os processos de alteração, bloqueio, liberação e categorização de sítios, assim como a criação e/ou alterações de perfis de acesso descritos nesta Norma, quando necessários, serão definidos pela Diretoria de Tecnologia da Informação e Inovação – DTI.

§ 3º Os novos usuários que não tiverem um perfil de acesso atribuído deverão ser direcionados para uma página da Intranet contendo orientações e normas relacionadas ao acesso à Internet no INSS, definidas pela DTI.

Art. 5º O acesso à Intranet e Internet a partir da rede de dados corporativa nas dependências do INSS e aos demais órgãos da Administração Pública Direta e Indireta, de qualquer das esferas de governo, será concedido exclusivamente a servidores e empregados públicos efetivos ou ocupantes de cargo em comissão.

§ 1º O acesso de usuários externos das entidades que compõem o Poder Público será concedido mediante o estabelecimento em convênio, contrato, acordo de cooperação técnica ou instrumento congênere, especificamente firmados com o INSS para este fim.

§ 2º O gestor ou Coordenador-Geral da área responsável pelo convênio, contrato, acordo de cooperação técnica ou instrumento congênere assumirá o papel de Autorizador do serviço de acesso à Internet para os usuários externos, e deverá fundamentar as solicitações com base no instrumento.

§ 3º Poderão ser concedidos acessos temporários para auditores de controle interno e externo, vinculados à Controladoria-Geral da União – CGU ou ao Tribunal de Contas da União - TCU, no uso de suas atribuições.

Art. 6º Nas situações em que a atividade necessitar o acesso à Internet por terceirizados, este deverá ser concedido a partir da infraestrutura de rede do INSS, desde que preenchidos os seguintes requisitos:

I - O contrato de prestação de serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

II - A empresa contratada deverá manter com seus funcionários Termo de Confidencialidade;

III - O contrato de prestação de serviços deverá prever a necessidade de acesso à Internet a partir das dependências do INSS; e

IV - O Autorizador, que para estes fins será o gestor do contrato ou o responsável pela área requisitante do serviço, deverá fundamentar as necessidades de acesso dos empregados da contratada, definindo os recursos que serão disponibilizados, endereços da Intranet e Internet necessários para o desenvolvimento das atividades e eventuais restrições a dias e horários para realização do acesso.

Art. 7º A conexão de equipamentos pessoais de visitantes à rede do INSS, quando necessária e motivada pelo interesse da Administração, deverá ser previamente autorizada pelo gestor da unidade onde o equipamento será utilizado.

Parágrafo único. Somente será permitida a utilização da rede local por visitantes caso seus equipamentos atendam a todos os requisitos estabelecidos pela DTI e o acesso se dará, exclusivamente à Internet, sendo vedado o acesso ao conteúdo disponibilizado na Intranet.

Art. 8º A todos os perfis de acesso descritos nesta Norma, aplicam-se as restrições de acesso a sítios que:

I - Contenham material pornográfico ou obsceno;

II - Contenham material ilegal;

III - Disponibilizem jogos, inclusive os da Internet (on line);

IV - Contenham material impróprio, ofensivo, preconceituoso ou discriminatório, que façam apologia à violência, ao terrorismo e às drogas; e

V - Contenham e/ou divulguem conteúdo de violação de direito autoral (pirataria) e/ou execução de quaisquer tipos ou formas de fraudes.

Art. 9º O processo de atribuição de acesso à Internet seguirá as seguintes diretrizes:

I - A atribuição dos perfis de acesso à Internet será feita pelos Autorizadores, de forma fundamentada e respeitando o princípio da necessidade de conhecer, de acordo com a tabela abaixo:

Perfil	Autorizador
Perfil 1, 2, 3	Presidente do INSS, Diretores, Coordenadores-Gerais, Chefes de Assessoria de Comunicação Social nas Superintendências-Regionais, Assessor de Comunicação Social (Administração Central), Auditor-Geral, Corregedor-Geral, Procuradores-Regionais, Procurador-Geral da PFE-INSS, Superintendentes-Regionais, Gerentes-Executivos e Gerentes de Agências da Previdência Social - APS.
Perfil 4	Presidente do INSS, Diretores, Coordenadores-Gerais, Chefes de Assessoria de Comunicação Social nas Superintendências-Regionais, Assessor de Comunicação Social (Administração Central), Auditor-Geral, Corregedor-Geral, Procuradores-Regionais, Procurador-Geral da PFE-INSS, Superintendentes-Regionais e Gerentes-Executivos.

II - Nos casos de novos usuários de rede (LDAP) criados por meio de registro de chamado técnico, quando o solicitante não indicar o perfil de acesso à internet, será atribuído o Perfil 1;

III - Para fins de alteração do perfil de acesso, os usuários deverão preencher o Formulário de Solicitação de Acesso à Internet (Anexo I) e providenciar a assinatura no sistema SEI pelo Autorizador do acesso; e

IV - Ao registrar a solicitação, deve-se anexar o Formulário de Solicitação de Acesso à Internet (Anexo I) devidamente preenchido e assinado no sistema SEI (pelo solicitante e Autorizador), conforme documento nato digital ou digitalizado no formato PDF.

Art. 10. A solicitação para perfis de acesso em caráter temporário, realizada mediante o Formulário de Solicitação de Acesso à Internet (Anexo I), deverá conter a motivação da necessidade e a data de início e de expiração do acesso.

Art. 11. As responsabilidades ficam estabelecidas na seguinte forma:

I - O usuário deverá:

a) Preencher os requisitos e termos estabelecidos nesta Norma;

b) Estar devidamente autorizado a utilizar a Internet nas formas estabelecidas nesta Norma;

c) Fazer uso da Internet de forma responsável e segura, utilizando o acesso exclusivamente em razão de trabalho, cumprindo os procedimentos dispostos nesta Norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal; e

d) Impedir a divulgação e compartilhamento das chaves de segurança atribuídas, que são pessoais e intransferíveis;

II - O autorizador deverá:

a) Conceder os perfis de acesso à Internet rigorosamente de acordo com as atribuições dos usuários de sua abrangência, observando os normativos do INSS;

b) Verificar periodicamente o uso dos acessos concedidos e, sempre que necessário, solicitar alteração dos perfis de acesso dos usuários de sua abrangência; e

c) Reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR-INSS;

III - A área responsável pela gestão de TI no INSS deverá:

a) Monitorar os acessos à internet e sua utilização de acordo com as diretrizes estabelecidas nesta Norma; e

b) Identificar os casos de mau uso da Internet e adotar uma ou mais das seguintes providências:

1. Alertar o usuário, responsável pelo acesso, e o Autorizador, responsável pela concessão, acerca do uso indevido da internet; e
2. Nos casos de reincidência, solicitar a revogação do acesso à internet concedido ao usuário e encaminhar a documentação que comprova a má utilização do acesso concedido, à Corregedoria do INSS, para análise e adoção das medidas cabíveis.

Art. 12. Configura-se como uso indevido da Internet:

- I - Acessar a Internet disponibilizada pelo INSS sem estar devidamente autorizado, conforme estabelecido nesta Norma;
- II - Não manifestar concordância com as regras estabelecidas nesta Norma e nas demais aplicáveis;
- III - Fazer uso dos recursos de Internet disponibilizados pelo INSS para fins alheios ao trabalho, em discordância com os procedimentos dispostos nesta Norma, sem prejuízo de demais normatizações vigentes na Administração Pública Federal;
- IV - Utilizar os serviços extrapolando os privilégios do perfil de acesso que lhe foi designado;
- V - Divulgar e/ou compartilhar as chaves de segurança, que são pessoais e intransferíveis, permitindo a utilização por terceiros do perfil que lhe foi atribuído;
- VI - Praticar atos de comercialização de produtos e serviços, em proveito próprio ou de terceiros, que não atendam aos interesses do INSS;
- VII - Utilizar recursos ou dispositivos para acesso a computadores ou redes externas ao INSS com o objetivo de obter informações não autorizadas ou provocar a interrupção de serviços de rede;
- VIII - Utilizar modem ou dispositivo de rede que interligue a rede interna do INSS a outras redes ou à Internet;
- IX - Expor, armazenar, distribuir, editar, gravar ou compartilhar, através do uso dos recursos computacionais e de comunicação do INSS, arquivos estranhos às atividades do INSS e não autorizados pela chefia imediata;
- X - Realizar qualquer atividade que apoie ou facilite o vazamento de dados;
- XI - Baixar arquivos ou programas da Internet que contrariem as diretrizes da POSIN vigente; e
- XII - Utilizar proxy não disponibilizado pelo INSS.

Art. 13. O acesso à Internet é passível de registro e monitoração, incluindo quaisquer dados transmitidos pela rede do INSS.

§ 1º Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a ETIR-INSS deverá ser imediatamente acionada para tomar as providências necessárias, a fim de sanar as causas, podendo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação do INSS;

§ 2º As ocorrências de mau uso do acesso à Internet não previstas nesta Norma, assim como os casos de dúvidas em relação à aplicação das disposições aqui estabelecidas, deverão ser encaminhadas à DTI para registro, análise e avaliação da necessidade de alterações de acordo com o processo de governança em vigência no INSS;

§ 3º O descumprimento desta Norma poderá acarretar ao usuário as penalidades previstas nas políticas e procedimentos internos e/ou, na forma da lei, responsabilidade administrativa, civil e criminal.

Art. 14. Esta portaria entra em vigor em 1º de abril de 2022.

GUILHERME GASTALDELLO PINHEIRO SERRANO

Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **MARCELO GENU BESERRA, Coordenador(a) de Governança e Planejamento de Tecnologia da Informação e Comunicação**, em 14/03/2022, às 17:22, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **6755345** e o código CRC **ACE93DCB**.

ANEXO I

PORTARIA Nº XX/DTI/INSS, DE XX DE XXXXXXXXXX DE 2022

FORMULÁRIO DE SOLICITAÇÃO DE ACESSO À INTERNET

Informações do Usuário		
Nome:	Login de Rede:	
Matrícula:	CPF:	
Lotação:	Código do Setor:	
Telefone: ()	E-mail:	@inss.gov.br
		@agu.gov.br

☐	Perfil 1		
☐	Perfil 2		
☐	Perfil 3		
☐	Perfil 4		
☐	Terceirizados	Contrato nº ou Convênio	Data de expiração

Descreva abaixo a justificativa e quais páginas devem ser acessadas pelo usuário terceirizado:

Declaro ter conhecimento e estar de acordo com as regras estabelecidas na Norma de Uso da internet do INSS (Resolução nº 12/CEGOV/INSS, de 1 de setembro de 2020) e demais normas aplicáveis.

, de de .
Local e Data

Informações do Autorizante		
Nome:		
Lotação:	Código do Setor:	
Telefone: ()	E-mail:	@inss.gov.br

Assinatura do Solicitante

Autorizo a concessão de Acesso Internet

_____, _____ de _____ de _____.
Local e Data

Assinatura do Autorizador



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação
Coordenação de Governança e Planejamento de TIC

DESPACHO

Coordenação de Governança e Planejamento de TIC, em 14/03/2022.

Ref.: Processo nº 35014.047735/2020-84.

Int.: Coordenação-Geral De Infraestrutura e Operações.

Ass.: Minuta de Portaria que regulamenta e define conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.

1. Trata-se de minuta de ato administrativo que regulamenta e define conjunto de perfis de acesso de internet, competências e conteúdo de acesso para cada perfil.
2. Feita a revisão na minuta propostas encaminhamos à DTI para consolidação do ato final.

MARCELO GENU BESERRA

Coordenador de Governança e Planejamento de TIC



Documento assinado eletronicamente por **MARCELO GENU BESERRA**, **Coordenador(a) de Governança e Planejamento de Tecnologia da Informação e Comunicação**, em 14/03/2022, às 17:21, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **6757334** e o código CRC **B07268C4**.



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria De Tecnologia da Informação e Inovação

PORTARIA DTI/INSS Nº 71, DE 16 DE MARÇO DE 2022

Disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.

O DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO - INSS, no uso da competência que lhe confere o Decreto nº 9.746, de 8 de abril de 2019, e tendo em vista o que consta no Processo Administrativo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Regularizar e definir o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.

§ 1º Esta Portaria se aplica a todos os servidores e colaboradores vinculados direta ou indiretamente ao INSS, bem como a servidores e empregados de entidades e órgãos da Administração Pública ou privados que necessitem ou estejam autorizados a acessar a Internet a partir da rede corporativa do Instituto.

§ 2º Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União – AGU que atuarem na consultoria, assessoramento jurídico e na representação judicial e extrajudicial do INSS e os servidores vinculados à Subsecretaria da Perícia Médica Federal.

Art. 2º Para os efeitos desta Portaria, ficam estabelecidos os seguintes conceitos e definições:

I - Autorizador: ocupante de cargo responsável pela autorização da concessão de perfis de acesso para usuários finais de sua área de abrangência;

II - Internet: rede mundial que interliga computadores de diferentes tipos e dimensões e permite a comunicação entre pessoas e organizações, independentemente da localização geográfica;

III - Intranet: rede de computadores administrada pelo INSS, que utiliza os mesmos serviços e tecnologias disponíveis na rede mundial;

IV - Perfil de acesso: atributo que estabelece as categorias de sítios acessíveis e tipos de arquivos que podem ser recebidos ou transmitidos pelos usuários;

V - Proxy: ferramenta que desempenha a função de conexão do computador local à rede externa (Internet);

VI - Sítio: conjunto de informações ou serviços disponíveis na Internet ou na Intranet, organizados em páginas eletrônicas e acessíveis por meio de endereços que identificam, de forma padronizada, sua origem e conteúdo;

VII - Usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada, para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal - APF, formalizada por meio da assinatura do Termo de Responsabilidade; e

VIII - VPN: Rede Privada Virtual (Virtual Private Network) construída sobre a infraestrutura de uma rede pública, possibilitando a conexão de dois computadores por meio de uma rede pública.

Art. 3º O acesso pelos usuários à Internet disponibilizado pelo INSS deverá pautar-se pelas seguintes diretrizes:

I - seu uso se dará exclusivamente em razão de trabalho e de acordo com os procedimentos dispostos nesta Portaria;

II - os recursos disponibilizados pelo INSS não poderão ser usados para quaisquer propósitos ilegais ou proibidos, que possam danificar, desativar, sobrecarregar ou prejudicar qualquer área, serviço ou conteúdo, ou interferir no uso e execução das atividades laborais de outros usuários;

III - o volume de tráfego de Internet e os endereços web visitados poderão ser monitorados, visando assegurar o cumprimento desta Portaria; e

IV - o acesso à Internet para propósitos particulares ou estranhos às atividades do INSS poderá ser bloqueado, sem prévia comunicação ao usuário e sem prejuízo das demais sanções aplicáveis.

Art. 4º O acesso aos sítios da Internet para todos os usuários será realizado mediante a atribuição de perfis de acesso, distribuídos nos seguintes níveis:

I - Perfil 1: Perfil Restrito, inicialmente atribuído a usuários com maior restrição de acesso à Internet, permitindo acesso somente a sítios governamentais, instituições bancárias e sítios considerados de interesse do INSS;

II - Perfil 2: Perfil Básico, inicialmente atribuído a estagiários, recepcionistas e usuários externos, permitindo acesso a todos os sítios permitidos pelo Perfil 1 e a sítios de provedores de e-mail pessoal e instituições de ensino;

III - Perfil 3: Perfil Padrão, para os servidores do quadro do Instituto, permitindo acesso a todos os sítios da Internet, exceto redes sociais e aqueles que contêm veiculação de material em áudio e vídeo; e

IV - Perfil 4: Perfil Avançado, atribuído preferencialmente a servidores, colaboradores e estagiários que desempenham funções relacionadas a Comunicação Social, Desenvolvimento de Pessoas e gestores, dentre outras situações específicas, respeitado o princípio da necessidade de conhecer e demandando designação dos Autorizadores deste Perfil, permitindo o acesso a todos os sítios da Internet, incluindo sítios que veiculam material em áudio e vídeo (streaming), sítios de compartilhamento de vídeos, blogs e redes sociais.

§ 1º O perfil concedido a agentes externos será de caráter temporário com validade equivalente à vigência do trabalho a ser executado.

§ 2º Os processos de alteração, bloqueio, liberação e categorização de sítios, assim como a criação e/ou alterações de perfis de acesso descritos nesta Portaria, quando necessários, serão definidos pela Diretoria de Tecnologia da Informação e Inovação – Diretoria de Tecnologia da Informação e Inovação - DTI.

§ 3º Os novos usuários que não tiverem um perfil de acesso atribuído deverão ser direcionados para uma página da Intranet contendo orientações e normas relacionadas ao acesso à Internet no INSS, definidas pela DTI.

Art. 5º O acesso à Intranet e Internet a partir da rede de dados corporativa nas dependências do INSS e aos demais órgãos da Administração Pública Direta e Indireta, de qualquer das esferas de governo, será concedido exclusivamente a servidores e empregados públicos efetivos ou ocupantes de cargo em comissão.

§ 1º O acesso de usuários externos das entidades que compõem o Poder Público será concedido mediante o estabelecimento em convênio, contrato, acordo de cooperação técnica ou instrumento congênere, especificamente firmados com o INSS para este fim.

§ 2º O gestor ou Coordenador-Geral da área responsável pelo convênio, contrato, acordo de cooperação técnica ou instrumento congênere assumirá o papel de Autorizador do serviço de acesso à Internet para os usuários externos, e deverá fundamentar as solicitações com base no instrumento.

§ 3º Poderão ser concedidos acessos temporários para auditores de controle interno e externo, vinculados à Controladoria-Geral da União – CGU ou ao Tribunal de Contas da União - TCU, no uso de suas atribuições.

Art. 6º Nas situações em que a atividade necessitar o acesso à Internet por terceirizados, este deverá ser concedido a partir da infraestrutura de rede do INSS, desde que preenchidos os seguintes requisitos:

I - o contrato de prestação de serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

II - a empresa contratada deverá manter com seus funcionários Termo de Confidencialidade;

III - o contrato de prestação de serviços deverá prever a necessidade de acesso à Internet a partir das dependências do INSS; e

IV - o Autorizador, que para estes fins será o gestor do contrato ou o responsável pela área requisitante do serviço, deverá fundamentar as necessidades de acesso dos empregados da contratada, definindo os recursos que serão disponibilizados, endereços da Intranet e Internet necessários para o desenvolvimento das atividades e eventuais restrições a dias e horários para realização do acesso.

Art. 7º A conexão de equipamentos pessoais de visitantes à rede do INSS, quando necessária e motivada pelo interesse da Administração, deverá ser previamente autorizada pelo gestor da unidade onde o equipamento será utilizado.

Parágrafo único. Somente será permitida a utilização da rede local por visitantes caso seus equipamentos atendam a todos os requisitos estabelecidos pela DTI.

Art. 8º A todos os perfis de acesso descritos nesta Portaria, aplicam-se as restrições de acesso a sítios que:

I - contenham material pornográfico ou obsceno;

II - contenham material ilegal;

III - contenham material impróprio, ofensivo, preconceituoso ou discriminatório, que façam apologia à violência, ao terrorismo e às drogas; e

IV - contenham e/ou divulguem conteúdo de violação de direito autoral (pirataria) e/ou execução de quaisquer tipos ou formas de fraudes.

Art. 9º O processo de atribuição de acesso à Internet seguirá as seguintes diretrizes:

I - a atribuição dos perfis de acesso à Internet será feita pelos Autorizadores, de forma fundamentada e respeitando o princípio da necessidade de conhecer, de acordo com a tabela abaixo:

Perfil	Autorizador
1, 2 e 3	Presidente do INSS, Diretores, Coordenadores-Gerais, Chefes de Assessoria de Comunicação Social nas Superintendências-Regionais, Assessor de Comunicação Social (Administração Central), Chefe de Gabinete da Presidência, Auditor-Geral, Corregedor-Geral, Procuradores-Regionais, Procurador-Geral da PFE-INSS, Superintendentes-Regionais, Gerentes-Executivos e Gerentes de Agências da Previdência Social - APS.
4	Presidente do INSS, Diretores, Coordenadores-Gerais, Chefes de Assessoria de Comunicação Social nas Superintendências-Regionais, Assessor de Comunicação Social (Administração Central), Chefe de Gabinete da Presidência, Auditor-Geral, Corregedor-Geral, Procuradores-Regionais, Procurador-Geral da PFE-INSS, Superintendentes-Regionais e Gerentes-Executivos.

II - nos casos de novos usuários de rede (LDAP) criados por meio de registro de chamado técnico, quando o solicitante não indicar o perfil de acesso à internet, será atribuído o Perfil 1;

III - para fins de alteração do perfil de acesso, os usuários deverão preencher o Formulário de Solicitação de Acesso à Internet (Anexo I) e providenciar a assinatura no sistema SEI pelo Autorizador do acesso; e

IV - registrar a solicitação através de chamado no *CA Service Desk Manager* (www-sdm/) ou sistema que venha a substituí-lo, na opção **Comunicação**, anexando o Formulário de Solicitação de Acesso à Internet (Anexo I) devidamente preenchido e assinado (pelo solicitante e Autorizador).

Art. 10. A solicitação para perfis de acesso em caráter temporário, realizada mediante o Formulário de Solicitação de Acesso à Internet (Anexo I), deverá conter a motivação da necessidade e a data de início e de expiração do acesso.

Art. 11. As responsabilidades ficam estabelecidas na seguinte forma:

I - o usuário deverá:

a) preencher os requisitos e termos estabelecidos nesta Portaria;

b) estar devidamente autorizado a utilizar a Internet nas formas estabelecidas nesta Portaria;

c) fazer uso da Internet de forma responsável e segura, utilizando o acesso exclusivamente em razão de trabalho, cumprindo os procedimentos dispostos nesta Portaria, sem prejuízo das demais normatizações vigentes na Administração Pública Federal; e

d) impedir a divulgação e compartilhamento das chaves de segurança atribuídas, que são pessoais e intransferíveis;

II - o autorizador deverá:

a) conceder os perfis de acesso à Internet rigorosamente de acordo com as atribuições dos usuários de sua abrangência, observando os normativos do INSS;

b) verificar periodicamente o uso dos acessos concedidos e, sempre que necessário, solicitar alteração dos perfis de acesso dos usuários de sua abrangência; e

c) reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR-INSS;

III - a equipe técnica da DTI deverá:

a) monitorar os acessos à internet e sua utilização de acordo com as diretrizes estabelecidas nesta Portaria; e

b) identificar os casos de mau uso da Internet e adotar uma ou mais das seguintes providências:

1. alertar o usuário, responsável pelo acesso, e o Autorizador, responsável pela concessão, acerca do uso indevido da internet; e

2. nos casos de reincidência, solicitar a revogação do acesso à internet concedido ao usuário e encaminhar a documentação que comprova a má utilização do acesso concedido, à Corregedoria do INSS, para análise e adoção das medidas cabíveis.

Art. 12. Configura-se como uso indevido da Internet:

I - acessar a Internet disponibilizada pelo INSS sem estar devidamente autorizado, conforme estabelecido nesta Portaria;

II - fazer uso dos recursos de Internet disponibilizados pelo INSS para fins alheios ao trabalho, em discordância com os procedimentos dispostos nesta Portaria, sem prejuízo de demais normatizações vigentes na Administração Pública Federal;

III - utilizar os serviços extrapolando os privilégios do perfil de acesso que lhe foi designado;

IV - divulgar e/ou compartilhar as chaves de segurança, que são pessoais e intransferíveis, permitindo a utilização por terceiros do perfil que lhe foi atribuído;

V - praticar atos de comercialização de produtos e serviços, em proveito próprio ou de terceiros, que não atendam aos interesses do INSS;

VI - utilizar recursos ou dispositivos para acesso a computadores ou redes externas ao INSS com o objetivo de obter informações não autorizadas ou provocar a interrupção de serviços de rede;

VII - expor, armazenar, distribuir, editar, gravar ou compartilhar, através do uso dos recursos computacionais e de comunicação do INSS, arquivos estranhos às atividades do INSS e não autorizados pela chefia imediata;

VIII - realizar qualquer atividade que apoie ou facilite o vazamento de dados;

IX - baixar arquivos ou programas da Internet que contrariem as diretrizes da POSIN vigente; e

X - utilizar proxy não disponibilizado pelo INSS.

Art. 13. O acesso à Internet é passível de registro e monitoração, incluindo quaisquer dados transmitidos pela rede do INSS.

§ 1º Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a ETIR-INSS deverá ser imediatamente acionada para tomar as providências necessárias, a fim de sanar as causas, podendo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação do INSS;

§ 2º As ocorrências de mau uso do acesso à Internet não previstas nesta Portaria, assim como os casos de dúvidas em relação à aplicação das disposições aqui estabelecidas, deverão ser encaminhadas à DTI para registro, análise e avaliação da necessidade de alterações de acordo com o processo de governança em vigência no INSS;

§ 3º O descumprimento desta Portaria poderá acarretar ao usuário as penalidades previstas nas políticas e procedimentos internos e/ou, na forma da lei, responsabilidade administrativa, civil e criminal.

Art. 14. Esta portaria entra em vigor em 1º de abril de 2022.

GUILHERME GASTALDELLO PINHEIRO SERRANO

Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **GUILHERME GASTALDELLO PINHEIRO SERRANO**, Diretor(a) de Tecnologia da Informação e Inovação, em 16/03/2022, às 08:00, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **6757423** e o código CRC **15E505E4**.

ANEXO I

PORTARIA Nº 71/DTI/INSS, DE 16 DE MARÇO DE 2022

FORMULÁRIO DE SOLICITAÇÃO DE ACESSO À INTERNET

Informações do Usuário		
Nome:	Login de Rede:	
Matrícula:	CPF:	
Lotação:	Código do Setor:	
Telefone: ()	E-mail:	@inss.gov.br (ou AGU; ou SPMF)

☐	Perfil 1	Data de expiração:	
☐	Perfil 2		
☐	Perfil 3		
☐	Perfil 4		
☐	Terceirizados	Contrato nº ou Convênio	Data de expiração

Descreva abaixo a justificativa e quais páginas devem ser acessadas pelo usuário terceirizado:

Declaro ter conhecimento e estar de acordo com as regras estabelecidas na Norma de Uso da internet do INSS e demais normas aplicáveis.

, de de .
Local e Data

Informações do Autorizador		
Nome:		
Lotação:	Código do Setor:	
Telefone: ()	E-mail:	@inss.gov.br

Assinatura do Solicitante

Autorizo a concessão de Acesso Internet

, de de .
Local e Data

Assinatura do Autorizador

ANEXO I
PORTARIA Nº 71/DTI/INSS, DE 16 DE MARÇO DE 2022

FORMULÁRIO DE SOLICITAÇÃO DE ACESSO À INTERNET

Informações do Usuário		
Nome:	Login de Rede:	
Matrícula:	CPF:	
Lotação:	Código do Setor:	
Telefone: ()	E-mail:	@inss.gov.br (ou AGU; ou SPMF)

☐	Perfil 1		
☐	Perfil 2		
☐	Perfil 3		
☐	Perfil 4		
☐	Terceirizados	Data de expiração:	
		Contrato nº ou Convênio	Data de expiração

Descreva abaixo a justificativa e quais páginas devem ser acessadas pelo usuário terceirizado:

Declaro ter conhecimento e estar de acordo com as regras estabelecidas na Norma de Uso da internet do INSS e demais normas aplicáveis.

, de .

Local e Data

Informações do Autorizador		
Nome:		
Lotação:	Código do Setor:	
Telefone: ()	E-mail:	@inss.gov.br

Assinatura do Solicitante

Autorizo a concessão de Acesso Internet

_____, _____ de _____ de
_____.
Local e Data

Assinatura do Autorizador



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

DESPACHO

Diretoria De Tecnologia da Informação e Inovação, em 16/03/2022

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria De Tecnologia da Informação e Inovação.

Ass.: Portaria para publicação

1. Trata-se de Portaria que disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.
2. À DIVCA para ampla divulgação.

GUILHERME GASTALDELLO PINHEIRO SERRANO

Diretor De Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **GUILHERME GASTALDELLO PINHEIRO SERRANO**, **Diretor(a) de Tecnologia da Informação e Inovação**, em 16/03/2022, às 08:02, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **6775920** e o código CRC **7400FF9F**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 6775920



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Assessoria De Comunicação Social
Coordenação De Comunicação Social
Divisão De Comunicação Administrativa

DESPACHO

Divisão De Comunicação Administrativa, em 16/03/2022

Ref.: Processo nº 35014.047735/2020-84

Int.: Diretoria De Tecnologia da Informação e Inovação

Ass.: Publicação de Portaria

1. Trata-se da publicação e divulgação da Portaria DTI/INSS nº 71, de 16 de março de 2022.
2. Informamos que o referido ato, foi publicado no BSE, de 16 de março de 2022 e no Portal-INSS, na intraprev.
3. À Diretoria De Tecnologia da Informação e Inovação, para conhecimento e providências julgadas necessárias.

ALDAMIR GERALDO DE LISBÔA LIMA

Chefe da Divisão de Comunicação Administrativa - DIVCA



Documento assinado eletronicamente por **ALDAMIR GERALDO DE LISBOA LIMA, Chefe da Divisão**, em 16/03/2022, às 14:32, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **6776835** e o código CRC **FA8827C6**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 6776835

Clarity PPM

MM Marcia Soares Salgado Nunes de Matos Logoff | Ajuda | Sobre

Página inicial

Favoritos

Propriedades

Histórico

Acompanhamento

Processos

Ideia: DM.098517 - [SSEG] Adequar perfis de acesso a internet com Portaria 71 DTI/INSS - *Propriedades - Principal - Geral*

Ações

Geral

*

Título

[SSEG] Adequar perfis de acesso a internet com Portaria 71 DTI/INSS

ID de ideia

DM.098517

Objetivo

Para realizar adequação dos perfis existentes de acesso a internet do INSS, conforme a Portaria 71 da DTI/INSS, solicitamos que seja efetuado regularização dos perfis de acesso a internet no âmbito do INSS.
- Efetuar batimento das autorizações constantes no perfil 50 com o perfil 40, para regularizar o perfil 40;
- Migrar os usuários constantes nos perfis: 45, 50, 60, 70 e 100 para os perfis autorizados pelo INSS (perfis: 10,20,30 e 40);
- Excluir os perfis: 45, 50, 60, 70 e 100 para que não seja mais atribuídos aos usuários do INSS.

Descrição

Ajustar configuração dos filtros de conteúdo para que reflitam a nova Portaria e Aplicar as todos os perfis, sem exceção, as restrições de acesso conforme disciplina a mencionada Portaria 71, enviada via Ofício da DTI.

Etapa

/Dataprev/Análise da Ideia

Status

Em andamento

Cliente

INSS

Solicitante de origem

Luzivan de Moura Gois

Selecionador

Rodrigo Gomes Rodrigues

Gestor técnico

Cleonice Maria Aparecida Barbosa Alves

Gestor do contrato

Marcia Soares Salgado Nunes de Matos

Sistema principal impactado

PDTI

19. Sistemas Estratégicos e Gerenciais

Conclusão desejada

Data da repactuação de entrega da PA

Anexos

Responsável atribuído

*

Responsável pela solução

Carlos Antonio Aglio

= Obrigatório

= Inserir uma vez

= Exclusivo

= Bloqueado por processo



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria De Tecnologia da Informação e Inovação
Coordenação-Geral De Projetos e Soluções Digitais
Coordenação De Ciência De Dados e Análises Estruturadas

Ofício SEI nº 29/2022/DTI-INSS

Brasília, 18 de março de 2022.

Ao Senhor Diretor

ALAN DO NASCIMENTO SANTOS

Diretoria de Relacionamento e Negócio – DRN

Departamento de Relacionamento Comercial – DERC

SAS Quadra 1 Bloco E/F 7º andar – Brasília DF

CEP: 70.070-931– Telefone: (61) 3207.3332

Assunto: Disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.

Referência: Caso responda este Ofício, indicar expressamente o Processo nº 35014.047735/2020-84.

1. Encaminha-se para conhecimento e providências necessárias a Portaria DTI/INSS nº 71, de 16 de março de 2022 (SEI nº 6757423), que disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.
2. Informa-se, ainda, que para ajustar a configuração dos filtros de conteúdo para que reflitam a nova Portaria e aplicar a todos os perfis de acesso à Internet deste Instituto, sem exceção, foi aberta uma demanda, via Clarity, DM.098517 (SEI nº 6811600).
3. Antecipa-se que esta demanda deverá ser priorizada, uma vez que essa regulamentação se aplica a todos os servidores e colaboradores vinculados direta ou indiretamente ao INSS, bem como a servidores e empregados de entidades e órgãos da Administração Pública ou Privados que necessitem ou estejam autorizados a acessar a Internet a partir da rede corporativa do Instituto.

Atenciosamente,

GUILHERME GASTALDELLO PINHEIRO SERRANO

Diretor de De Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **GUILHERME GASTALDELLO PINHEIRO SERRANO**, **Diretor(a) de Tecnologia da Informação e Inovação**, em 18/03/2022, às 14:28, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **6803101** e o código CRC **65D3D057**.

Referência: Caso responda este Ofício, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 6803101

Data de Envio:

18/03/2022 15:57:05

De:

INSS/DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO <dti@inss.gov.br>

Para:

institucional@dataprev.gov.br

alan.santos@dataprev.gov.br

Assunto:

Disciplina o uso da Internet no INSS

Mensagem:

Encaminha para conhecimento e providências, Portaria nº 71, que disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.

Atenciosamente,

Márcia Salgado
DPLAN/DTI

Anexos:

Oficio_SEI_6803101.html

Portaria_6757423.html

Anexo_6811075_Anexo_pt71.pdf

Anexo_6811600_DM.098517.pdf

Re: Disciplina o uso da Internet no INSS

Equipe Institucional <institucional@dataprev.gov.br>

Sex, 18/03/2022 16:09

Para: DTI - Diretoria de Tecnologia Informação e Inovação <dti@inss.gov.br>

Boa tarde.

Acusamos o recebimento.

Atenciosamente,

sombra superior esquerdasombra superior direitaimagem do qrcode da assinatura

Equipe Institucional
Institucional
COAA/CGPR/PR
institucional@dataprev.gov.br
(61)3207-3000

Logo marca Dataprevwww.dataprev.gov.brsombrainfesqsombrainfdir

Aponte a câmera do celular para o QRcode para salvar o contato.

Esta mensagem da Dataprev, empresa pública federal, é enviada exclusivamente a(os) seu(s) destinatário(s) e protegida por sigilo profissional. Sua utilização desautorizada é ilegal e sujeita o infrator às penas da lei. Se você a recebeu indevidamente, queira, por gentileza, reenviá-la ao emissor, esclarecendo o equívoco.

De: INSS/DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO <dti@inss.gov.br>**Enviado:** sexta-feira, 18 de março de 2022 15:57**Para:** Equipe Institucional; Alan do Nascimento Santos**Assunto:** Disciplina o uso da Internet no INSS

Encaminha para conhecimento e providências, Portaria nº 71, que disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.

Atenciosamente,

Márcia Salgado
DPLAN/DTI

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 28/03/2022 | Edição: 59 | Seção: 1 | Página: 205

Órgão: Ministério do Trabalho e Previdência/Instituto Nacional do Seguro Social

COMITÊ ESTRATÉGICO DE GOVERNANÇA

RESOLUÇÃO CEGOV/INSS Nº 16, DE 17 DE MARÇO DE 2022

Revoga Resoluções do Comitê Estratégico de Governança - CEGOV do Instituto Nacional do Seguro Social.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o constante dos autos do Processo nº 35014.072365/2022-85, resolve:

Art. 1º Revogar as seguintes Resoluções do CEGOV:

I - Resolução nº 10/CEGOV/INSS, de 31 de agosto de 2020;

II - Resolução nº 11/CEGOV/INSS, de 31 de agosto de 2020; e

III - Resolução nº 12/CEGOV/INSS, de 31 de agosto de 2020.

Art. 2º Esta Resolução entra em vigor em 1º de abril de 2022.

JOSÉ CARLOS OLIVEIRA

Presidente do Comitê

SEBASTIÃO FAUSTINO DE PAULA

Diretor de Benefícios

JOBSON DE PAIVA SILVEIRA SALES

Diretor de Atendimento

LARISSA ANDRADE MORA

Diretora de Gestão de Pessoas e Administração

ALEXANDRE GUIMARÃES

Diretor de Integridade, Governança e Gerenciamento de Riscos

GUILHERME GASTALDELLO PINHEIRO SERRANO

Diretor de Tecnologia da Informação e Inovação

Este conteúdo não substitui o publicado na versão certificada.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

PORTARIA DTI/INSS Nº 75, DE 01 DE ABRIL DE 2022

Institui a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR do Instituto Nacional do Seguro Social.

O DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO do **INSTITUTO NACIONAL DO SEGURO SOCIAL**, no uso das atribuições que lhe conferem o Decreto nº 9.746, de 8 de abril de 2019, e considerando o que consta no processo administrativo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Instituir, no âmbito do INSS, a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR-INSS.

Art. 2º Para os efeitos desta Portaria ficam estabelecidos os seguintes conceitos e definições:

I - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR: equipe de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

II - CTIR Gov: Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI;

III - agente responsável: servidor público ocupante de cargo efetivo de órgão ou entidade da Administração Pública Federal, direta ou indireta ou militar de carreira incumbido de chefiar e gerenciar uma ETIR;

IV - artefato malicioso: qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

V - comunidade ou público alvo: conjunto de pessoas, setores, órgãos ou entidades atendidas por uma ETIR ou estrutura equivalente;

VI - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VII - serviço: conjunto de procedimentos, estruturados em processo definido, oferecido à comunidade pela ETIR;

VIII - tratamento de incidentes de segurança em redes computacionais: serviço consistente em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de

segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

IX - usuário: pessoas que fazem uso de serviços de TI e sistemas de informação de propriedade do INSS, independentemente do cargo ocupado (contratados, consultores, conselheiros, servidores, temporários e etc.);

X - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que possam resultar em risco para um sistema ou por uma organização, e que possam ser evitados por uma ação interna de segurança da informação;

XI - CSIRT (Computer Security Incident Response Team): Grupo de Segurança e Resposta a Incidentes de Segurança Computacionais;

XII - CERT.br: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil; e

XIII – FIRST (Forum of Incident Response and Security Teams): Fórum de Resposta a Incidentes e de Equipes de Segurança.

Art. 3º A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR-INSS tem por objetivo agir proativamente, receber, analisar, monitorar, coordenar e propor respostas a notificações e atividades relacionadas a incidentes cibernéticos no âmbito do INSS.

Art. 4º As atividades pertinentes à ETIR-INSS englobam os usuários dos serviços de Tecnologia da Informação e Comunicações e os sistemas de informação do INSS e serão realizadas com intercâmbio de informações e em cooperação com as seguintes instâncias:

I - Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov;

II - outros Grupos Segurança e Resposta a Incidentes de Segurança Computacionais (CSIRTs) nacionais (reconhecidos pelo CERT.br) e internacionais (membros do FIRST);

III - a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR de empresas prestadoras de serviços de tecnologia contratadas pelo INSS;

IV - as ETIRs ou estrutura (de controle ou policial) equivalente dos demais órgãos, entidades e empresas, públicas ou privadas, que tenham contratos, acordos, convênios ou instrumentos congêneres com o INSS; e

V - Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República – GSI/PR.

Art. 5º A implementação e o funcionamento da ETIR-INSS seguirão metodologia e diretrizes definidas pelo GSI/PR na NC 05/IN01/DSIC/GSIPR de 14 de agosto de 2019, a saber:

I - basear-se no “Modelo 2 – Centralizado”, consubstanciada na Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos, vinculada à Diretoria de Tecnologia da Informação;

II - os integrantes da Equipe deverão ser profissionais da área de Tecnologia da Informação, servidores públicos efetivos ou empregados públicos efetivos, com dedicação exclusiva, dentro da jornada institucional, às atividades de tratamento e resposta a incidentes cibernéticos e com experiência ou conhecimentos técnicos compatíveis com a satisfação da missão da ETIR-INSS, sem prejuízo da colaboração excepcional de integrantes de outras áreas do INSS;

III - na ausência do Chefe e de seu substituto, formalmente nomeados, as atribuições relacionadas à coordenação da equipe serão desempenhadas pelo Gestor de Segurança da Informação do INSS.

Art. 6º A ETIR-INSS será composta por membros:

I - permanentes, que efetivamente atuarão em todos os incidentes registrados;

II - colaboradores, que atuarão, de forma esporádica, no tratamento de incidentes relacionados às suas áreas de atuação; e

III - opcionais, servidores das unidades descentralizadas do INSS sob supervisão da DTI.

§ 1º Os membros da ETIR-INSS serão designados por meio de ato do Diretor de Tecnologia da Informação e Inovação.

§ 2º A distribuição dos membros da ETIR-INSS se dará da seguinte forma:

I - Gestor de Segurança da Informação do INSS, responsável por prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos membros da ETIR, bem como prover a infraestrutura necessária ao seu funcionamento;

II – Chefe da Equipe, agente responsável pela ETIR-INSS perante o gestor de segurança da informação e comunicações do INSS, as demais esferas decisórias da organização, o CTIR Gov e quaisquer outros entes de intercâmbio e cooperação já definidos;

III - servidores públicos que compartilham as funções, responsabilidades, forma de atuação e dedicação temporal definidas pela implementação e funcionamento do modelo escolhido;

IV - empregados públicos que compartilham as funções, responsabilidades, forma de atuação e dedicação temporal definidas pela implementação e funcionamento do modelo escolhido; e

V - colaboração excepcional de integrantes de outras áreas do INSS.

Art. 7º A ETIR-INSS terá autonomia compreendida pelo seguinte escopo de atuação, níveis de responsabilidades e independência dispostos a seguir:

I - a ETIR-INSS terá autonomia compartilhada, participando do processo decisório ao lado do Gestor de Segurança da Informação e do Diretor de Tecnologia da Informação, condicionada ao nível de classificação relacionado, de quaisquer processos referentes a incidentes cibernéticos no âmbito do INSS.

II - no âmbito da ETIR-INSS, a apuração ou a investigação de incidentes (análise forense) que ultrapassem suas capacidades técnicas, que não sejam satisfeitas pelo seu poder de gestão ou que requeiram autorização externa, serão, conforme sua natureza e necessidades, encaminhadas ao Centro de Tratamento e Resposta a Incidentes (CTIR Gov), à Comissão de Tratamento e Resposta a Incidentes Cibernéticos (CTIR/Dataprev) ou demais órgãos, entidades e empresas, públicas ou privadas, que tenham contratos, acordos, convênios ou instrumentos congêneres com o INSS, conforme respectivos procedimentos a serem definidos por eles, com vistas a viabilizar soluções integradas para a Administração Pública Federal - APF, bem como a geração de relatórios e estatísticas.

§ 1º A Equipe recomendará formalmente os procedimentos a serem executados ou as medidas de recuperação durante um ataque e discutirá as ações a serem tomadas, apresentando também os riscos envolvidos no não acatamento.

§ 2º No caso de incidentes que representem iminente risco de dano grave ou de difícil reparação e não sendo possível o contato tempestivo com os demais participantes do processo decisório elencados no inciso I do caput deste artigo, fica autorizada a ETIR a adotar as medidas emergenciais de mitigação, mediante imediata formalização às áreas afetadas.

Art. 8º A ETIR-INSS fornecerá serviços relacionados a todas as fases do gerenciamento de incidentes cibernéticos em ativos computacionais, que compreendem o seguinte:

I - recepção de solicitações e alertas diversos, utilizando como canal de comunicação a caixa postal etir@inss.gov.br;

II - filtragem de todo conteúdo direcionado à ETIR-INSS, para fins de verificação quanto à necessidade de tratamento pela Equipe e, caso não se trate de incidente de segurança em redes computacionais, encaminhar para a área competente;

III - catalogação dos incidentes detectados em ferramenta a ser prospectada e homologada pela ETIR e implantada pela DTI, com nível de acesso restrito;

IV - classificação dos incidentes detectados quanto ao nível de severidade e impacto;

V - tratamento do incidente com medidas corretivas e indicação de formas de se evitar que ocorra novamente;

VI - resposta às solicitações e alertas encaminhados para a ETIR;

VII - monitoramento da aplicação das medidas e controles definidos pelo processo de tratamento dos incidentes recebidos;

VIII - recomendação de ações de mitigação de riscos iminentes alertados ou informados por painéis internos de monitoramento ou investigação, consultas externas, notificações e identificação de ameaças; e

IX - cooperação com outras equipes de tratamento e resposta a incidentes.

§ 1º A ETIR-INSS deverá analisar os incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências.

§ 2º O detalhamento dos serviços prestados pela ETIR-INSS deverá ser publicado em página específica da Intranet do INSS, no prazo de 30 (trinta) dias a partir da publicação desta Portaria.

Art. 9º Esta portaria entra em vigor na data da publicação.

GUILHERME GASTALDELLO PINHEIRO SERRANO

Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **GUILHERME GASTALDELLO PINHEIRO SERRANO**, **Diretor(a) de Tecnologia da Informação e Inovação**, em 01/04/2022, às 16:30, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site

https://sei.inss.gov.br/sei/controlador_externo.php?

[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **6982722** e o código CRC **2DAF5EAC**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

DESPACHO

Diretoria De Tecnologia da Informação e Inovação, em 01/04/2022

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria De Tecnologia da Informação e Inovação.

Ass.: Portaria para publicação

1. Trata-se de Portaria 75 que Institui a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR do Instituto Nacional do Seguro Social..
2. À DIVCA para ampla divulgação.

GUILHERME GASTALDELLO PINHEIRO SERRANO

Diretor De Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **GUILHERME GASTALDELLO PINHEIRO SERRANO**, **Diretor(a) de Tecnologia da Informação e Inovação**, em 01/04/2022, às 16:33, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7003204** e o código CRC **CB46813B**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 7003204



INSTITUTO NACIONAL DO SEGURO SOCIAL

PORTARIA CONJUNTA DTI/DIRAT/INSS Nº 3, DE 01 DE ABRIL DE 2022

Institui a Norma de Controle de Acesso Lógico - NCAL do INSS.

O DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO e o DIRETOR DE ATENDIMENTO do INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS, no uso das atribuições que lhes conferem o Decreto nº 9.746, de 8 de abril de 2019, e considerando o que consta no processo administrativo nº 35014.047735/2020-84,

RESOLVEM:

Art. 1º Instituir a Norma de Controle de Acesso Lógico - NCAL do INSS e aprovar os Anexos I e II.

Art. 2º Os termos definidos nesta Portaria Conjunta se aplicam a todos os agentes públicos e privados com vínculo direto ou indireto, permanente ou temporário, com o INSS.

Parágrafo único. Equiparam-se a usuários do INSS, para os fins desta Portaria Conjunta, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União - AGU que atuarem em consultoria, assessoramento jurídico, e representação judicial e extrajudicial do INSS, e os servidores e contratados vinculados à Subsecretaria da Perícia Médica Federal - SPMF com atuação junto ao INSS.

Art. 3º Para os efeitos desta Portaria Conjunta são estabelecidos os seguintes conceitos e definições:

I - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um Órgão ou Entidade;

II - administrador de domínio: usuário responsável pela administração de um domínio por meio da aplicação de políticas globais, criação, edição e exclusão de usuários e grupos, e instalação de programas em um grande número de estações de trabalho;

III - administrador local: usuário responsável pela administração de partes de um domínio (geralmente restrito a um setor ou abrangência), por meio de políticas locais, edição de grupos e usuários locais, e instalação de programas em estações de trabalho limitadas a um setor ou abrangência;

IV - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo oficial, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta;

V - ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VI - contas de serviço: contas de acesso à rede corporativa de computadores, necessárias

para a execução de procedimentos automáticos (aplicação, script, dentre outros), sem qualquer intervenção humana no seu uso;

VII - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais;

VIII - credenciamento: processo pelo qual o usuário recebe credenciais que possibilitarão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer;

IX - desativação: processo pelo qual o usuário tem as credenciais de acesso desativadas em função de encerramento ou perda de vínculo oficial como usuário interno ou externo;

X - reativação: processo pelo qual o usuário já credenciado e que foi desativado tem as credenciais de acesso reativadas em função de retorno ao INSS ou renovação de contrato;

XI - necessidade de conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

XII - credenciais ou contas de acesso: permissões, concedidas por autoridade competente, após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física, como crachá, cartão e selo, ou lógica, como identificação com usuário e senha;

XIII - dado: é um elemento informativo concreto, e sua forma plural expressa uma informação; é o registro do atributo de um ente objeto ou fenômeno, onde "registro" indica o ato de registrar, ou seja, é a gravação ou a impressão de caracteres ou símbolos que tenham um significado em algum documento ou suporte físico;

XIV - domínio: agrupamento lógico de computadores em rede que compartilham recursos em um banco de dados de segurança comum, onde a administração e autenticação são centralizadas. Desta forma um usuário precisa de uma conta para ter acesso ao domínio e aos recursos compartilhados;

XV - endereço IP (Internet Protocol): conjunto de elementos numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores. Sequência de números associada a cada computador conectado à Internet. No caso de IPv4, o endereço IP é dividido em quatro grupos, separados por "." e compostos por números entre 0 e 255. No caso de IPv6, o endereço IP é dividido em até oito grupos, separados por ":" e compostos por números hexadecimais (números e letras de "A" a "F") entre 0 e FFFF;

XVI - entidade externa: organização governamental, não governamental ou privada, amparada por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica, ou instrumento congênere com o INSS;

XVII - e-SIC: Sistema Eletrônico do Serviço de Informações ao Cidadão, aplicação disponibilizada na internet, que centraliza todos os pedidos de informações dirigidos ao Poder Executivo Federal;

XVIII - ferramenta de gestão de acessos: um ou mais softwares que possibilitem a gestão integrada de papéis e permissões de acesso dos usuários a rede, sistemas e outros recursos corporativos;

XIX - gestor da informação: usuário que gerou a informação, que responde pelo seu conteúdo, ou que foi formalmente designado para definir ou alterar sua classificação nos graus de sigilo e de acesso;

XX - gestão de identidades: combinação de sistemas técnicos, regras e procedimentos que definem a posse, utilização e segurança de uma identidade. Seu objetivo primário é estabelecer a confiança na associação de atributos a uma identidade digital e conectar esta identidade com uma entidade individual;

XXI - informação: dados, processados ou não, que podem ser utilizados para produção e

transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXII - informação custodiada: informações pessoais e de terceiros obtidas pelo INSS em razão de suas atribuições;

XXIII - log ou registro de auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional;

XXIV - perfil de acesso do usuário: conjunto de atributos de cada usuário, definidos previamente como necessários para a credencial de acesso;

XXV - recursos de rede: dispositivos (impressoras, scanners, multifuncionais, dentre outros) ou serviços (sistemas, portais, dentre outros) disponibilizados para os usuários por meio de uma rede de dados;

XXVI - serviço de diretório: serviço que armazena e organiza informações relativas a recursos disponíveis e usuários de uma rede de dados. Permite que o administrador da rede gerencie o acesso de usuários e sistemas aos recursos disponíveis;

XXVII - sistemas corporativos: sistemas de operação, ou finalísticos, ou seja, que se coadunam com os fins da Previdência Social. Assim, entende-se que este conceito comporta o conjunto de sistemas e subsistemas que garantem a operação dos Regimes Geral e Próprio de Previdência Social, inclusive de previdência complementar;

XXVIII- sistemas legados: compreendem o conjunto de aplicações desenvolvidas com tecnologias obsoletas que permanecem em operação no INSS;

XXIX: usuário: integrantes do quadro de Pessoal em atividade do INSS, terceirizados, outros colaboradores indicados pela área de TI, consultores e auditores que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um Órgão ou Entidade da Administração Pública Federal, formalizada por meio da assinatura ou aceite eletrônico do Termo de Responsabilidade;

XXX - usuário interno: integrante do quadro de Pessoal em atividade do INSS ou da Subsecretaria de Perícia Médica Federal, terceirizado, ou colaborador autorizado pela área de Segurança de TI, lotado ou em exercício em uma Unidade Orgânica - UO, que se utiliza da rede, do e-mail e/ou dos sistemas corporativos do INSS;

XXXI - usuário externo: usuários vinculados a uma Entidade Externa, que se utiliza dos sistemas corporativos do INSS por meio de um perfil de acesso concedido por um Gestor de Acesso Externo;

XXXII - GERID (Gerenciador de Identidades): software provido pela DATAPREV e que gerencia os perfis e permissões de acesso de cada usuário às aplicações corporativas integradas;

XXXIII - OpenLDAP: software livre de código aberto que implementa o protocolo LDAP (Lightweight Directory Access Protocol - Protocolo Leve de Acesso a Diretório) e que se comunica com base de dados de usuários mantida e gerida pela DATAPREV, e utilizada, dentre outras, para acesso às aplicações integradas ao GERID e sistemas legados; e

XXXIV - conta Microsoft: registro em base de dados de usuários mantida pela Microsoft, gerida pela Diretoria de Tecnologia da Informação e Inovação - DTI e utilizada para acesso aos recursos da suíte de colaboração, comunicação e produtividade contratada pelo INSS.

Art. 4º São diretrizes desta NCAL-INSS:

I - o acesso à rede e aos sistemas corporativos do INSS dar-se-á por meio de autenticação integrada de domínio baseado em serviço de diretório, administrado por meio de uma ferramenta de gestão de identidades;

II - as concessões de acesso à rede de dados e aos recursos e sistemas corporativos são distintas. Sendo assim, o usuário pode obter permissão de acesso apenas à rede de dados, ou apenas a determinado(s) sistema(s) ou recurso(s) corporativo(s), tal qual o correio eletrônico;

III - as credenciais de acesso à rede de dados e aos recursos e sistemas corporativos são conferidas aos usuários com base na necessidade de conhecer, para viabilizar o exercício de suas

atribuições funcionais e atividades a serem desenvolvidas no INSS; e

IV - o uso indevido do acesso à rede de dados e aos recursos e sistemas corporativos do INSS, assim como das informações veiculadas nesses meios sujeitará o agente às penalidades previstas na legislação.

Art. 5º Para manutenção da base cadastral do OpenLDAP, até que seja implementada rotina automatizada, a área de Gestão de Pessoas do INSS disponibilizará, em periodicidade acordada e com a supervisão da área de TI do INSS, as informações extraídas do Sistema Integrado de Administração de Recursos Humanos - SIAPE para a DATAPREV, contendo os dados necessários ao povoamento das bases cadastrais de usuários internos.

Parágrafo único. Até que haja rotina automatizada, a DTI demandará à DATAPREV a atualização da base cadastral do OpenLDAP e implementará o necessário quanto às contas Microsoft e outros recursos corporativos que requeiram essas informações, bem como realizará a validação das informações eventualmente disponibilizadas ou obtidas pelo INSS por meio de outras bases, na periodicidade do envio das informações, e a área de Gestão de Pessoas do INSS poderá acordar com a área responsável pela Segurança de TI a revisão das informações necessárias à administração de contas de usuários.

Art. 6º O processo de credenciamento de usuário aos Ativos de Informação deve observar os seguintes critérios:

I - a credencial de acesso concedida para acesso à rede de dados e aos recursos e sistemas corporativos do INSS é de caráter pessoal e intransferível; e

II - as credenciais de acesso devem ser concedidas após a data de contratação ou entrada em exercício do usuário.

Art. 7º Para viabilizar ao acesso de usuários internos à rede ou outros recursos corporativos, a área de Gestão de Pessoas do INSS deverá utilizar, de forma centralizada, os canais de atendimento disponibilizados pela DATAPREV, ou outro canal informado pela DTI do INSS, para solicitar:

I - o credenciamento de usuários ingressantes do quadro de Pessoal em atividade do INSS, após o cadastro no SIAPE, para acesso à rede e ao e-mail corporativos;

II - a desativação de usuários do quadro de Pessoal do INSS cedidos a outros órgãos;

III - a desativação de usuários do quadro de Pessoal do INSS na data do ato administrativo de aposentadoria ou de outras ocorrências que ensejem desligamento para fins de acesso lógico, independentemente de cadastro no SIAPE;

IV - a desativação de usuários do quadro de Pessoal do INSS cedidos a outros Órgãos;

V - a desativação de usuários do quadro de Pessoal em atividade do INSS com licenças ou afastamentos por período superior a 60 (sessenta) dias ininterruptos; e

VI - a reativação de usuários internos após o retorno ao Órgão ou a renovação de contrato com o INSS.

Art. 8º Quanto ao processo de formação das credenciais de acesso fica estabelecido que o nome do usuário será composto de acordo com os padrões estabelecidos no Guia de Interoperabilidade do Governo Eletrônico - e-Ping, mais especificamente no documento “Caixas Individuais-Fundacionais no Governo Federal” (Rede do Governo, 2010) que define regras de formação de nomes para a composição de endereços eletrônicos.

Art. 9º Com relação às senhas de acesso deve-se observar que:

I - deverão conter no mínimo oito caracteres e, obrigatoriamente, letras, números e caracteres especiais;

II - é vedada a reutilização das últimas quatro senhas utilizadas pelo usuário;

III - podem ser alteradas sempre que preciso ou quando o usuário achar necessário;

IV - o prazo de validade não deve ultrapassar 90 (noventa) dias; e

V - o usuário receberá, por meio de comunicado direto (via interface do sistema ou por

mensagem no correio eletrônico), a informação do prazo de vencimento da senha, quando esta estiver a 15 (quinze) dias da sua data de expiração.

Art. 10. As senhas de acesso serão gradativamente e sempre que possível substituídas pela exigência de certificado digital A3.

Art. 11. Os perfis de acesso aos sistemas corporativos do INSS deverão contemplar um conjunto de permissões e ações vinculadas às atividades desenvolvidas pelo usuário, sendo que:

I - caberá à área de Segurança de TI do INSS estabelecer, em conjunto com as áreas responsáveis pela gestão dos sistemas corporativos, a Portaria de criação dos perfis de acesso;

II - as áreas responsáveis pela gestão dos sistemas corporativos são responsáveis pelas permissões, transações e ações que devem compor cada perfil de acesso; e

III - os perfis de acesso e de gestão concedidos para usuários internos e externos deverão ser objeto de revisão contínua pelos gestores responsáveis, que não pode ultrapassar o prazo máximo de 30 (trinta) meses.

Art. 12. Quanto à utilização das credenciais e perfis de acesso, o usuário deve:

I - ter conhecimento prévio desta Portaria Conjunta e preencher os requisitos estabelecidos nesta;

II - estar devidamente autorizado a utilizar a rede de dados e aos recursos e sistemas corporativos do INSS, de acordo com os requisitos estabelecidos nesta Portaria Conjunta;

III - utilizar os serviços e as informações obtidas por meio do perfil de acesso, única e exclusivamente em razão do exercício da função pública e para os fins que lhe foi designado, cumprindo os procedimentos dispostos nesta Portaria Conjunta, sem prejuízo das demais normatizações vigentes na Administração Pública Federal;

IV - não divulgar, nem mesmo compartilhar, os códigos de segurança que lhe forem atribuídos (credenciais de acesso), os quais são pessoais e intransferíveis;

V - não fazer uso das credenciais de acesso de outros usuários;

VI - fornecer informações acessadas à rede de dados e aos recursos e sistemas corporativos do INSS somente mediante demanda formalizada de quem tenha competência para tal;

VII - comunicar à chefia imediata ou responsável pela administração do sistema ou rede corporativa do INSS quaisquer violações ou incidentes referentes à proteção do equipamento utilizado, do software ou de outros ativos da informação;

VIII - sempre que necessário afastar-se da estação de trabalho, certificar-se de que a sessão de à rede de dados e aos recursos e sistemas corporativos do INSS esteja encerrada ou bloqueada;

IX - efetuar processo de alteração da sua senha em seu primeiro acesso à rede de dados corporativa do INSS; e

X - informar conta de e-mail pessoal próprio para recebimento das credenciais de acessos, sendo vedada a utilização de e-mail pessoal de terceiros.

Parágrafo único. É vedada a utilização das credenciais para acesso à rede de dados e aos recursos e sistemas corporativos do INSS em mais de uma estação de trabalho simultaneamente, salvo em caso de autorização expressa da área de segurança de TI, no interesse da Administração.

Art. 13. O processo de autenticação de usuários deve ser definido pela área de Segurança de TI do INSS e poderá ser baseada em autenticação simples (nome de usuário e senha) agregada a autenticação multifator (certificação digital ou outros meios disponíveis).

Art. 14. O credenciamento de usuários internos se dá pelo cadastro de ingressantes ao quadro de Pessoal em atividade do INSS, de terceirizados, ou de outros colaboradores indicados pela área de Gestão de TI do INSS e deve ser solicitado por meio dos canais de atendimento disponibilizados pela DATAPREV ou outro informado pela DTI.

Art. 15. O credenciamento de estagiários se dará com a emissão de credencial de acesso, tendo como requisito as seguintes condições:

I - a empresa que atuar como agente de integração do estágio supervisionado deve manter contrato com o INSS;

II - o contrato de estágio supervisionado deverá conter cláusula de confidencialidade e sigilo de informações preestabelecidos com a Administração Pública;

III - a criação de perfis específicos e restritos às atividades do estagiário pelos gestores dos sistemas corporativos para o acesso dos estagiários;

IV - é vedada a concessão de perfis de acesso aos sistemas corporativos do INSS para estagiários com permissão de alteração das bases de dados institucionais, bem como a concessão de perfis de gestão de acessos de qualquer natureza;

V - o acesso será concedido mediante solicitação expressa do supervisor do estagiário, que deverá avaliar os riscos de utilização indevida de informações institucionais e as eventuais restrições referentes aos dias e horários para a realização dos acessos;

VI - o acesso será precedido da assinatura do Termo de Confidencialidade e de Manutenção de Sigilo - TCMS, Anexo II, o qual deverá ser firmado pelo estagiário ou pelo estagiário e seu responsável legal, no caso de se tratar de estagiário menor de 18 (dezoito) anos;

VII - as solicitações de acesso à rede e ao e-mail corporativo por estagiários devem ser direcionadas à unidade de Gestão de Pessoas de vinculação do estagiário pela chefia imediata ou pelo responsável pela supervisão de estágio, e a unidade de Gestão de Pessoas de vinculação encaminhará a solicitação de credenciamento à área centralizada responsável pelo encaminhamento das informações à DATAPREV ou outro canal informado pela área de Gestão de TI do INSS.

VIII - o supervisor do estagiário deverá, periodicamente, orientá-lo quanto ao uso responsável e adequado do acesso à rede de dados e aos recursos e sistemas corporativos do INSS ; e

IX - o acesso do estagiário limitar-se-á à data final do contrato ou à data de eventual rescisão antecipada, e caberá à unidade de Gestão de Pessoas de vinculação encaminhar a solicitação de desativação à área centralizada, responsável pelo encaminhamento das informações à DATAPREV, ou outro canal informado pela área de Gestão de TI do INSS.

Art. 16. O credenciamento de usuários terceirizados obedecerá as seguintes diretrizes:

I - as credenciais de acesso para usuários terceirizados devem ser emitidas tendo em vista unicamente o interesse do INSS, devidamente justificadas e previstas no contrato ou instrumento congênere; e

II - as solicitações de emissão de credenciais de acesso à rede corporativa do INSS para usuários terceirizados estabelecida por contrato ou instrumento congênere devem ser feitas pelo gestor da unidade/área responsável pela gestão do instrumento legal no âmbito do INSS.

Parágrafo único. A emissão de credenciais de acesso à rede corporativa do INSS para usuários terceirizados nas dependências do INSS, quando necessária, deverá atender os seguintes requisitos:

I - a organização à qual o usuário é vinculado deve manter contrato ou instrumento congênere vigente com o INSS;

II - o instrumento deve conter cláusulas prevendo:

a) necessidade e justificativa para acesso;

b) a confidencialidade e sigilo de informações preestabelecidas junto ao INSS; e

c) a obrigatoriedade da organização ou do ente contratado de informar previamente ao representante legal do INSS, responsável pela gestão do contrato, quaisquer alterações em seu corpo de colaboradores que impacte na emissão/exclusão das contas de acesso.

III - a organização ou ente contratado também deverá manter com seus colaboradores Termo de Confidencialidade de Manutenção de Sigilo - TCMS;

IV - o gestor do contrato por parte do INSS deve fundamentar a necessidade do acesso à rede para usuários terceirizados, com definição dos recursos a serem disponibilizados e eventuais

restrições a dias e horas para realização do acesso à rede;

V - os TCMS deverão ser arquivados junto aos instrumentos assinados com o INSS e uma cópia ou link eletrônico deverá ser encaminhada ao gestor do contrato. O mesmo deve ocorrer para quaisquer alterações ocorridas na vigência dos contratos ou instrumentos congêneres; e

VI - caso os Termos sejam gerados de forma eletrônica, deverá ser disponibilizado o arquivo correspondente, atendendo aos requisitos necessários para garantia de integridade e disponibilidade de acesso, assim como os requisitos específicos previstos em contrato.

Art. 17. O credenciamento de usuários externos obedecerá as seguintes diretrizes:

I - as credenciais de acesso para usuários externos devem ser emitidas tendo em vista o interesse do INSS, devidamente justificadas e previstas no convênio, acordo de cooperação técnica ou instrumento congênere;

II - as solicitações de emissão de credenciais de acesso à rede corporativa do INSS para usuários amparados por força de legislação específica ou estabelecida em convênio, acordo de cooperação técnica, contrato ou instrumento congênere devem:

a) ser feitas pelo gestor da unidade/área responsável pela gestão do instrumento legal; e

b) ser atendidas somente após validação das credenciais do gestor solicitante do INSS, mediante verificação dos dados contidos na Tabela de Unidade Orgânica do INSS (TB 0700);

Parágrafo único. A emissão de credenciais de acesso à rede corporativa do INSS para usuários externos, quando necessária, será provida unicamente pelo interesse do INSS, devendo ser atendidos os seguintes requisitos:

I - a organização a qual o usuário é vinculado deve manter contrato, acordo de cooperação, convênio ou instrumento congênere vigente com o INSS;

II - o instrumento deve conter cláusulas prevendo:

a) necessidade e justificativa para acesso;

b) a confidencialidade e sigilo de informações preestabelecidas junto ao INSS; e

c) a obrigatoriedade da organização ou do ente contratado de informar previamente ao representante legal do INSS, responsável pela gestão do contrato, quaisquer alterações em seu corpo de colaboradores que impacte na emissão/exclusão das contas de acesso.

III - a organização ou ente contratado também deverá manter com seus colaboradores Termo de Confidencialidade de Manutenção de Sigilo - TCMS;

IV - o gestor do contrato por parte do INSS deve fundamentar a necessidade do acesso à rede para usuários externos com definição dos recursos a serem disponibilizados e eventuais restrições a dias e horas para realização do acesso à rede;

V - os TCMS deverão ser arquivados junto aos instrumentos assinados com o INSS e uma cópia ou link eletrônico deverá ser encaminhada ao gestor do contrato. O mesmo deve ocorrer para quaisquer alterações ocorridas na vigência dos contratos, acordos ou convênios; e

VI - caso os Termos sejam gerados de forma eletrônica, deverá ser disponibilizado o arquivo correspondente, atendendo aos requisitos necessários para garantia de integridade e disponibilidade de acesso, assim como os requisitos específicos previstos em contrato.

Art. 18. A DTI poderá estabelecer a obrigatoriedade de utilização de múltiplos fatores de autenticação para acesso à rede do INSS.

Art. 19. O acesso aos prestadores de serviço vinculados à Central de Atendimento 135 se observará as seguintes condições:

I - a empresa deve manter contrato com o INSS;

II - o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

III - a empresa contratada deverá manter com seus funcionários Termos de

Confidencialidade - TCMS;

IV - o acesso será concedido mediante solicitação expressa do gestor do contrato, por parte do INSS, o qual irá definir quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;

V - os acessos deverão ser realizados única e exclusivamente por necessidade de serviço;

VI - os contratos de prestação de serviços de teleatendimento devem conter documento a ser utilizado para formalização das indicações de gestores de acesso aos sistemas corporativos do INSS; e

VII - o INSS pode disponibilizar às Centrais 135, de forma restrita, uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias ao desempenho de suas funções.

Art. 20. Nos casos referentes a prestadores de serviço vinculados aos serviços de Ouvidoria governamental, o acesso se dará observando-se as seguintes condições:

I - a empresa deve manter contrato direto com o Ministério do Trabalho e Previdência ou o INSS;

II - o Contrato de Prestação de Serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

III - a empresa contratada deverá manter com seus funcionários Termos de Confidencialidade;

IV - o acesso será concedido mediante solicitação expressa do gestor do contrato, que irá definir quais informações serão disponibilizadas e eventuais restrições a dias e horários para a realização do acesso;

V - os acessos deverão ser realizados única e exclusivamente por necessidade de serviço; e

VI - o INSS pode disponibilizar, de forma restrita, uma versão do sistema corporativo utilizado por seus atendentes contendo apenas as informações necessárias ao desempenho de suas funções.

Art. 21. O acesso à rede corporativa do INSS por servidores vinculados a Órgãos de controle externo envolvidos em ações de auditoria no âmbito do INSS será concedido mediante apresentação da equipe de auditoria por meio de documento formal que conste:

I - dados necessários ao cadastro de usuários externos;

II - informações acerca dos objetivos dos trabalhos a serem executados;

III - os prazos envolvidos; e

IV - informações complementares eventualmente solicitadas pela DTI.

Parágrafo único. O tipo de acesso de que trata este artigo deverá observar:

I - as parcerias institucionalmente estabelecidas entres esses Órgãos e o INSS no que tange à cobertura/previsão de acesso à rede corporativa do INSS;

II - o atendimento de pedido de solicitação de informações advindo de pessoas físicas ou jurídicas externas, respeitadas as restrições de acesso às informações previstas na Lei nº 12.527, de 18 de novembro de 2011, serão analisadas pela área designada para responder as demandas dos cidadãos por meio do e-SIC; e

III - os procedimentos referentes às solicitações de credenciamento, reativação e desativação de contas de acesso de usuários devem ser executados tendo como premissa a preservação dos registros para efeito de auditoria.

Art. 22. A autoridade máxima da Corregedoria-Geral do INSS, quando necessário, poderá solicitar a desativação ou bloqueio imediatos de contas de acesso de usuários que estiverem envolvidos em inquérito penal, em Processo Administrativo Disciplinar - PAD ou em Sindicância, decorrente de infrações cometidas no exercício das atribuições do cargo, quando o usuário estiver na seguinte situação:

I - afastado temporariamente do cargo ou função pública em razão de ato que se encontra sob apuração, enquanto durar o afastamento;

II - indiciado em processo administrativo disciplinar, por incursão nos incisos IX, XI, XII, XV, XVI e XVII do art. 117 e arts. 130 e 132 da Lei nº 8.112, de 11 de dezembro de 1990, ou cuja proposta pela Comissão Processante, no relatório final, seja pela aplicação de penalidade a partir de suspensão de 30 (trinta) dias, enquanto durar o processo, ou até o efetivo cumprimento da penalidade porventura aplicada; e

III - submetido à prisão em flagrante, temporária ou preventiva decorrente do cometimento de suposta infração no exercício das atribuições do cargo, enquanto durarem as investigações.

Art. 23. A Rede de Dados Corporativa compõe a infraestrutura de rede, que é disponibilizada para uso institucional, logo, apenas equipamentos de propriedade do INSS são autorizados e devem ser conectados à rede corporativa.

Art. 24. Em casos excepcionais, será permitida a conexão de computadores particulares à rede corporativa em razão de interesse do INSS e sob autorização do responsável pela gestão da unidade em que o equipamento estiver localizado, sendo recomendável consulta à área de TI em caso de dúvidas quanto a eventuais riscos.

Parágrafo único. A conexão de qualquer outro tipo de dispositivo à rede corporativa requererá autorização expressa da área de Segurança de TI do INSS.

Art. 25. O INSS poderá disponibilizar o acesso à rede de dados corporativa por meio de tecnologia wireless (sem fio). Para tanto, os seguintes critérios deverão ser adotados:

I - os projetos que envolvam a utilização de pontos de acesso sem fio à rede corporativa no âmbito do Instituto deverão ser previamente aprovados pela DTI;

II - os pontos de acesso à rede de dados corporativa sem fio poderão ser objeto de testes periódicos de intrusão, e de auditoria a critério da área de Segurança da DTI; e

III - as conexões à rede sem fio serão avaliadas pela área de Segurança de TI do INSS em relação aos requisitos de segurança, e deverão atender ao princípio do privilégio mínimo.

§ 1º A DTI poderá disponibilizar rede sem fio com regras específicas de acesso para visitantes nas unidades do INSS.

§ 2º Os dispositivos conectados à rede do INSS por meio de conexão sem fio deverão suportar configurações de criptografia estabelecidas pela DTI;

§ 3º Qualquer tecnologia de acesso sem fio implementada no INSS deverá suportar autenticação forte, com possibilidade de efetuar checagens em bancos de dados externos, e a DTI deve dispor de mecanismos automáticos que possibilitem:

I - a detecção e bloqueio de equipamentos externos conectados à rede corporativa; e

II - a identificação e rastreamento dos endereços IP de origem e destino, bem como os serviços utilizados na rede corporativa, inclusive nos acessos remotos.

§ 4º Até que haja contratação do serviço de provimento de links diretamente pelo INSS, a administração da rede corporativa é realizada pela DATAPREV, e segue as seguintes premissas:

I - prover, gerenciar e operacionalizar os ativos, acessos e serviços que compõem a rede de dados corporativa do INSS; e

II - submeter-se a monitoramento executado pelo INSS ou por prestador de serviço contratado, seguindo as regras desta Portaria Conjunta.

§ 5º Quanto ao processo de geração de contas de serviço, fica estabelecido que:

I - os critérios para a emissão de contas de serviço serão vinculados a um processo formal estabelecido pela DTI;

II - a concessão de contas de serviço deve ser feita conforme a necessidade de uso de acordo com os critérios estabelecidos nesta Portaria Conjunta;

III - o direito de acesso privilegiado, por meio de contas de serviço, associado a sistemas ou processos, deve ser identificado;

IV - deve ser viabilizada ferramenta que possibilite a gestão das contas de serviço de forma automatizada, possibilitando o registro e verificação de todos os privilégios concedidos;

V - as contas de serviço fornecidas devem ser utilizadas exclusivamente para os fins aos quais foram concedidas;

VI - as contas de serviço emitidas devem ser revalidadas periodicamente com base na função exercida e na área de atuação do servidor; e

VII - as contas de serviço com credenciais de acesso de uso compartilhado devem ter suas senhas alteradas periodicamente, conforme estabelecido nesta Portaria Conjunta, ou sempre que ocorrerem mudanças no grupo de usuários que utilizam as mesmas.

Art. 26. É vedado:

I - o acesso por meio de equipamento não homologado ou não autorizado pelo INSS;

II - o download, instalação ou utilização de sistemas ou aplicativos que não sejam estritamente necessários à execução das atribuições do usuário nos equipamentos de propriedade do INSS ou providos por este;

III - a utilização de softwares particulares em equipamentos de propriedade do INSS sem autorização expressa da área de Segurança de TI, facultada à Administração a instalação de soluções de proteção contra ameaças provida pelo Instituto;

IV - a instalação e conexão de equipamentos particulares à rede corporativa do INSS sem a prévia autorização do gestor responsável pela unidade ou da DTI;

V - o uso dos recursos de rede para fins particulares ou de terceiros alheios aos interesses do INSS, em especial, quando tal procedimento prejudique o tráfego da rede de dados;

VI - o uso para fins de divulgação ou distribuição de material que não possua vínculo com as atividades desenvolvidas pelo INSS;

VII - a instalação ou utilização de ferramentas de monitoramento de rede sem a anuência e autorização expressa da DTI;

VIII - a instalação de dispositivos particulares de comunicação ou de compartilhamento de dados sem fio à rede corporativa do INSS sem autorização expressa da DTI; e

IX - burlar ou desativar mecanismos de controle das regras de acesso à internet, gerenciamento de conteúdo ou outros recursos de segurança e monitoramento institucionais nos equipamentos de propriedade do Instituto ou providos por este.

Parágrafo único. Cabe à DTI definir os aspectos relacionados à plataforma tecnológica, gestão operacional, forma de autenticação e sustentação do domínio de rede do INSS.

Art. 27. A Gestão do Acesso aos Sistemas Corporativos seguirá as seguintes premissas:

I - sistemas legados:

a) as regras estabelecidas nesta Portaria Conjunta devem ser aplicadas, guardando-se as devidas limitações tecnológicas, aos sistemas legados; e

b) o controle de acesso aos sistemas legados é efetuado por base própria.

II - sistemas de apoio à administração:

a) os ambientes de hospedagem desses sistemas são suportados por terceiros;

b) o ambiente deverá ser gerenciado e operacionalizado pela DTI;

c) o acesso pelos usuários a esses sistemas deverá ser autenticado pelo serviço de diretório utilizado pelo INSS; e

d) as regras de hospedagem de sistemas serão definidas, em ato próprio, pela DTI.

III - armazenamento de logs:

a) as áreas responsáveis pela gestão de sistemas corporativos e demais aplicações devem definir, em conjunto com a DTI, a temporalidade de guarda dos logs de acesso e transações;

b) o INSS poderá alterar a temporalidade destes dados em ato específico; e

c) os logs de acesso devem contemplar minimamente os registros relacionados no Anexo II.

Art. 28. A operacionalização da gestão dos acessos aos sistemas corporativos do INSS se dará por meio dos seguintes papéis:

I - administrador de sistema do INSS: servidor do quadro de Pessoal em atividade do INSS, lotado, ou em Programa de Gestão da DTI, designado por meio de Portaria da autoridade máxima de TI do INSS, a ser publicada em Boletim de Serviço - BS, responsável pela administração da ferramenta de gestão de acesso aos sistemas corporativos do INSS;

II- gestor de sistema: servidor do quadro de Pessoal em atividade do INSS, lotado na Administração Central do INSS, indicado e designado por meio de Portaria a ser publicada em BS por titular da Presidência e suas Coordenações-Gerais, das Diretorias, da Auditoria-Geral, da Corregedoria-Geral ou da Procuradoria Federal Especializada junto ao INSS - PFE-INSS. O gestor de sistema é responsável pela implementação de sistemas corporativos do INSS;

III - gestor de acesso central: servidor do quadro de Pessoal em atividade do INSS, lotado na Administração Central do INSS, indicado e designado por meio de Portaria a ser publicada em BS por titular da Presidência e suas Coordenações-Gerais, das Diretorias, da Auditoria-Geral, da Corregedoria-Geral ou da Procuradoria Federal Especializada junto ao INSS - PFE-INSS. É responsável pela manutenção dos perfis de gestão dos usuários nas áreas que compõem a Administração Central e, quando necessário, dos gestores de acesso das Superintendências Regionais - SR;

IV - gestor de acesso interno: servidor do quadro de Pessoal em atividade do INSS, lotado na Administração Central do INSS, SR, Gerência Executiva - GEX ou Agência da Previdência Social - APS, indicado pelo Gestor de Acesso Central ou por um Gestor de Acesso, responsável pela atribuição do perfil de acesso e de gestão dos usuários no INSS; e

V - gestor de acesso externo: pessoa formalmente indicada por documento previsto no instrumento legal que firmou a parceria, ou por meio de Ofício de lavra do representante máximo de uma Entidade Externa, responsável pelo cadastro de usuários externos e pela gestão dos acessos aos sistemas corporativos do INSS.

Art. 29. A área de Segurança de TI, em conjunto com as áreas gestoras de sistemas corporativos, deverá formular regras que visem impedir que um usuário possa atribuir a outro o mesmo grau de privilégios que possuir, ou superior.

Art. 30. Os perfis de acesso serão atribuídos de acordo com a necessidade do fluxo de operação definido para cada sistema corporativo do INSS.

Art. 31. A substituição dos responsáveis pela gestão dos acessos aos sistemas corporativos do INSS observará os seguintes procedimentos:

I - o substituto do gestor de acesso será designado pela autoridade responsável pela indicação do titular;

II - quando não houver um gestor responsável ou substituto por uma unidade devidamente designado, a gestão dos usuários será transferida, preferencialmente de forma automática, para o gestor superior da área da abrangência daquela unidade e assim subsequentemente; e

III - o gestor de acesso é corresponsável pelos perfis atribuídos.

Art. 32. Ao usuário interno cabe:

I - fazer uso dos perfis de acesso atribuídos aos sistemas corporativos do INSS, de acordo com as regras e requisitos estabelecidos nesta Portaria Conjunta e suas normas complementares;

II - solicitar, ao gestor de acesso responsável pela gestão da unidade de lotação à qual é vinculado, a suspensão do seu perfil de acesso nos períodos de afastamento do serviço por mais de 30 (trinta) dias consecutivos;

III - manter sigilo das informações não públicas obtidas por meio do perfil concedido para acesso à rede de dados e aos recursos e sistemas corporativos do INSS; e

IV - ter conhecimento e estar de acordo com o disposto nesta Portaria Conjunta.

Art. 33. Ao usuário externo cabe:

I - fazer uso dos perfis de acesso atribuídos aos sistemas corporativos do INSS de acordo com as regras e requisitos estabelecidos nesta Portaria Conjunta;

II - solicitar, ao gestor de acesso responsável pela gestão da unidade de lotação a qual é vinculado a suspensão do seu perfil de acesso nos períodos de afastamento do serviço por mais de 30 (trinta) dias consecutivos;

III - manter sigilo das informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS; e

IV - ter conhecimento e estar de acordo com o disposto nesta Portaria Conjunta.

Art. 34. Ao administrador do sistema INSS cabe:

I - criar os sistemas e subsistemas, devidamente homologados pela área de negócio responsável, no ambiente de produção, por meio de ferramenta de gestão de acesso;

II - mediante apresentação de Portaria de designação para Gestores de Acesso Central, efetuar a atribuição ou alteração dos perfis de gestão por meio de ferramenta de gestão de acessos, e orientar os gestores quanto à atribuição dos perfis de gestão; e

III - mediante apresentação de Portaria de designação para Gestores de Sistema, efetuar a atribuição ou alteração dos perfis de gestão por meio de ferramenta de gestão de acessos, e orientar os gestores acerca do processo de implementação dos sistemas corporativos do INSS.

Art. 35. Ao gestor de sistema cabe:

I - efetuar os procedimentos de importação, inclusão, alteração e exclusão de papéis e permissões nos sistemas corporativos do INSS em ambiente de produção; e

II - atuar, em conjunto com o Administrador do Sistema do INSS e a DATAPREV, no planejamento e execução do processo de implementação dos sistemas corporativos do INSS dos quais for designado responsável.

Art. 36. Ao gestor de acesso central cabe:

I - efetuar o credenciamento, suspensão ou exclusão de perfis de gestão dos sistemas corporativos do INSS aos Gestores de Acesso na Administração Central e, quando necessário, dos Gestores de Acesso da SR, GEX, APS e demais usuários de sua abrangência; e

II - orientar os usuários de sua abrangência e os gestores da Administração Central, SR, GEX e APS acerca das regras para o acesso aos sistemas corporativos do INSS.

Art. 37. Ao gestor de acesso interno cabe:

I - efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos do INSS aos usuários da Administração Central, SR, GEX e APS;

II - atribuir, alterar ou excluir os perfis de acesso aos usuários da Administração Central, SR, GEX e APS;

III - orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS;
e

IV - suspender os perfis de acesso atribuídos a usuários sob sua responsabilidade nos períodos de afastamento do serviço por mais de 30 (trinta) dias consecutivos.

Art. 38. Ao gestor de acesso externo cabe:

I - efetuar o credenciamento ou exclusão dos perfis de gestão dos sistemas corporativos do INSS aos usuários do seu Órgão/Entidade;

II - atribuir, alterar ou excluir os perfis de acesso aos usuários do seu Órgão/Entidade;

III - orientar os usuários acerca das regras para o acesso aos sistemas corporativos do INSS;
e

IV - suspender os perfis de acesso atribuídos a usuários sob sua responsabilidade nos

períodos de afastamento do serviço por mais de 30 (trinta) dias consecutivos.

Art. 39. Configura-se mau uso, sujeito a responsabilidade penal, civil e disciplinar:

I - a divulgação, sem autorização expressa da chefia imediata ou do gestor de acesso de sua abrangência, de informações obtidas por meio do perfil concedido para acesso aos sistemas corporativos do INSS;

II - acessar sistemas corporativos do INSS sem autorização prévia, de acordo com os requisitos estabelecidos nesta Portaria Conjunta;

III - utilizar-se das informações obtidas por meio de acesso concedido em desacordo com os procedimentos dispostos nesta Portaria Conjunta e demais atos vigentes na Administração Pública Federal;

IV - compartilhar ou fazer uso das credenciais de acesso de outros usuários aos sistemas corporativos do INSS; e

V - instalar sistemas corporativos do INSS em equipamentos particulares.

Art. 40. Todo acesso à rede de dados e aos recursos e sistemas corporativos do INSS deve ser registrado e monitorado de modo que permita a rastreabilidade, a identificação e o bloqueio de usuários e equipamentos não autorizados. Estas informações devem ser armazenadas por um período de, no mínimo, doze (12) meses.

§ 1º As ocorrências de mau uso do acesso à rede de dados ou dos recursos e sistemas corporativos do INSS não previstas nesta Portaria Conjunta e os casos omissos serão encaminhados para a área de Segurança de TI do INSS para análise e pronunciamento.

§ 2º Identificado mau uso da rede de dados ou dos recursos e sistemas corporativos do INSS, poderá ocorrer o bloqueio preventivo do acesso pela DTI, o encaminhamento de dossiê com as informações para a Corregedoria-Geral do INSS ou Corregedorias-Regionais, nas suas áreas de abrangência, a fim de que seja realizada a análise no âmbito disciplinar.

§ 3º O descumprimento dessa Portaria Conjunta poderá acarretar sanções administrativas, civis e criminais.

Art. 41. As disposições desta Portaria Conjunta deverão ser objeto de comunicação e eventuais solicitações de adequação à DATAPREV, a cargo da DTI.

Art. 42. Esta Portaria Conjunta entra em vigor em 1º de abril de 2022 e deve ser revisada em um período máximo de 3 (três) anos.

**GUILHERME GASTALDELLO PINHEIRO
SERRANO**

Diretor de Tecnologia da Informação e Inovação

JOBSON DE PAIVA SILVEIRA SALES

Diretor de Atendimento



Documento assinado eletronicamente por **GUILHERME GASTALDELLO PINHEIRO SERRANO, Diretor(a) de Tecnologia da Informação e Inovação**, em 01/04/2022, às 18:47, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



Documento assinado eletronicamente por **JOBSON DE PAIVA SILVEIRA SALES, Diretor(a) de Atendimento**, em 01/04/2022, às 18:54, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **6982795** e o código CRC **7ED5731F**.

ANEXO I

PORTARIA CONJUNTA DTI/DIRAT/INSS Nº 3, DE 01 DE ABRIL DE 2022

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF nº _____, documento de identidade nº _____, expedida pelo(a) _____, em _____ lotado no(a) do Instituto Nacional do Seguro Social - INSS, DECLARO, sob pena das sanções cabíveis nos termos da Política de Segurança da Informação - POSIN do INSS que assumo a responsabilidade por:

- I - tratar o(s) ativo(s) de informação como patrimônio do Instituto Nacional do Seguro Social;
- II - utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do INSS;
- III - contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que disciplina a gestão de segurança da informação na Administração Pública Federal, direta e indireta, e dá outras providências;
- IV - utilizar as credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do INSS; e
- V - responder, perante o INSS, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação.

_____, de _____ de _____.

Nome e assinatura do usuário:	Unidade de Lotação:
Nome e assinatura da Autoridade Responsável pela Autorização do Acesso:	

PORTARIA CONJUNTA DTI/DIRAT/INSS Nº 3, DE 01 DE ABRIL DE 2022

REGISTRO DE LOGS

1. Relação dos campos de registros de logs do GERID

1.1. Dados Gerais

1.1.1. Data

1.1.2. Sistema

1.1.3. Ambiente

1.1.4. IP destino

1.1.5. IP origem

1.1.6. CPF usuário

1.1.7 URL de origem

2. Ações:

2.1. CAS (autenticação): Central Authentication Service - Serviço Central de Autenticação

2.1.1. Criação de service ticket (ST)

2.1.2. Criação de ticket granting ticket (TGT)

2.1.3. Validação de ST

2.1.4. Exclusão de ticket TGT

2.1.5. Autenticação com sucesso (login+password)

2.1.6. Autenticação com sucesso (certificado digital)

2.1.7. Autenticação com falha

2.2. GPA: Gerenciamento de Permissão de Acesso

2.2.1. Início de sessão

2.2.2. Dados do usuário em sessão (CPF, NOME, PAPEL)

2.2.3. Requisição de logout

2.2.4. Dados de credenciais

2.2.5. Concessão de credenciais

2.2.6. Alteração de Credenciais

2.2.7. Dados de receptor (CPF, NOME, Lotação)

2.2.8. Inserção de credencial no usuário

2.2.9. Revogação de Credenciais

2.2.10. Pesquisa de credenciais

2.2.11. Pesquisa de usuários

2.2.12. Substituição de gestor

Referência: Processo nº 35014.047735/2020-84

SEI nº 6982795



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Assessoria De Comunicação Social
Coordenação De Comunicação Social
Divisão De Comunicação Administrativa

DESPACHO

Divisão De Comunicação Administrativa, em 01/04/2022

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria De Tecnologia da Informação e Inovação.

Ass.: Publicação de Portaria

1. Trata-se da publicação e divulgação da Portaria DTI/INSS nº 75, de 1º de abril de 2022.
2. Informamos que o referido ato, foi publicado no BSE, de 1º de abril de 2022 e no Portal-INSS, na intraprev.
3. À Diretoria de Tecnologia da Informação e Inovação, para conhecimento e providências julgadas necessárias.

ALDAMIR GERALDO DE LISBÔA LIMA

Chefe da Divisão de Comunicação Administrativa - DIVCA



Documento assinado eletronicamente por **ALDAMIR GERALDO DE LISBOA LIMA, Chefe da Divisão**, em 01/04/2022, às 18:33, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7004857** e o código CRC **FC924DE0**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 7004857



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Tecnologia da Informação e Inovação

DESPACHO

Diretoria De Tecnologia da Informação e Inovação, em 01/04/2022

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria De Tecnologia da Informação e Inovação.

Ass.: Portaria para publicação

1. Trata-se de Portaria Conjunta 3 que institui a Norma de Controle de Acesso Lógico - NCAL do INSS.
2. À DIVCA para ampla divulgação.

GUILHERME GASTALDELLO PINHEIRO SERRANO

Diretor De Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **GUILHERME GASTALDELLO PINHEIRO SERRANO**, **Diretor(a) de Tecnologia da Informação e Inovação**, em 01/04/2022, às 19:07, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7005017** e o código CRC **5F1483BC**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 7005017



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Assessoria De Comunicação Social
Coordenação De Comunicação Social
Divisão De Comunicação Administrativa

DESPACHO

Divisão De Comunicação Administrativa, em 01/04/2022

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria De Tecnologia da Informação e Inovação.

Ass.: Publicação de Portaria Conjunta

1. Trata-se da publicação e divulgação da Portaria Conjunta DTI/DIRAT/INSS nº 3, de 1º de abril de 2022.
2. Informamos que o referido ato, foi publicado no BSE, de 1º de abril de 2022 e no Portal-INSS, na intranet.
3. À Diretoria de Tecnologia da Informação e Inovação, para conhecimento e providências julgadas necessárias.

ALDAMIR GERALDO DE LISBÔA LIMA

Chefe da Divisão de Comunicação Administrativa - DIVCA



Documento assinado eletronicamente por **ALDAMIR GERALDO DE LISBOA LIMA, Chefe da Divisão**, em 01/04/2022, às 19:29, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7005096** e o código CRC **44FE913F**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 7005096



INSTITUTO NACIONAL DO SEGURO SOCIAL
PORTARIA CONJUNTA DTI/DGP/INSS Nº 4, DE 8 DE ABRIL DE 2022

Altera a Portaria Conjunta DTI/DIRAT/INSS nº 3, de 01 de abril de 2022.

O **DIRETOR DE TECNOLOGIA DA INFORMAÇÃO - SUBSTITUTO** e o **DIRETOR DE GESTÃO DE PESSOAS** do **INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS**, no uso das atribuições que lhes conferem o Decreto nº 10.995, de 14 de março de 2022, e considerando o que consta no processos administrativos nºs 35014.126172/2022-51 e 35014.047735/2020-84, e no disposto na Norma de Controle de Acesso Lógico - NCAL instituída pela Portaria Conjunta DTI/DIRAT/INSS Nº 3, de 01 de Abril de 2022,

RESOLVEM:

Art. 1º Alterar o inciso V do Art. 39 da Portaria Conjunta DTI/DIRAT/INSS Nº 3, de 01 de Abril de 2022, que passa a vigorar com a seguinte redação:

"Art. 39

(...)

V - instalar sistemas corporativos do INSS em equipamentos particulares, salvo em caso autorização expressa da DTI ou de permissão normativa específica, sendo presumida nas modalidades de teletrabalho instituídas no âmbito do INSS;"

Art. 2º - Esta Portaria entra em vigor na data de sua publicação, retroagindo seus efeitos a 1º de abril de 2022.

JOÃO RODRIGUES DA SILVA FILHO
Diretor de Tecnologia da Informação - Substituto

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Gestão de Pessoas



Documento assinado eletronicamente por **JOAO RODRIGUES DA SILVA FILHO, Diretor(a) de Tecnologia da Informação Substituto(a)**, em 08/04/2022, às 18:56, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



Documento assinado eletronicamente por **JOBSON DE PAIVA SILVEIRA SALES, Diretor(a) de Gestão de Pessoas**, em 08/04/2022, às 19:52, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7083819** e o código CRC **DBD844CA**.

Brasília, 13 de maio de 2022.

Ao Senhor

JOÃO RODRIGUES DA SILVA FILHO

Diretor de Tecnologia da Informação e Inovação – DTI

Instituto Nacional do Seguro Social

Setor de Autarquias Sul, Quadra 02, Bloco O

70070-946 – Brasília/DF

Assunto: **Portaria DTI/INSS n. 71, de 16 de março de 2022.**
Referência: OFÍCIO SEI N. 29/2022/DTI-INSS - Processo n. 35014.047735/2020-84.

Senhor Diretor,

1. Cumprimentando-o cordialmente, em atenção ao Ofício em referência - pelo qual essa Diretoria envia cópia da Portaria DTI/INSS n. 71, de 16 de março de 2022, que disciplina o uso da internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil, para que a DATAPREV procedesse com as devidas configurações e ajustes necessários para o atendimento do então regulamento pelo normativo - **encaminhamos a V.Sa. o Memorando n. 011/2022, emitido pela Divisão de Indicadores e Conformidade – DIIC/DETI/SUGS/DIT/PR desta Estatal**, contendo o posicionamento da DATAPREV S.A. acerca do assunto.
2. Destarte, aproveitamos a oportunidade para renovar nossos votos de mais alta estima e consideração, bem como para nos colocarmos à disposição para quaisquer esclarecimentos que se façam necessários.

Respeitosamente,



VALTER VINICIUS DE FREITAS
BERNARDES BORGES:01298265614
c=BR, o=ICP-Brasil, ou=Autoridade
Certificadora Raiz Brasileira v2, ou=AC
SOLUTI, ou=AC SOLUTI Multipla,
ou=09461647000195, ou=Certificado PF
A3, cn=VALTER VINICIUS DE FREITAS
BERNARDES BORGES:01298265614
2022.05.13 17:24:59 -03'00'

VINÍCIUS BERNARDES BORGES
Coordenador-Geral do Gabinete da Presidência

Anexo: Memo/DIIC/011/2022 (03 páginas).



**PORTARIA DTI/INSS Nº 71, DE 16 DE
MARÇO DE 2022, constante no OFÍCIO SEI
29/2022/DTI-INSS, de 18 de março de 2022**

MEMO/DIIC/011/2022

Data: 27/04/2022

De: Divisão de Indicadores e Conformidade - DIIC

Para: Diretoria de Relacionamento e Negócio

Assunto: PORTARIA DTI/INSS Nº 71, DE 16 DE MARÇO DE 2022, constante no OFÍCIO SEI 29/2022/DTI-INSS, de 18 de março de 2022

Senhor Diretor,

Cumprimentando-o cordialmente, informamos que, conforme informação do gestor da DAIC (Divisão de Atendimento Interno Computacional), no dia 11 de abril de 2022 ocorreu uma reunião de alinhamento entre a Dataprev e o cliente INSS, onde a Dataprev informou sobre os argumentos técnicos não constantes na referida portaria. Posto isso, ficou definido que o cliente irá interpretar a PORTARIA DTI/INSS Nº 71, DE 16 DE MARÇO DE 2022, constante no OFÍCIO SEI 29/2022/DTI-INSS, de 18 de março de 2022, com os requisitos necessários e irá remeter à Dataprev tão logo seja possível.

Dentro do tratamento a ser realizado mediante ao que foi solicitado, foi observado que, para os usuários enquadrados nos respectivos perfis, será necessário que seja informado (via planilha) que acessos cada perfil irá possuir. A Dataprev irá fornecer uma documentação (planilha) com os perfis e as *urls* para que o cliente possa especificar o que será permitido ou bloqueado em cada item

Atenciosamente,

Claudio Medeiros Utrini dos Santos

Gerente



Documento assinado eletronicamente por CLAUDIO MEDEIROS UTRINI DOS SANTOS
Autenticidade e dados de assinatura podem ser conferidos em:
<http://edoc.dataprev.gov.br/verificarAutenticidadeDocumento.xhtml>
Informando o código de verificação S6V4Mt2e e o contra código k80b6fSG



Assinado digitalmente por:

Claudio Medeiros Utrini dos Santos (Aprovador)



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação

DESPACHO

Diretoria de Tecnologia da Informação, em 16/05/2022

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria de Tecnologia da Informação.

Ass.: Portaria 71.

1. Trata-se da Portaria DTI/INSS nº 71, de 16 de março de 2022 (6757423), que disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.
2. Dada ciência ao OFÍCIO N. 444/2022/CGPR/PR (7458804) e ao MEMO/DIIC/011/2022 (7458813), emitidos pela Dataprev em resposta ao Ofício SEI nº 29/2022/DTI-INSS (6803101).
3. Encaminhe-se à Divisão de Segurança em TI - DSEG, com ciência da Coordenação-Geral de Infraestrutura e Segurança em TI - CGIS, para ciência, avaliação e providências cabíveis.

JOÃO RODRIGUES DA SILVA FILHO

Diretor de Tecnologia da Informação



Documento assinado eletronicamente por **JOAO RODRIGUES DA SILVA FILHO**, Diretor(a) de **Tecnologia da Informação**, em 16/05/2022, às 18:49, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7458959** e o código CRC **D1F507C4**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 7458959



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação

MINUTA DE PORTARIA DTI/INSS Nº 7578375, DE 30 DE MAIO DE 2022

Designa o Gestor de Segurança da Informação e o Gestor de Segurança da Informação Substituto.

O PRESIDENTE DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso das atribuições que lhe confere o Decreto nº 10.995, de 14 de março de 2022, e considerando o que dispõe o art. 15, inciso I, da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, bem como o que consta no Processo Administrativo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Designar o servidor JULLYANO LINO DA SILVA, matrícula nº 1.786.967, como Gestor de Segurança da Informação do INSS.

Parágrafo único. O servidor designado no **caput** será substituído pelo servidor LUZIVAN DE MOURA GOIS, matrícula nº 1.784.525, em suas ausências e afastamentos legais.

Art. 2º São competências do Gestor de Segurança da Informação do INSS, de acordo com o disposto no art. 19 da Instrução Normativa GSI/PR nº 1, de 2020:

- I - coordenar o Comitê de Segurança da Informação ou estrutura equivalente;
- II - coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do órgão, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;
- III - assessorar a alta administração na implementação da Política de Segurança da Informação;
- IV - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;
- V - promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade;
- VI - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

VII - propor recursos necessários às ações de segurança da informação;

VIII - acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes Cibernéticos;

IX - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

X - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

XI - manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Art. 3º A gestão da Segurança da Informação é considerada serviço de natureza relevante e não ensejará qualquer tipo de remuneração adicional.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

Art. 5º Ficam revogados os seguintes atos:

I - Portaria nº 1.246/PRES/INSS, de 18 de dezembro de 2020;

II - Portaria nº 1.377/PRES/INSS, de 8 de novembro de 2021.

GUILHERME GASTALDELLO PINHEIRO SERRANO

Presidente



Documento assinado eletronicamente por **JOAO RODRIGUES DA SILVA FILHO**, **Diretor(a) de Tecnologia da Informação**, em 30/05/2022, às 21:27, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7578375** e o código CRC **63C6F4CA**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação

DESPACHO

Diretoria de Tecnologia da Informação, em 30/05/2022

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria de Tecnologia da Informação.

Ass.: Minuta de Portaria | Designação do Gestor de Segurança da Informação do INSS.

1. Trata-se da Minuta Portaria (7578375), emitida por esta DTI, em substituição às Portarias nº 1.246/PRES/INSS, de 18 de dezembro de 2020 (2489775) e 1.377/PRES/INSS, de 8 de novembro de 2021 (5463068), que designam o Gestor de Segurança da Informação e o Gestor de Segurança da Informação Substituto do INSS.
2. Encaminhe-se à Coordenação de Suporte ao Gabinete - CSG para avaliação e prosseguimento.

JOÃO RODRIGUES DA SILVA FILHO

Diretor de Tecnologia da Informação



Documento assinado eletronicamente por **JOAO RODRIGUES DA SILVA FILHO**, **Diretor(a) de Tecnologia da Informação**, em 30/05/2022, às 21:27, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7578593** e o código CRC **09634EDA**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 7578593



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência

Gabinete

Coordenação De Suporte ao Gabinete

PORTARIA PRES/INSS Nº , DE DE JUNHO DE 2022

O **PRESIDENTE DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS**, no uso das atribuições que lhe confere o Decreto nº 10.995, de 14 de março de 2022, e considerando o que dispõe o inciso I do art. 15 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, bem como o que consta no Processo Administrativo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Designar o servidor JULLYANO LINO DA SILVA, matrícula nº 1.786.967, como Gestor de Segurança da Informação do INSS.

Parágrafo único. O servidor designado no **caput** será substituído pelo servidor LUZIVAN DE MOURA GOIS, matrícula nº 1.784.525, nos afastamentos e impedimentos legais do titular e na vacância do encargo.

Art. 2º As competências do Gestor de Segurança da Informação estão elencadas no art. 19 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020.

Parágrafo único. A gestão da Segurança da Informação é considerada serviço de natureza relevante e não ensejará qualquer tipo de remuneração adicional.

Art. 3º Fica revogada a Portaria nº 1.246/PRES/INSS, de 18 de dezembro de 2020, publicada no Boletim de Serviço nº 242, de 18 de dezembro de 2020.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

GUILHERME GASTALDELLO PINHEIRO SERRANO

Presidente



Documento assinado eletronicamente por **CINTHYA DE AVILA OLIVEIRA TROJAN REPISO**, **Assistente**, em 03/06/2022, às 10:26, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7633704** e o código CRC **735D4A7A**.

Referência: Processo nº 35014.047735/2020-84

SEI nº 7633704



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Gabinete
Coordenação de Suporte ao Gabinete

DESPACHO

Coordenação de Suporte ao Gabinete, em 2/6/2022.

Ref.: Processo
nº 35014.047735/2020-84.

Int.: Diretoria de
Tecnologia da Informação
- DTI.

Ass.: Minuta de portaria.

1. Trata-se de minuta de de Portaria, advinda da DTI, com intuito de designar o Gestor de Segurança da Informação do INSS e seu substituto, em substituição à Portaria nº 1.246/PRES/INSS, de 18 de dezembro de 2020 (2489775).

2. Consigna-se que não consta dos autos a Nota Técnica prevista no inciso III do art. 13 da Portaria PRES/INSS nº 1.313, de 17 de junho de 2021, com vistas a apresentar as justificativas e fundamentações da edição da Portaria em questão, ausência que poderá ser suprida posteriormente.

3. Sobre a adequação do Ato em comento, dispõem o art. 9º e o inciso II do art. 17 da Portaria PRES/INSS nº 1.313, de 2021, que versa sobre a elaboração, redação, alteração e revogação dos atos administrativos no âmbito do INSS:

Art. 9º A revogação e a alteração deverão ser procedidas por ato de mesma denominação e hierarquia, salvo disposição legal em contrário.

Art. 17. Portaria é o ato administrativo, editado por uma ou mais autoridades singulares competentes, no âmbito de suas atribuições regimentais, com caráter:

.....

II - constitutivo, quando tratar de matéria de pessoal ou não contiver conteúdo normativo, ou seja:
a) for portaria de pessoal, referente a agente público nominalmente identificado;

4. Logo, está adequada a modalidade de ato constitutivo escolhida, pois identifica o agente público nominalmente.

5. Sobre as regras para elaboração, articulação e redação da proposta em questão, consigna-se a adequação com as regras estabelecidas na Lei Complementar nº 95, de 26 de fevereiro de 1998, no Decreto nº 9.191, de 1º de novembro de 2017, e na Portaria PRES/INSS nº 1.313, de 2021, sendo analisada e formatada por esta Coordenação, com alterações de cunho meramente formal.

6. Salienta-se que é dispensável o trâmite pela Procuradoria Federal Especializada junto ao INSS, no caso de minuta de portaria de designação ou destituição de gestores de sistemas ou de contratos, nos termos da alínea "b" do inciso I do § 1º do art. 14 da Portaria PRES/INSS nº 1.313, de 2021.

7. Ante o exposto, encaminhe-se ao Gabinete da Presidência, não havendo óbice para sua assinatura.

CINTHYA DE ÁVILA O. T. REPISO

Analista do Seguro Social

DIOGO FREITAS FIGUEIREDO

Coordenador de Suporte ao Gabinete



Documento assinado eletronicamente por **DIOGO FREITAS FIGUEIREDO, Coordenador(a)**, em 03/06/2022, às 10:14, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



Documento assinado eletronicamente por **CINTHYA DE AVILA OLIVEIRA TROJAN REPISO, Assistente**, em 03/06/2022, às 10:21, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7633960** e o código CRC **895B6001**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 7633960



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência

PORTARIA PRES/INSS Nº 728, DE 3 DE JUNHO DE 2022

O **PRESIDENTE DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS**, no uso das atribuições que lhe confere o Decreto nº 10.995, de 14 de março de 2022, e considerando o que dispõe o inciso I do art. 15 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, bem como o que consta no Processo Administrativo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Designar o servidor JULLYANO LINO DA SILVA, matrícula nº 1.786.967, como Gestor de Segurança da Informação do INSS.

Parágrafo único. O servidor designado no **caput** será substituído pelo servidor LUZIVAN DE MOURA GOIS, matrícula nº 1.784.525, nos afastamentos e impedimentos legais do titular e na vacância do encargo.

Art. 2º As competências do Gestor de Segurança da Informação estão elencadas no art. 19 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020.

Parágrafo único. A gestão da Segurança da Informação é considerada serviço de natureza relevante e não ensejará qualquer tipo de remuneração adicional.

Art. 3º Fica revogada a Portaria nº 1.246/PRES/INSS, de 18 de dezembro de 2020, publicada no Boletim de Serviço nº 242, de 18 de dezembro de 2020.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

GUILHERME GASTALDELLO PINHEIRO SERRANO

Presidente



Documento assinado eletronicamente por **GUILHERME GASTALDELLO PINHEIRO SERRANO, Presidente**, em 03/06/2022, às 15:45, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7686939** e o código CRC **BD0463EB**.

Referência: Processo nº 35014.047735/2020-84

SEI nº 7686939



INSTITUTO NACIONAL DO SEGURO SOCIAL
GABINETE DA PRESIDÊNCIA
Serviço Técnico Administrativo

DESPACHO

SERVIÇO TÉCNICO ADMINISTRATIVO DO GABINETE, em 3/6/2022

Ref.: Processo nº
35014.047735/2020-84

Int.: Diretoria de
Tecnologia da Informação

Ass.: Gestor de Segurança
da Informação do INSS

Restitua-se à Diretoria de Tecnologia da Informação, de ordem, após publicação da Portaria PRES/INSS nº 728, de 3 de junho de 2022, no BSE de 3 de junho de 2022, para as providências decorrentes.

VINICIUS ROSA RODRIGUES

Chefe de Serviço Técnico Administrativo do Gabinete



Documento assinado eletronicamente por **VINICIUS ROSA RODRIGUES, Chefe de Serviço Técnico Administrativo do Gabinete**, em 03/06/2022, às 15:58, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7696406** e o código CRC **C42B570C**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 7696406



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Assessoria De Comunicação Social
Coordenação De Comunicação Social
Divisão De Comunicação Administrativa

DESPACHO

Divisão De Comunicação Administrativa, em 03/06/2022

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria de Tecnologia da Informação

Ass.: Publicação de Portaria

1. Trata-se da publicação e divulgação da Portaria PRES/INSS nº 728, de 3 de junho de 2022.
2. Informamos que o referido ato, foi publicado no BSE, de 3 de junho de 2022 e no Portal-INSS, na intranet.
3. Ao Serviço Técnico Administrativo da Diretoria de Tecnologia da Informação, para conhecimento e providências julgadas necessárias.

ALDAMIR GERALDO DE LISBÔA LIMA

Chefe da Divisão de Comunicação Administrativa - DIVCA



Documento assinado eletronicamente por **ALDAMIR GERALDO DE LISBOA LIMA**, Técnico do Seguro Social, em 03/06/2022, às 16:42, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7696669** e o código CRC **797933B0**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 7696669



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação
Serviço Técnico Administrativo

DESPACHO

Serviço Técnico Administrativo, em 06/06/2022

Ref.: Processo nº 35014.047735/2020-84.

Int.: DTI

Ass.: Portaria para publicação.

1. Após publicação, encerre-se na unidade.

CLEONICE MARIA APARECIDA BARBOZA ALVES

Chefe do Serviço Técnico Administrativo



Documento assinado eletronicamente por **CLEONICE MARIA APARECIDA BARBOZA ALVES**, **Chefe de Serviço Técnico Administrativo**, em 07/06/2022, às 11:38, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7725588** e o código CRC **06747251**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 7725588



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação
Coordenação-Geral de Infraestrutura e Segurança em Tecnologia da Informação
Coordenação de Infraestrutura e Monitoramento de Tecnologia da Informação
Divisão de Segurança em Tecnologia da Informação

DESPACHO

Divisão de Segurança em Tecnologia da Informação, em 09/06/2022

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria de Tecnologia da Informação.

Ass.: Portaria DTI/INSS nº 71, de 16 de março de 2022

1. Trata-se da Portaria DTI/INSS nº 71, de 16 de março de 2022 (6757423), que disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.

2. Ciente do Despacho DTI 7458959.

3. Com base em dados que solicitamos à Dataprev com os perfis de acesso à internet atualmente existentes e com usuários atribuídos, identificamos a existência de sete perfis de acesso à internet em nossa rede com as seguintes quantidades de usuários para cada perfil:

Perfis Internet INSS	
Perfil	Quantidade
0	1582
1	8296
2	5897
3	13184
4	342
5	58
6	2
TOTAL	29361

4. Considerando inexistir a previsão de perfis 0, 5 e 6 na citada Portaria DTI/INSS nº 71, de 16 de março de 2022 (6757423), abrimos chamados junto à Dataprev para que procedessem conforme a seguir:

I - Chamado 2580447/2022: Solicitado que fosse atribuído o **perfil 1** a todos os usuários com atual *perfil 0*.

II - Chamado 2580458/2022: Solicitado que fosse atribuído o **perfil 4** a todos os usuários com atual *perfil 5* e *perfil 6*.

5. Os chamados acima foram atendidos em 30/05/2022.
6. Feitas as considerações, encaminhe-se à DTIR, COIM, CGIS e DTI para conhecimento.

LUZIVAN DE MOURA GOIS

Chefe da Divisão de Segurança em Tecnologia da Informação



Documento assinado eletronicamente por **LUZIVAN DE MOURA GOIS, Chefe de Divisão de Segurança em Tecnologia da Informação**, em 09/06/2022, às 22:17, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7769927** e o código CRC **1F7503C8**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 7769927



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação

DESPACHO

Diretoria de Tecnologia da Informação, em 10/06/2022

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria de Tecnologia da Informação.

Ass.: Portaria DTI/INSS nº 71 - disciplina o uso da Internet no INSS.

1. Trata-se da Portaria DTI/INSS nº 71, de 16 de março de 2022 (6757423), que disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.
2. Ciente do despacho DSEG 7769927.
3. Conclui-se o presente nesta unidade.

JOÃO RODRIGUES DA SILVA FILHO

Diretor de Tecnologia da Informação



Documento assinado eletronicamente por **JOAO RODRIGUES DA SILVA FILHO**, Diretor(a) de **Tecnologia da Informação**, em 14/06/2022, às 18:50, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7781605** e o código CRC **A3A03470**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 7781605



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação
Coordenação-Geral de Infraestrutura e Segurança em Tecnologia da Informação

DESPACHO

Coordenação-Geral de Infraestrutura e Segurança em Tecnologia da Informação, em 15/08/2022

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria de Tecnologia da Informação.

Ass.: Portaria DTI/INSS nº 71 - disciplina o uso da Internet no INSS.

1. Trata-se da Portaria DTI/INSS nº 71, de 16 de março de 2022 (6757423), que disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.
2. Ciente do despacho DSEG 7769927.
3. Conclui-se o presente nesta unidade.

JOÃO HENRIQUE MOURÃO DE MARCO

Coordenador-Geral de Infraestrutura e Segurança em Tecnologia da Informação



Documento assinado eletronicamente por **JOAO HENRIQUE MOURAO DE MARCO**, Coordenador(a)-Geral de Infraestrutura e Segurança em Tecnologia da Informação, em 16/08/2022, às 00:15, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **8539552** e o código CRC **373DFA33**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 8539552



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação
Coordenação-Geral de Infraestrutura e Segurança em Tecnologia da Informação
Coordenação de Infraestrutura e Monitoramento de Tecnologia da Informação
Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos

DESPACHO

Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos, em 17/08/2022

Ref.: Processo nº 35014.047735/2020-84.

Int.: DTI.

Ass.: Portaria DTI/INSS nº 71 - disciplina o uso da Internet no INSS.

1. Trata-se da Portaria DTI/INSS nº 71, de 16 de março de 2022 (6757423), que disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.
2. Ciente do despacho DSEG 7769927.
3. Conclua-se nessa Divisão.

FRANCISCO HUMBERTO MENDONÇA DE ARAUJO

Chefe da Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos



Documento assinado eletronicamente por **FRANCISCO HUMBERTO MENDONÇA DE ARAUJO**, **Chefe da Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos**, em 17/08/2022, às 09:51, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **8564402** e o código CRC **B36D845D**.



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria de Tecnologia da Informação
Coordenação-Geral de Tecnologia da Informação e Segurança

DESPACHO

Coordenação-Geral de Tecnologia da Informação e Segurança, em 22/11/2023

Ref.: Processo nº 35014.047735/2020-84.

Int.: DTI.

Ass.: Nomeação Gestor de Segurança da Informação

1. Trata-se da proposta de nomeação dos servidores relacionados para substituição dos Gestor de Segurança da Informação do Instituto Nacional do Seguro Social e substituto.
3. Tal substituição se faz necessária considerando a cessão do Gestor JULLYANO LINO DA SILVA e as alterações ocorridas na estrutura do INSS.
4. Feitas as considerações, encaminhe-se à DTI para avaliação com sugestão de envio à Presidência para publicação.

ISRAEL EDUARDO ZEBULON MARTINS DE SOUZA

Coordenação-Geral de Tecnologia da Informação e Segurança



Documento assinado eletronicamente por **ISRAEL EDUARDO ZEBULON MARTINS DE SOUZA**, Coordenador(a)-Geral de Dados e Sistemas de Informação, em 22/11/2023, às 14:39, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **14074996** e o código CRC **17EFA79D**.



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria de Tecnologia da Informação
Coordenação-Geral de Tecnologia da Informação e Segurança

MINUTA DE PORTARIA CGTIS/INSS Nº 4, DE 04 DE MARÇO DE 2024

Disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.

O DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO - INSS, no uso da competência que lhe confere o Decreto nº 9.746, de 8 de abril de 2019, e tendo em vista o que consta no Processo Administrativo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Esta norma se aplica a todos os servidores e colaboradores, vinculados direta ou indiretamente ao INSS, bem como a servidores e empregados de entidades e órgãos da Administração Pública ou privados que necessitem ou estejam autorizados a acessar a Internet a partir da rede corporativa do Instituto.

Parágrafo único. Equiparam-se a usuários do INSS, para todos os efeitos, os Advogados e Procuradores Públicos Federais vinculados à Advocacia-Geral da União – AGU que atuem na consultoria, assessoramento jurídico e na representação judicial e extrajudicial do INSS e os servidores vinculados à Subsecretaria da Perícia Médica Federal.

Art. 2º Para os efeitos desta norma, ficam estabelecidos os seguintes conceitos e definições:

- I - Autorizador: ocupantes de cargo responsáveis pela autorização da concessão de perfis de acesso para usuários finais de sua área de abrangência;
- II - Internet: rede mundial que interliga computadores de diferentes tipos e dimensões e permite a comunicação entre pessoas e organizações, independentemente da localização geográfica;
- III - Intranet: rede de computadores administrada pelo INSS, que utiliza os mesmos serviços e tecnologias disponíveis na rede mundial;
- IV - Perfil de acesso: atributo que estabelece as categorias de sítios acessíveis e tipos de arquivos que podem ser recebidos ou transmitidos pelos usuários;
- V - Proxy: ferramenta que desempenha a função de conexão do computador local à rede externa (Internet);
- VI - Sítio: conjunto de informações ou serviços disponíveis na Internet ou na Intranet, organizados em páginas eletrônicas e acessíveis por meio de endereços que identificam, de forma padronizada, sua origem e conteúdo;
- VII - Usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal - APF, formalizada por meio da assinatura do Termo de Responsabilidade; e
- VIII - VPN: Rede Privada Virtual (Virtual Private Network) conexão segura e criptografada sobre uma rede, garantindo que os dados transmitidos através desse túnel sejam privados e protegidos.

Art. 3º O acesso pelos usuários à Internet disponibilizado pelo INSS deverá pautar-se pelas seguintes diretrizes:

- I - Seu uso se dará exclusivamente em razão de trabalho e de acordo com os procedimentos dispostos nesta Norma;
- II - Os recursos disponibilizados pelo INSS não poderão ser usados para quaisquer propósitos ilegais ou proibidos, que possam danificar, desativar, sobrecarregar ou prejudicar qualquer área, serviço ou conteúdo, ou interferir no uso e execução das atividades laborais de outros usuários;
- III - O volume de tráfego de Internet e os endereços web visitados poderão ser monitorados, visando assegurar o cumprimento desta norma; e
- IV - O acesso à Internet para propósitos particulares ou estranhos às atividades do INSS poderá ser bloqueado, sem prévia comunicação ao usuário e sem prejuízo das demais sanções aplicáveis.

Art. 4º O acesso aos sítios da Internet para todos os usuários será realizado mediante a atribuição de perfis de acesso, distribuídos nos seguintes níveis:

- I - Perfil 1: Perfil Restrito, inicialmente atribuído a usuários com maior restrição de acesso à Internet, permitindo acesso somente a sítios governamentais, instituições bancárias e sítios considerados de interesse do INSS;
- II - Perfil 2: Perfil Básico, inicialmente atribuído a estagiários, recepcionistas e usuários externos, permitindo acesso a todos os sítios permitidos pelo Perfil 1 e a sítios de provedores de e-mail pessoal e instituições de ensino;
- III - Perfil 3: Perfil Padrão, para os servidores do quadro do Instituto, permitindo acesso a todos os sítios da Internet, exceto redes sociais e aqueles que contêm veiculação de material em áudio e vídeo; e
- IV - Perfil 4: Perfil Avançado, atribuído preferencialmente a servidores, colaboradores e estagiários que desempenham funções relacionadas a Comunicação Social, Desenvolvimento de Pessoas e gestores, dentre outras situações específicas, respeitado o princípio da necessidade de conhecer e demandando designação dos Autorizadores deste Perfil, permitindo o acesso a todos os sítios da Internet, incluindo sítios que veiculam material em áudio e vídeo (streaming), sítios de compartilhamento de vídeos, blogs e redes sociais.

§ 1º O perfil concedido a agentes externos será de caráter temporário, com validade equivalente à vigência do trabalho a ser executado.

§ 2º Os processos de alteração, bloqueio, liberação e categorização de sítios, assim como a criação e/ou alterações de perfis de acesso descritos nesta Norma, quando necessários, serão definidos pela Diretoria de Tecnologia da Informação e Inovação – DTI.

§ 3º Os novos usuários que não tiverem um perfil de acesso atribuído deverão ser direcionados para uma página da Intranet contendo orientações e normas relacionadas ao acesso à Internet no INSS, definidas pela DTI.

Art. 5º O acesso à Intranet e Internet a partir da rede de dados corporativa nas dependências do INSS e aos demais órgãos da Administração Pública Direta e Indireta, de qualquer das esferas de governo, será concedido exclusivamente a servidores e empregados públicos, efetivos ou ocupantes de cargo em comissão.

§ 1º O acesso de usuários externos das entidades que compõem o Poder Público será concedido mediante o estabelecimento em convênio, contrato, acordo de cooperação técnica ou instrumento congênere, especificamente firmados com o INSS para este fim.

§ 2º O gestor ou Coordenador-Geral da área responsável pelo convênio, contrato, acordo de cooperação técnica ou instrumento congênere assumirá o papel de Autorizador do serviço de acesso à Internet para os usuários externos, e deverá fundamentar as solicitações com base no instrumento.

§ 3º Poderão ser concedidos acessos temporários para auditores de controle interno e externo, vinculados à Controladoria-Geral da União – CGU ou ao Tribunal de Contas da União - TCU, no uso de suas atribuições.

Art. 6º Nas situações em que a atividade necessitar, o acesso à Internet por terceirizados deverá ser concedido a partir da infraestrutura de rede do INSS, desde que preenchidos os seguintes requisitos:

I - O contrato de prestação de serviços deverá conter cláusula de confidencialidade e sigilo de informações preestabelecido com a Administração Pública;

II - A empresa contratada deverá manter com seus funcionários Termo de Confidencialidade;

III - O contrato de prestação de serviços deverá prever a necessidade de acesso à Internet a partir das dependências do INSS; e

IV - O Autorizador, que para estes fins será o gestor do contrato ou o responsável pela área requisitante do serviço, deverá fundamentar as necessidades de acesso dos empregados da contratada, definindo os recursos que serão disponibilizados, endereços da Intranet e Internet necessários para o desenvolvimento das atividades e eventuais restrições a dias e horários para realização do acesso.

Art. 7º A conexão de equipamentos pessoais de visitantes à rede do INSS, quando necessária e motivada pelo interesse da Administração, deverá ser previamente autorizada pelo gestor da unidade onde o equipamento será utilizado.

Parágrafo único. Só será permitida a utilização da rede local por visitantes, caso seus equipamentos atendam a todos os requisitos estabelecidos pela DTI e o acesso se dará, exclusivamente, à Internet, sendo vedado o acesso ao conteúdo disponibilizado na Intranet.

Art. 8º A todos os perfis de acesso descritos nesta Norma aplicam-se as restrições de acesso a sítios que:

I - Contenham material pornográfico ou obsceno;

II - Contenham material ilegal;

III - Disponibilizem jogos, inclusive os da Internet (on line);

IV - Contenham material impróprio, ofensivo, preconceituoso ou discriminatório, que façam apologia à violência, ao terrorismo e às drogas; e

V - Contenha e/ou divulgue conteúdo de violação de direito autoral (pirataria) e/ou execução de quaisquer tipos ou formas de fraudes.

Art. 9º O processo de atribuição de acesso à Internet seguirá as seguintes diretrizes:

I - A atribuição dos perfis de acesso à Internet será feita pelos Autorizadores, de forma fundamentada e respeitando o princípio da necessidade de conhecer, de acordo com a tabela abaixo:

Perfil	Autorizador
Perfil 1, 2, 3	Presidente do INSS, Diretores, Coordenadores-Gerais, Chefes de Assessoria de Comunicação Social nas Superintendências-Regionais, Assessor de Comunicação Social (Administração Central) Auditor-Geral, Corregedor-Geral, Procuradores-Regionais, Procurador-Geral da PFE-INSS, Superintendentes-Regionais, Gerente-Executivo e Gerente de Agência da Previdência Social - APS.
Perfil 4	Presidente do INSS, Diretores, Coordenadores-Gerais, Ouvidor, Chefes de Assessoria de Comunicação Social nas Superintendências-Regionais, Assessor de Comunicação Social (Administração Central), Auditor-Geral, Corregedor-Geral, Procuradores-Regionais, Procurador-Geral da PFE-INSS, Superintendentes-Regionais e Gerentes-Executivos.

II - Nos casos de novos usuários de rede (LDAP), criados por meio de registro de chamado técnico, quando o solicitante não indicar o perfil de acesso à internet, será atribuído o Perfil 1;

III - Para fins de alteração do perfil de acesso, os usuários deverão preencher o Formulário de Solicitação de Acesso à Internet (Anexo II) e providenciar a assinatura no sistema SEI pelo Autorizador do acesso; e

IV - Ao registrar a solicitação, deve-se anexar o Formulário de Solicitação de Acesso à Internet (Anexo I) devidamente preenchido e assinado no sistema SEI (pelo solicitante e autorizador), conforme documento nato digital ou digitalizado no formato PDF.

Art. 10. A solicitação para perfis de acesso em caráter temporário, realizada mediante o Formulário de Solicitação de Acesso à Internet (Anexo II), deverá conter a motivação da necessidade e a data de início e de expiração do acesso.

Art. 11. As responsabilidades ficam estabelecidas na seguinte forma:

I - O usuário deverá:

a) Preencher os requisitos e termos estabelecidos nesta Norma;

b) Estar devidamente autorizado a utilizar a Internet nas formas estabelecidas nesta Norma;

c) Fazer uso da Internet de forma responsável e segura, utilizando o acesso exclusivamente em razão de trabalho, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Federal; e

d) Impedir a divulgação e compartilhamento das chaves de segurança atribuídas, que são pessoais e intransferíveis;

II - O autorizador deverá:

- a) Conceder os perfis de acesso à Internet rigorosamente de acordo com as atribuições dos usuários de sua abrangência, observando os normativos do INSS;
- b) Verificar periodicamente o uso dos acessos concedidos e, sempre que necessário, solicitar alteração dos perfis de acesso dos usuários de sua abrangência; e
- c) Reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR-INSS;

III - A área responsável pela gestão de TI no INSS deverá:

- a) Monitorar os acessos à internet e sua utilização de acordo com as diretrizes estabelecidas nesta Norma; e
- b) Identificar os casos de mau uso da Internet e adotar uma ou mais das seguintes providências:
 - 1. Alertar o usuário, responsável pelo acesso, e o Autorizador, responsável pela concessão, acerca do uso indevido da internet; e
 - 2. Nos casos de reincidência, solicitar a revogação do acesso à internet concedido ao usuário e encaminhar a documentação que comprova a má utilização do acesso concedido à Corregedoria do INSS, para análise e adoção das medidas cabíveis.

Art. 12. Configura-se como uso indevido da Internet:

- I - Acessar a Internet disponibilizada pelo INSS sem estar devidamente autorizado, conforme estabelecido nesta Norma;
- II - Não manifestar concordância com as regras estabelecidas nesta Norma e nas demais aplicáveis;
- III - Fazer uso dos recursos de Internet disponibilizados pelo INSS para fins alheios ao trabalho, em discordância com os procedimentos dispostos nesta Norma, sem prejuízo de demais normatizações vigentes na Administração Pública Federal;
- IV - Utilizar os serviços extrapolando os privilégios do perfil de acesso que lhe foi designado;
- V - Divulgar e/ou compartilhar as chaves de segurança, que são pessoais e intransferíveis, permitindo a utilização por terceiros do perfil que lhe foi atribuído;
- VI - Praticar atos de comercialização de produtos e serviços, em proveito próprio ou de terceiros, que não atendam os interesses do INSS;
- VII - utilizar recursos ou dispositivos para acesso a computadores ou redes externas ao INSS com o objetivo de obter informações não autorizadas ou provocar a interrupção de serviços de rede;
- VIII - utilizar modem ou dispositivo de rede que interligue a rede interna do INSS a outras redes ou à Internet;
- IX - Expor, armazenar, distribuir, editar, gravar ou compartilhar, através do uso dos recursos computacionais e de comunicação do INSS, arquivos estranhos às atividades do INSS e não autorizados pela chefia imediata;
- X - Realizar qualquer atividade que apoie ou facilite o vazamento de dados;
- XI - Baixar arquivos ou programas da Internet que contrariem as diretrizes da POSIN vigente; e
- XII - Utilizar proxy não disponibilizado pelo INSS.

Art. 13. O acesso à Internet é passível de registro e monitoração, incluindo quaisquer dados transmitidos pela rede do INSS.

§ 1º Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a ETIR-INSS deverá ser imediatamente acionada, para tomar as providências necessárias a fim de sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação do INSS;

§ 2º As ocorrências de mau uso do acesso à Internet não previstas nesta norma, assim como os casos de dúvidas em relação à aplicação das disposições aqui estabelecidas, deverão ser encaminhadas à DTI para registro, análise e avaliação da necessidade de alterações de acordo com o processo de governança em vigência no INSS;

§ 3º O descumprimento desta Norma poderá acarretar ao usuário as penalidades previstas nas políticas e procedimentos internos e/ou, na forma da lei, responsabilidade administrativa, civil e criminal.

Art. 14. Fica revogada a PORTARIA DTI/INSS Nº 71, DE 16 DE MARÇO DE 2022

Art. 14. Esta portaria entra em vigor a partir da sua publicação.

MARIO GALVÃO DE SOUZA SÓRIA
Diretor de Tecnologia da Informação e Inovação



Documento assinado eletronicamente por **ISRAEL EDUARDO ZEBULON MARTINS DE SOUZA**, Coordenador(a)-Geral de Dados e Sistemas de Informação, em 04/03/2024, às 16:44, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **15177157** e o código CRC **98386D32**.

ANEXO I

PORTARIA Nº XX/DTI/INSS, DE XX DE XXXXXXXXXX DE 2022

FORMULÁRIO DE SOLICITAÇÃO DE ACESSO À INTERNET

Informações do Usuário	
Nome:	Login de Rede:
Matrícula:	CPF:

Lotação:	Código do Setor:	
Telefone: ()	E-mail:	@inss.gov.br
		@agu.gov.br

☐	Perfil 1	
☐	Perfil 2	
☐	Perfil 3	
☐	Perfil 4	
☐	Terceirizados	Data de expiração:
	Contrato nº ou Convênio	Data de expiração

Descreva abaixo a justificativa e quais páginas devem ser acessadas pelo usuário terceirizado:

Declaro ter conhecimento e estar de acordo com as regras estabelecidas na Norma de Uso da internet do INSS (Resolução nº 12/CEGOV/INSS, de 1 de setembro de 2020) e demais normas aplicáveis.

, de de .
Local e Data

Informações do Autorizante		
Nome:		
Lotação:	Código do Setor:	
Telefone: ()	E-mail:	@inss.gov.br

Assinatura do Solicitante

Autorizo a concessão de Acesso Internet

, de de .
Local e Data

Assinatura do Autorizador



INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria de Tecnologia da Informação
Coordenação-Geral de Tecnologia da Informação e Segurança

DESPACHO

Coordenação-Geral de Tecnologia da Informação e Segurança, em 04/03/2024

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria de Tecnologia da Informação.

Ass.: Minuta de Instrução Normativa que disciplina

1. Trata-se de minuta de ato administrativo que regulamenta e define conjunto de perfis de acesso de internet, competências e conteúdo de acesso para cada perfil.
2. Considerando a necessidade de inclusão do cargo de OUVIDOR com papel de autorizador, enviamos a proposta de modificação na portaria.
3. Feitas as considerações, encaminhe-se à DTI.

ISRAEL EDUARDO ZEBULON MARTINS DE SOUZA

Coordenação-Geral de Tecnologia da Informação e Segurança



Documento assinado eletronicamente por **ISRAEL EDUARDO ZEBULON MARTINS DE SOUZA**, **Coordenador(a)-Geral de Dados e Sistemas de Informação**, em 04/03/2024, às 16:42, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **15177538** e o código CRC **0AD7E6E1**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 15177538



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação

PORTARIA DTI/INSS Nº 112, DE 27 DE MARÇO DE 2024

Disciplina o uso da Internet no Instituto Nacional do Seguro Social - INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.

O DIRETOR DE TECNOLOGIA DA INFORMAÇÃO DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso da competência que lhe confere o Decreto nº 10.995, de 14 de março de 2022, em conformidade no que dispõe no Processo Administrativo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Disciplinar o uso da Internet, no âmbito do INSS, por servidores e demais colaboradores, vinculados direta ou indiretamente ao Instituto, incluídos os vinculados a outros Órgãos da Administração Pública, a Empresas Públicas e a entidades privadas que necessitem ou estejam autorizados a utilizar a rede Corporativa deste Instituto.

Art.2º Para os efeitos desta Portaria são estabelecidos os seguintes conceitos e definições:

I - autorizador: ocupante de função de confiança ou cargo em comissão, responsável pela autorização da concessão de perfis de acesso para os usuários finais de sua área de abrangência;

II - internet: rede mundial que interliga computadores de diferentes tipos e dimensões e permite a comunicação entre pessoas e organizações, independentemente da localização geográfica;

III - intranet: rede de computadores administrada pelo INSS, que utiliza os mesmos serviços e tecnologias disponíveis na rede mundial;

IV - perfil de acesso: atributo que estabelece as categorias de sítios acessíveis e tipos de arquivos que podem ser recebidos ou transmitidos pelos usuários;

V - proxy: ferramenta que desempenha a função de conexão do computador local à rede externa (Internet);

VI - sítio: conjunto de informações ou serviços disponíveis na Internet ou na Intranet, organizados em páginas eletrônicas e acessíveis por meio de endereços que identificam, de forma padronizada, sua origem e conteúdo;

VII - usuários: rol de colaboradores enquadrados no Art. 1º desta portaria;

IX - ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso; e

X – OpenLDAP (LDAP): software livre de código aberto que implementa o protocolo LDAP (Lightweight Directory Access Protocol - Protocolo Leve de Acesso a Diretório) e que se comunica com base de dados de usuários mantida e gerida pela Dataprev.

Art. 3º O acesso pelos usuários à Internet disponibilizado pelo INSS deverá pautar-se pelas seguintes diretrizes:

I - o uso se dará exclusivamente em razão de trabalho e de acordo com os procedimentos dispostos nesta Portaria;

II - os recursos disponibilizados pelo INSS não poderão ser usados para quaisquer propósitos ilegais ou proibidos, ou que possam: danificar, desativar, sobrecarregar ou prejudicar qualquer área, serviço ou conteúdo, ou interferir no uso e execução das atividades laborais de outros usuários;

III - o volume de tráfego de Internet e os endereços web visitados poderão ser monitorados, visando assegurar o cumprimento desta Portaria; e

IV - o acesso à Internet para propósitos particulares ou estranhos às atividades do INSS poderá ser bloqueado, sem prévia comunicação ao usuário e sem prejuízo das demais sanções aplicáveis.

Art. 4º O acesso aos sítios da Internet para todos os usuários será realizado mediante a atribuição de perfis de acesso, distribuídos nos seguintes níveis:

I - Perfil 1: atribuído a usuários com maior restrição de acesso à Internet, com permissão de acesso à Intranet e a sítios governamentais, instituições bancárias, e sítios considerados de interesse do INSS;

II- Perfil 2: atribuído a usuários com permissão de acesso a todos os sítios contemplados no Perfil 1 e a sítios de provedores de e-mail pessoal e de instituições de ensino;

III - Perfil 3: atribuído a usuários com permissão de acesso a todos os sítios da Internet, exceto redes sociais e aqueles que contêm veiculação de material em áudio e vídeo; e

IV - Perfil 4: atribuído a usuários que desempenham atividades que necessitem acesso a todos os sítios da Internet, incluindo sítios que veiculam material em áudio e vídeo (streaming), sítios de compartilhamento de vídeos, blogs e redes sociais.

§ 1º O perfil concedido a usuários de Entes Externos será de caráter temporário, com validade equivalente à vigência das atividades a serem executadas no âmbito do INSS.

§ 2º Na análise da autorização e concessão de acesso à Internet deverá ser observado o Princípio de Privilégio Mínimo, o qual garanta somente o nível de acesso estritamente necessário para o usuário executar as suas atividades.

§ 3º Os processos de alteração, bloqueio, liberação e categorização de sítios, assim como a criação e/ou as alterações de perfis de acesso descritos nesta Norma, quando necessários, serão definidos pela DTI.

Art. 5º Será dado acesso à Internet, a partir da rede de dados Corporativa, nas dependências do INSS, aos servidores e demais colaboradores em atividade no INSS ou junto ao INSS.

§ 1º O acesso de usuários de Entes Externos será concedido mediante o estabelecimento em convênio, contrato, acordo de cooperação técnica ou instrumento congênere, especificamente firmados com o INSS para este fim.

§ 2º O gestor da área responsável pelo convênio, contrato, acordo de cooperação técnica ou instrumento congênere assumirá o papel de Autorizador do serviço de acesso à Internet para os usuários de Entes Externos, e deverá fundamentar as solicitações com base no instrumento.

§ 3º Poderão ser concedidos acessos temporários para auditores vinculados à Controladoria-Geral da União - CGU ou ao Tribunal de Contas da União - TCU, no uso de suas atribuições, e com vigência limitada ao período necessário para desenvolvimento de suas atividades junto ao INSS.

Art. 6º A conexão de equipamentos pessoais de visitantes à rede do INSS, quando necessária e motivada pelo interesse da Administração, deverá ser previamente autorizada pelo gestor da unidade onde o equipamento será utilizado.

Parágrafo único. Só será permitida a utilização da rede local por visitantes, caso seus equipamentos atendam a todos os requisitos estabelecidos pela DTI.

Art. 7º A todos os perfis de acesso descritos nesta Portaria aplicam-se as restrições de acesso a sítios que:

I - contenham material pornográfico ou obsceno;

II - contenham material ilegal;

III - disponibilizem jogos, inclusive os da Internet (on line);

IV - contenham material impróprio, ofensivo, preconceituoso ou discriminatório, que façam apologia à violência, ao terrorismo e às drogas; e

V - contenham e/ou divulguem conteúdo de violação de direito autoral (pirataria) e/ou execução de quaisquer tipos ou formas de fraudes.

Art. 8º O processo de atribuição de acesso à Internet seguirá as seguintes diretrizes:

I - a atribuição dos perfis de acesso à Internet será feita pelos Autorizadores, de forma fundamentada e respeitando o princípio da necessidade de conhecer, de acordo com a tabela abaixo:

Perfil	Autorizador
Perfil 2 e 3	Presidente do INSS, Diretores, Coordenadores-Gerais, Ouvidor, Assessor de Comunicação Social da Administração Central, Chefes de Assessoria de Comunicação Social das Superintendências-Regionais, Auditor-Geral, Corregedor-Geral, Procurador-Geral da PFE-INSS, Procuradores-Regionais, Superintendentes-Regionais, Gerentes-Executivos e Gerentes de Agências da Previdência Social - APS.
Perfil 4	Presidente do INSS, Diretores, Coordenadores-Gerais, Ouvidor, Assessor de Comunicação Social da Administração Central, Chefes de Assessoria de Comunicação Social das Superintendências-Regionais, Auditor-Geral, Corregedor-Geral, Procurador-Geral da PFE-INSS, Procuradores-Regionais, Superintendentes-Regionais e Gerentes-Executivos.

II - aos novos usuários da rede lógica (OpenLDAP) do INSS, cujas contas forem credenciadas por meio de registro de chamado técnico, será atribuído o Perfil 1, mediante o preenchimento e assinatura do TCMS (Anexo I);

III - para fins de alteração do perfil de acesso, os usuários deverão preencher o Formulário de Solicitação de Acesso à Internet (Anexo II) e providenciar a assinatura no sistema SEI pelo Autorizador do acesso; e

IV - ao registrar a solicitação, deve-se anexar o Formulário de Solicitação de Acesso à Internet (Anexo II) devidamente preenchido e assinado.

Art. 9º A solicitação para perfis de acesso em caráter temporário, dar-se-á mediante o preenchimento do TCMS (Anexo I) e do Formulário de Solicitação de Acesso à Internet (Anexo II), e deverá conter a motivação da necessidade, a data de início e data de fim do acesso temporário.

Art. 10. As responsabilidades ficam estabelecidas na seguinte forma:

I - o usuário deverá:

- preencher os requisitos e termos estabelecidos nesta Portaria;
- estar devidamente autorizado a utilizar a Internet nas formas estabelecidas nesta Portaria;
- fazer uso da Internet de forma responsável e segura, utilizando o acesso em razão do trabalho, cumprindo os procedimentos dispostos nesta Portaria, sem prejuízo das demais normatizações vigentes na Administração Pública Federal; e
- impedir a divulgação e compartilhamento das chaves de segurança atribuídas, que são pessoais e intransferíveis;

II - o autorizador deverá:

- conceder os perfis de acesso à Internet rigorosamente de acordo com as atribuições dos usuários de sua abrangência, observando os normativos do INSS;
- verificar periodicamente o uso dos acessos concedidos e, sempre que necessário, solicitar alteração dos perfis de acesso dos usuários de sua abrangência; e
- reportar os incidentes que afetam a segurança dos Ativos de informação ou o descumprimento da Política de Segurança da Informação - POSIN vigente à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR-INSS.

III - a DTI-INSS deverá:

- monitorar os acessos à internet e sua utilização de acordo com as diretrizes estabelecidas nesta Portaria;
- e
- identificar os casos de mau uso da Internet e adotar uma ou mais das seguintes providências:
 - alertar o usuário, responsável pelo acesso, e o autorizador, responsável pela concessão, acerca do uso indevido da Internet; e
 - nos casos de reincidência, solicitar a revogação do acesso à Internet do usuário e encaminhar a documentação, que comprova a má utilização, para análise e adoção das medidas cabíveis.

Art. 11. Configura-se como uso indevido da Internet:

I - acessar a Internet disponibilizadas pelo INSS sem estar devidamente autorizado, conforme estabelecido

nesta Portaria;

II - não manifestar concordância com as regras estabelecidas nesta Portaria e nas demais regras aplicáveis;

III - fazer uso dos recursos da Internet disponibilizados pelo INSS para fins alheios ao trabalho, em discordância com os procedimentos dispostos nesta Portaria, sem prejuízo das demais normatizações vigentes na Administração Pública Federal;

IV - utilizar os serviços extrapolando os privilégios do perfil de acesso que lhe foi atribuído;

V - divulgar e/ou compartilhar as chaves de segurança, que são pessoais e intransferíveis, permitindo a utilização por terceiros do perfil que lhe foi atribuído;

VI - praticar atos de comercialização de produtos e serviços, em proveito próprio ou de terceiros, que não atendam os interesses do INSS;

VII - utilizar recursos ou dispositivos para acesso a computadores ou redes externas ao INSS com o objetivo de obter informações não autorizadas ou provocar a interrupção de serviços de rede;

VIII - utilizar modem ou dispositivo de rede que interligue a rede interna do INSS a outras redes ou à Internet;

IX - expor, armazenar, distribuir, editar, gravar ou compartilhar, através do uso dos recursos computacionais e de comunicação do INSS, arquivos estranhos às atividades do INSS e não autorizados pela chefia imediata;

X - realizar qualquer atividade que apoie ou facilite o vazamento de dados;

XI - baixar arquivos ou programas da Internet que contrariem as diretrizes da POSIN vigente; e

XII - utilizar proxy não autorizados pelo INSS.

Art. 12. O acesso à Internet é passível de registro e monitoração, incluindo quaisquer dados transmitidos pela rede do INSS.

§ 1º Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a DTI deverá ser imediatamente acionada, para tomar as providências necessárias a fim de sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação do INSS;

§ 2º As ocorrências de uso incorreto do acesso à Internet não previstas nesta Portaria, assim como os casos de dúvidas em relação à aplicação das disposições aqui estabelecidas, deverão ser encaminhadas à DTI para registro, análise e avaliação da necessidade de alterações de acordo com o processo de governança em vigência no INSS;

§ 3º O descumprimento desta Portaria poderá acarretar ao usuário as penalidades previstas nas políticas e procedimentos internos e/ou, na forma da lei, a responsabilidade administrativa, civil e criminal.

Art. 13. Fica revogada a Portaria DTI/INSS Nº 71, de 16 de março de 2022.

Art. 14. Esta portaria entra em vigor na data de sua publicação.

MARIO GALVÃO DE SOUZA SÓRIA

Diretor de Tecnologia da Informação



Documento assinado eletronicamente por **MARIO GALVAO DE SOUZA SORIA**, Diretor(a) de Tecnologia da Informação, em 27/03/2024, às 23:22, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **15178715** e o código CRC **4D863D9D**.

ANEXO I

FORMULÁRIO DE SOLICITAÇÃO DE ACESSO À INTERNET

Informações do Usuário		
Nome:	Login de Rede:	
Matrícula:	CPF:	
Lotação:	Código do Setor:	
Telefone: ()	E-mail:	@inss.gov.br
		@agu.gov.br
☐ Perfil 1	Data da expiração:	
☐ Perfil 2		
☐ Perfil 3		
☐ Perfil 4		
☐ Terceirizados	Contrato nº ou Convênio	Data da vigência:
Descreva abaixo a justificativa e quais páginas devem ser acessadas pelo usuário terceirizado:		
_____ _____ _____		
Declaro ter conhecimento e estar de acordo com as regras estabelecidas na Portaria de Uso da internet do INSS (Resolução nº 12/CEGOV/INSS, de 1 de setembro de 2020) e demais normas aplicáveis.		
_____, _____ de _____ de _____. Local e Data		
Informações do Autorizante		
Nome:		
Lotação:	Código do Setor:	
Telefone: ()	E-mail:	@inss.gov.br
_____ Assinatura do Solicitante		
Autorizo a concessão de Acesso Internet _____, _____ de _____ de _____. Local e Data _____ Assinatura do Autorizador		

Referência: Processo nº 35014.047735/2020-84

SEI nº 15178715



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação

DESPACHO

Diretoria de Tecnologia da Informação, em 2/4/2024

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria de Tecnologia da Informação.

Ass.: Portaria DTI/INSS nº112 - disciplina o uso da Internet no INSS.

1. Trata-se da Portaria DTI/INSS nº 112, de 27 de março de 2024 (15178715), que disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.
2. De ordem, encaminhe-se à DIVCA, para ampla divulgação.

MÁRCIA S. SALGADO N. DE MATOS

Assessora da DTI



Documento assinado eletronicamente por **MARCIA SOARES SALGADO NUNES DE MATOS**, **Assessor Técnico**, em 02/04/2024, às 12:24, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **15542580** e o código CRC **B5E9A51A**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 15542580



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Assessoria de Comunicação Social
Serviço de Publicidade Legal

DESPACHO

Serviço de Publicidade Legal, em 02/04/2024

1. Estamos devolvendo, conforme solicitado pela Márcia.

Daniela Miranda da Silva Oliveira

Técnica do Seguro Social



Documento assinado eletronicamente por **DANIELA MIRANDA DA SILVA OLIVEIRA, Técnico do Seguro Social**, em 02/04/2024, às 12:53, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **15543338** e o código CRC **631B931A**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 15543338



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Assessoria de Comunicação Social
Divisão de Comunicação Administrativa

DESPACHO

Divisão de Comunicação Administrativa, em 02/04/2024

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria de Tecnologia da Informação.

Ass.: Publicação de Portaria

1. Trata-se da publicação e divulgação da Portaria DTI/INSS nº 112, de 27 de março de 2024.
2. Informamos que o referido ato, foi publicado no BSE, de 2 de abril de 2022 e no Portal-INSS, na intraprev.

3 Cabe ressaltar que existe um erro de grafia na ementa na palavra Social.

4. Ao Serviço Técnico Administrativo da Diretoria de Tecnologia da Informação e Inovação, para conhecimento e providências julgadas necessárias.

ALDAMIR GERALDO DE LISBÔA LIMA

Chefe da Divisão de Comunicação Administrativa - DIVCA



Documento assinado eletronicamente por **ALDAMIR GERALDO DE LISBOA LIMA**, Técnico do Seguro Social, em 02/04/2024, às 16:06, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **15548657** e o código CRC **F9433A10**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 15548657



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação

PORTARIA DTI/INSS Nº 112, DE 27 DE MARÇO DE 2024 (*)

Disciplina o uso da Internet no Instituto Nacional do Seguro Social - INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.

O DIRETOR DE TECNOLOGIA DA INFORMAÇÃO DO INSTITUTO NACIONAL DO SEGURO SOCIAL – INSS, no uso da competência que lhe confere o Decreto nº 10.995, de 14 de março de 2022, em conformidade no que dispõe no Processo Administrativo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Disciplinar o uso da Internet, no âmbito do INSS, por servidores e demais colaboradores, vinculados direta ou indiretamente ao Instituto, incluídos os vinculados a outros Órgãos da Administração Pública, a Empresas Públicas e a entidades privadas que necessitem ou estejam autorizados a utilizar a rede Corporativa deste Instituto.

Art.2º Para os efeitos desta Portaria são estabelecidos os seguintes conceitos e definições:

I - autorizador: ocupante de função de confiança ou cargo em comissão, responsável pela autorização da concessão de perfis de acesso para os usuários finais de sua área de abrangência;

II - internet: rede mundial que interliga computadores de diferentes tipos e dimensões e permite a comunicação entre pessoas e organizações, independentemente da localização geográfica;

III - intranet: rede de computadores administrada pelo INSS, que utiliza os mesmos serviços e tecnologias disponíveis na rede mundial;

IV - perfil de acesso: atributo que estabelece as categorias de sítios acessíveis e tipos de arquivos que podem ser recebidos ou transmitidos pelos usuários;

V - proxy: ferramenta que desempenha a função de conexão do computador local à rede externa (Internet);

VI - sítio: conjunto de informações ou serviços disponíveis na Internet ou na Intranet, organizados em páginas eletrônicas e acessíveis por meio de endereços que identificam, de forma padronizada, sua origem e conteúdo;

VII - usuários: rol de colaboradores citados no Art.1º desta Portaria, que obtiveram autorização de acesso aos Ativos de informação do Instituto, formalizada por meio da assinatura ou aceite eletrônico do Termo de Confidencialidade e Manutenção de Sigilo - TCMS (Anexo I da Norma de Controle de Acesso Lógico - NCAL-INSS, instituída pela Portaria Conjunta DTI/DIRAT-INSS nº 3, de 01 de abril de 2022, ou norma posterior que venha a substituí-la), disponível nos modelos do sistema SEI;

VIII - ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso; e

IX - openLDAP (LDAP): software livre de código aberto que implementa o protocolo LDAP (Lightweight Directory Access Protocol - Protocolo Leve de Acesso a Diretório) e que se comunica com base de dados de usuários mantida e gerida pela Dataprev.

Art. 3º O acesso pelos usuários à Internet disponibilizado pelo INSS deverá pautar-se pelas seguintes diretrizes:

I - o uso se dará exclusivamente em razão de trabalho e de acordo com os procedimentos dispostos nesta Portaria;

II - os recursos disponibilizados pelo INSS não poderão ser usados para quaisquer propósitos ilegais ou proibidos, ou que possam: danificar, desativar, sobrecarregar ou prejudicar qualquer área, serviço ou conteúdo, ou interferir no uso e execução das atividades laborais de outros usuários;

III - o volume de tráfego de Internet e os endereços web visitados poderão ser monitorados, visando assegurar o cumprimento desta Portaria; e

IV - o acesso à Internet para propósitos particulares ou estranhos às atividades do INSS poderá ser bloqueado, sem prévia comunicação ao usuário e sem prejuízo das demais sanções aplicáveis.

Art. 4º O acesso aos sítios da Internet para todos os usuários será realizado mediante a atribuição de perfis de acesso, distribuídos nos seguintes níveis:

I - Perfil 1: atribuído a usuários com maior restrição de acesso à Internet, com permissão de acesso à Intranet e a sítios governamentais, instituições bancárias, e sítios considerados de interesse do INSS;

II - Perfil 2: atribuído a usuários com permissão de acesso a todos os sítios contemplados no Perfil 1 e a sítios de provedores de e-mail pessoal e de instituições de ensino;

III - Perfil 3: atribuído a usuários com permissão de acesso a todos os sítios da Internet, exceto redes sociais e aqueles que contêm veiculação de material em áudio e vídeo; e

IV - Perfil 4: atribuído a usuários que desempenham atividades que necessitem acesso a todos os sítios da Internet, incluídos sítios que veiculam material em áudio e vídeo (streaming), sítios de compartilhamento de vídeos, blogs e redes sociais.

§ 1º O perfil concedido a usuários de Entes Externos será de caráter temporário, com validade equivalente à vigência das atividades a serem executadas no âmbito do INSS.

§ 2º Na análise da autorização e concessão de acesso à Internet deverá ser observado o Princípio de Privilégio Mínimo, o qual garanta somente o nível de acesso estritamente necessário para o usuário executar as suas atividades.

§ 3º Os processos de alteração, bloqueio, liberação e categorização de sítios, assim como a criação e/ou as alterações de perfis de acesso descritos nesta Norma, quando necessários, serão definidos pela DTI.

Art. 5º Será dado acesso à Internet, a partir da rede de dados Corporativa, nas dependências do INSS, aos servidores e demais colaboradores em atividade no INSS ou junto ao INSS.

§ 1º O acesso de usuários de Entes Externos será concedido mediante o estabelecimento em convênio, contrato, acordo de cooperação técnica ou instrumento congênere, especificamente firmados com o INSS para este fim.

§ 2º O gestor da área responsável pelo convênio, contrato, acordo de cooperação técnica ou instrumento congênere assumirá o papel de Autorizador do serviço de acesso à Internet para os usuários de Entes Externos, e deverá fundamentar as solicitações com base no instrumento.

§ 3º Poderão ser concedidos acessos temporários para auditores vinculados à Controladoria-Geral da União - CGU ou ao Tribunal de Contas da União - TCU, no uso de suas atribuições, e com vigência limitada ao período necessário para desenvolvimento de suas atividades junto ao INSS.

Art. 6º A conexão de equipamentos pessoais de visitantes à rede do INSS, quando necessária e motivada pelo interesse da Administração, deverá ser previamente autorizada pelo gestor da unidade onde o equipamento será utilizado.

Parágrafo Único. Só será permitida a utilização da rede local por visitantes, caso seus equipamentos atendam a todos os requisitos estabelecidos pela DTI.

Art. 7º A todos os perfis de acesso descritos nesta Portaria aplicam-se as restrições de acesso a sítios que:

I - contenham material pornográfico ou obsceno;

II - contenham material ilegal;

III - disponibilizem jogos, inclusive os da Internet (on-line);

IV - contenham material impróprio, ofensivo, preconceituoso ou discriminatório, que façam apologia à violência, ao terrorismo ou às drogas; e

V - contenham e/ou divulguem conteúdo de violação de direito autoral (pirataria) e/ou execução de quaisquer tipos ou formas de fraudes.

Art. 8º O processo de atribuição de acesso à Internet seguirá as seguintes diretrizes:

I - a atribuição dos perfis de acesso à Internet será feita pelos Autorizadores, de forma fundamentada e respeitado o princípio da necessidade de conhecer, de acordo com a tabela abaixo:

Perfil	Autorizador
Perfil 2 e 3	Presidente do INSS, Diretores, Coordenadores-Gerais, Ouvidor, Assessor de Comunicação Social da Administração Central, Chefes de Assessoria de Comunicação Social das Superintendências-Regionais, Auditor-Geral, Corregedor-Geral, Procurador-Geral da PFE-INSS, Procuradores-Regionais, Superintendentes-Regionais, Gerentes-Executivos e Gerentes de Agências da Previdência Social - APS.
Perfil 4	Presidente do INSS, Diretores, Coordenadores-Gerais, Ouvidor, Assessor de Comunicação Social da Administração Central, Chefes de Assessoria de Comunicação Social das Superintendências-Regionais, Auditor-Geral, Corregedor-Geral, Procurador-Geral da PFE-INSS, Procuradores-Regionais, Superintendentes-Regionais e Gerentes-Executivos

II - aos novos usuários da rede lógica (OpenLDAP) do INSS, cujas contas forem credenciadas por meio de registro de chamado técnico, será atribuído o Perfil 1, mediante o preenchimento e assinatura do TCMS;

III - para fins de alteração do perfil de acesso, os usuários deverão preencher o Formulário de Solicitação de Acesso à Internet (Anexo I desta Portaria) e providenciar a assinatura no sistema SEI pelo Autorizador do acesso; e

IV - ao registrar a solicitação, deve-se anexar o Formulário de Solicitação de Acesso à Internet devidamente preenchido e assinado.

Art. 9º A solicitação para perfis de acesso em caráter temporário, dar-se-á mediante o preenchimento do TCMS e do Formulário de Solicitação de Acesso à Internet, e deverá conter a justificativa da necessidade, a data de início e data de fim do acesso temporário.

Art. 10. As responsabilidades ficam estabelecidas da seguinte forma:

I - o usuário deverá:

- a) preencher os requisitos e termos estabelecidos nesta Portaria;
- b) estar devidamente autorizado a utilizar a Internet nas formas estabelecidas nesta Portaria;
- c) fazer uso da Internet de forma responsável e segura, utilizando o acesso em razão do trabalho, cumprindo os procedimentos dispostos nesta Portaria, sem prejuízo das demais normatizações vigentes na Administração Pública Federal; e
- d) impedir a divulgação e compartilhamento das chaves de segurança atribuídas, que são pessoais e intransferíveis;

II - o autorizador deverá:

- a) conceder os perfis de acesso à Internet rigorosamente de acordo com as atribuições dos usuários de sua abrangência, observando os normativos do INSS;
- b) verificar periodicamente o uso dos acessos concedidos e, sempre que necessário, solicitar alteração dos perfis de acesso dos usuários de sua abrangência; e
- c) reportar os incidentes que afetam a segurança dos Ativos de informação ou o descumprimento da Política de Segurança da Informação - POSIN vigente à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR-INSS.

III - a DTI-INSS deverá:

- a) monitorar os acessos à Internet e sua utilização de acordo com as diretrizes estabelecidas nesta Portaria; e
- b) identificar os casos de mau uso da Internet e adotar uma ou mais das seguintes providências:
 - 1. alertar o usuário, responsável pelo acesso, e o autorizador, responsável pela concessão, acerca do uso indevido da Internet; e
 - 2. nos casos de reincidência, solicitar a revogação do acesso à Internet do usuário e encaminhar a documentação, que comprova a má utilização, para análise e adoção das medidas cabíveis.

Art. 11. Configura-se como uso indevido da Internet:

I - acessar a Internet disponibilizada pelo INSS sem estar devidamente autorizado, conforme estabelecido nesta Portaria;

II - não manifestar concordância com as regras estabelecidas nesta Portaria e nas demais regras aplicáveis;

III - fazer uso dos recursos da Internet disponibilizados pelo INSS para fins alheios ao trabalho, em discordância com os procedimentos dispostos nesta Portaria, sem prejuízo das demais normatizações vigentes na Administração Pública Federal;

IV - utilizar os serviços extrapolando os privilégios do perfil de acesso que lhe foi atribuído;

V - divulgar e/ou compartilhar as chaves de segurança, que são pessoais e intransferíveis, permitindo a utilização por terceiros do perfil que lhe foi atribuído;

VI - praticar atos de comercialização de produtos e serviços, em proveito próprio ou de terceiros, que não atendam os interesses do INSS;

VII - utilizar recursos ou dispositivos para acesso a computadores ou redes externas ao INSS com o objetivo de obter informações não autorizadas ou provocar a interrupção de serviços de rede;

VIII - utilizar modem ou dispositivo de rede que interligue a rede interna do INSS a outras redes ou à Internet;

IX - expor, armazenar, distribuir, editar, gravar ou compartilhar, através do uso dos recursos computacionais e de comunicação do INSS, arquivos estranhos às atividades do INSS e não autorizados pela chefia imediata;

X - realizar qualquer atividade que apoie ou facilite o vazamento de dados;

XI - baixar arquivos ou programas da Internet que contrariem as diretrizes da POSIN vigente; e

XII - utilizar proxy não autorizado pelo INSS.

Art. 12. O acesso à Internet é passível de registro e monitoração, incluindo quaisquer dados transmitidos pela rede do INSS.

§ 1º Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a DTI deverá ser imediatamente acionada, para tomar as providências necessárias a fim de sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação do INSS.

§ 2º As ocorrências de uso incorreto do acesso à Internet não previstas nesta Portaria, assim como os casos de dúvidas em relação à aplicação das disposições aqui estabelecidas, deverão ser encaminhadas à DTI para registro, análise e avaliação da necessidade de alterações de acordo com o processo de governança em vigência no INSS.

§ 3º O descumprimento desta Portaria poderá acarretar ao usuário as penalidades previstas nas políticas e procedimentos internos e/ou, na forma da lei, a responsabilidade administrativa, civil e criminal.

Art. 13. Fica revogada a Portaria DTI/INSS nº 71, de 16 de março de 2022.

Art. 14. Esta portaria entra em vigor na data de sua publicação.

MARCELO GENU BESERRA

Diretor de Tecnologia da Informação, Substituto

(*) Republicada por ter saído com erro na original publicada no Boletim de Serviço Eletrônico em 02/04/2024.



Documento assinado eletronicamente por **MARCELO GENU BESERRA**, **Diretor(a) de Tecnologia da Informação Substituto(a)**, em 03/04/2024, às 14:04, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **15563381** e o código CRC **B1469045**.

ANEXO I

FORMULÁRIO DE SOLICITAÇÃO DE ACESSO À INTERNET

Usuário/Solicitante	
Nome Completo:	Login de Rede:
Matrícula SIAPE:	CPF:
Nome e Sigla da Unidade (UO):	Código da Unidade (UO):
Telefone: ()	E-mail Corporativo:
☐ Perfil 2	Acesso Temporário:
☐ Perfil 3	Data de Início:
☐ Perfil 4	Data Fim:
Justificativa do nível do Perfil de acesso solicitado, e sítios que precisam ser acessados	
Declaro ter conhecimento e estar de acordo com as regras estabelecidas na Portaria de Uso da Internet do INSS, e demais normas aplicáveis.	
_____, _____ de _____ de _____. Local e Data	
_____ Assinatura do Usuário/Solicitante	
Autorizador	
Nome Completo:	
Nome e Sigla da Unidade (UO):	Código da Unidade (UO):
Telefone: ()	E-mail Corporativo:
Autorizo a concessão de Acesso à Internet do INSS conforme nível do Perfil de acesso solicitado.	
_____, _____ de _____ de _____. Local e Data	
_____ Assinatura do Autorizador	



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação

DESPACHO

Diretoria de Tecnologia da Informação, em 3/4/2024

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria de Tecnologia da Informação.

Ass.: Portaria DTI/INSS nº112 - disciplina o uso da Internet no INSS.

1. Trata-se republicação da Portaria DTI/INSS nº 112, de 27 de março de 2024 (15178715), que disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil, publicada no BSE de 02/02/2024, por ter saído com incorreções.
2. De ordem, encaminhe-se à DIVCA, para ampla divulgação.

MÁRCIA S. SALGADO N. DE MATOS

Assessora da DTI



Documento assinado eletronicamente por **MARCIA SOARES SALGADO NUNES DE MATOS**, **Assessor Técnico**, em 03/04/2024, às 15:39, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **15567175** e o código CRC **75D6041A**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 15567175



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Assessoria de Comunicação Social
Divisão de Comunicação Administrativa

DESPACHO

Divisão de Comunicação Administrativa, em 03/04/2024

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria de Tecnologia da Informação.

Ass.: Republicação de Portaria

1. Trata-se da republicação e divulgação da Portaria DTI/INSS nº 112, de 27 de março de 2024.
2. Informamos que o referido ato, foi republicado no BSE, de 3 de abril de 2022 e no Portal-INSS, na intraprev.
3. Ao Serviço Técnico Administrativo da Diretoria de Tecnologia da Informação e Inovação, para conhecimento e providências julgadas necessárias.

ALDAMIR GERALDO DE LISBÔA LIMA

Chefe da Divisão de Comunicação Administrativa - DIVCA



Documento assinado eletronicamente por **ALDAMIR GERALDO DE LISBOA LIMA**, Técnico do Seguro Social, em 03/04/2024, às 18:10, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **15568190** e o código CRC **4C7D94D8**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 15568190



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação
Serviço Técnico Administrativo

DESPACHO

Serviço Técnico Administrativo, em 04/04/2024

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria de Tecnologia da Informação.

Ass.: Republicação de Portaria.

1. Trata-se da republicação e divulgação da Portaria DTI/INSS nº 11, de 27 de março de 2024.
2. Informamos que o referido ato foi republicado, conforme despacho DIVCA(15568190).
3. À Diretoria de Tecnologia da Informação em devolução.

CLEONICE MARIA APARECIDA BARBOZA ALVES

Chefe do Serviço Técnico Administrativo



Documento assinado eletronicamente por **CLEONICE MARIA APARECIDA BARBOZA ALVES**, **Chefe de Serviço Técnico Administrativo**, em 04/04/2024, às 11:56, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **15577673** e o código CRC **C4BCFFD5**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 15577673



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação
Coordenação-Geral de Tecnologia da Informação e Segurança

MINUTA DE PORTARIA CGTIS/DTI/INSS Nº 14065620, DE 22 DE NOVEMBRO DE 2023

Exonera e Designa o Gestor de Segurança da Informação e o Gestor de Segurança da Informação Substituto.

O PRESIDENTE DO INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS, no uso da competência que lhe confere o Decreto nº 10.995, de 14 de março de 2022, e considerando o que dispõe o inciso I do artigo 15 da Instrução Normativa GSIOPR nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, bem como o que consta no Processo Administrativo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Exonerar os servidores JULLYANO LINO DA SILVA, matrícula nº 1.786.967, cargo de Gestor de Segurança da Informação do Instituto Nacional do Seguro Social - INSS e LUZIVAN DE MOURA GOIS, matrícula 1.784.525, cargo de Gestor substituto.

Art. 2º Designar o servidor Hugo Rafael Torma de Lima, matrícula nº 1.637.047, como Gestor de Segurança da Informação do Instituto Nacional do Seguro Social - INSS.

Parágrafo único. O servidor designado no caput será substituído pelo servidor Nelson Antonio Pimentel Jacinto, matrícula 1.095.044, nos afastamentos e impedimentos legais do titular e na vacância do encargo.

Art. 2º São competências do Gestor de Segurança da Informação do INSS, de acordo com o disposto no art. 19 da Instrução Normativa GSI/PR nº 1, de 2020:

I - coordenar o Comitê de Segurança da Informação ou estrutura equivalente;

II - coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do órgão, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

III - assessorar a alta administração na implementação da Política de Segurança da Informação;

IV - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

V - promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade;

VI - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

VII - propor recursos necessários às ações de segurança da informação;

VIII - acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes Cibernéticos;

IX - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

X - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

XI - manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Art. 3º A gestão da Segurança da Informação é considerada serviço de natureza relevante e não ensejará qualquer tipo de remuneração adicional.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

Art. 5º Fica revogada a Portaria nº 728/PRES/INSS, de 3 de junho de 2022.

ALESSANDRO ANTÔNIO STEFANUTTO

Presidente



Documento assinado eletronicamente por **ISRAEL EDUARDO ZEBULON MARTINS DE SOUZA**, **Coordenador(a)-Geral de Dados e Sistemas de Informação**, em 22/11/2023, às 14:28, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **14065620** e o código CRC **3A1B9D0C**.

Referência: Processo nº 35014.047735/2020-84

SEI nº 14065620



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação

DESPACHO

Diretoria de Tecnologia da Informação, em 07/08/2023

Ref.: Processo nº 35014.295116/2023-47.

Int.: Coordenação-Geral de Tecnologia da Informação e Segurança-CGTIS.

Ass.: Publicação de Portaria.

1. De ordem, encaminha-se minuta de portaria de ato administrativo destinado a exonerar e designar o Gestor de Segurança da Informação e o Gestor de Segurança da Informação Substituto do Instituto Nacional do Seguro Social - INSS .
2. Encaminhe-se à Coordenação de Normas e Procedimentos do Gabinete para as providências necessárias.

CLEONICE M. A. BARBOZA ALVES

Chefe do STADM-DTI



Documento assinado eletronicamente por **CLEONICE MARIA APARECIDA BARBOZA ALVES, Técnico do Seguro Social**, em 03/05/2024, às 15:33, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **15963227** e o código CRC **A68CF737**.



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência

PORTARIA PRES/INSS Nº 90, DE 15 DE MAIO DE 2024

O **PRESIDENTE DO INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS**, no uso da competência que lhe confere o Decreto nº 10.995, de 14 de março de 2022, e considerando o que consta no Processo Administrativo nº 35014.047735/2020-84,

RESOLVE:

Art. 1º Designar, no âmbito do INSS, os seguintes servidores como Gestores de Segurança da Informação:

I - titular: Hugo Rafael Torma de Lima, matrícula nº 1.637.047; e

II - substituto: Nelson Antonio Pimentel Jacinto, matrícula nº 1.095.044.

Art. 2º São competências do Gestor de Segurança da Informação do INSS, de acordo com o disposto no art. 19 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020:

I - coordenar o Comitê de Segurança da Informação ou estrutura equivalente;

II - coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do órgão, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

III - assessorar a alta administração na implementação da Política de Segurança da Informação;

IV - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

V - promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade;

VI - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

VII - propor recursos necessários às ações de segurança da informação;

VIII - acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes Cibernéticos;

IX - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

X - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

XI - manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Art. 3º A gestão da Segurança da Informação é considerada serviço de natureza relevante e não ensejará qualquer tipo de remuneração adicional.

Art. 4º Fica revogada a Portaria PRES/INSS nº 728, de 3 de junho de 2022, publicada no Boletim de Serviço Eletrônico em 3 de junho de 2022.

Art. 5º Esta Portaria entra em vigor na data de sua publicação.

ALESSANDRO ANTONIO STEFANUTTO

Presidente



Documento assinado eletronicamente por **ALESSANDRO ANTONIO STEFANUTTO, Presidente**, em 15/05/2024, às 20:58, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **15964247** e o código CRC **61BF3C39**.



INSTITUTO NACIONAL DO SEGURO SOCIAL
GABINETE DA PRESIDÊNCIA
Serviço Técnico Administrativo

DESPACHO

SERVIÇO TÉCNICO ADMINISTRATIVO DO GABINETE, em 16/5/2024

Ref.: Processo nº
35014.047735/2020-84

Int.: INSS

Ass.: Designar servidores
como Gestores de
Segurança da Informação

Restitua-se à Diretoria de Tecnologia da Informação, de ordem, após publicação da Portaria PRES/INSS nº 90, de 15 de maio de 2024, no BSE de 16 de maio de 2024, para as providências decorrentes.

VINICIUS ROSA RODRIGUES

Chefe de Serviço Técnico Administrativo do Gabinete



Documento assinado eletronicamente por **VINICIUS ROSA RODRIGUES, Chefe de Serviço Técnico Administrativo do Gabinete**, em 16/05/2024, às 10:27, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **16118321** e o código CRC **1B228F29**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 16118321



INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Assessoria de Comunicação Social
Divisão de Comunicação Administrativa

DESPACHO

Divisão de Comunicação Administrativa, em 16/05/2024

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria de Tecnologia da Informação.

Ass.: Publicação de Portaria

1. Trata-se da republicação e divulgação da Portaria DTI/INSS nº 90, de 15 de maio de 2024.
2. Informamos que o referido ato, foi republicado no BSE, de 16 de maio de 2024 e no Portal-INSS, na intraprev.
3. Ao Serviço Técnico Administrativo da Diretoria de Tecnologia da Informação, para conhecimento e providências julgadas necessárias.

ALDAMIR GERALDO DE LISBÔA LIMA

Chefe da Divisão de Comunicação Administrativa - DIVCA



Documento assinado eletronicamente por **ALDAMIR GERALDO DE LISBOA LIMA**, Técnico do Seguro Social, em 16/05/2024, às 12:13, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **16122076** e o código CRC **D4A72CA0**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 16122076



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação
Serviço Técnico Administrativo

DESPACHO

Serviço Técnico Administrativo, em 16/05/2024

Ref.: Processo nº 35014.047735/2020-84.

Int.: Diretoria de Tecnologia da Informação.

Ass.: Publicação de Portaria.

1. Trata-se da republicação e divulgação da Portaria DTI/INSS nº 90, de 15 de maio de 2024.
2. Ciente do despacho DIVCA(16122076).
3. Após publicação, encerre-se nessa unidade.

CLEONICE M. A. BARBOZA ALVES

Chefe do STADM-DTI



Documento assinado eletronicamente por **CLEONICE MARIA APARECIDA BARBOZA ALVES**, **Chefe de Serviço Técnico Administrativo**, em 22/05/2024, às 16:24, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **16127920** e o código CRC **74D366DE**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 35014.047735/2020-84

SEI nº 16127920