INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação
Coordenação-Geral de 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 05/12/2025

Ref.: Processo nº 35014.451616/2025-37.

Int.: SENADO FEDERAL Secretaria-Geral da Mesa Secretaria de Comissões Coordenação de Comissões Especiais, Temporárias e Parlamentares de Inquérito.

Ass.: Relatório de Medidas Adotadas pela Segurança Cibernética do INSS.

1. Vistos etc.

2. Aportam os autos nesta divisão para que relate sobre as medidas adotadas para proteção de dados pessoais dos segurados, incluindo incidentes de vazamento de dados reportados desde 2020.

3. Nesse embalo, as medidas adotadas foram, inclusive aquelas sustentadas em 19955.102272/2022-14:

3.1. **Instituição da Política de Segurança da Informação (POSIN-INSS, Processo SEI nº 35014.047735/2020-84) :**

3.1.1. A POSIN, aprovada pela Resolução CEGOV Nº 9, de 31 de agosto de 2020, tem por objetivo estabelecer e difundir diretrizes e princípios de Segurança da Informação, com vistas à orientação para uso e proteção adequados das informações produzidas e custodiadas pelo Instituto, preservando sua disponibilidade, integridade, confidencialidade e autenticidade, aplicando-se a todos os agentes públicos que têm vínculo direto e/ou indireto com o Instituto.

3.2. **Instituição da Norma de Concessão de Acesso Lógico (NCAL-INSS, Processo SEI nº 35014.047735/2020-84)**

3.2.1. A NCAL, aprovada pela Resolução CEGOV Nº 10, de 31 de agosto de 2020, regula a concessão e gestão de acesso à rede e aos sistemas corporativos a todos os agentes públicos e privados com vínculo direto ou indireto, permanente ou temporário com o INSS, aí incluídos os Advogados e Procuradores Federais vinculados à AGU que tenham atuação relacionada ao órgão, além de órgãos de controle externo em ações de auditoria e usuários vinculados a entidades externas, no interesse do INSS, mediante Convênio, Acordo de Cooperação Técnica (ACT) ou instrumento congênere.

3.2.2. Em 2022, a Resolução CEGOV Nº 10, de 31 de agosto de 2020 foi substituída pela Portaria Conjunta DTI/DIRAT/INSS Nº 3, de 01 de abril de 2022. A Portaria Conjunta DTI/DIRAT/INSS nº 3, de 2022, reescreveu a Norma de Controle de Acesso Lógico (NCAL) do INSS, estabelecendo diretrizes e procedimentos para o acesso lógico à rede de dados, recursos e sistemas corporativos do Instituto. A norma se aplica a todos os agentes públicos e privados com vínculo direto ou indireto, permanente ou temporário, com o INSS, e define conceitos-chave como credenciamento, perfis de acesso e necessidade

de conhecer. O documento detalha os critérios para concessão, desativação e reativação de credenciais, o processo de autenticação (incluindo senhas e certificado digital A3), as responsabilidades dos diferentes papéis de gestão de acesso (como Gestor de Acesso Central, Interno e Externo), e as vedações e sanções para o mau uso do acesso lógico. Além disso, estabelece as condições de credenciamento para estagiários, terceirizados, usuários externos e prestadores de serviço, e define a necessidade de registro e monitoramento de todos os acessos (logs).

3.3. **Instituição da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR-INSS) (Processo SEI nº 35014.047735/2020-84)**

3.3.1. Aprovada em complementação à POSIN-INSS pela Resolução CEGOV Nº 11, de 31 de agosto de 2020, a 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".

3.3.2. Posteriormente, no ano de 2022, a Resolução CEGOV Nº 11, de 2020 foi revogada e substituída pela Portaria DTI/INSS nº 75, de 1 abril de 2022. A Portaria DTI/INSS nº 75, de 2022, redefine a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR-INSS) no âmbito do Instituto Nacional do Seguro Social. O objetivo da ETIR-INSS é agir proativamente, além de receber, analisar, monitorar, coordenar e propor respostas a notificações e atividades relacionadas a incidentes cibernéticos. A equipe segue o "Modelo 2 Centralizado" e está vinculada à Diretoria de Tecnologia da Informação. Ela é composta por membros permanentes, colaboradores e opcionais, sendo os membros designados pelo Diretor de Tecnologia da Informação e Inovação. A ETIR-INSS tem autonomia compartilhada no processo decisório de incidentes cibernéticos com o Gestor de Segurança da Informação e o Diretor de Tecnologia da Informação. Os serviços fornecidos pela equipe abrangem a recepção de alertas, filtragem, catalogação, classificação, tratamento e resposta a incidentes, além do monitoramento e cooperação com outras instâncias, como o CTIR Gov e CSIRTs nacionais e internacionais.

3.4. **Norma de Uso da Internet (Processo SEI nº 35014.047735/2020-84)**

3.4.1. Ao aprovar a Resolução CEGOV Nº 12, 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, o INSS tornou mais objetivos os critérios de concessão frente às efetivas necessidades das áreas de negócio e de Segurança da Informação.

3.4.2. Em 2024, novas regras passaram a disciplinar o uso da internet no âmbito do INSS, destacando-se, entre elas, a Portaria DTI/INSS nº 112, de 27 de março de 2022. Essa Portaria regulamenta o uso da Internet pelos servidores e demais colaboradores vinculados, direta ou indiretamente, ao Instituto, estabelecendo diretrizes como o uso estritamente relacionado às atividades laborais e a possibilidade de monitoramento do tráfego e dos endereços eletrônicos acessados.

3.4.3. O eixo central da norma é a definição de quatro perfis de acesso (Perfis 1 a 4), que categorizam os tipos de sítios que podem ser acessados. As permissões variam desde restrições severas — como no Perfil 1, limitado à Intranet, a sítios governamentais e a páginas essenciais ao funcionamento das atividades do INSS — até o Perfil 4, que admite acesso amplo, incluindo conteúdos de áudio, vídeo e redes sociais. A atribuição desses perfis deve observar o Princípio do Privilégio Mínimo, sendo a autorização concedida por diferentes níveis hierárquicos, conforme o nível de acesso requerido.

3.4.4. A Portaria também relaciona categorias de sítios cujo acesso é vedado, tais como páginas com conteúdo pornográfico, ilegal, jogos ou material inadequado, além de detalhar as responsabilidades dos usuários, dos autorizadores e da DTI. Define, ainda, condutas configuradas como uso indevido da Internet e prevê que seu descumprimento poderá acarretar responsabilização administrativa, civil e penal.

3.5. **Cultura do uso de Certificado Digital no âmbito do INSS (Processo SEI nº 35014.390907/2021-18)**

3.5.1. Com o advento do uso intensivo de certificados digitais na Administração Pública, a Portaria DTI/INSS nº 72, de 29 de março de 2022, passou a estabelecer as diretrizes e os requisitos para a solicitação, emissão, ativação e distribuição de Certificados Digitais do tipo Pessoa Física e dos respectivos tokens físicos no âmbito do Instituto Nacional do Seguro Social (INSS).

3.5.2. A norma designa o Serviço Federal de Processamento de Dados (SERPRO) como responsável pela gestão e pela prestação dos serviços de emissão dos certificados, os quais devem observar

integralmente as regras da ICP-Brasil. O certificado previsto é o do tipo A3, com validade de até três anos, gerado e armazenado em token ou dispositivo criptográfico homologado. Ele é destinado exclusivamente a usuários que comprovem necessidade efetiva para o exercício de suas atribuições institucionais, incluindo servidores ativos, cedidos, ocupantes de cargos em comissão, entre outros.

3.5.3. A Portaria também disciplina o fluxo operacional para a emissão desde a solicitação pelo aplicativo SouGov, passando pela aprovação da chefia imediata e pela entrega pessoal do token ao usuário, até a efetivação do certificado. Além disso, detalha as responsabilidades dos diversos atores envolvidos, como o Gestor do Contrato, os Fiscais Técnicos e os Fiscais Requisitantes, no tocante à gestão, ao controle e à fiscalização da distribuição dos tokens e da emissão dos certificados.

3.6. ***Squad Seg*** **da Secretaria de Governo Digital (SGD)**

3.6.1. A área de segurança da DTI ganhou no ano de 2021 o reforço de projeto da Secretaria de Governo Digital do Ministério da Economia (SGD/ME), o qual alocou recursos humanos para algumas das ações estratégicas descritas nesta Nota Técnica, a saber:

a) Aperfeiçoamento do monitoramento da rede, de ativos e de aplicações;

b) Melhorias no GERID, como o Duplo Fator de Autenticação (2FA/*Google Authenticator*/*Microsoft Authenticator*) e a automação de rotinas de saneamento a partir da integração de bases de dados;

c) Contratação e Implantação de Certificados Digitais;

d) Contratação e implantação de novo link de dados.

3.7. **Duplo Fator de Autenticação (2FA) para acesso às aplicações parceiras ao GERID e Solução de correio, comunicação, colaboração e produtividade (Processos SEI nº 35000.002467/2019-97, 35014.327974/2020-15 e 35014.014513/2021-66)**

3.7.1. Até a contratação e implementação do pacote Microsoft 365, ocorrida em 2021, a Dataprev provia ao INSS o serviço de correio eletrônico baseado na solução *opensource* Expresso. A nova solução trouxe significativos ganhos em recursos de segurança e monitoramento de acesso e utilização, como *antispam*, *antimalware* e *antiphishing*, sendo este último de vital importância para o contexto.

3.7.2. Além disso, o múltiplo fator de autenticação (MFA) também é uma funcionalidade da solução, tendo sido habilitada de forma obrigatória para toda a organização e cabendo a cada usuário a opção por utilizar SMS ou o aplicativo *Microsoft Authenticator*.

3.7.3. Outro ponto que merece destaque é o fato de que a suíte contratada oferece espaço de armazenamento em nuvem, mitigando e até mesmo eliminando a necessidade de armazenamento local de arquivos e seu compartilhamento na rede.

3.8. **Uso do solução *Microsft Entra ID - Azure* (Processo SEI nº 35014.014513/2021-66)**

3.8.1. A Portaria DTI/INSS nº 113, de 27 de março de 2024, estabelece a adoção e o uso obrigatório do serviço *Microsoft Entra ID* (*Azure AD*) como o único meio de identidade e a solução de autenticação para acesso às estações de trabalho e à rede Corporativa do INSS, aplicando-se a todos os seus usuários.

3.8.2. O principal objetivo é centralizar, modernizar e fortalecer a segurança do gerenciamento de acesso e identidade. Para suportar essa implementação, a Portaria exige que todas as estações de trabalho utilizem Sistema Operacional Windows 10 ou superior compatível com o *Microsoft Entra ID*, proibindo o *downgrade* de sistemas operacionais que já o suportem.

3.8.3. Adicionalmente, todos os sistemas e serviços do Instituto que sejam compatíveis com protocolos de autenticação modernos devem implementar o *Microsoft Entra ID* como sua solução de autenticação.

3.9. **Exigência de Perfil Proxy nível 3 para o uso dos aplicativos de mensagens instantâneas *WhatsApp*, *Telegram*, *Discord* e *Signal* no âmbito do INSS (Processo SEI nº 35014.327423/2025-66).**

3.9.1. A Portaria DTI/INSS nº 136, de 27 de agosto de 2025, institui medida relevante de proteção de dados sensíveis e de fortalecimento da segurança da informação no âmbito do Instituto. A norma torna **obrigatória** a utilização do **Perfil *Proxy* – Nível 3** para o acesso a determinados aplicativos de mensagens

instantâneas instalados ou utilizados em ambiente institucional. Entre os serviços alcançados pela regra estão, de forma expressa, ***WhatsApp***, ***Telegram***, ***Discord*** e ***Signal***, sem prejuízo de futura ampliação para outras plataformas de comunicação.

3.9.2. A Portaria atribui à DTI a responsabilidade pela execução integral da medida, abrangendo atividades de monitoramento, orientação, fiscalização e controle, em coordenação com as demais diretorias e gerências do INSS.

3.10. **Interação com as Autoridades Policiais em Caso de Vazamento de Dados em Incidente Cibernético**

3.10.1. Nos incidentes cibernéticos com potencial relevância penal e que envolvam vazamento de dados, a interação com as autoridades policiais passou a ser conduzida de forma meticulosa, observando estritamente a legislação vigente e as diretrizes internas do INSS.

3.10.2. O INSS possui histórico comprovado de atuação tempestiva e coordenada nessa matéria. Exemplo disso é o incidente amplamente divulgado pela mídia, no qual a Autarquia reduziu drasticamente o número de servidores com acesso a dados sensíveis gerado pela aplicação SUIBE (https://www.cnnbrasil.com.br/politica/fraudes-levaram-inss-a-reduzir-drasticamente-servidores-com-acesso-a-dados/). A interação com a autoridade policial ocorreu de forma imediata, conforme registrado no processo **35014.154241/2024-89** e já comunicada a CPMI do INSS, evidenciando a observância rigorosa aos protocolos internos de resposta a incidentes, em especial aquele relacionados à vazamento de dados.

3.10.3. Outro caso emblemático encontra-se no processo **35014.314772/2024-37**, decorrente de monitoramento proativo da ETIR-INSS. Nessa ocasião, foram identificadas páginas na internet — VERIFIQ DATA SOLUTION e AMTRUTH — voltadas à comercialização indevida de listas de benefícios indeferidos por unidade federativa, mês e ano. A pronta articulação entre a autoridade policial competente, a Coordenação-Geral de Inteligência do Ministério da Previdência Social (CGINP/MPS) e a ETIR-INSS resultou na deflagração da **Operação Truth**, em 20 de agosto de 2025, ação que desarticulou organização criminosa especializada na venda de dados sigilosos de segurados do INSS.

4. Feitas as considerações, à CGTI.

FRANCISCO HUMBERTO MENDONÇA DE ARAÚJO

Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos

Documento assinado eletronicamente por **FRANCISCO HUMBERTO MENDONCA DE ARAUJO**, **Chefe da Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos** , em 07/12/2025, 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 **23479858** e o código CRC **49560130**.