MINISTÉRIO DO TRABALHO E PREVIDÊNCIA
Gabinete do Ministro

DESPACHO Nº 314/2022/GMTP-MTP

Processo nº 19955.102272/2022-14.

Encaminhe-se à **Presidência do INSS** para conhecimento e providências subsequentes.

Brasília, 11 de agosto de 2022.

OMAR MOHAMED FARES

Chefe de Gabinete

Documento assinado eletronicamente por **Omar Mohamed Fares**, **Chefe de Gabinete**, em 12/08/2022, às 12:11, 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.economia.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **27168880** e o código CRC **E48DA840**.

Referência: Processo nº 19955.102272/2022-14. SEI nº 27168880

SERVIÇO PÚBLICO FEDERAL
MJSP - POLÍCIA FEDERAL

OFÍCIO Nº 146/2022/ASS/GAB/PF

Brasília-DF, *na data da assinatura eletrônica*.

A Sua Excelência o(a) Senhor(a)
JOSÉ CARLOS OLIVEIRA
Ministro do Trabalho e Previdência
Esplanada dos Ministérios, S/N, Bloco F
Brasília-DF

Assunto: **Comunica ocorrência de prováveis fraudes massivas contra o INSS**

Senhor Ministro do Trabalho e Previdência,

Chegou ao conhecimento desta Polícia Federal, por meio de análises de dados e via canal de inteligência, ocorrência de prováveis fraudes massivas contra o INSS. Os informes foram transmitidos, via canal de inteligência, à Coordenação-Geral de Inteligência/MTP e às inteligências dos principais bancos afetados.

As fraudes consistem, em tese, na reativação fraudulenta de benefícios, gerando pagamento de retroativos próximo ao limite de cinco anos, o que perfaz um valor estimado em torno de R$70.000,00 por benefício fraudulentamente reativado. Encaminho, em anexo (SEI nº 24143030), lista com 9694 benefícios suspeitos de fraude na reativação praticada nos últimos 60 dias, (perfazendo um total estimado em torno de R$680.000.000,00 (seiscentos e oitenta milhões de reais). Não se sabe ainda a informação precisa sobre quantos desses benefícios foram efetivamente pagos, bloqueados ou devolvidos pelos bancos, mas informes iniciais apontam que os bancos já teriam bloqueado pagamentos que ultrapassam a casa de R$100.000.000,00 (cem milhões de reais).

Análises iniciais apontam para a massiva utilização indevida de senhas de servidores do INSS nesses processos de reativação, o que demanda providências urgentes em termos de segurança das credenciais dos servidores e beneficiários e/ou bloqueio cautelar desse tipo de atividade. Além disso, solicita-se a esse Ministério a determinação de prioridade e urgência nas análises por parte da CGINT a fim de que esta Polícia Federal possa adotar providências na sua esfera de atribuições.

Respeitosamente,

SANDRO TORRES AVELAR
Delegado de Polícia Federal
Diretor-Geral substituto

Documento assinado eletronicamente por **SANDRO TORRES AVELAR**, **Diretor Executivo**, em

18/07/2022, às 18:14, 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 http://sei.dpf.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **24180458** e o código CRC **E36175EE**.

Luis Roberto da Silva

De:	Agenda
Enviado em:	sexta-feira, 22 de julho de 2022 16:07
Para:	Gab MTP
Assunto:	ENC: Comunica ocorrência de prováveis fraudes massivas contra o INSS
Anexos:	Lista_24143030_NB_lista.zip; Oficio_24180458.html

Prezados,

Por não se tratar de agenda, encaminho para análise e tratativas cabíveis.

Gisele Kunzendorff
Assessora de Agenda

-----Mensagem original-----
De: PF/gab@pf.gov.br <gab@pf.gov.br>
Enviada em: sexta-feira, 22 de julho de 2022 15:13
Para: gab.mtep@mte.gov.br; Agenda <agenda@mte.gov.br>; agenda.mte@mte.gov.br
Assunto: Comunica ocorrência de prováveis fraudes massivas contra o INSS

Prezados,

De ordem, encaminho o OFÍCIO Nº 146/2022/ASS/GAB/PF para conhecimento e providências que entenderem pertinentes.

Oportunamente, rogo a gentileza de confirmação de recebimento.

Obs.: favor desconsiderar e-mail anterior, em virtude da ausência do anexo.

Respeitosamente,
ELI JOSÉ BATISTA JÚNIOR
Assessor - GAB/PF

MINISTÉRIO DO TRABALHO E PREVIDÊNCIA
Gabinete do Ministro

DESPACHO Nº 260/2022/GMTP-MTP

Processo nº 19955.102272/2022-14.

Encaminhe-se à **Secretaria de Previdência** Ofício nº 146/2022/ASS/GAB/PF (26642828) para análise e providências subsequentes.

Brasília, 28 de julho de 2022.

Documento assinado eletronicamente
LUCAS TEIXEIRA GRILLO
Coordenador-Geral do Gabinete do Ministro

Documento assinado eletronicamente por **Lucas Teixeira Grillo**, **Coordenador(a)-Geral**, em 02/08/2022, às 02:02, 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.economia.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **26790170** e o código CRC **03161488**.

Referência: Processo nº 19955.102272/2022-14. SEI nº 26790170

MINISTÉRIO DO TRABALHO E PREVIDÊNCIA
Secretaria de Previdência

DESPACHO Nº 2954/2022/SPREV-MTP

Processo nº 19955.102272/2022-14

Encaminhe-se à Coordenação-Geral de Inteligência Previdenciária e Trabalhista, para providências necessárias.

Brasília, 02 de agosto de 2022.

Documento assinado eletronicamente

NÁGILA LIMA DE SOUSA BITTENCOURT

Chefe de Gabinete da Secretaria de Previdência

Documento assinado eletronicamente por **Nágila Lima de Sousa Bittencourt**, **Chefe de Gabinete**, em 02/08/2022, às 10:38, 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.economia.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **26879920** e o código CRC **98BF7E1F**.

Referência: Processo nº 19955.102272/2022-14. SEI nº 26879920

DESPACHO

1. Trata o presente de notícia de supostas "fraudes massivas" em benefícios, encaminhada pela Direção Geral da Polícia Federal ao Ministro de Estado do Trabalho e Previdência, por meio do Ofício nr. 146/2022/ASS/GAB/PF, de 18/07/2022 (26642828).

2. O referido expediente relata que chegou ao conhecimento daquela Polícia Federal, *por meio de análises de dados e via canal de inteligência,* da ocorrência de *prováveis fraudes massivas* contra o INSS e que tais informes foram transmitidos, *via canal de inteligência,* à Coordenação-Geral de Inteligência/MTP e às inteligências dos principais bancos afetados.

3. Segundo o relato, **as fraudes consistiriam, em tese, na reativação fraudulenta de benefícios, gerando pagamento de retroativos próximo ao limite de cinco anos, o que perfaria um valor estimado médio em torno de R$70.000,00, por beneficio fraudulentamente reativado.**

4. O ofício encaminha como anexo uma listagem de 9.694 benefícios suspeitos de fraudes na reativação (Arquivo "Lista NB" - doc 26643017) que teriam sido praticadas nos 60 dias anteriores à lavra do expediente, perfazendo, segundo relata, um total estimado em torno de R$680.000.000,00 (seiscentos e oitenta milhões de reais). A Polícia Federal afirma no ofício não saber precisamente sobre quantos desses benefícios teriam sido efetivamente pagos, bloqueados ou devolvidos pelos bancos. No entanto, assevera, sem maiores detalhes, que "informes iniciais" apontam que os bancos já teriam bloqueado pagamentos que ultrapassariam a cifra de R$ 100.000,00 (cem milhões de reais).

5. O Ofício complementa que análises iniciais apontam para a ***massiva utilização indevida de senhas de servidores*** **do INSS nesses processos de reativação**, o que demandaria, segundo preceitua, **providências urgentes em termos de segurança das credenciais dos servidores e beneficiários e/ou bloqueio cautelar desse tipo de atividade**.

6. Por fim, solicita ao MTP determinar prioridade e urgência nas análises por parte da CGINT a fim de que a Polícia Federal possa adotar providências na sua esfera de atribuições.

7. Contextualizada a situação trazida pela PF, cumpre informar que, desde 2019, esta CGINT tem monitorado diferentes tipologias de fraude envolvendo o comprometimento de credenciais de servidores, tendo sido elaborados diversos Relatórios de Informação atinentes ao assunto, todos já devidamente encaminhados à Polícia Federal para subsidiar investigações dos casos identificados, bem como ao INSS, para subsidiar o bloqueio cautelar e reanálise dos processos.

8. Em relação ao item 2, acima, temos a registrar que esta Coordenação Geral, por meio de seu Coordenador-Geral, recebeu, conforme relacionado abaixo, três arquivos no formato . xlsx (Excel), diretamente do titular da Divisão de Repressão aos Crimes Previdenciários (DPREV), área integrante da Coordenação Geral de Polícia Fazendária (CGFAZ) da Diretoria de Combate ao Crime Organizado (DICOR) da Polícia Federal:

Nome do arquivo	Quantidade de registros	Quantidade de NB distintos	Data do recebimento
LIsta_banco_com_contas.xlsx	5.623	5.623	06/07/2022
LIsta_banco_com_contas_COMPLEMENTAR.xlsx	901	900	08/07/2022
LIsta_banco_com_contas_COMPLEMENTAR_14_07_2022.xlsx	3.213	3.167	14/07/2022
TOTAL	9.737	9.689	

9. O arquivo Lista NB (listagem 26643017), anexo ao Ofício nr. 146/2022/ASS/GAB/PF, de 18/07/2022 (26642828), é composto por planilha contendo coluna única de nome "NB", contendo 9.694 registros. Numa análise preliminar da planilha, verifica-se que na verdade **tais registros correspondem a 9.689 NB distintos, correspondendo à totalização dos três arquivos recebidos anteriormente pela CGINT, conforme item 8,** havendo total correspondência entre as listagens.

10. Em face do exposto no item 6, acima, informe-se, por oportuno, que, no campo investigativo, assim que recebidas as listagens mencionadas no item 8, esta Coordenação-Geral designou equipe para trabalhar as devidas análises de inteligência, o que foi formalizado por meio da PORTARIA CGINT/SE/MTP Nº 1957, DE 12 DE JULHO DE 2022 (26338143), publicada no Boletim de Serviço Eletrônico de 13/07/2022 (Processo SEI 10135.100897/2022-12). Ato contínuo, o titular da DPREV/CGFAZ/DICOR/PF foi informado sobre a priorização dada, por esta Coordenação-Geral, ao início das análises de inteligência.

11. Acrescenta-se ao exposto, que esta Coordenação-Geral vem envidando esforços no sentido de monitorar essas tipologias de fraudes em parceria com as áreas técnicas do INSS, nos âmbitos da Diretoria de Benefícios e Relacionamento com o Cidadão (Dirben), da Diretoria de Tecnologia da Informação (DTI) e da Diretoria de Governança, Planejamento e Inovação (DIGOV). Esse trabalho conjunto visa buscar a identificação proativa de novos casos de fraudes, possibilitando uma resposta mais célere a tais ameaças.

12. Nesse sentido, foi desenvolvido pela CGINT, em parceria com o INSS, painel específico denominado "Argus - Power BI", buscando fornecer indicadores que subsidiem e possibilitem uma atuação mais célere do INSS na prevenção, detecção e neutralização de incidentes de fraudes relacionados à tipologia de fraude relacionada à listagem de benefícios encaminhada pela Polícia Federal por meio do Ofício nr. 146/2022/ASS/GAB/PF, de 18/07/2022 (26642828).

13. Adiciona-se, ainda, que esta CGINT, encaminhou ao INSS, por canal técnico informal, a relação de benefícios recebidos conforme descrito no item 8.

14. No que diz respeito às "providências urgentes em termos de segurança das credenciais dos servidores e beneficiários e/ou bloqueio cautelar desse tipo de atividade" prescritas pela PF, conforme item 5, entendemos que o teor do Ofício nr. 146/2022/ASS/GAB/PF, de 18/07/2022 (26642828) e o anexo deveria ser levado ao conhecimento da Presidência do INSS, para subsidiar as eventuais providências de competência daquela Autarquia.

15. À Secretaria Executiva para conhecimento.

16. Em que pese a comunicação anteriormente feita, pelo canal técnico informal desta CGINT com o INSS (item 13), sugere-se que este processo seja encaminhado ao gabinete do Ministro de Estado, destinatário do Ofício nr. 146/2022/ASS/GAB/PF, de 18/07/2022, para que este avalie a oportunidade de encaminhar cópia do referido expediente (e anexo) à Presidência do INSS, com a brevidade que o caso requer.

Brasília, 08 de agosto de 2021.

Documento assinado eletronicamente

MARCELO HENRIQUE DE ÁVILA

Coordenador-Geral de Inteligência Previdenciária

sei! assinatura eletrônica

Documento assinado eletronicamente por **Marcelo Henrique De Ávila**, **Coordenador(a)-Geral**, em 08/08/2022, às 19:00, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Referência: Processo nº 19955.102272/2022-14. SEI nº 26949273

DESPACHO

Processo nº 19955.102272/2022-14

1. Trata-se de notícia de supostas "fraudes massivas" em benefícios, encaminhada pela Direção Geral da Polícia Federal ao Ministro de Estado do Trabalho e Previdência, por meio do Ofício nº 146/2022/ASS/GAB/PF, de 18/07/2022 (26642828).

2. Com a análise procedida pela Coordenação-Geral de Inteligência Previdenciária e Trabalhista (26949273), encaminhe-se ao Gabinete do Ministro, para conhecimento, com a sugestão de encaminhamento à presidência do INSS.

Brasília, 08 de agosto de 2022.

Documento assinado eletronicamente

LUCIO RODRIGUES CAPELLETTO

Secretário-Executivo

ENC: Concessão de Aposentadoria.

DANIELLA SUELEN SIQUEIRA BARBOSA <daniella.siqueira@inss.gov.br>

Seg, 15/08/2022 10:07

Para: Apoio Presidencia - INSSDF <sap@inss.gov.br>

De: MTP/Gabinete do Ministro do Trabalho e Previdência <gab.mtp@mte.gov.br>
Enviado: sexta-feira, 12 de agosto de 2022 15:29
Para: Coordenacao de Suporte ao Gabinete- INSSDF <csg@inss.gov.br>
Assunto: Concessão de Aposentadoria.

Referência: Processo nº 19955.102272/2022-14

Prezados,

Encaminho documentação pertinente em anexo, para conhecimento e providências subsequentes.

Gentileza confirmar recebimento.

Atenciosamente,

Gabinete do MTP

INSTITUTO NACIONAL DO SEGURO SOCIAL

Gabinete da Presidência

DESPACHO

Gabinete, em 15/8/2022.

Ref.: Processo nº 19955.102272/2022-14 _ **URGENTE**

Int.: Diretor-Geral Substituto da Policia Federal SANDRO TORRES AVELAR.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Preliminarmente, consigna-se o recebimento dos presentes autos nesta data.

2. Encaminhe-se ao Diretor de Benefícios e Relacionamento com o Cidadão para conhecimento e adoção das providências a seu cargo com **URGÊNCIA.**

SIDNEI CICERO COTTET

Chefe de Gabinete da Presidência

sei! assinatura eletrônica

Documento assinado eletronicamente por **SIDNEI CICERO COTTET**, **Chefe de Gabinete da Presidência**, em 15/08/2022, às 15:25, 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 **8538005** e o código CRC **77070592**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 8538005

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Benefícios e Relacionamento com o Cidadão

DESPACHO

Diretoria de Benefícios e Relacionamento com o Cidadão, em 15/08/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: Diretor-Geral Substituto da Policia Federal SANDRO TORRES AVELAR.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se do Despacho Nº 314/2022/GMTP-MTP (8536675), emitido pelo Gabinete do Ministro, do Ministério do Trabalho e Previdência que, em apertada síntese, solicitando informações sobre supostas fraudes massivas em benefícios.

2. De ordem, encaminha-se à CGMOB para exame.

JANAINA DOS SANTOS DE QUEIROZ

Assessora da Diretoria de Benefícios e Relacionamento com o Cidadão

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Benefícios e Relacionamento com o Cidadão
Coordenação-Geral de Monitoramento e Cobrança Administrativa de Benefícios

DESPACHO

Coordenação-Geral de Monitoramento e Cobrança Administrativa de Benefícios, em 24/08/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Reativações indevidas

1. Trata-se de demanda recebida da Diretoria de Benefícios e relacionamento com o Cidadão proveniente da Coordenação Geral de Inteligência Previdenciária e Trabalhista versando sobre procedimentos de supostas reativações indevidas processadas em benefícios.

2. O encaminhamento decorre de apontamento realizado em ofício expedido pela Direção Geral da Polícia Federal.

3. Foi encaminhado no processo a lista de benefícios que constam no documento SEI 8536719, trata-se de lista contendo apenas os números de benefícios e constam nela 9.689 benefícios distintos e, conforme já mencionados pela CGINT a avaliação preliminar realizada antes do direcionamento ao INSS.

CONTEXTUALIZAÇÃO

4. A CGMOB desenvolve atividades de monitoramento com o propósito de identificar procedimentos fraudulentos de reativações em benefícios, esse monitoramento possibilita a atuação na cessação em bloco dos benefícios que respondam a um cenário de fraudes em reativações bem como subsidiar as demais áreas do INSS envolvidas.

5. Atualmente está em andamento o tratamento de reativações indevidas operadas nos meses de junho e julho de 2022 - que estão inseridas dentro dos 60 dias mencionados no ofício da Direção da Polícia Federal. Por essa razão procedemos o batimento da lista de benefícios com aquela que é resultado dessa atividade de monitoramento. Aproveita-se para registrar de que o tema aqui trazido já vem sendo tratado no âmbito da Autarquia, por meio de processos SEI, ocasião em que foram identificados outros benefícios que passaram por semelhante modus operandi fraudulento.

6. Por meio desses processos vem sendo registradas as constatações e demandadas as providências no âmbito da Coordenação Geral de Monitoramento e Cobrança de Benefícios, sendo identificado que a fraude massiva contra o INSS tem acontecido por diversos meios como reativações indevidas de benefícios de espécies extintas, com renda mensal elevada e, em sua grande maioria, cessados por óbitos dos titulares; inclusão de empréstimos consignados, reativações de benefícios, e utilização de documentos fraudulentos; usurpação de acesso de servidores da Autarquia em diversas Unidades e a concessão indevida de benefícios com uso das referidas matrículas; fraudes em reativações de benefícios de pensão por morte concedidos irregularmente.

DA ANÁLISE PRELIMINAR

7. Impende salientar que os primeiros casos envolvendo reativações massivas de benefícios de forma irregular chegaram ao conhecimento desta Coordenação a partir do segundo semestre de 2021, ocasião em que as primeiras notas técnicas foram elaboradas no sentido de demandar cessações/suspensões em lote nos benefícios, desde então vem sendo tratado com as áreas competentes possíveis alterações nas regras de negócio das reativações nos sistemas de manutenção.

8. Assim como em trabalhos anteriores empreendidos pela Coordenação de Ações Corretivas e Cobrança Administrativa de Benefícios, o trabalho envolvendo o cenário das reativações se vale de algumas premissas que permitiram a identificação das fraudes e portanto conferem assertividade aos achados, elencamos de forma exemplificativa algumas dessas premissas:

a) Volumetria de reativações concentradas em credenciais;

b) Comportamento anômalo da credencial em relação a região geográfica e atividades diárias;

c) Inexistência de instrução formal que justifique o procedimento;

d) Variação do volume de reativação como um todo;

e) Tempo decorrido entre a cessação e a reativação.

9. Além da verificação da correta instrução do processo foi necessária a verificação da contemporaneidade da tarefa em relação ao procedimento bem como em relação ao responsável pelo procedimento, ou seja, a existência da tarefa não é elemento bastante para descartar a possibilidade de fraude.

10. O trabalho de monitoramento no qual se inserem os casos apresentados pela Polícia Federal refere-se a atividade de análise e detecção realizada por esta Coordenação nas ações de reativação processadas em junho e julho de 2022 em busca de anomalias dentro das premissas elencadas acima.

DA ANÁLISE DO CONTEXTO ESPECÍFICO DO OFÍCIO DA DIREÇÃO DA POLÍCIA FEDERAL

11. A partir de uma primeira análise identificamos que 9.677 casos estão dentro do cenário mapeado pela CGMOB e foram alvo de atuação para cessar em lote e bloquear pagamentos que eventualmente ainda não tenha sido efetivados, por meio de demanda registrada na DATAPREV em 24/08/2022 que é a Empresa de Tecnologia responsável por estas ações junto ao INSS, cabendo, mas uma vez destacar, que a abertura da demanda é a conclusão do trabalho em desenvolvimento e já mencionado no presente relatório, isto é, tem como ponto de partida a ação de monitoramento que já vem sendo desenvolvida pela Coordenação.

12. Outros 11 casos representam situações de Pensões alimentícias que estavam associadas a benefícios cessados e que foram reativadas automaticamente em razão da reativação do benefício de origem, porém o benefício de origem foi alvo de reativação indevida já mapeada pela CGMOB e serão igualmente cessados.

13. Por fim 1 caso se trata de benefício corretamente mantido e o que houve foi a reativação indevida de uma PA que já havia sido encerrada.

14. O monitoramento é feito a partir das informações de reativações ocorridas nessas competências, entretanto há a necessidade de identificar as situações suspeitas e separa-las da atuação ordinária nas reativações em benefícios para então adotar a medida de cessação dos mesmos.

15. Considerando o volume de problemas identificados, a atuação em bloco para reverter os benefícios que foram reativados indevidamente, se mostra o método mais adequado para racionalizar a força de trabalho envolvida na contenção do problema.

16. Diante do trabalho já realizado até o momento é possível afirmar que os casos listados no presente processo respondem a um cenário reconhecido de fraude - com exceção do caso mencionado no item 8 - compreendendo reativações feitas de forma indevida, sem que tenha havido a instrução processual adequada, tampouco a formalização do pedido pelo cidadão.

17. No conjunto de 9,6 mil benefícios há 19 credenciais distintas envolvidas, até o momento não há elemento que permita afirmar que há envolvimento dos servidores. O que é possível inferir, com os elementos à disposição da CGMOB, é que há indícios de utilização indevida de credencial sem o consentimento dos servidores, entretanto há necessidade de informações complementares para emissão de parecer conclusivo sobre esse aspecto.

18. As credenciais envolvidas nas reativações processadas nos benefícios que constam na lista da Polícia Federal foram responsáveis pela reativação de 19.209 benefícios - já incluídos os casos que constam nesse processo e foram objeto de análise pela Coordenação de Ações Corretivas e Cobrança Administrativa de Benefícios desta Coordenação Geral dentro de um contexto que envolve 54 credenciais e ações de reativação em 22.327 benefícios distintos.

RESUMO DOS ACHADOS NA AÇÃO DE MONITORAMENTO

19. Passamos agora ao registro dos achados da CGMOB, REFORÇANDO que as constatações apontada a seguir se referem ao conjunto de 54 credenciais mencionados e que o trabalho está em andamento e há outras credenciais em monitoramento e no caso de identificar novas situações irregulares serão igualmente documentados e corrigidos.

I - VOLUME DE REATIVAÇÕES

a) Algumas credenciais apresentaram um volume alto e concentrado de tal forma que é possível inferir a possibilidade de ação automatizada, como é o exemplo da credencial **2040923**, com operações entre 20 e 27/06, totalizando 7,2 mil ações de reativação envolvendo 3,6 mil benefícios distintos, com pico no dia 26/06 quando foram processadas 2.306 reativações em único dia;

b) Essa mesma credencial operou esse volume majoritariamente por meio de IPs associados a rede da APS Belém - Icoaraci, nesse IP foram processadas 97% das operações de reativação nessa credencial.

c) Vale observar que esse mesmo IP da APS Belém Icoaraci aparece relacionado a outras 11 credenciais com reativações indevidas;

d) O quadro a seguir apresenta um resumo do volume de benefícios associados a cada uma das credenciais baseado na análise realizada até o momento, no total de 54 credenciais identificadas, sendo passível de ajuste em razão da continuidade do monitoramento:

CREDENCIAIS ENVOLVIDAS NAS REATIVAÇÕES JUNHO/JULHO 2022											
ACIMA DE 1000			ENTRE 300 E 1000			ENTRE 100 E 300			MENOR DO QUE 100		
CREDENCIAL	QTDE BENEF	UF	CREDENCIAL	QTDE BENEF	UF	CREDENCIAL	QTDE BENEF	UF	CREDENCIAL	QTDE BENEF	UF
2040923	3.633	PA	252619	684	PB	156178	287	MG	6880628	94	AM
545456	2.819	ES	899485	624	PB	923592	266	RN	2210170	80	RS
2409376	2.497	PA	880592	609	AM	905824	263	PI	752048	74	SE
755401	2.212	SP	922294	577	RJ	898499	261	PB	1815946	67	DF
2948077	1.417	RO	1637392	543	CE	939934	258	SP	914231	61	RJ
1250181	1.056	RJ	1424970	379	CE	890313	217	MT	2024845	63	SC
940436	1.046	SP	896448	337	MG	1420719	209	SP	899391	59	PB
						1534762	147	SC	1376234	57	PE
						1960829	147	SC	880572	53	AM
						1444636	143	RJ	2058151	46	AM
						2297793	143	GO	885165	42	CE
						221549	140	DF	1379883	42	MT
						1376869	134	SP	1782277	41	SP
						880930	125	AM	1564545	30	BA
						1108223	124	SP	1376000	25	SP
						543634	109	GO	1517109	23	SP
									880727	17	AM
									1492428	12	PA
									1786313	12	MG
									938568	9	PR
									1375576	8	RJ
									1450846	5	MG
									1563349	2	DF
									935153	1	SP

II - LOCAIS DE ONDE PARTIRAM AS OPERAÇÕES (Avaliação por IPs)

a) Diversos IPs identificados como foco de operações indevidas aparecem em registros de credenciais diferentes, em diversos casos não havendo relação do local do IP com a lotação do servidor tampouco relação aparente entre os servidores cujas credencias se associaram aquele determinado IP, abaixo dois quadros demonstrando este cenário:

NÚMERO DE BENEFÍCIOS ALVOS DAS AÇÕES DE REATIVAÇÃO - IP DE BELÉM ICOARACI							
	CREDENCIAIS						TOTAL IP
BELÉM - ICOARACI	1	2	3	4	5	6	
10.88.102.119	545456						19
10.88.102.122	2409376						1
10.88.102.124	752048	2040923	2409376				681
10.88.102.137	1250181						235
10.88.102.153	2040923						389
10.88.102.157	545456						15
10.88.102.158	752048	2040923					765
10.88.102.164	2040923	2409376					987
10.88.102.168	2040923	2409376					117
10.88.102.170	1250181						104
10.88.102.172	896448	939934	1376234	1420719	1424970	1786313	776
10.88.102.175	2409376						27
10.88.102.179	1379883	2040923					415
10.88.102.180	2040923	2409376					1.659
10.88.102.94	545456						93
			TOTAL NA REDE BELÉM - ICOARACI				6.283

NÚMERO DE BENEFÍCIOS ALVOS DAS AÇÕES DE REATIVAÇÃO - IP DE TAMBORIL - CE							
	CREDENCIAIS						TOTAL IP
TAMBORIL - CE	1	2	3	4	5	6	
10.65.114.100	1492428	2297793					9
10.65.114.111	545456						17
10.65.114.117	1250181						21
10.65.114.118	545456						112
10.65.114.119	1375576						7
10.65.114.122	899391	923592	1250181	1492428			176
10.65.114.123	896448	939934	1108223	1420719	1517109	2948077	267
10.65.114.127	545456	896448	898499	935153	2948077		101
10.65.114.129	545456	923592	1250181				278
10.65.114.131	545456	923592	1250181				342
10.65.114.132	545456	923592	1250181	2297793			426
10.65.114.133	898499	1420719	1564545	2948077			143
10.65.114.86	2297793						1
10.65.114.89	899391						1
			TOTAL NA REDE BELÉM - ICOARACI				1.901

b) Considerando a situação apresentada nota-se que há uma transversalidade de credenciais que foram utilizadas a partir da mesma rede evidenciando a conexão entre as operações e, ao menos em tese, indicando o mesmo grupo organizado que pode ter se apropriado das credenciais com o propósito de cometer a fraude.

c) Há outros IPs com menor volume de operações mas que apresentam o mesmo padrão de Belém - Icoaraci e Tamboril:

Camocim - CE	2.092
10.65.134.62	**2.092**
545456	1.164
755401	2
896448	125
2948077	801
923592	21
2297793	6

Nilopolis - RJ	2126
10.1.154.91	**2126**
545456	823
755401	892
940436	177
1250181	150
1420719	84

Peruibe - SP	483
10.19.200.129	**5**
1450846	5
10.19.200.130	**41**
1782277	41
10.19.200.131	**32**
755401	32
10.19.200.132	**71**
755401	69
1250181	2
10.19.200.138	**300**
543634	109
885165	42
1563349	2
1960829	147
10.19.200.140	**34**
755401	34

Copacabana - RJ	1206
10.1.121.100	**188**
940436	188
10.1.121.101	**597**
940436	149
2948077	448
10.1.121.105	**57**
940436	57
10.1.121.57	**7**
2948077	7
10.1.121.64	**1**
1375576	1
10.1.121.74	**81**
896448	21
2948077	60
10.1.121.75	**8**
1250181	8
10.1.121.77	**51**
896448	30
2948077	21
10.1.121.79	**15**
2948077	15
10.1.121.87	**197**
940436	197
10.1.121.91	**1**
545456	1
10.1.121.98	**3**
899391	3

Itapema - SC	1044
10.107.180.73	**5**
755401	5
10.107.180.74	**45**
755401	45
10.107.180.75	**23**
755401	23
10.107.180.82	**28**
755401	28
10.107.180.94	**943**
755401	496
940436	277
1250181	170

GEx Goiania	568
10.74.0.115	**104**
755401	104
10.74.0.120	**56**
755401	49
2409376	7
10.74.0.122	**215**
755401	196
2409376	19
10.74.0.162	**101**
755401	101
10.74.0.163	**1**
755401	1
10.74.0.44	**91**
2409376	91

GEx Manaus	272
10.62.1.213	**40**
880572	6
6880628	34
10.62.1.60	**232**
880572	47
880930	125
6880628	60

S Paulo-Centro	87
10.17.32.108	**31**
545456	31
10.17.33.74	**56**
545456	56

Cabo Frio	135
10.1.112.78	**135**
755401	135

d) Houve ainda a identificação de um volume de operações em duas redes com sequenciais 10.69.130 e 10.69.131, sobre as quais esta Coordenação não possui informação para indicar o local a que se referem, abaixo o quadro de operações dessas redes:

REDE 10.69.130	1808
10.69.130.101	**43**
1815946	43
10.69.130.110	**1446**
156178	115
221549	26
252619	276
880592	353
880727	17
890313	21
898499	46
899485	247
922294	281
1108223	37
1637392	27
10.69.130.116	**8**
1637392	8
10.69.130.129	**309**
221549	61
252619	1
940436	1
1376000	25
1376869	79
1444636	142
10.69.130.96	**2**
1444636	1
1815946	1

REDE 10.69.131	2656
10.69.131.112	**1408**
156178	106
252619	217
880592	256
890313	106
898499	68
899485	323
922294	296
938568	9
1108223	27
10.69.131.126	**806**
221549	53
252619	190
1376869	55
1637392	508
10.69.131.29	**69**
1815946	23
2058151	46
10.69.131.56	**373**
156178	66
890313	90
898499	72
899485	54
1108223	28
2024845	63

e) Um outro conjunto de casos foram operados a partir do uso de VPN para acesso a rede do INSS, foram reativação relacionadas a 1.639 benefícios e 6 credenciais distintas. Vale o registro de que para as credenciais 905824, 1534762 e 2210170 todas as operações identificadas foram por meio de VPN; já as credenciais 2040923 e 2409376 tem operações em outros IPs, conforme verificado nos quadros 2, 3 e 4.

CREDENCIAIS COM REGISTRO DE REATIVAÇÕES POR VPN	
VPN	**1639**
2409376	993
905824	263
1534762	147
2040923	95
2210170	80
914231	61

III - LOCAIS DE LOTAÇÃO DOS SERVIDORES

a) As 54 credenciais aqui analisadas referem-se a servidores que estão lotados em 20 Unidades da Federação distintas, sendo São Paulo com o maior número verificado de 10 (dez) credenciais, seguido do Amazonas com 6 (seis). Já os locais de manutenção dos benefícios identificados remetem a todas as 27 unidades da federação. **Sendo assim o que se nota é existência de benefícios para localidades em todos os estados da federação, entretanto há uma proporção maior nos estados do Rio de Janeiro e São Paulo.**

b) Confrontando a UF dos benefícios reativados com a UF de lotação do servidores é possível notar que para a maior parte das credenciais não há correlação entre essas informações, isto é, a localidade dos benefícios reativados não condiz com a localidade onde o servidor trabalha.

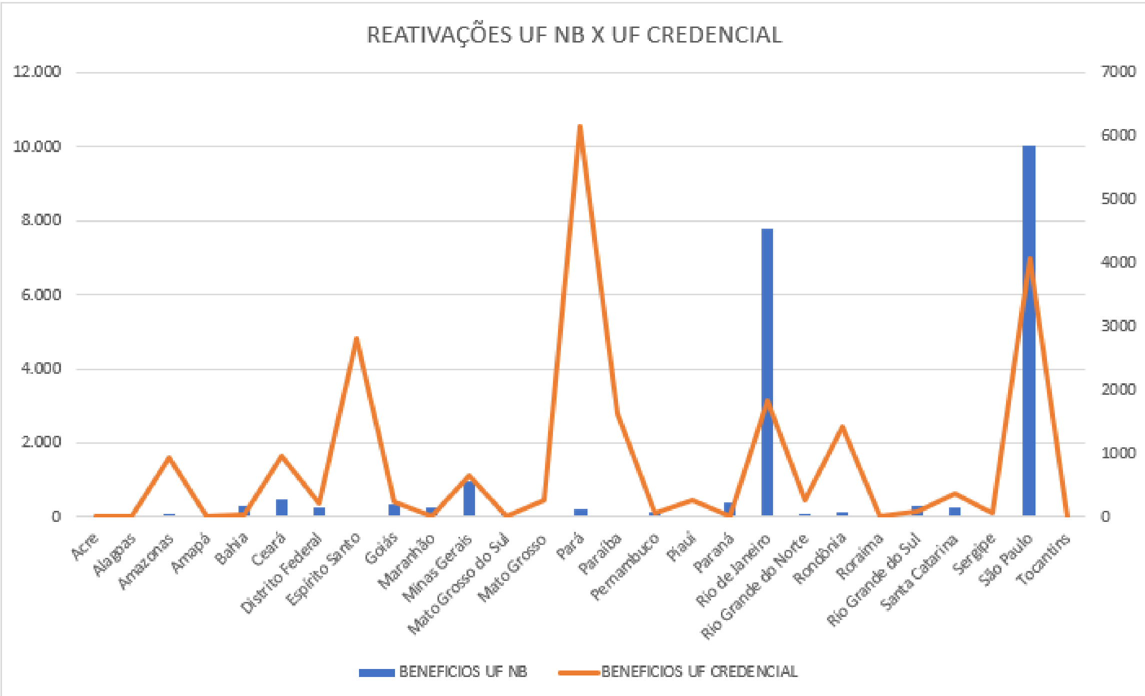
c) Estas percepções preliminares permitem chegar a conclusões parecidas com aquelas a que se chegaria a partir do que foi observado pela avaliação dos IPs - de que as credenciais aqui referidas compõem um rol de credenciais associadas a uma prática unificada. Em linhas gerais, é possível inferir, ao menos em tese, que não são ações isoladas praticadas por cada credencial. A fraude consiste em reativar benefícios de forma irregular, para tanto é necessário realizar a operação em sistema do INSS e com credencial de servidor, logo, há indícios de que a captura da credencial e sua utilização indevida faz parte do modus operandi.

d) Quadro comparativo, quantidade de benefícios reativados UF CREDENCIAL X UF BENEFÍCIO:

UF DAS	UF DO LOCAL DE MANUTENÇÃO DO BENEFÍCIO																										
CREDENCIAIS	AC	AL	AM	AP	BA	CE	DF	ES	GO	MA	MG	MS	MT	PA	PB	PE	PI	PR	RJ	RN	RO	RR	RS	SC	SE	SP	TO	TOTAL
AM			22		2	4	20		3		33	7	2			13	1	8	531	5	10		36	15		232		944
BA						5	3		8																	14		30
CE			4		9	20	14	1	4	6	51	11	20	20	1	5	1	6	502		22		34	3		223	5	962
DF	1					1	8		2			3	4						168		15		1			6		209
ES		7		3	68	66	36	3	47	24	84	12	6	28	6	31	1	44	1.013		2		23	48		1.260	7	2.819
GO				1	6	25	5		25	13	3			8					129				1			36		252
MG		4			8	8	36	2	5	4	78	1	1	12		6		9	288		1		2	4		167	5	641
MT					1		1								4			1	182	1				5		64		259
PA	1	7	14		26	64	31	6	11	18	473	2	4	22	5	11	1	57	614	19	2	1	77	68	2	4.604	2	6.142
PB			3	1	16	17	14	5	12	2	26	5		1	1	8		4	523	33			19	37		900	1	1.628
PE					3	1	1		14	1	20			1					4		7		1			4		57
PI		6				61	3	8	29	5	10	13	1	8	5	15	4	31	34		3		8	2	10		7	263
PR																			9									9
RJ	1	4	5		29	81	15	1	11	12	52	9	8	8	4	2	2	51	982	2	27		9	22	3	500	5	1.845
RN			1		20	6	1				1	4			1		3	21	142	2	10		5			49		266
RO		2			28	26	26		26	40	22	1	2	9	4	10	6	22	502	2	1		17	18	1	648	4	1.417
RS		3			1	5				2	13	3		11					39				1			2		80
SC					1	1	12		20	89	14			20	3	1	5	2	119				9	5		56		357
SE						1										1		3	1	13						55		74
SP	4	3	45	1	77	93	32	8	114	26	99	11	7	58	2	38	15	144	1.982		21		43	19	4	1.220	7	4.073
TOTAL	7	36	94	6	295	485	258	34	331	242	979	82	55	206	36	141	39	403	7.764	77	121	1	286	246	20	10.040	43	22.327

IV - LOCAIS DE MANUTENÇÃO DOS BENEFÍCIOS REATIVADOS APÓS A REATIVAÇÃO.

a) Os benefícios avaliados apresentam uma concentração nos locais de manutenção no estado do Rio de Janeiro e de São Paulo, distribuídos conforme o gráfico, porém a UF das credenciais não são coincidentes.



V - CARACTERÍSTICAS DOS PAGAMENTOS EMITIDOS APÓS AS REATIVAÇÕES

a) Os pagamentos emitidos em razão dessa reativação e que foram processados para envio ao banco, isto é, constam como autorizados, esses pagamentos estão associados a 16.111 benefícios do total de 22.327.

b) Sobre esses pagamentos os dados dos quais a Coordenação dispõe está relacionado aos créditos emitidos e autorizados, portanto não temos informação sobre o retorno, isto é, se houve rejeição desses créditos pela rede bancária, razão pela qual, estamos atuando em conjunto com a área competente e tal levantamento detalhado já lhe foi demandado, porém somente após estes levantamentos poderá ao final ser confirmado eventual prejuízo;

c) Abaixo avaliações preliminares relacionadas aos bancos destinatários dos créditos:

CRÉDITOS EMITIDOS EM RAZÃO DA REATIVAÇÃO POR BANCO	
BANCO DESTINATÁRIO DO CRÉDITO	QTDE BENEFÍCIOS
033-Banco Santander (Brasil) S.A	13.642
341-Banco Itau S.A	1.652
237-Bradesco	497
001-Banco do Brasil	152
104-Caixa	126
756-Bancoob	16
069-Bpn	6
037-Banco do Estado do Pará S.A	5
003-Banco da Amazonia S.A	3
004-Bnb	3
318-Bmg	3
748-Banco Cooperativo Sicredi S.A	2
070-Brb	2
047-Banese	1
389-Banco Mercantil do Brasil S.A	1
TOTAL	16.111

d) Créditos por UF:

CRÉDITOS EMITIDOS EM RAZÃO DA REATIVAÇÃO POR UF	
ESTADO	QTDE BENEFÍCIOS
São Paulo	6.922
Rio de Janeiro	5.818
Minas Gerais	672
Ceará	340
Paraná	289
Goiás	257
Distrito Federal	213
Bahia	208
Rio Grande do Sul	204
Maranhão	178
Santa Catarina	172
Amazonas	154
Pará	130
Pernambuco	112
Rondônia	100
Rio Grande do Norte	61
Mato Grosso do Sul	60
Mato Grosso	50
Tocantins	30
Espírito Santo	29
Piauí	28
Paraíba	24
Alagoas	19
Sergipe	14
{ñ class}	12
Acre	8
Amapá	6
Roraima	1
TOTAL	16.111

VI - DISTRIBUIÇÃO DAS REATIVAÇÕES POR ESPÉCIE

a) Conforme quadro abaixo, no cenário avaliado, há uma predominância dos benefícios assistenciais que respondem por 56% do total (considerando idoso e deficiente), seguido do auxilio reclusão com o percentual de 14%, depois a aposentadoria por idade com 13%, e por último, até o momento a pensão por morte com 9,7%, estas 4 espécies representam 93% do volume das reativações indevidas.

ESPÉCIE	QTDE DE BENEF.	%
87	7532	33,73%
88	4983	22,31%
25	3175	14,22%
41	3068	13,74%
21	2166	9,70%

CASOS IDENTIFICADOS EM AGOSTO

20. Durante a análise dos casos que compuseram o presente relatório, em continuidade ao trabalho de monitoramento foi

possível identificar a repetição do comportamento na competência 08 (agosto) envolvendo outras credenciais. Em razão da urgência da necessidade de tomada de providências à respeito dos mais de 22.000 casos identificados para junho e julho, no presente momento adiantamos a análise de três 3 credenciais referentes aos achados de agosto, visando, principalmente, chamar a atenção para o fato da continuidade do comportamento de possível fraude massiva contra o INSS e que necessita de atuação das áreas correlacionadas de forma conjunta e visando minimizar, dificultar, impedir essas atuações.

21. Em relação às credenciais que realizaram operações no mês de agosto, somam-se 795 benefícios nos quais foram praticadas ações de reativação.

22. As credencias aqui tratadas realizaram operações a partir de IP associado a GEX São Paulo e uma delas a um IP da rede 10.69.131, conforme informações no quadro a seguir:

REDE	CREDENCIAL	QTDE DE BENEFÍCIOS
	0942846	**405**
São Paulo Centro	10.17.32.165	7
São Paulo Centro	10.17.32.38	6
São Paulo Centro	10.17.33.29	2
São Paulo Centro	10.17.33.33	6
São Paulo Centro	10.17.33.42	236
São Paulo Centro	10.17.33.46	150
	0927737	**334**
São Paulo Centro	10.17.32.38	1
São Paulo Centro	10.17.33.42	84
São Paulo Centro	10.17.33.46	237
São Paulo Centro	10.17.33.74	10
São Paulo Centro	10.17.33.85	2
	1871600	**56**
	10.69.131.171	56

23. Os casos identificados em agosto também foram alvo de ação para retornar os benefícios para a situação anterior como cessados.

ENCAMINHAMENTOS E PROVIDÊNCIAS ADOTADAS

24. A Coordenação de Ações Corretivas e Cobrança Administrativa conforme acima informado registrou demanda específica junto à DATAPREV para retornar os benefícios para a situação de cessados decorrente de ação de monitoramento com o propósito de mitigar os efeitos das ações ilícitas.

25. Considerando todo o exposto, sugerimos ainda, no intuito de oferecer maiores informações à Polícia Federal, a manifestação de outras áreas envolvidas, antes do retorno do presente à CGINT, conforme sugestão:

I - Coordenação Geral de Pagamentos de Benefícios:

a) No que se refere as regras de negócio envolvendo os procedimentos de reativação e emissão de pagamentos associados e;

b) Dados sobre os pagamentos emitidos para os benefícios envolvidos (incluindo situação do crédito, instituição destinatária, modalidade de pagamento).

II - Diretoria de Tecnologia da Informação:

a) Informações relacionadas aos acessos ocorridos a partir das credenciais.

b) Informações sobre os acessos VPN, a forma que ocorrem e quais credenciais foram responsáveis pelos acessos que culminaram nas ações acima;

c) Informações sobre os IPS de VPN e IPs das redes 10.69.130 e 10.69.131.

d) Informações sobre os dispositivos que foram encontrados conectados a rede do INSS e que podem ter servido de porta de acesso a rede por pessoas não autorizadas;

e) Com respeito às credenciais identificadas e informadas no presente processo, sugerimos providências da DTI no sentido de que as mesmas não sejam objeto de reincidência de monitorar estas matrículas impedindo a utilização indevida das mesmas repetidamente.

26. Feitas as considerações, encaminhe-se à Diretoria de Benefícios e relacionamento com cidadão, sugerindo a remessa às áreas acima mencionadas para prestarem também suas informações a serem apresentadas à Polícia Federal.

ANDERSON WILLIAN GONÇALVES BORGES
Assessor Técnico Especializado

ARIANE ELIZABETH DOS SANTOS CAMARGO ORESTES

Coordenadora de Ações Corretivas e Cobrança Administrativa

CATIA CRISTINA DA SILVA BAUM
Coordenadora Geral de Monitoramento e Cobrança Administrativa de Benefícios

Documento assinado eletronicamente por **ANDERSON WILLIAN GONCALVES BORGES**, **Técnico do Seguro Social**, em 25/08/2022, às 11:01, 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 **CATIA CRISTINA DA SILVA BAUM**, **Coordenador(a) Geral**, em 25/08/2022, às 11:27, 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 **ARIANE ELIZABETH DOS SANTOS CAMARGO ORESTES**, **Coordenador(a)**, em 25/08/2022, às 11:55, 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 **8575180** e o código CRC **C69EC1B4**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 8575180

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Benefícios e Relacionamento com o Cidadão

DESPACHO

Diretoria de Benefícios e Relacionamento com o Cidadão, em 25/08/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Ciente e de acordo.

2. Encaminhe-se na forma proposta no item 25 do despacho 8575180, inicialmente a Coordenação-Geral de Pagamentos de Benefícios após, Diretoria de Tecnologia da Informação para informações pertinentes.

EDSON AKIO YAMADA

Diretor de Benefícios e Relacionamento com o Cidadão

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Benefícios e Relacionamento com o Cidadão
Coordenação-Geral de Pagamento de Benefícios

DESPACHO

Coordenação-Geral de Pagamento de Benefícios, em 31/08/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Ciente do Despacho DIRBEN (8676929).

2. Encaminha-se à DMAND para prosseguimento.

ANDRESSA FARIAS

Assistente Administrativo-CGPAG

INGRID AMBROZIO CAMILO

Coordenação Geral de Pagamento de Benefícios.

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação

DESPACHO

Diretoria de Tecnologia da Informação, em 05/09/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Minuta de Instrução Normativa que disciplina ….

1. Trata-se do DESPACHO Nº 314/2022/GMTP-MTP, oriundo do Ministério de Trabalho e Previdência cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, proveniente da Polícia Federal comunicando a ocorrência de prováveis fraudes massivas contra o INSS.

2. Dada ciência ao Diretor de Tecnologia da Informação dos Despachos GABPRE 8538005 e DIRBEN 8676929.

3. De ordem, encaminhe-se:

a) à DTIR - Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos, para ciência, subsídios e demais providências cabíveis, com **URGÊNCIA**.

b) à CGIS - Coordenação-Geral de Infraestrutura e Segurança em Tecnologia da Informação, para ciência e o devido acompanhamento.

ANA LÚCIA ARAÚJO BESERRA

Analista de TI

Documento assinado eletronicamente por **ANA LUCIA ARAUJO BESERRA**, **Analista em Tecnologia da Informação**, em 05/09/2022, às 12:36, 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 **8799248** e o código CRC **69D7D665**.

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 05/09/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se do Despacho Nº 314/2022/GMTP-MTP (8536675), oriundo do Ministério de Trabalho e Previdência, cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, proveniente da Polícia Federal comunicando a ocorrência de prováveis fraudes massivas contra o INSS.

2. Ciente do Despacho GABPRE (8538005) e do Despacho DIRBEN (8538569).

3. O Despacho CGMOB (8575180) fez uma análise da questão e elencou alguns pontos a serem esclarecidos:

> "25. *Considerando todo o exposto, sugerimos ainda, no intuito de oferecer maiores informações à Polícia Federal, a manifestação de outras áreas envolvidas, antes do retorno do presente à CGINT, conforme sugestão:*
>
> I - *Coordenação Geral de Pagamentos de Benefícios:*
>
> a) *No que se refere as regras de negócio envolvendo os procedimentos de reativação e emissão de pagamentos associados e;*
>
> b) *Dados sobre os pagamentos emitidos para os benefícios envolvidos (incluindo situação do crédito, instituição destinatária, modalidade de pagamento).*
>
> II - ***Diretoria de Tecnologia da Informação:***
>
> a) ***Informações relacionadas aos acessos ocorridos a partir das credenciais.***
>
> b) ***Informações sobre os acessos VPN, a forma que ocorrem e quais credenciais foram responsáveis pelos acessos que culminaram nas ações acima;***
>
> c) ***Informações sobre os IPS de VPN e IPs das redes 10.69.130 e 10.69.131.***
>
> d) ***Informações sobre os dispositivos que foram encontrados conectados a rede do INSS e que podem ter servido de porta de acesso a rede por pessoas não autorizadas;***
>
> e) ***Com respeito às credenciais identificadas e informadas no presente processo, sugerimos providências da DTI no sentido de que as mesmas não sejam objeto de reincidência de monitorar estas matrículas impedindo a utilização indevida das mesmas repetidamente."***

4. Dessa forma, encaminhe-se à Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - **DTIR**, para ciência, subsídios e demais providências cabíveis, com **URGÊNCIA**.

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 05/09/2022, às 15:47, 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 **8800442** e o código CRC **903A6DB1**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 8800442

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Benefícios e Relacionamento com o Cidadão
Coordenação-Geral de Pagamento de Benefícios
Coordenação De Pagamentos e Gestão De Benefícios
Divisão De Manutenção De Direitos

DESPACHO

Divisão De Manutenção De Direitos, em 05/09/2022

Ref.: Processo nº 19955.102272/2022-14

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS

1. Trata-se do DESPACHO Nº 314/2022/GMTP-MTP, oriundo do Ministério de Trabalho e Previdência cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, no qual a Polícia Federal comunica a ocorrência de prováveis fraudes massivas contra o INSS e que veio a esta Divisão para prestar os esclarecimentos, abaixo transcritos, levantados pela Coordenação-Geral de Monitoramento e Cobrança Administrativa de Benefícios - CGMOB (ID 8575180):

> 25. Considerando todo o exposto, sugerimos ainda, no intuito de oferecer maiores informações à Polícia Federal, a manifestação de outras áreas envolvidas, antes do retorno do presente à CGINT, conforme sugestão:
>
> I - Coordenação Geral de Pagamentos de Benefícios:
>
> a) No que se refere as regras de negócio envolvendo os procedimentos de reativação e emissão de pagamentos associados e;
>
> b) Dados sobre os pagamentos emitidos para os benefícios envolvidos (incluindo situação do crédito, instituição destinatária, modalidade de pagamento).

2. Em relação aos quesitos acima, entendemos que compete a esta Divisão, o pronunciamento acerca do item "a"; sendo de competência da Divisão de Agentes Pagadores - DAGPG, a manifestação quanto ao item "b".

3. Assim sendo, passamos às considerações pertinentes.

4. Visando coibir as tentativas de fraude, foi criada a demanda DM.100261 em 11.07.2022, com o objetivo de alterar as regras de reativação de benefícios, para que os pagamentos sejam direcionados para cartão magnético, pois desta forma, para o recebimento dos valores gerados, há

necessidade de identificação junto ao órgão pagador e implementada crítica (OPERAÇÃO NÃO PERMITIDA - MR TIPO 5) quando a alteração for feita para tipo de microrregião "5" (que só paga benefício em conta corrente), obrigando o servidor a efetuar a troca para microrregião tipo 1 ou 4, que destinará aquele benefício, obrigatoriamente, para cartão magnético.

5. Continuando, no comando efetuado no SIBE PU, quando finalizada a demanda, o sistema passará a exigir também, preenchimento de novo campo (NÚMERO DA TAREFA DO GERENCIADOR DE TAREFAS - GET) que após comunicação sistêmica verificará a existência ou não de tarefa de reativação no GET; .

6. Feitas as considerações, retorne-se à Coordenação-Geral de Pagamento de Benefícios - CGPAG, para ciência e se acordo, envio à Divisão de Agentes Pagadores - DAGPG, conforme proposto no item 2.

LÍVIA IVO E SILVA COLLE
Colaboradora DMAND

CÉLIA REGINA KILL
Chefe da Divisão de Manutenção de Direitos

Documento assinado eletronicamente por **CELIA REGINA KILL**, **Chefe de Divisão de Manutenção de Direitos**, em 08/09/2022, às 14:38, 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 **LIVIA IVO E SILVA COLLE**, **Técnico do Seguro Social**, em 08/09/2022, às 15:04, 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 **8802692** e o código CRC **756C5C50**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 8802692

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 03/09/2022

Ref.: Processo nº 35014.349892/2022-93.

Int.: INSS.

Ass.: Reativações Indevidas.

1. Trata-se de processo administrativo instaurado no âmbito da Coordenação de Ações Corretivas e Cobrança Administrativa de Benefícios, que decorre de achados de monitoramento em relação a reativações potencialmente indevidas, durante o período de 01/06/2022 a 31/07/2022.

2. Em atenção ao que se pede na letra a) do inciso II do item 25, do despacho CGOMOB (8575180), informamos as posições daquelas credenciais, nesta data, na tabela abaixo:

CREDENCIAL	STATUS	INCIDENTE CIBERNÉTICO	REATIVAÇÃO DA SENHA	VPN	ACESSO AO GERID RESTRITO AO USO DE CERTIFICADO DIGITAL (DESDE 25/08/22)
0156178	ATIVO	202207003942	29/07/2022	X	ok
0221549	ATIVO	202206003895	01/09/2022	X	ok
0252619	ATIVO	202207003937	29/07/2022	ATIVA (DE 22/03 A 20/09/22)	ok

0543634	ATIVO	X	03/08/2022 (troca de senha)	X	ok
0545456	ATIVO	202207003925	29/07/2022	X	ok
0752048	ATIVO	X	01/08/2022 (troca de senha)	X	ok
0755401	QUARENTENA	202207003952	28/07/2022	ATIVA (DE 23/03 A 21/09/22)	ok
0880572	ATIVO	X	01/08/2022 (troca de senha)	X	**NÃO**
0880592	ATIVO	202207003942	05/08/2022	X	ok
0880727	ATIVO	202207003913	04/08/2022	ATIVA (DE 24/03 A 22/09/22)	ok
0880930	ATIVO	X	06/08/2022 (troca de senha)	X	ok
0885165	ATIVO	202207003942	29/07/2022	X	ok
0890313	QUARENTENA	202207003942	28/07/2022	X	ok
0896448	ATIVO	202207003929	29/07/2022	X	ok
0898499	ATIVO	202207003923	11/08/2022	X	ok
0899391	ATIVO	202207003937	02/08/2022	ATIVA (DE 23/03 A 21/09/22)	ok
0899485	ATIVO	202207003913	04/08/2022	X	ok
0905824	ATIVO	X	29/07/2022 (troca de senha)	X	ok
0914231	ATIVO	X	10/08/2022 (troca de senha)	X	ok
0922294	ATIVO	202207003942	29/07/2022	X	ok
0923592	ATIVO	202207003925	03/08/2022	X	ok
0935153	ATIVO	202207003942	22/08/2022	ATIVA (DE 07/07 A 05/01/23)	ok
0938568	ATIVO	X	29/07/2022 (troca de senha)	ATIVA (DE 23/03 A 21/09/22)	ok
0939934	ATIVO	X	29/07/2022 (troca de senha)	X	ok
0940436	ATIVO	202206003905	01/09/2022	ATIVA (DE 25/03 A 23/09/22)	ok
1108223	ATIVO	202207003937	29/07/2022	X	ok
1250181	ATIVO	202207003925	09/08/2022	X	ok
1375576	ATIVO	202207003937	29/07/2022	X	ok
1376000	ATIVO	202207003942	03/08/2022	X	**NÃO**
1376234	ATIVO	X	05/08/2022 (troca de senha)	X	ok
1376869	ATIVO	X	29/07/2022 (troca de senha)	X	ok

1379883	ATIVO	X	29/07/2022 (troca de senha)	ATIVA (DE 23/03 A 21/09/22)	ok
1420719	ATIVO	X	29/07/2022 (troca de senha)	ATIVA (DE 18/03 A 16/09/22)	ok
1424970	ATIVO	202207003942	03/08/2022	ATIVA (DE 23/03 A 21/09/22)	ok
1444636	ATIVO	202207003952	02/09/2022	X	ok
1450846	ATIVO	202207003942	28/07/2022	X	ok
1492428	ATIVO	202207003952	04/08/2022	ATIVA (DE 22/03 A 20/09/22)	ok
1517109	ATIVO	202207003937	01/09/2022	ATIVA (DE 23/09 A 21/09/22)	ok
1534762	ATIVO	202207003913	29/07/2022	ATIVA (DE 24/03 A 22/09/22)	ok
1563349	ATIVO	202207003942	29/07/2022	ATIVA (DE 24/03 A 22/09/22)	ok
1564545	ATIVO	202207003942	29/07/2022	X	ok
1637392	ATIVO	202206003895	29/07/2022	X	ok
1782277	ATIVO	X	29/07/2022 (troca de senha)	X	ok
1786313	ATIVO	202207003938	09/08/2022	ATIVA (DE 24/03 A 22/09/22)	ok
1815946	ATIVO	X	26/07/2022 (troca de senha)	ATIVA (DE 24/03 A 22/09/22)	**NÃO**
1960829	ATIVO	X	29/07/2022 (troca de senha)	ATIVA (DE 18/03 A 16/09/22)	ok
2024845	ATIVO	202207003942	03/08/2022	ATIVA (DE 23/03 A 21/09/22)	ok
2040923	ATIVO	202206003895	29/07/2022	X	ok
2058151	ATIVO	202206003866	30/07/2022	ATIVA (DE 25/03 A 23/09/22)	ok
2210170	ATIVO	202207003916	01/09/2022	X	ok

2297793	ATIVO	202207003952	29/07/2022	X	ok
2409376	ATIVO	202206003854	29/07/2022	X	ok
2948077	ATIVO	202207003932	08/08/2022	X	ok
6880628	ATIVO	X	29/07/2022 (troca de senha)	X	ok

3. Ao mesmo tempo, em atenção ao que se pede na letra c) , esclarecemos que esta DTIR tem o seguinte levantamento, onde foram encontrados equipamentos desconhecidos ou, em algum momento, onde esses equipamentos foram plugados a nossa rede:

LOCALIDADE	IP	PORTA	DATA DA IDENTIFICAÇÃO	PROCESSO SEI
APS PENHA - SC	10.107.172.0	24	07/06/2022	35014.133819/2022-00
GEX GOIÂNIA - GO	10.74.0.0	22	14/06/2022	35014.242947/2022-35
	10.74.72.0	24		
APS COPACABANA - RJ	10.1.121.0	24	21/06/2022	NÃO HÁ
APS PERUÍBE - SP	10.19.200.0	24	28/06/2022	NÃO HÁ
APS CABO FRIO - RJ	10.1.112.0	24	01/07/2022	NÃO HÁ
APS TIMBÓ - SC	10.107.121.0	24	05/07/2022	35014.284634/2022-54
APS BELÉM ICOARACI - PA	10.88.102.0	24	12/07/2022	NÃO HÁ
APS CAMPO LARGO - PR	10.53.237.0	24	13/07/2022	35014.286582/2022-51
APS BERTIOGA - SP	10.19.170.0	24	15/07/2022	NÃO HÁ
APS TAMBORIL - CE	10.65.114.0	24	25/07/2022	NÃO HÁ
APS CAMOCIM - CE	10.65.134.0	24	04/08/2022	NÃO HÁ
APS NILÓPOLIS - RJ	10.1.154.0	24	NÃO HÁ	NÃO HÁ
APS ARICANDUVA - SP	10.16.101.0	24	NÃO HÁ	NÃO HÁ
APS ITAPEMA - SC	10.107.180.0	24	NÃO HÁ	NÃO HÁ
APS SÃO PAULO CENTRO	10.17.32.0	24	22/08/2022	NÃO HÁ
APS MAGÉ - RJ	10.1.115.0	24	22/08/2022	NÃO HÁ
APS MÉIER - RJ	10.1.105.0	24	30/08/2022	NÃO HÁ

4. Assim, após a análise criteriosa do que foi constatado com estas detecções, pudemos concluir que todos os ativos de rede devem ser autorizados antes de se conectar a nossa rede. Nessa análise e monitoramento, foram identificadas inúmeras portas abertas, em especial, a porta 3389, que é porta padrão de acesso remoto do Windows. Foram identificadas, até o momento, 3271 equipamentos com esta porta aberta, o que permite fácil acesso de invasores à rede interna do INSS. É por essa razão, que esta DTIR recomenda enfaticamente que toda a rede do INSS seja monitorada 24x7 (todos os dias da semana, por 24 horas), e que todas as entradas físicas e lógicas, de todos os ativos de rede, possam ser controladas, adotando assim algumas boas práticas que são aplicadas e recomendadas pelos órgãos de controle.

5. Em atenção às solicitações das letras b), d), e e), esta DTIR, no dia 06/09/2022,

encaminhou o Ofício SEI Nº 23/2022/DTIR/COIM/CGIS/DTI-INSS (8823612), constante nos autos deste processo, à Dataprev para colher informações a respeito, haja vista que trata-se de prerrogativa daquela empresa a governança sobre os referidos apontamentos.

FRANCISCO HUMBERTO MENDONÇA DE ARAUJO

Chefe da Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos

JOÃO HENRIQUE MOURÃO DE MARCO
Coordenador-Geral de Infraestrutura e Segurança em Tecnologia da Informação

Documento assinado eletronicamente por **FRANCISCO HUMBERTO MENDONCA DE ARAUJO**, **Chefe da Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos** , em 06/09/2022, às 16:01, 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 **JOAO HENRIQUE MOURAO DE MARCO**, **Coordenador(a) Geral de Infraestrutura e Operações**, em 06/09/2022, às 16:23, 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 **8823583** e o código CRC **211543E1**.

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

OFÍCIO SEI Nº 23/2022/DTIR/COIM/CGIS/DTI-INSS

Brasília, 06 de setembro de 2022.

Ao Senhor
VINÍCIUS BERNARDES BORGES
Coordenador-Geral do Gabinete da Presidência
Empresa de Tecnologia e Informações da Previdência - Dataprev

Assunto: Solicitação de informações para fins de investigação de reativações de benefício potencialmente indevidas.

Referência: Caso responda este Ofício, indicar expressamente o Processo nº 35014.349892/2022-93.

Senhor (a) Coordenador-Geral,

1. Trata-se de processo administrativo instaurado no âmbito da Coordenação de Ações Corretivas e Cobrança Administrativa de Benefícios, que decorre de achados de monitoramento em relação a reativações potencialmente indevidas, durante o período de 01/06/2022 a 31/07/2022, conforme referendado pelo Despacho Coordenação-Geral de Monitoramento e Cobrança Administrativa de Benefícios (SEI nº 8575180) anexo e suscitado pelo Despacho nº 314/2022/GMTP-MTP do Ministério do Trabalho e Previdência (SEI nº 8536675), após o pedido expresso no Ofício nº 146/2022/ASS/GAB/PF, também anexos.

2. Vimos, portanto, por meio do presente, para atendimento às solicitações da Coordenação-Geral de Monitoramento e Cobrança Administrativa de Benefícios, manifestas no despacho CGMOB supracitado, visando, em última instância, encaminhamentos que embasem a adoção de providências pela Polícia Federal, solicitar os bons préstimos dessa empresa de tecnologia para nos fornecer os dados a seguir durante o período de 01/06/2022 a 31/07/2022:

a) Informações sobre os acessos VPN, a forma que ocorrem e quais credenciais foram responsáveis pelos acessos que culminaram nas ações descritas no despacho CGMOB em questão; e

b) Informações sobre os dispositivos que foram encontrados conectados a rede do INSS e que podem ter servido de porta de acesso a rede por pessoas não autorizadas.

3. Além disso, solicitamos que:

a) Com respeito às credenciais identificadas e informadas no despacho CGMOB em questão, sejam tomadas providências de monitoramento no sentido de que as mesmas não sejam objeto de reutilização indevida repetidamente.

Atenciosamente,

JULLYANO LINO DA SILVA
Gestor de Segurança da Informação do INSS

JOÃO HENRIQUE MOURÃO DE MARCO
Coordenador-Geral de Infraestrutura e Segurança em Tecnologia da Informação

Anexos:	I - Despacho 314/2022/GMTP-MTP do Ministério do Trabalho e Previdência (SEI nº 8536675). II -Despacho da Coordenação de Ações Corretivas e Cobrança Administrativa de Benefícios (SEI nº 8631689).

Documento assinado eletronicamente por **JULLYANO LINO DA SILVA**, **Coordenador(a) Geral de Infraestrutura e Operações**, em 06/09/2022, às 15:59, 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 **JOAO HENRIQUE MOURAO DE MARCO**, **Coordenador(a) Geral de Infraestrutura e Operações**, em 06/09/2022, 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 **8823612** e o código CRC **4715EDF6**.

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Benefícios e Relacionamento com o Cidadão
Coordenação-Geral de Pagamento de Benefícios

DESPACHO

Coordenação-Geral de Pagamento de Benefícios, em 08/09/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS

1. Trata-se do DESPACHO Nº 314/2022/GMTP-MTP, oriundo do Ministério de Trabalho e Previdência cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, no qual a Polícia Federal comunica a ocorrência de prováveis fraudes massivas contra o INSS.

2. Ciente e de acordo com o Despacho DMAND (8802692).

3. Conforme o sugerido encaminha-se à DAGPG para atendimento do item 2.

ANDRESSA FARIAS

Assistente Administrativo-CGPAG

CARLOS HENRIQUE GONÇALVES

Substituto

Coordenação-Geral de Pagamento de Benefícios.

sei! assinatura eletrônica

Documento assinado eletronicamente por **CARLOS HENRIQUE GONCALVES**, **Coordenador(a) Geral Substituto(a)**, em 09/09/2022, 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 .

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Benefícios e Relacionamento com o Cidadão

DESPACHO

Diretoria de Benefícios e Relacionamento com o Cidadão, em 15/09/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se do DESPACHO Nº 314/2022/GMTP-MTP, oriundo do Ministério de Trabalho e Previdência cujo propósito é o encaminhamento ao INSS do OFÍCIO Nº 146/2022/ASS/GAB/PF, no qual a Polícia Federal comunica a ocorrência de prováveis fraudes massivas contra o INSS.

2. Ciente e de acordo com o Despacho DMAND (8802692), CGMOB (8575180) .

3. Encaminhe-se à Coordenação de Suporte ao Gabinete para resposta ao demandante.

EDSON AKIO YAMADA

Diretor de Benefícios e Relacionamento com o Cidadão

INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Gabinete

DESPACHO

Gabinete, em 20/09/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Ciente quanto às manifestações da Diretoria de Benefícios e Relacionamento com o Cidadão e da Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos da Diretoria de Tecnologia da Informação- DTI (8823583).

2. Encaminhe-se à DTI para acompanhamento dos autos após a emissão do Ofício SEI nº 23/2022/DTIR/COIM/CGIS/DTI-INSS (8823612) e manifestação conclusiva.

SIDNEI CICERO COTTET

Chefe de Gabinete da Presidência

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação

NOTA TÉCNICA Nº 9/2022/DTI-INSS
PROCESSO Nº 19955.102272/2022-14
INTERESSADOS: INSTITUTO NACIONAL DO SEGURO SOCIAL; MINISTÉRIO DO TRABALHO E PREVIDÊNCIA; POLÍCIA FEDERAL

Discorre acerca da implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS

1. Trata-se de Nota Técnica destinada a prestar contas das atividades desenvolvidas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS, em seguimento ao exposto na NOTA TÉCNICA Nº 1/2021/CGIN/DTI-INSS (4651370), de 13/09/2021, em decorrência, sobretudo, do recebimento do DESPACHO Nº 314/2022/GMTP-MTP, de 11/08/2022 (8536675), oriundo do Gabinete do Sr. Ministro de Estado do Trabalho e Previdência.

2. Referido Despacho carreia aos autos o OFÍCIO Nº 146/2022/ASS/GAB/PF, de 18/07/2022, expedido pelo Direção Geral da Polícia Federal (PF), dando conta da "ocorrência de prováveis fraudes massivas contra o INSS", consistindo na "reativação fraudulenta de benefícios, gerando pagamentos de retroativos" na casa de centenas de milhões de reais. Ainda segundo o expediente, "análises iniciais apontam para a massiva utilização de senhas de servidores do INSS nesses processos de reativação, **o que demanda providências urgentes em termos de segurança das credenciais dos servidores** e beneficiários e/ou bloqueio cautelar desse tipo de atividade".

HISTÓRICO

3. Em setembro de 2021, a então Coordenação-Geral de Infraestrutura e Operações (CGIN) da denominada Diretoria de Tecnologia da Informação e Inovação (DTI) emitiu NOTA TÉCNICA Nº 1/2021/CGIN/DTI-INSS (4651370), apresentando o contexto de incidentes cibernéticos enfrentados pela Autarquia, centrando em resumir a natureza desses eventos, assim como as medidas adotadas, pretendidas e os riscos à sua consecução.

4. Em apertada síntese, a Nota carrega, à luz do contexto da época **(setembro de 2021)**:

4.1. Histórico

> 3.1. Trata-se do registro e apuração de incidentes cibernéticos envolvendo a utilização indevida de credenciais de acesso a sistemas acarretando o comprometimento de ativos de rede no INSS e na Dataprev objetivando o acesso a sistemas corporativos e a mineração de dados.
>
> 3.2. As bases de dados do INSS, custodiadas pela Dataprev, são visadas para a prática de ilícitos em face da possibilidade de sua utilização na obtenção de vantagens financeiras, tais quais a concessão e manutenção de benefícios irregulares, a alteração do local de crédito de benefícios, a realização de empréstimos consignados em benefícios sem o consentimento dos titulares ou mesmo a captação clandestina de clientes em potencial para a oferta de produtos financeiros.
>
> 3.3. Do comportamento enfrentado desde 2019, o modus operandi mais reiteradamente identificado - com base na compreensão atual - consiste aparentemente no ingresso do(s) atacante(s) em ativos de rede (equipamentos servidores) do INSS - a partir da rede da AGU

(Infovia) e se valendo de permissões privilegiadas (senha de root) - onde instala/executa aplicações maliciosas com o objetivo de acessar e exportar dados de sistemas corporativos utilizando credenciais de acesso válidas e obtidas ilicitamente. Por vezes, o(s) atacante(s) se utiliza(m) de credenciais de gestores de acesso com a finalidade de multiplicar sua ação através da atribuição de papeis mais permissivos às credenciais utilizadas.

3.4. É certo, portanto, que o grande cerne da problemática abordada é o roubo/vazamento de credenciais de usuários. Nessa esteira, são rotineiras as campanhas de phishing (páginas fraudulentas que imitam a interface de páginas legítimas com a finalidade de capturar as credenciais digitadas pelas vítimas). Essas ameaças são frequentes e veiculadas por correio eletrônico ou mesmo por meio de impulsionamento das páginas falsas em sites de busca, como o Google.

3.5. Para o acesso à rede interna também são utilizadas nos ataques credenciais com acesso à VPN, sobretudo após o cerco aplicado em relação aos acessos oriundos do NAT (Network Address Translation) da AGU. Nesses casos, o atacante provavelmente, de posse da credencial roubada/vazada e se aproveitando de ser uma senha única, acessa(va) o e-mail do usuário (ExpressoBR, serviço de correio eletrônico também opensource provido pela Dataprev ao INSS até recentemente, cuja infraestrutura legada foi desativada em 24/08/2021). Dentro da caixa postal, buscava o e-mail contendo o certificado digital A1 para acesso à VPN (serviço também provido pela Dataprev). Em poder do certificado, o hacker instala a ferramenta em seu computador e acessa livremente a intranet do INSS, onde busca ativos em que possa atuar da forma exposta no item acima.

3.6. As aplicações principalmente visadas nos ataques são o ConsigWEB e, com largo destaque, o SAT.

3.7. Destarte, nota-se pelo menos a existência de duplo alvo: credenciais com acesso à VPN - para acesso à intranet do INSS, precipuamente quando inviável o acesso por meio da rede da AGU - e credenciais com perfis vinculados aos sistemas visados - para a obtenção dos dados propriamente. Nesse segundo caso, há a preferência por perfis de gestão de acesso aos papeis privilegiados.

3.8. Isso porque a possibilidade de que uma credencial de gestão de acesso conceda - horizontal e ilimitadamente - o mesmo grau de privilégio a tantas outras acarreta o alastramento exponencial do número credenciais comprometidas a partir de um único vazamento.

3.9. Os ativos comprometidos se dividem em equipamentos servidores instalados em Agências da Previdência Social ou em datacenters da Dataprev, podendo ser de propriedade do INSS (serviço de colocation) ou da própria Dataprev (serviço de hosting).

3.10. As notificações de incidentes quase que invariavelmente partem da Comissão de Tratamento e Resposta a Incidentes Cibernéticos da Dataprev (CTIR-DATAPREV), vez que a empresa é a provedora e gestora não só da rede corporativa de dados do INSS (indiretamente), mas do serviço de diretório/base de usuários (OpenLDAP - solução opensource), a solução de autenticação (CAS - também de código aberto) e o sistema de gerenciamento de credenciais (GERID), este último desenvolvido pela Dataprev. Daí porque praticamente todo mecanismo de prevenção, detecção e tratamento de incidentes cibernéticos depende de informações e ações concentradas na Dataprev.

4.2. Tratamento e Resposta

4.1. O INSS, por sua vez, conta tão somente com ferramenta opensource de monitoramento (Zabbix) baseada em rotinas configuradas pela Divisão de Operações da DTI e em fase de aperfeiçoamento pela equipe do SquadSEG, projeto da Secretaria de Governo Digital do Ministério da Economia (SGD). O software antimalware disponível no órgão encontra-se sem licença de atualização desde o ano de 2017, situação essa agravada pelo fato de que a maioria do parque tecnológico roda o sistema operacional Microsoft Windows 7, software descontinuado e sem suporte do fabricante desde 14/01/2020, o que faz com que o sistema deixe de receber atualizações e correções de segurança que, ainda que disponíveis, teriam dificuldade de implementação em face da limitação de banda de internet nas unidades.

4.2. Dada a ausência de solução de domínio e de ferramentas robustas de segurança e monitoramento, a implementação de atualizações, padronização de aplicativos instalados e de dispositivos conectados à rede fogem ao controle da DTI aumentando a vulnerabilidade, por exemplo, a sniffers (software ou dispositivo capaz de interceptar dados trafegados na rede).

4.3. A partir dos incidentes notificados pela CTIR-DATAPREV, a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do INSS (ETIR-INSS), tendo determinado o bloqueio preventivo de credenciais pela Dataprev, adota medidas básicas, tais quais a inspeção manual ou via script dos ativos, não havendo ferramenta "institucional" para varredura e detecção de códigos maliciosos. Para os incidentes envolvendo o comprometimento de credenciais de acesso, reportados com elevada frequência, a ETIR-INSS submete os titulares das contas a uma entrevista visando identificar elementos que auxiliem no entendimento da dinâmica dessas ocorrências. (...)

4.4. O fluxo em questão encontra-se em revisão pela ETIR visando conferir-lhe maior efetividade e celeridade.

4.5. Afora isso, os ativos eventualmente comprometidos são bloqueados ou desconectados fisicamente da rede como medida de neutralização. Em que pese a boa prática recomende a conservação dos ambientes para posterior análise forense, isso nem sempre é possível, sobretudo em servidores que hospedam aplicações - por vezes, críticas - do INSS. Nesse cenário, as máquinas são formatadas e voltam à operação com as mesmas aplicações após procedimento de sanitização. Esse método é suscetível a erros, por não envolver ferramenta automatizada de detecção de ameaças, contando unicamente com o conhecimento técnico das equipes.

4.6. Questionada acerca dos critérios para a caracterização de incidentes, a Dataprev, por meio do Ofício 4651756, informou o quanto segue: a) acesso de múltiplas credenciais pelo mesmo IP público; b) acesso de múltiplas credenciais pelo mesmo IP privado (VPN); c) acesso credencial de conexão diferente da credencial de acesso ao sistema (lP VPN x login no GERID); d) acesso de múltiplos endereços IP conectados com uma única credencial; e) trocas de senha sucessivas em um curto período (são alertadas 5 trocas de senhas sucessivas em intervalo inferior a 120 segundos); f) conexão VPN por ativo conhecidamente malicioso (ativos que se conectaram a VPN e que são reincidentes, já tendo tido envolvimento em algum outro Incidente de Segurança); e g) volumetria de acessos fora do padrão normal (não há critérios objetivos definidos; o SOC alerta sempre que identifica um gráfico de tráfego de dados que se destaca da curva histórica, e este critério é sempre avaliado em conjunto com outros indicativos).

4.7. Apesar dos procedimentos em questão, fato é que a rotina de bloqueio de usuários é nitidamente ineficaz, já que conforme mencionado no item 3.7, as credenciais de alguma forma seguem sendo roubadas/vazadas continuamente, o que merece efetivamente o esforço das equipes de investigação, assim como o tratamento da fragilidade estrutural de SIC e da TI como um todo no INSS.

4.8. Ilustrativamente, descreve-se abaixo incidentes de maior representatividade, seja pelo impacto ou pela relevância às apurações, permitindo até mesmo uma avaliação cronológica das ameaças e das providências adotadas.

4.9. Ainda em setembro de 2019, foram registrados incidentes de segurança (35014.030953/2019-46 e 35014.004216/2019-98) caracterizados pelo acesso indevido às aplicações SAT e ConsigWeb, a partir de ativo do INSS localizado na Dataprev (contrato de colocation), o qual abrigava aplicações da PFE-INSS, tendo origem no NAT da AGU. Ações e encaminhamentos com vistas à solução foram providenciadas, tais como: a) identificação e bloqueio de credenciais comprometidas; b) identificação do código malicioso na máquina comprometida; c) dada a ciência do ocorrido à DIRBEN, visto ser esta a diretoria gestora do Consigweb; d) desativação do equipamento comprometido após autorização da área gestora das aplicações hospedadas (PFE-INSS); e) bloqueio de acesso ao GERID fora do Brasil; f) bloqueio de acesso direto de ativos do proxy ao Sistema ConsigWEB; g) análise dos scripts encontrados.

4.10. Há registro de evento semelhante ocorrido em meados de novembro de 2020 (35014.313048/2020-62), quando foi constatado acesso indevido às aplicações SAT e SIBE, oriundo da rede da AGU, a partir de saltos utilizando ativos da Dataprev e do INSS, dentre os quais os que hospedam as aplicações 'CONSULTAR', ´SGPP', 'SISEDITAIS e 'PORTAL MOB'. Ações e encaminhamentos foram providenciados para o contorno do incidente:

> **a) desabilitação da interface de rede e interrupção dos serviços do Apache (Servidor de aplicação) e MySQL (Banco de dados) nos ativos que hospedam as aplicações 'CONSULTAR' e 'PORTAL MOB';**
>
> **b) dada a ciência à DIRBEN e à DTI da AGU;**
>
> **c) bloqueio de tráfego no ambiente de colocation entre as redes da AGU e do INSS;**
>
> **d) criação de whitelist (lista branca) dos destinos na rede do INSS necessários à AGU;**
>
> **e) bloqueio do tráfego que não constava na lista branca;**
>
> **f) análise e elaboração de relatório dos arquivos encontrados nos servidores da GEX/APS Pelotas/RS e da APS Cambé/PR;**
>
> **g) snapshot e restabelecimento das aplicações com implantação de protocolo https;**
>
> **h) solicitação de informações à Dataprev com a finalidade de comunicação à ANPD, a pedido da DIGOV;**
>
> **i) Comunicação às áreas: I - Diretoria de Governança, Integridade e Gerenciamento de Riscos do INSS; II - Diretoria de Atendimento do INSS; III - Diretoria de Benefícios do INSS; IV - Coordenação-Geral de Serviços de Tecnologia da Informação da Advocacia-Geral da União - AGU; V - Coordenação-Geral de**

Inteligência Previdenciária e Trabalhista - CGINT/SEPT/ME;

4.11. A comunicação pela ETIR às áreas gestoras dos sistemas se faz por imposição do artigo 6º na norma que a instituiu (grifamos): *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.*

4.12. Em que pese a fundada preocupação com a continuidade do negócio, essa restrição constituiu fragilidade ao processo de tratamento e resposta a incidentes, ante o potencial dano de determinados ataques, seja considerando risco às aplicações - sobretudo as mantidas pelo INSS - ou, mais preocupantemente, aos dados de benefícios e pessoais.

4.13. Em março/2021, a ETIR-INSS oficiou (OFÍCIO SEI Nº 5/2021/ETIR) as Diretorias de Governança, Integridade e Gerenciamento de Riscos, de Atendimento e de Benefícios do INSS e ainda a Coordenação-Geral de Serviços de Tecnologia da Informação da Advocacia-Geral da União - AGU e a Coordenação-Geral de Inteligência Previdenciária e Trabalhista - CGINT/SEPT/ME, acerca de novo incidente cibernético envolvendo acessos indevidos a servidores de aplicação localizados em unidades do Instituto, originados da rede da Advocacia Geral da União - AGU (Infovia) e muito possivelmente relacionados a vazamento de credenciais e/ou roubo de senhas. A ETIR-INSS sugeriu, para tratamento do incidente, a inativação preventiva de algumas aplicações, até a adoção, pelas áreas responsáveis, das medidas necessárias para correção das vulnerabilidades identificadas, sendo procedidas as seguintes ações:

a) implementação de processo de lista branca das aplicações da AGU que acessam o ambiente de rede do INSS;

b) início do processo de saneamento da base de usuários da AGU com acesso aos sistemas corporativos;

c) implementação de autenticação por meio de certificado SSL para os sistemas afetados;

d) alteração das senhas de administrador (root) dos servidores de aplicação locados nas unidades do Instituto.

4.14. Em reforço à gravidade da questão, no dia 23/07/2021, o Centro de Tratamento e Resposta a Incidentes CIbernéticos - CTIR Gov notificou a ocorrência de vazamento e exposição de dados titularizados por membro da Alta Gestão da Repúbllica. Na ocasião, por configurar possível violação à LGPD, a Autoridade Nacional de Proteção de Dados foi comunicada, bem como o titular dos dados vazados, nos termos exigidos pela legislação. O incidente encontra-se em tratamento, resguardado e dever de sigilo.

4.15. Naquele mesmo mês, de posse de informações extraídas dos sistemas de benefícios, a Coordenação-Geral de Conformidade e Combate a Fraudes do INSS passou a capitanear **"Força-Tarefa"** dedicada à detecção, tratamento e resposta desses ilícitos, em articulação com a Coordenação-Geral de Inteligência Previdenciária e Trabalhista (CGINT) do Ministério do Trabalho e Previdência (MTP) e envolvendo as Diretorias: de Benefício; de Atendimento; de Governança, Integridade e Gerenciamento de Riscos; e, naturalmente, de Tecnologia da Informação e Inovação, além da Dataprev e do Departamento de Polícia Federal.

4.16. Vislumbra-se aí um oportuno divisor de águas, inclusive do ponto de vista preventivo - pleito esse, objeto de reiterados apelos desta Coordenação-Geral - sobretudo quando a Lei Geral de Proteção de Dados Pessoais (LGPD) encontra-se em voga, haja visto que as sanções administrativas previstas passaram a vigorar em 1º de agosto último.

4.17. No bojo desse grupo de trabalho foram desencadeadas as ações emergenciais aduzidas a seguir:

a) Extrações de logs de acesso e transacionais do SAT, dentre outras;

b) Inativação de credenciais comprometidas;

c) Desconexão de ativos comprometidos;

d) Restrição de privilégios em determinados perfis de acesso;

e) Priorização da implantação do Duplo Fator de Autenticação nos sistemas SAT Central, GPA e GET.

4.3. Ações junto à Advocacia-Geral da União (AGU)

5.1. Denota-se que o acesso à rede do INSS utilizando como ponte a rede interna da AGU constitui o ponto de vulnerabilidade mais explorado desde os primeiros registros de incidentes dessa natureza, em 2019. Desde à época, esforços são envidados no sentido de implementar medidas de contenção.

5.2. Não obstante, o número de credenciais da AGU envolvidos em incidentes é proporcionalmente maior que o de credenciais do INSS, de modo que no período de janeiro a junho de 2021, representando cerca de 40% das credenciais bloqueadas pela CTIR-Dataprev, embora o total de credenciais da AGU represente algo em torno de 1/4 das contas deste Instituto. Essa "preferência" se dá provavelmente em virtude da existência de perfil destinado ao uso pela AGU no GERID (papel "JUDICIAL") com permissão para 10 mil consultas diárias, multiplicando por 50 o limite padrão de 200 consultas/dia.

5.3. Nessa toada, evidenciou-se: a) usuários da AGU com comportamento de robô com papeis diversos dos da AGU (DATAPREV_SUPORTE, DATAPREV_GERENCIAL, DATAPREV_CONSULTA); b) gestores de acesso não encontrados no Portal da Transparência; c) usuários do com perfil JUDICIAL não pertencentes à whitelist de usuários autorizados ao uso de robôs; d) estagiário da AGU desligado da AGU em 2018 com papel de gestor de acesso concedendo permissões em 2021 envolvidas em incidentes de segurança;

5.4. Em decorrência, foi estabelecido:

a) **allowlist para acesso à rede do INSS a partir da AGU restrita aos IPs das aplicações necessárias, além do bloqueio da rota de acesso ao SAT Central no ambiente intranet do INSS**;

b) **saneamento da base de usuários da AGU** no OpenLDAP, após a constatação de que 2.843 usuários cadastrados na árvore da AGU não constavam na base de pessoal da AGU nem eram servidores ativos do INSS lotados em unidades da PFE. A demanda foi levada a efeito pela Dataprev sob demanda da DTI, havendo o compromisso por parte dos envolvidos de que tal ação passe a ser repetida semanalmente, a exemplo do que ocorre no INSS;

c) **política de expiração de senhas a cada 90 dias**;

d) **regra no GERID para que usuários da árvore da AGU somente possam acessar as aplicações parceiras mediante a utilização de certificado digital**. Evolução encontra-se em fase de homologação, nos termos da MINUTA DE OFÍCIO SEI Nº 4793094/2021/CGIN/CGIN/DTI-INSS, sob avaliação do Gabinete da Presidência deste Instituto.

6. Ademais, com base em levantamentos efetuados pela Coordenação-Geral de Conformidade e Combate a Fraudes e pela Diretoria de Benefícios que consideraram o comportamento na aplicação e também a existência de credenciais de acesso incompatíveis ou com permissões além do estritamente necessário, a DTI demandou à Dataprev a **revogação de perfis e a reinicialização da senha de cerca de outros 1.360 usuários válidos da AGU**.

4.4. Ações junto à Dataprev

O elevado grau de interação entre o INSS e a Dataprev, sobretudo pelo domínio detido pela empresa em relação às informações e recursos relacionados à implementação de atividades de SIC, gera naturalmente demandas que, pela gravidade da temática, merecem tratamento prioritário. Abaixo histórico não exaustivo de demandas: (...)

4.4.1. Nesse particular, menciona-se a existência de aproximadamente três dezenas de demandas abertas à Dataprev, em fase de atendimento.

4.5. Medidas preventivas e estruturantes

8.1. Como exposto nos itens 3 e 4 supra, as ações reativas não apenas são insuficientes frente ao volume de incidentes de segurança como também não atacam a raiz do problema. Desse modo, no afã de fazer frente à situação posta e apesar das limitações enfrentadas, a DTI tem buscado fomentar a construção, a médio e longo prazo, de um ambiente de SIC compatível com a grandeza do INSS e da importância e sensibilidade dos dados tratados. Com esse propósito, destacam-se as ações a seguir:

8.2. Instituição da Política de Segurança da Informação (POSIN-INSS)

8.2.1. 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.

(...)

8.3. Instituição da Norma de Concessão de Acesso Lógico (NCAL-INSS)

8.3.1. 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.

(...)

8.4. Instituição da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR-INSS)

8.4.1. 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".

(...)

8.5. Norma de Uso da Internet

8.5.1. 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 (...)

(...)

8.6. Programa contínuo de conscientização em Segurança da Informação

8.6.1. Desde a aprovação do novo regramento, o Serviço de Segurança da Informação da DTI vem produzindo uma série de conteúdos, com diagramação e veiculação pela Assessoria de Comunicação Social, dando origem à campanha "Neo Posin", em alusão à novel Política de Segurança da Informação, visando alertar e conscientizar os usuários de TI do INSS acerca das boas práticas de SI, além de orientar quanto a aspectos normativos e os riscos trazidos pela sua inobservância.

8.6.2. O primeiro trabalho realizado foi o desenvolvimento e a publicação da "Cartilha do Usuário de TI no INSS", trazendo como plano de fundo a temática de SIC.

(...)

8.6.4. Além disso, sempre que identificadas campanhas de phishing ou outras ações maliciosas em massa, comunicados e alertas são divulgados a toda a corporação.

8.7. Squad Seg da Secretaria de Governo Digital (SGD)

8.8. 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) 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.**

8.9. Saneamento da base de usuários

8.9.1. Apesar da demanda de automação das rotinas de saneamento de usuários com acesso à rede e aos sistemas corporativos do INSS, até que estas se concretizem, a DTI, a DGPA e a Dataprev vêm as sustentando "manualmente", sendo que semanalmente são derrubadas as credenciais de usuários desligados, enquanto todos os dias são revogados todos os perfis de acesso concedidos indevidamente a estagiários.

8.9.2. Demandas que visam a automação dessas rotinas estão em desenvolvimento pela Dataprev desde 2019.

8.10. Duplo Fator de Autenticação (2FA) para acesso às aplicações parceiras ao GERID

8.10.1. A autenticação de dois fatores é um recurso que acrescenta uma camada adicional de segurança para o processo de login da conta, exigindo que o usuário forneça duas formas de autenticação.

(...)

8.10.3. Existem várias soluções disponíveis no mercado para viabilizar a autenticação em dois fatores, sendo que foi adotado pela Dataprev o "Google Authenticator", aplicativo gratuito que viabiliza a autenticação em dois fatores ao gerar "chaves de acesso" para serem usadas neste processo. A primeira etapa dessa autenticação é formada pelo identificador e senha da conta do GERID. Após este passo, o aplicativo "Google Authenticator" deve ser consultado para que se verifique o código numérico aleatório de 6 dígitos a ser preenchido no campo correspondente. Esta chave numérica se renova a cada 30 segundos. Estes códigos numéricos de segurança podem ser consultados sem conexão à interne.

(...)

8.10.4. A funcionalidade vem sendo implementada paulatinamente nas aplicações parceiras ao GERID, a saber: Seguro Defeso, ConsigWeb, GET Gestão (concluídos), SAT Central, GPA/GID (em andamento), GET e outras a critério da DTI e das áreas de negócio.

8.11. Solução de correio, comunicação, colaboração e produtividade

8.11.1. 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.

8.11.2. 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.

8.11.3. 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.

8.12. Mapeamento e gestão de "robôs" legítimos

8.12.1. Em meio ao projeto de implantação do Duplo Fator de Autenticação nas aplicações parceiras ao GERID, emergiu a problemática relacionada a rotinas automatizadas criadas pelas áreas de negócio e pela AGU com o fito de otimizar os processos de trabalho.

8.12.2. Rotinas automatizadas representam um risco na medida em que possibilitam a realização de acessos, consultas e extrações de forma volumétrica. Em regra, comportamentos dessa natureza, ao serem identificados, devem ser reprimidos. Ocorre, no entanto, a existência de rotinas tais que proporcionam significativo ganho de produtividade e, portanto, merecem tratamento diferenciado.

8.12.3. Por essa razão, promoveu-se consulta às diversas áreas do INSS - e também à AGU - acerca da utilização desse tipo de mecanismo, tendo então sido catalogados robôs legítimos em uso pela Diretoria de Benefícios (DIRBEN) e pela AGU. Com vistas à conciliar sua operacionalização com a implantação do 2FA, foi demandado que os respectivos desenvolvedores promovessem as devidas adequações nos códigos. De outro lado, para assegurar a garantia de que apenas robôs autorizados funcionassem legitimamente, foi estabelecida restrição de acesso em nível de usuário, a partir de relação fornecida pelas áreas interessadas.

8.12.4. Como meio de contenção, também foi providenciada a criação de subsistemas e perfis específicos no GERID para esse fim, evitando assim a utilização de parâmetros de risco nos sistemas corporativos, como o número elevado de consultas diárias permitidas. Reafirma-se a identificação de perfil AGU liberado para exatas 10 mil consultas diárias, equivalente a 50 credenciais "padrão" (200 consultas/dia). Noutra banda, apesar da preocupação inspirada pelo limite diário de consultas, o modus operandi observado nos ataques demonstra que mesmo o limite padrão de 200 consultas/dia não inviabiliza a ação do invasor, que compensa o retardo através da utilização de vasta quantidade de credenciais.

(...)

8.13. Melhorias no monitoramento

8.13.1. No ano de 2020, a equipe da Divisão de Operações da DTI recebeu capacitação na ferramenta opensource Zabbix, um dos únicos meios de atuação existentes na Casa para o monitoramento da rede, de ativos e de aplicações.

8.13.2. A iniciativa foi reforçada com a atuação do Squad Seg da SGD, cuja equipe cuidou de reconstruir o ambiente desde a infraestrutura, a configuração de novas triggers e criação de novos dashboards, em fase de implantação.

8.14. Alocação de empregados públicos da Dataprev cedidos ao INSS em ações de SIC

8.14.1. Também no ano de 2020, o INSS foi contemplado com a cessão de dezenas de empregados da Dataprev, os quais foram alocados descentralizadamente nas diversas áreas da DTI de acordo com suas aptidões e experiências.

8.14.2. A esse respeito merecem realce:

> **a) reforço da equipe do Serviço de Segurança da Informação e Comunicação (SSEG) e da ETIR-INSS;**

b) reforço da equipe de Demandas e Serviços em TIC (DIDEM), auxiliando nos processos de contratação relacionados à Segurança da Informação, como links de dados, certificados digitais, serviço de diretório, antimalware, dentre outros.

c) reforço da equipe da Divisão de Operações em TIC (DIOP), sendo possível a constituição de células dedicadas ao suporte aos servidores locais e à rede interna, viabilizando ações estratégicas como:

I - sanitização de contas de root em servidores,

II - configuração padronizada de switches;

III - inventário do parque;

IV - intervenções emergenciais nos casos de incidentes cibernéticos;

V - implantação de certificado SSL (Secure Sockets Layer) em aplicações;

VI - análise e migração de ambientes e aplicações legados/inseguros

(...)

8.16. Plano Diretor de Segurança da Informação (PDSI)

8.16.1. O Plano Diretor de Segurança da Informação - PDSI é definido como um instrumento de gestão confeccionado para balizar a execução das ações de segurança da informação na Organização, que possibilita justificar os recursos aplicados na área, minimizar os desperdícios, garantir o controle, aplicar esforços naquilo que é considerado mais relevante e, por fim, melhorar a eficácia da segurança da informação.

4.6. Recomendações e conclusão

12.1. Diante da gravidade dos fatos narrados e da urgência em prover estrutura mínima suficiente a fazer frente às ameaças descritas, em observância às obrigações contida no item 5 da Norma Complementar nº 05/IN01/DSIC/GSIPR e no Art. 2º, VII, da Portaria nº 1.246/PRES/INSS, de 18 de dezembro de 2020,

R E C O M E N D A - S E:

12.2. Atendimento prioritário das demandas de **contratação de serviços e de soluções de TIC**, devidamente previstas no Plano Diretor de Tecnologia da Informação (PDTI) e refletidas no Projeto de Transformação Tecnológica do INSS e do iminente Plano Diretor de Segurança da Informação, sendo as listadas abaixo consideradas emergenciais:

a) serviço de operação de infraestrutura e segurança em TIC, viabilizando assim a implantação de um SOC (Security Operations Center - Centro de Operações de Segurança) e de um NOC (Network Operations Center - Centro de Operação de Rede);

b) implementação de rede de dados gerida pelo INSS;

c) atualização do parque computacional, por meio da Ata de Registro de Preços vigente até 28/12/2021 (Pregão Eletrônico Nº 8/2020); d) solução antimalware; e

e) solução de domínio;

f) serviço de diretório.

12.3. Atendimento prioritário, pela Dataprev, das demandas de evolução do Sistema de Gerenciamento de Identidade e Acesso - GERID enumeradas no item 7.1, face tempo decorrido, criticidade e recomendações de órgãos de controle;

12.4. Disponibilização, pela Dataprev, à área de Segurança da Informação e afins, de módulo de consulta aos logs de acessos à internet, intranet, VPN e de acessos e transações em sistemas parceiros ao GERID;

12.5. Aprovação, pelo CEGOV, do Plano Diretor de Segurança da Informação (PDSI) tão logo submetido à sua apreciação;

12.6. Capacitação da equipe de Segurança da Informação do INSS, na forma das necessidades identificadas no Plano de Desenvolvimento de Pessoas e outros;

12.7. Rediscussão pelo CTGD, mediante provimento de estrutura compatível, do formato e da autonomia da ETIR-INSS;

12.8. Avaliação, pela Equipe de Gestão e Fiscalização dos contratos mantidos junto à Dataprev, dos eventuais impactos - financeiros e/ou em ANS - de transações realizadas indevidamente em decorrência de incidentes de segurança da informação;

12.9. Migração emergencial de qualquer aplicação do INSS hospedada em infraestrutura própria (colocation ou ambientes locais) para ambiente de nuvem;

12.10. Condicionamento do acesso a usuários externos de aplicações parceiras ao GERID à adoção das políticas de acesso praticadas no INSS;

4.7. Ciência às partes interessadas

> 13.1. Ante o exposto, encaminhe-se a presente Nota Técnica, para conhecimento e eventuais providências e determinações, ao/à:
>
> I - Gabinete da Presidência do INSS;
>
> II - Diretoria de Tecnologia da Informação e Inovação;
>
> III - Diretoria de Atendimento;
>
> IV - Diretoria de Benefícios;
>
> V - Diretoria de Gestão de Pessoas e Administração;
>
> VI - Diretoria de Governança, Integridade e Gerenciamento de Riscos;
>
> VII - Auditoria-Geral;
>
> VIII - Procuradoria-Federal Especializada;
>
> IX - Coordenação-Geral de Conformidade e Combate a Fraudes;
>
> X - Serviço de Segurança da Informação em Tecnologia da Informação e Comunicação;
>
> XI - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do INSS (ETIR-INSS);
>
> XII - Gabinete da Presidência da Dataprev;
>
> XIII - Coordenação-Geral de Inteligência Previdenciária e Trabalhista (CGINT) do Ministério do Trabalho e Previdência;
>
> XIV - Diretoria de Tecnologia da Informação da Advocacia-Geral da União;
>
> XV - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov.

IRREGULARIDADES EM BENEFÍCIOS

4.8. A integração entre as áreas envolvidas no combate - Tecnologia da Informação, Benefícios, Inteligência e Policial - é essencial ao enfrentamento eficaz do mal perpetrado, o que se evidencia na medida em que verificou-se relação entre os dispositivos clandestinos e as reativações indevidas de benefícios previdenciários.

5. Isso porque os ataques cibernéticos não representam um fim em si mesmos, mas apenas meio para sabotagem ou obtenção ilícita de informações ou vantagens, tal qual relatado em Despacho da Coordenação-Geral de Inteligência Previdenciária e Trabalhista do Ministério do Trabalho e Previdência, de 08 de agosto de 2022 (grifamos):

> 1. Trata o presente de notícia de supostas "fraudes massivas" em benefícios, encaminhada pela Direção Geral da Polícia Federal ao Ministro de Estado do Trabalho e Previdência, por meio do [RESERVADO].
> 2. O referido expediente relata que chegou ao conhecimento daquela Polícia Federal, por meio de análises de dados e via canal de inteligência, da ocorrência de prováveis fraudes massivas contra o INSS e que tais informes foram transmitidos, via canal de inteligência, à Coordenação-GeraI de Inteligência/MTP e às inteligências dos principais bancos afetados.
> 3. Segundo o relato, as fraudes consistiriam, em tese, na **reativação fraudulenta de benefícios**, gerando pagamento de retroativos próximo ao limite de cinco anos, o que perfaria um valor estimado médio em torno de R$70.000,00, por benefício fraudulentamente reativado.
> (...)
> 5. O Ofício complementa que análises iniciais apontam para a massiva utilização indevida de senhas de servidores do INSS nesses processos de reativação, o que demandaria, segundo preceitua, providências urgentes em termos de segurança das credenciais dos servidores e beneficiários e/ou bloqueio cautelar desse tipo de atividade.
> 6. Por fim, solicita ao MTP determinar prioridade e urgência nas análises por parte da CGINT a fim de que a Polícia Federal possa adotar providências na sua esfera de atribuições.
> 7. Contextualizada a situação trazida pela PF, cumpre informar que, desde 2019, esta CGINT tem monitorado diferentes tipologias de fraude envolvendo o comprometimento de credenciais de servidores, tendo sido elaborados diversos Relatórios de Informação atinentes ao assunto, todos já devidamente encaminhados à Polícia Federal para subsidiar investigações dos casos identificados, bem como ao INSS, para subsidiar o bloqueio cautelar e reanálise dos processos.
>
> (...)

10. Em face do exposto no item 6, acima, informe-se, por oportuno, que, no campo investigativo, assim que recebidas as listagens mencionadas no item 8, esta Coordenação-Geral designou equipe para trabalhar as devidas análises de inteligência, o que foi formalizado por meio da PORTARIA CGINT/SE/MTP Nº 1957, DE 12 DE JULHO DE 2022 (26338143), publicada no Boletim de Serviço Eletrônico de 13/07/2022 (Processo SEI 10135.100897/2022-12). Ato contínuo, o titular da DPREV/CGFAZ/DICOR/PF foi informado sobre a priorização dada, por esta Coordenação-Geral, ao início das análises de inteligência.
11. Acrescenta-se ao exposto, que esta Coordenação-Geral vem envidando esforços no sentido de **monitorar essas tipologias de fraudes em parceria com as áreas técnicas do INSS, nos âmbitos da Diretoria de Benefícios e Relacionamento com o Cidadão (Dirben), da Diretoria de Tecnologia da Informação (DTI) e da Diretoria de Governança, Planejamento e Inovação (DIGOV)**. Esse trabalho conjunto visa buscar a identificação proativa de novos casos de fraudes, possibilitando uma resposta mais célere a tais ameaças.
12. Nesse sentido, foi desenvolvido pela CGINT, em parceria com o INSS, **painel específico denominado "Argus - Power BI"**, buscando fornecer indicadores que subsidiem e possibilitem uma atuação mais célere do INSS na prevenção, detecção e neutralização de incidentes de fraudes relacionados à tipologia de fraude relacionada à listagem de benefícios encaminhada pela Polícia Federal

(...)

14. No que diz respeito às "providências urgentes em termos de segurança das credenciais dos servidores e beneficiários e/ou bloqueio cautelar desse tipo de atividade" prescritas pela PF, conforme item 5, entendemos que o teor do Ofício [RESERVADO] deveria ser levado ao conhecimento da Presidência do INSS, para subsidiar as eventuais providências de competência daquela Autarquia.

6. Acionada, a Coordenação de Ações Corretivas e Cobrança Administrativa de Benefícios, vinculada à Coordenação-Geral de Monitoramento e Cobrança Administrativa de Benefícios da DIRBEN atuou conforme abaixo (8631689) (grifos nossos):

(...)

3. A fraude aqui tratada está relaciona a reativações processadas de forma indevida, sem observância dos procedimentos normativos adequados para a situação e tem como uma das características a **utilização de credenciais de servidores, processamento via SIBE-PU e volume massivo de reativações processados de benefícios de todo o país**.

4. Há questões relevantes e que foram detalhadas no relatório e que dizem respeito a regras de negócio, **regras de segurança de rede e de acesso e que precisam de especial atenção pelas áreas responsáveis dentro do INSS e DATAPREV**. Questões essas que extrapolam a área de atuação da CGMOB mas que tem impacto direto nas fraudes consumadas.

(...)

6. Assim como em trabalhos anteriores empreendidos pela Coordenação de Ações Corretivas e Cobrança Administrativa de Benefícios, o trabalho envolvendo o cenário das reativações se vale de algumas premissas que permitiram a identificação das fraudes e portanto conferem assertividade aos achados, elenco de forma exemplificativa algumas dessas premissas:

a) Volumetria de reativações concentradas em credenciais;

b) Comportamento anômalo da credencial em relação a região geográfica e atividades diárias;

c) Inexistência de instrução formal que justifique o procedimento;

d) Variação do volume de reativação como um todo;

e) Tempo decorrido entre a cessação e a reativação;

(...)

9. A análise seguiu algumas etapas que podemos resumir da seguinte forma:

a) Definição do objeto: O fenômeno definido para estudo no presente trabalho foram as reativações processadas, por servidor, nas competências de junho e julho que, em um primeiro momento não apresentavam tarefas de reativação de benefícios;

b) Objetivo: Identificar a extensão da fraude nestas competências a partir do conhecimento prévio do modus operandi e consequentemente permitir a adoção das medidas de correção;

c) Análise descritiva: O trabalho se baseou em: - variáveis qualitativas como IP de onde partiram as operações, credenciais que realizaram as operações, localização geográfica das operações e credenciais e instrução formal do pedido; - variáveis quantitativas como quantidade de NBs reativados, valores de créditos emitidos e valores de renda mensal;

d) Depuração dos dados: A partir de um levantamento preliminar dos dados de reativação ocorridos nessas competências foi realizado batimento com as informações de tarefas, ocasião em que identificamos a existência de outros serviços - diferentes de reativação - que poderiam justificar a reativação, sendo eles: serviços associados a qualificação da folha; serviços de renovação da declaração de cárcere; reativações após a realização do CADúnico de benefícios assistenciais; cadastramento de representante legal e solicitação de pagamento não recebido. Além disso avaliadas as situações processadas por decisão judicial que fugiam ao escopo de fraude.?

e) Análise estatística: A partir dos dados depurados procedemos a consolidação das informações em alguns cenários que serão melhor detalhados, mas resumidamente foram analisados volumetria por IP e credencial, volumetria por UF, ramificação credencial x IP, ramificação UF credencial x UF NB, ramificação UF credencial x UF IP.

10. A partir das premissas do trabalho foi possível segmentar com alto grau de assertividade um total de 22.327 benefícios que respondem a alguns cenários definidos como de risco combinados ou não entre eles:

a) Inexistência de instrução processual que justifique a ação;

b) Operação realizada em local não compatível com a lotação do servidor;

c) Operação realizada em OL do sistema diverso da OL de manutenção do benefício (Superintendências diferentes);

d) Operações realizadas em locais diversos pelas mesmas credenciais;

e) Múltiplas credenciais operando do mesmo IP interno;

f) Locais que abrigam volume de operações não compatíveis com as atividades ordinárias;

g) Volumetria de operações da credencial incompatível com atividade ordinária de servidor.

(...)

ENCAMINHAMENTOS E MEDIDAS CORRETIVAS

15. A partir dos elementos verificados, a Coordenação de Ações Corretivas e Cobrança Administrativa de Benefícios, foi aberta DEMANDA junto à Dataprev sob número DM 100880, para que seja efetivada a **cessação** dos benefícios referidos no presente processo, retornando para a data de cessação que constava antes da reativação irregular, bem como o bloqueio de todos os créditos ainda em condições de serem bloqueados. Esta ação foi aberta a partir da planilha que consta no documentos SEI e conta com 22.977 benefícios, incluídos nesse quantitativo os cenários analisados sendo retirados 164 casos de benefícios por incapacidade já cessados.

16. Vale o registro de que há benefícios que podem já estar cessados em razão de ações das Superintendências Regionais ou Ações da própria CGMOB, dessa forma, os benefícios que já estiverem cessados deverão permanecer dessa forma. 17. Por fim, entendemos pela necessidade, de encaminhamento do presente a outras áreas do INSS para ciência e providências que lhe forem pertinentes, conforme:

I - Coordenação Geral de Pagamentos de Benefícios:

a) No que se refere, às regras de negócio, envolvendo os procedimentos de reativação e emissão de pagamentos associados, considerando os apontamentos aqui feitos, sugere-se a implementação de novas regras mais capazes de estabelecerem tratamento diferenciado para benefícios cessados há mais de um ano ou que tenham situações específicas de cessação, combinando com outros elementos que foram objeto da análise do presente relatório. No que diz respeito ao uso de credenciais cujas atividades inerentes às atividades do servidor, não permite correlação, com a tarefa de reativar benefícios, sugere-se a implementação de condições que impossibilitem esta atribuição sem crítica no Sistema, melhor seria o Sistema não aceitar tal atribuição a servidores que pela própria natureza da sua atividade dentro da Instituição não executa "tarefas de manutenção de benefícios".

b) Há ainda questões envolvendo as regras de autorização automática dos pagamentos que podem ser submetidas a trilhas que permitem visualizar os cenários de maior risco, considerando como ponto de partida os apontamentos do presente relatório.

c) Considerando o volume representativo que a espécie auxílio-reclusão representou em reativações indevidas, sugere-se, também a verificação de mecanismos que estabeleçam tratamento mais rigoroso quando se tratar de reativações ocorridas a partir de um determinado tempo da interrupção dos pagamentos.

d) Em razão da predominância dos benefícios assistenciais no cenário de fraudes, sugere-se a avaliação dos motivos que ensejam a cessação do BPC para um melhor controle das ações levando em conta esses motivos.

e) Apesar de um volume pequeno no cenário avaliado, chamou a atenção, as reativações intentadas em benefícios por incapacidade que obtiveram êxito em reativar e manter o benefício nessa condição. Por essa razão, entendemos que há a necessidade de avaliar a implementação de regras que restrinjam esse tipo de reativação, lembrando que a base de cessados conta com cerca de 52 milhões de benefícios das espécies 31 e 91, o que pode traduzir grande potencial de prejuízo, se empreendidas ações ilícitas voltadas também para estas espécies.

f) Reforçando a sugestão já contida na letra "a", outra necessidade verificada por esta CACB é a de avaliar a possibilidade de restringir concessão de perfil de atualização no SIBE-PU para servidores que ocupam cargos que não lhes conferem competência para atuar na manutenção de benefícios - ou mais especificamente na reativação, a exemplo de perito médico e assistente sociais.

g) Sugere-se também que seja juntado ao presente processo, pela CGPAG, Relatório emitido sobre os pagamentos emitidos para os benefícios envolvidos (incluindo situação do crédito, instituição destinatária, município do local de pagamento, modalidade de pagamento).

h) Por fim, sugere-se diante de todo o cenário apresentado, que se defina uma tratativa junto às instituições financeiras envolvidas, com o intuito de retornar os valores eventualmente ainda bloqueados.

II - **Diretoria de Tecnologia da Informação**, considerando a importância de informações mais específicas e que sejam capazes de melhor esclarecerem as apurações e investigações necessita-se junto a esta Diretoria:

a) Complementar o presente processo com informações de incidentes sobre as credenciais referidas no presente relatório;

b) Relatório de acessos e VPNs das credenciais envolvidas no período de 01/06/2022 a 31/07/2022, inclusive se há multiplicidade de VPNs pra uma mesma credencial ou cruzamento de credencial VPN x Credencial GERID, isto é, se houve acesso ao VPN por uma credencial e ao GERID por outra credencial;

c) Informações sobre as operações realizadas em IPs diversos e associados a rede interna do INSS, bem como a associação dessas operações a eventual localização de dispositivos desconhecidos conectados à rede do INSS a exemplo dos que foram encontrados em [RESERVADO];

d) Informações sobre as operações que foram feitas a partir de IP das redes iniciadas por [RESERVADO];

e) Outras informações técnicas que a Diretoria julgar pertinente para a elucidação das questões afetas as irregularidades praticada;

f) Com respeito às credenciais identificadas e informadas no presente processo, sugerimos providências da DTI no sentido de que as mesmas não sejam objeto de reincidência de monitorar estas matrículas impedindo a utilização indevida das mesmas repetidamente.

III - Diretoria de Integridade e Governança para ciência e manifestações que julgarem necessárias.

18. Feitas as considerações, encaminhe-se ao Diretor de Benefícios para ciência das medidas adotadas bem como manifestações que julgar pertinentes, com sugestão de encaminhamento, urgente, às áreas mencionadas no item 17.

7. Considerando a gestão da rede de dados do INSS ser ainda predominantemente da Dataprev, esta DTI cuidou-se de solicitar elementos àquela empresa por meio do OFÍCIO SEI Nº 23/2022/DTIR/COIM/CGIS/DTI-INSS, de 06 de setembro de 2022, sem prejuízo das demais medidas a seu cargo, como já mencionado na presente Nota.

8. Em outro caso sob apuração da PF (2020.0059047-SR/PF/PA), asseverou a autoridade policial:

Diante da gravidade dos fatos acima expostos, solicito medidas urgentes e eficazes de segurança aos sistemas supracitados e de proteção das senhas de acesso dos servidores do INSS, de forma a se evitar novas invasões aos sistemas do INSS, captura de centenas de senhas de acesso de servidores do INSS, e milhares de liberações fraudulentas de benefícios.

Na oportunidade, solicito ainda o levantamento das ações efetuadas (reativações, transferências de contas, liberações de funções de empréstimos, etc) com o uso indevido das senhas de acesso relacionadas aos logins dos servidores constante na planilha e anexo, a fim de serem identificados os valores dos respectivos benefícios previdenciários recebidos indevidamente pelo grupo criminoso, e consequente cancelamento dos benefícios reativados/gerados com fraude.

9. A despeito da inovação delitiva, nota-se que o grande ponto de vulnerabilidade segue sendo o vazamento de credenciais.

DISPOSITIVOS DE REDE CLANDESTINOS

10. A despeito e até mesmo em consequência das medidas mitigadoras apresentadas ao longo desta Nota Técnica, o *modus operandi* dos cibercriminosos, como comumente ocorre, vem sofrendo alterações perceptíveis.

11. Nessa esteira, a DTIR passou a receber relatos de gestores de unidades do INSS de várias Unidades da Federação dando conta da identificação de dispositivos de rede encontrados furtivamente instalados nas dependências dos imóveis, em locais como partes inferiores de móveis ou na própria sala do rack.

11.1. Via de regra, os equipamentos consistem em *access points* acoplados a um *modem* roteador 4G e conectados à rede interna e/ou a uma estação de trabalho. Tais incidentes são frequentemente associados a arrombamentos, furtos ou acesso de terceiros, sob investigação.

11.2. Como resposta, o INSS expediu dois Ofícios-Circulares estabelecendo procedimentos obrigatórios de prevenção e tratamento, a saber:

11.2.1. **OFÍCIO SEI CONJUNTO CIRCULAR Nº 2/2022/DTI/DIROFL/INSS**, de 04 de julho de 2022 (8018446), trazendo orientações e procedimentos em casos de incidentes envolvendo a identificação de equipamentos eletrônicos de origem desconhecida nas unidades do INSS;

11.2.2. **OFÍCIO SEI CONJUNTO CIRCULAR Nº 3/2022/DTI/DIRBEN/DIROFL/INSS**, de 29 de julho de 2022 (8339418), o qual estabelece Fluxo de Manutenção Programada e Manutenção Emergencial de Prestadores de Serviços de Infraestrutura e Telecomunicações nas Unidades do INSS.

11.3. Consequentemente, as unidades iniciaram **varreduras físicas**, tendo sido encontrados outros equipamentos semelhantes.

11.4. Em paralelo, no âmbito das ações técnicas **proativas**, a DTI logrou rastrear outros equipamentos do tipo realizando **monitoramento** e se valendo de **scanners de rede.**

11.5. O rol de dispositivos até agora identificados consta do Despacho DTIR 8823583 - sigiloso - tendo sido devidamente comunicados por meio de correio eletrônico à CGINT/MTP e emitido OFÍCIO SEI Nº 23(24)/2022/DTIR/COIM/CGIS/DTI-INSS (8823612), que solicita à Dataprev informações adicionais.

OPERAÇÃO TARRAFA

12. É valido também trazer à baila os achados e esclarecimentos no que tange à intitulada "Operação Tarrafa" da PF, deflagrada em 17/03/2022, tendo como objeto fraudes na concessão do benefício Seguro Defeso Pescador Artesanal, na qual foram encontrados, em poder dos investigados, arquivos contendo credenciais de acesso aos sistemas do INSS de numerosos servidores do INSS.

13. Na ocasião, informou a PF consignou na INFORMAÇÃO POLICIAL Nº 45/2022, "grave comprometimento do controle de acesso aos sistemas informatizados do INSS, permitindo execução de fraudes em larga escala, como constatado na Operação Tarrafa, causando perdas de milhões de reais em recursos públicos".

14. O INSS, no que tange a tal situação, produziu a NOTA TÉCNICA Nº 15/2022/CGGOV/DIGOV-INSS, aqui transcrita parcialmente:

> III. AÇÕES CONJUNTAS
>
> (...)
>
> 9. A fim de dar efetividade nas ações, se faz oportuno citar que outras medidas de segurança já estão sendo adotadas pela DTI a fim de fortalecer a segurança dos acessos dos servidores, das quais podemos destacar a implementação do duplo fato de autenticação e distribuição de certificado digital A3 (35014.029274/2021-49) para todos servidores desta Autarquia. De forma efetiva para este caso, as senha de todos os usuários será reiniciada.
>
> 10. Além das providências e encaminhamentos já enumerados, a DTI segue buscando a promoção de ações de TIC para prevenir e mitigar ataques e danos causados por incidentes de segurança, dentre as quais destacam-se:
>
> a) Hardening (endurecimento) - técnica usada para mapear ameaças e depois executar possíveis

correções nos sistemas, preparando-os para determinadas tentativas de ataques ou violação na segurança da informação;

b) Avaliação contínua dos incidentes objetivando melhor compreensão do(s) modus operandi e a definição de estratégias de defesa;

c) Contratações da rede corporativa de dados (35014.028319/2019-43);

d) Atualização do parque computacional (35014.075314/2020-43);

e) Serviços técnicos especializados de operação de infraestrutura e segurança em tecnologia da informação e comunicação (35014.339174/2020-47);

f) Solução para Gerenciamento e Controle de Acesso a Recursos de TIC (35014.048551/2021-12);

g) Solução de Proteção para Endpoint (EPS) contra malware e ameaças afins (35014.048537/2021-19);

h) Construção do Plano Diretor de Segurança da Informação (PDSI) para todo o Instituto;

i) Implementação, com apoio da Procuradoria Federal Especializada junto ao INSS, de processo de cooperação, engajamento, comprometimento e parceria com as áreas da Advocacia-Geral da União, notadamente as ligadas à Tecnologia da Informação e ao Controle de Acessos;

j) Consultoria pela Gartner do Brasil à gestão e as equipes de segurança da DTI em relação às melhores práticas a serem adotadas para o aperfeiçoamento do fluxo de tratamento de incidentes de segurança;

k) Migração das aplicações sustentadas pelo INSS para o ambiente de nuvem da Amazon, provedor de serviços contratado;

l) Revisão do conteúdo, configuração e permissões de acesso dos equipamentos servidores presentes em todas as unidades do INSS;

m)Saneamento da base de usuários com acesso à VPN;

n) Revisão dos perfis de acesso aos sistemas corporativos;

o) Migração de usuários de órgãos externos ao INSS a árvores próprias;

p) Fluxo diário centralizado de credenciamento e inativação de usuários;

q) Rotina de execução de listas de bloqueio;

r) Ferramenta de registro de incidentes;

s) Integração de bases cadastrais para cruzamento de dados de usuários com acesso à rede e sistemas corporativos;

t) Aperfeiçoamento de mecanismos de monitoramento de rede e aplicações;

u) Ampliação do uso de certificados digitais A3, iniciando para todos os gestores de acesso;

v) Implementação de protocolo seguro (https) nas aplicações que requerem usuário/senha;

w) Atualização de procedimentos de trabalho no Instituto com ações de melhorias da segurança da informação;

x) Uma série de outras medidas carecem de estudo mais aprofundado e, deveras, ensejam reforço na estrutura atual da área de Segurança da Informação, como as indicadas a seguir:

y) Bloqueio da comunicação via intranet entre ativos de unidades do INSS, exceto nos casos em que faça estritamente necessário;

z) Avaliação da necessidade e/ou busca de alternativas à alocação de equipamentos servidores locais nas unidades;

aa) Padronização do desenvolvimento de software e sustentação no âmbito do INSS e integração com as áreas de infraestrutura e operações com olhar para a Segurança da Informação;

ab) Definição de política de acesso à VPN, criando perfis de acesso à rede, limitando acesso a sistemas mais críticos, etc.

ac) Restrição do acesso a rede mediante autenticação (Protocolo 802.1x);

ad) Descontinuação prioritária de todos os ambientes mantidos em colocation ou nas dependências do INSS e que hospedem sistemas corporativos;

PLANO DIRETOR DE SEGURANÇA DA INFORMAÇÃO - PDSI

15. Passa-se a expor o núcleo duro no que tange às ações adotadas desde então a fim de satisfazer minimamente o cenário descrito, progredindo com as iniciativas em andamento e desencadeando

os projetos recomendados por esta área técnica, contando com o apoio da Alta Gestão do Instituto e do Ministério do Trabalho e Previdência.

16. O PDSI (7582721), cujo planejamento findou-se em 31/08/2021, foi apresentado e aprovado no Comitê Temático de Governança Digital (CTGD) em reunião extraordinária realizada em 19/11/2021 (5597640) e pelo Comitê Estratégico de Governança (CEGOV) em 24/03/2022 (6880618).

17. O Plano é definido como um instrumento de gestão confeccionado para balizar a execução das ações de segurança da informação (SI) na Organização, que possibilita justificar os recursos aplicados em Segurança da Informação (SI), minimizar os desperdícios, garantir o controle, aplicar esforços naquilo que é considerado mais relevante e, por fim, melhorar a eficácia da segurança da informação. Esse plano diretor descreve, em relação a segurança da informação, onde a organização está, aonde precisa chegar, visando promover adequada infraestrutura, suporte logístico, recursos tecnológicos, humanos e financeiros para segurança da informação. Busca definir objetivos de curto e médio prazo com o foco específico em SI e sua elaboração envolveu o gestor da segurança da informação e uma equipe interdisciplinar, em um processo de planejamento participativo.

18. A metodologia utilizada na elaboração do Plano Diretor de Segurança da Informação considerou os normativos publicados pelo GSI/PR, combinado com o diagnóstico da situação atual de Segurança da Informação no INSS, com a elaboração da Matriz SWOT, a análise dos riscos identificados, a Política de Segurança da Informação (POSIN) e o alinhamento com os objetivos estratégicos da instituição.

19. Também foram alvos de análise os documentos internos fornecidos pelo INSS, além dos dados consolidados em produtos de etapas anteriores ao projeto: o Planejamento Estratégico do INSS e o Plano Diretor de Tecnologia da Informação 2020-2022 do Instituto do Seguro Social.

20. As necessidades identificadas foram apontadas em projetos especificados no PDSI que foram divididos em dois grupos de acordo com a sua abrangência:

I - Corporativos - abrangem toda a organização e foram definidos conforme as melhores práticas descritas nas normas do GSI/PR;

II - Específicos para a TI - abrangem de forma individual os controles associados as ações que envolvam TI no INSS. Cada prática não atendida plenamente gerou projetos destinados a corrigir as não conformidades.

21. Fundamentado no modelo de administração PDCA, que define uma estrutura de gestão cíclica focada na melhoria contínua de processos, maior qualidade na execução e aumento do nível de segurança do ambiente, os projetos também foram categorizados de acordo com o resultado gerado após sua implementação, a saber:

I - Estruturação – tem por objetivo a definição de modelos e metodologias de gestão, o tratamento de incidentes e a definição de índices e indicadores de segurança;

II - Normatização – tem por objetivo a definição de diretrizes, normas, procedimentos e instruções de trabalho;

III - Diagnóstico – tem por objetivo o levantamento de problemas, falhas ou vulnerabilidades existentes nos ativos pertencentes ao escopo do projeto;

IV - Capacitação e conscientização – tem por objetivo a capacitação e a conscientização dos gestores, técnicos e usuários;

V - Manutenção e aprimoramento – tem por objetivo a revisão dos controles implementados (sejam lógicos, físicos e ou de processos), por meio de processos de análise de riscos, auditoria de conformidade e análise crítica.

22. Em seu bojo, rol de ações concretas visando o atendimento das necessidades básica de Segurança da Informação no órgão identificadas a partir de metodologia aplicada pela Coordenação de Governança e Planejamento de Tecnologia da Informação (COGPL) da DTI, a saber:

I - Estímulo à priorização perene das ações de Segurança de TIC do INSS;

II - Provimento de infraestrutura de Segurança de TIC;

III - Consolidar serviço de monitoramento de Segurança de TIC;

IV - Provimento de estrutura para a detecção, tratamento e resposta a incidentes de Segurança de TIC;

V - Consolidação da atuação preventiva em Segurança de TIC

23. De tais necessidades, emergiu a priorização das Ações de Segurança (AS) abaixo, cujo andamento atual também reportar-se-á nos tópicos a seguir.

23.1. **AS1 - Implantar sistema de registro de incidentes de segurança**

23.1.1. Com a implantação, pretendeu-se automatizar as fases do ciclo de gestão de incidentes cibernéticos do INSS, alinhando-se às boas práticas de CSIRT (Computer Security Incident Response Team) mundiais.

23.1.2. *Status:* Implementado. Sistema disponível desde 08/09/2022.

23.2. **AS2 - Construir *dashboard* de segurança de TI**

23.2.1. A disponibilização de painéis que apresentam informações táticas e indicadores acerca dos incidentes de segurança de tecnologia da informação, ocorridos no âmbito da Autarquia, apresenta-se seguramente como apoio substancial para a gestão na tomada de decisão. Tal painel servirá de subsídio para que a Alta Gestão, por meio do Comitê Estratégico de Governança, permaneça informada do diagnóstico da área.

23.2.2. *Status*: Em andamento. Painel desenvolvido e em fase de homologação.

23.3. **AS3 - Apresentar diagnóstico de Segurança de TI nas reuniões de CTGD e do CEGOV**

23.3.1. No intuito de manter o *board* atualizado acerca de temática tão sensível e assegurar sua priorização ao longo do tempo e independentemente das pessoas envolvidas se propôs item fixo da pauta do Comitê Temático de Governança Digital - CTGD e do Comitê Estratégico de Governança - CEGOV. Tal reporte pode se valer do painel referido no item anterior.

23.3.2. *Status:* Implementado, de modo que em todas as reuniões ordinárias de ambos os colegiados a temática segurança é de alguma forma abordada.

23.4. **AS4 - Implantar serviço de operação de infraestrutura e segurança em TI**

23.4.1. Consiste no planejamento de contratação (35014.339174/2020-47) para fornecimento de serviços técnicos especializados de operação de infraestrutura e segurança em tecnologia da informação e comunicação, compreendendo a implantação, manutenção, melhorias e execução continua de serviços relacionados à monitoração e à sustentação de infraestrutura de TIC, implicando em aumento do nível de controle em relação à segurança e confidencialidade das informações e dados armazenados pelos sistemas corporativos do INSS.

23.4.2. *Status:* Contratação despriorizada para otimização do uso da força de trabalho da equipe de planejamento da contratação em virtude da elevada estimativa de custos frente à insuficiência orçamentária e limitação de pessoal.

23.5. **AS5 - Assumir a gestão das políticas de segurança de TI na rede de dados do INSS**

23.5.1. Com o propósito de entregar solução corporativa de rede de dados de longa distância - WAN, para acesso à Internet e interligação das unidades do INSS localizadas em todo território nacional, contemplando serviços de gerenciamento, monitoração e de segurança da rede corporativa de dados, foi firmado contrato entre o INSS e a empresa Telebrás em maio/2022 (35014.028319/2019-43). Com o feito, a Autarquia assume a implementação e a gestão das políticas relativas à rede de dados, inclusive de segurança, serviço que esteve, até então, a cargo da Dataprev.

23.5.2. A Telebrás deverá prover os serviços de segurança da informação com o intuito de municiar o INSS de uma estrutura que centraliza a prestação de serviços de prevenção, detecção, reação e tratamento de incidentes de segurança relativos a serviços e infraestrutura de TI, bem como a gestão proativa para detectar e tratar ameaças no ambiente e serviços de TI.

23.5.3. Nesse sentido, o contrato prevê:

a) Serviço de proteção contra ataques de negação de serviço (*Distributed Denial of Service-DdoS*);

b) Monitoramento 24x7 (24 horas por dia, 7 dias da semana);

c) Ações preventivas e tratamento de incidentes de segurança da informação;

d) Filtro Web (Web filter);

e) Controle de Aplicação (Application Control);

f) virusservice database (ISDB);

g) DNS Filter;

h) Antivírus (anti-propagação a partir de meio externo à rede);

i) IPS;

j) Bloqueio a URLs maliciosas;

k) Bloqueio a redes Botnet C&C;

l) Bloqueio a destinos baseados em geolocalização;

m) Autenticação ativa;

n) Sincronização por meio de NTP (Network Time Protocol), que facilitará possíveis auditorias e análises de logs;

o) Gerencia de Logs e Configuração

23.5.4. *Status:* Em andamento. A migração dos 1.700 links iniciou-se em agosto/2022 e tem finalização prevista para julho/2023, sendo 304 pontos ainda em 2022.

23.6. **AS6 - Implantar solução de proteção de *endpoints***

23.6.1. Com a contratação de segurança avançada para *endpoints* (35014.048537/2021-19) fecha-se importante canal de vulnerabilidade atualmente exposto na instituição em vista da ausência de segurança eficaz e atualizada para computadores desktops, notebooks, servidores de arquivos e de rede físicos e virtuais.

23.6.2. Além de prover soluções de antivírus mais modernas, considerando as novas abordagens de detecção e prevenção de ameaças, a aquisição também alimentará a cadeia de informações de segurança e de incidentes cibernéticos do INSS, fornecendo insumos para equipes de tratamento de incidentes e de SOC agirem tempestivamente com a intenção de evitar que ameaças digitais, como a inserção de dados fraudulentos em sistemas, o roubo de dados previdenciários, o roubo de credenciais de acesso de seus servidores e ataques de ransomware nas estações dos servidores.

23.6.3. *Status:* Em andamento. Artefatos de planejamento da contratação concluídos e em análise na Procuradoria Federal Especializada do INSS.

23.7. **AS7 - Atualizar parque computacional do INSS**

23.7.1. Manter a infraestrutura de TI atualizada é um dos passos para garantir a proteção dos dados da instituição, posto que as atualizações são imprescindíveis à correção de vulnerabilidades.

23.7.2. Os microcomputadores e notebooks que compõe o parque tecnológico da Autarquia possuem, em sua maioria, o Windows 7 como sistema operacional, sendo que a Microsoft encerrou o suporte técnico para esta versão desde 14/01/2020. Assim, a assistência técnica e as atualizações de software não estão mais disponíveis.

23.7.3. Em vista disso, tendo a segurança da informação como uma das premissas, vem se buscando a aquisição de microcomputadores e notebooks, inclusive para os servidores em regime de telerabalho, a saber:

I - Aquisição de 2.724 microcomputadores e 593 notebooks (35014.075314/2020-43, 35014.102986/2022-09, 35014.103046/2022-29, 35014.103061/2022-77 e 35014.103083/2022-37), em fase de efetivação final das entregas.

II - Aquisição de 12.319 microcomputadores e 6.900 notebooks

(35014.040622/2022-10), que aguarda ateste orçamentário para possível adimplemento por meio de adesão às Atas de Registro de Preços nº 34/2021 e 39/2021 do Ministério da Economia.

III - Aquisição de 1.186 switches (35014.204608/2022-51), cujos artefatos de planejamento da contratação já foram concluídos.

23.7.4. Particularmente quanto ao empréstimo de equipamentos a servidores em trabalho fora das dependências do INSS (Programa de Gestão), a DTI emitiu a NOTA TÉCNICA Nº 2/2022/DTI-INSS (6358611):

> 41. O custo, inicialmente suportado em razão da compra, passa a ser percebido como verdadeiro investimento em segurança cibernética. Isso porque o uso de equipamentos de propriedade do instituto pelos servidores permite maior controle do que um usuário tem permissão para fazer, contribuindo para o fortalecimento da segurança na medida em que se mitiga a possibilidade de roubo de credenciais, vazamento de dados e outros incidentes, garantindo-se assim a diminuição das perdas financeiras ocorridas em razão de fraudes financeiras, bem como a segurança dos dados dos usuários (potenciais alvos dos ataques).
>
> 42. Ao se adotar o trabalho remoto como um programa do Instituto, diversos controles de segurança que existem nas dependências físicas do INSS deixaram de alcançar a maioria dos computadores utilizados pelos servidores, como por exemplo controle e monitoramento dos acessos feitos a sítios de internet, suporte remoto seguro, bloqueio do equipamento em caso detecção de vírus, realização de auditorias e principalmente visibilidade do equipamento. Em que pese nossas políticas de proteção de dados, não é possível conhecer a realidade do equipamento pessoal do servidor muito menos saber que os acessa. Se esta estação estiver sob rege do INSS, poderemos ter essa questão elucidada.
>
> 43. A compra de notebooks para uso de servidores designados em programas de gestão permitirá que se utilize o serviço de diretório nesses equipamentos. Como os dispositivos a serem utilizados agora serão de propriedade do INSS, e não mais do servidor, será possível conceder a este um perfil de usuário com permissões restritas, realizando-se, através de GPO (Group Policy Object), o controle do que este usuário poderá instalar e acessar no equipamento. Será possível, ainda, vincular que este usuário apenas poderá se conectar à internet através de um proxy, realizando-se a gestão de quais recursos na rede ele terá permissão para acessar.
>
> (...)
>
> 48. Em resumo, a compra desses equipamentos permitirá diminuir a superfície de ataque, tanto física quanto digital, uma vez que os ativos utilizados pelos servidores em trabalho remoto estarão sob um controle mais rigoroso do Instituto e deverão ser utilizados como instrumento de trabalho (e nunca recurso pessoal), seguindo as disposições e normas específicas a serem definidas para o caso, além de relevantes ganhos operacionais.

23.7.5. Já em relação à mencionada aquisição de *switches*, irá viabilizar a criação de uma rede mais robusta e interconectada, muito mais estável, segura, confiável e ainda mais monitorada, permitindo atuação mais célere em caso de incidentes. Para além da reposição de elementares ativos de rede obsoletos, danificados e sem garantia, trata-se de aperfeiçoar o gerenciamento e controle da rede de dados, elevando consideravelmente o nível de segurança da rede interna do INSS, principalmente em relação à detecção de acessos de equipamentos não permitidos.

23.8. **AS8 - Assumir a gestão das políticas de segurança do serviço de diretório do INSS**

23.8.1. Considerando a dimensão e complexidade do ambiente computacional do INSS, a quantidade de recursos de TIC (mais de 50.000) e de usuários que os utilizam, fez-se necessário que o INSS buscasse solução, via processo de aquisição, para assumir o gerenciamento e controle de acesso a esses recursos (35014.048551/2021-12).

23.8.2. *Status:* Em andamento. Artefatos de planejamento da contratação concluídos e em análise na Procuradoria Federal Especializada do INSS.

23.9. **AS9 - Monitorar proteção de *endpoints***

23.9.1. O gerenciamento das estações de trabalho e equipamentos servidores do INSS será possível a partir da implantação da solução de proteção avançada contra ameaças a endpoints e servidores (Antivírus + Endpoint Detection and Response), contemplada na retromencionada AS6 - "Implantar solução de proteção de *endpoints"* (35014.048537/2021-19).

23.9.2. *Status:* Em andamento. Artefatos de planejamento da contratação concluídos e em análise na Procuradoria Federal Especializada do INSS.

23.10. **AS10 - Monitorar rede de dados do INSS**

23.10.1. O monitoramento da rede de dados do INSS integra a solução corporativa contratada junto à empresa Telebras e será realizado por seu NOC (Network Operation Center ou Centro de Operação de Rede), com acesso do INSS, à medida que os novos links contratados vão sendo ativados.

23.10.2. *Status:* Em andamento. Implantação dos novos links iniciada em agosto/22 e finalização prevista para agosto/23.

23.11. **AS11 - Monitorar Serviço de Diretório**

23.11.1. O monitoramento dos recursos de TIC será viabilizado com a contratação da solução para controle de acesso a recursos de TIC, cujo processo de aquisição está em andamento, o que será possível após o alcance da AS8 - "Assumir a gestão das políticas de segurança do serviço de diretório do INSS".

23.11.2. *Status:* Em andamento. Artefatos de planejamento da contratação concluídos e em análise na Procuradoria Federal Especializada do INSS (35014.048551/2021-12).

23.12. **AS12 - Monitorar ativos de TI**

23.12.1. **Ferrramenta *Zabbix***

23.12.1.1. O *Zabbix* é a plataforma de monitoramento que permite acompanhamento dos níveis de serviço, disponibilidade dos sistemas e da infraestrutura do INSS apresentando alertas para situações de indisponibilidade, performance e requisitos básicos de segurança. Esta ferramenta ainda possui um repositório com o inventário dos ativos de TI, permitindo o acompanhamento e levantamento de eventuais necessidades de melhorias no parque computacional do INSS.

23.12.1.2. *Status:*

I - Implementado monitoramento dos serviços críticos do INSS;

II - Implementado monitoramento da infraestrutura de switches, links e aplicações;

III - Implementado painel de aplicações que apresentam os índices de níveis de serviços previstos nos contratos do INSS com a Dataprev e hospedadas em ambiente de nuvem.

23.12.2. **Sistema Observador**

23.12.2.1. Desde expor as vulnerabilidades da rede até se tornar uma passagem para intrusos, as portas abertas podem representar vetores de risco que ameaçam a confidencialidade, integridade e disponibilidade da rede. E por isso é prática recomendada fechar as portas abertas.

23.12.2.2. Para enfrentar os riscos introduzidos por portas abertas, foi desenvolvido o sistema OBERVADOR, cujo propósito é fazer a varredura diária de portas e identificar aquelas que estejam eventualmente abertas na rede do INSS, municiando as equipes de suporte para inspecionar, analisar e providenciar o que for cabível para cada situação, inclusive o seu fechamento.

23.12.2.3. Por trás do Observador, roda um NMAP (*Network Mapper* ou *scanner* de rede) em *Python*, integrado com a base do *Zabbix* (software de monitoramento do INSS), o que permite a identificação do IP da máquina (sua identificação na rede). Além disso, é possível identificar quais portas foram abertas recentemente, o tipo de máquina, a unidade a qual pertence e o sistema operacional presente no equipamento.

23.12.2.4. *Status:* Implementado. Sistema Observador operacional produzindo insumos diários para análise e tratativas.

23.13. **AS13 - Capacitar equipe de segurança nas disciplinas de segurança de TIC e nas soluções disponibilizadas**

23.13.1. Há em curso processo de capacitação, treinamento e educação dos membros componentes das áreas de segurança da informação do INSS.

23.13.2. *Status:*

I - Equipe da DIOP - Divisão de Operações em TI capacitada na ferramenta *Zabbix*

II - Em novembro/2022 será concluído ciclo de capacitação de parte da DTIR - Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos:

III - Em outubro/2022 o ciclo de treinamento de parte da DSEG - Divisão de Segurança em Tecnologia da Informação será concluído.

23.14. **AS14 - Revisar processo de tratamento de incidentes de Segurança de TIC - interação com Dataprev**

23.14.1. Consiste em estabelecer assertividade e celeridade nas solicitações de bloqueio e desbloqueio de credenciais envolvidas em incidentes de segurança cibernética do INSS.

23.14.2. *Status:*

I - Executados ajustes operacionais do processo de bloqueio/desbloqueio junto à DATAPREV por meio do sistema PRONTO.

II - Rediscussão sobre a necessidade/eficiência do PRONTO.

23.15. **AS15 - Revisar processo de tratamento de incidentes de Segurança de TIC - investigação interna**

23.15.1. Compreende a definição de fluxos de gestão de incidentes de segurança cibernética que envolvem usuários sob gestão direta do INSS.

23.15.2. *Status:*

I - O fluxo básico de gestão de incidentes do INSS foi definido e está em produção.

II - O fluxo referente à gestão de incidentes relacionados a equipamentos suspeitos em unidades do INSS foi definido e está em produção.

III - O fluxo de gestão de incidentes cibernéticos relacionados a fraudes em benefícios junto à CGMOB - Coordenação-Geral de Monitoramento e Cobrança Administrativa de Benefícios da DIRBEN - Diretoria de Benefícios e Relacionamento com o Cidadão e à CGCONF - Coordenação-Geral de Conformidade da DIGOV - Diretoria de Governança, Planejamento e Inovação, foi preliminarmente definido e segue em processo de refinamento.

23.16. **AS16 - Revisar processo de tratamento de incidentes de Segurança de TIC - encaminhamentos externos**

23.16.1. Compreende a definição do fluxo de gestão de incidentes de segurança cibernética que envolvem usuários externos geridos por algum acordo, contrato ou instrumento congênere que envolvem sistemas e serviços corporativos do INSS.

23.16.2. *Status:*

I - Definidos fluxos, reativo e proativo, de tratamento de incidentes cibernéticos envolvendo credenciados de entes que celebram ACT junto ao INSS;

II - Definido fluxo relacionado à análise forense de equipamentos físicos junto à PF e com apoio da Coordenação-Geral de Inteligência Previdenciária e Trabalhista - CGINT do Ministério do Trabalho e Previdência - MTP;

III - Em andamento - definição do fluxo de tratamento de incidentes cibernéticos envolvendo usuários do MTP, Ministério da Economia e de Cartórios.

23.17. **AS17 - Implantar obrigatoriedade de certificado digital para acesso a sistemas críticos e para acesso à VPN**

23.17.1. O aperfeiçoamento do modelo de autenticação do INSS para um sistema multifator (usuário/senha + certificado digital), eleva o nível de controle de segurança do acesso aos sistemas e foi viabilizado pela aquisição dos serviços de emissão e renovação de certificação digital do tipo A3 eCPF padrão ICP-Brasil.

23.17.2. *Status*:

I - Fornecidos *tokens* físicos a 100% dos servidores do INSS;

II - Desde 02/09/2022 o acesso aos sistemas críticos parceiros do Sistema de Gerenciamento de Identidades – GERID, passou a exigir a certificação digital para 100% dos servidores do INSS;

III - Todos os Peritos Médicos Federais em exercício no INSS igualmente receberão os *tokens*, já em fase de distribuição, após o que igualmente somente poderão acessar os sistemas integrados ao com a utilização de certificado digital;

IV - Está em vias de implantação pela Dataprev, a pedido do INSS, regra para que todo acesso à VPN do INSS somente será possível por meio de Certificado Digital A3;

23.18. **AS18 - Migrar aplicações hospedadas em infraestrutura própria para ambiente de nuvem**

23.19. Descomissionar sistemas e aplicações de ambientes frágeis e transferi-los para um ambiente mais seguro e robusto, mantidos via contrato de sustentação, contribui para que os principais requisitos de segurança e conformidade como localidade, proteção e confidencialidade de dados sejam atendidos.

23.20. Estas migrações ocorrem para duas zonas: GovCloud/Dataprev e Amazon Web Services - AWS. Cada zona com segmentos intranet e internet, o que garante segurança na disponibilidade de aplicações que não precisam de exposição externa, reduzindo a superfície de ataque. Além disso, existem ambientes segregados para desenvolvimento, homologação e produção.

23.20.1. Encontra-se em andamento, no INSS, a migração de todas as aplicações hospedadas em infraestrutura própria para ambiente de nuvem.

23.20.2. *Status:*

I - Avaliação/execução do processo de migração dos scripts de automação da ferramenta de gestão de incidentes do INSS (TheHive4) da Sala Segura para a GovCloud.

II - Contamos com aproximadamente 119 aplicações da área meio catalogadas. No corrente ano foi planejada a migração de 40 aplicações que ainda eram mantidas em ambiente *on premise/hosting*, 26 já foram migradas e 14 estão em andamento para conclusão até o final de outubro.

23.21. **S19 - Implantar *hardening* nos servidores Linux de propriedade do INSS**

23.21.1. Considerado boa prática, a realização de *hardening* em servidores visa robustecer a segurança cibernética dos ambientes tecnológicos da Instituição, como estabelecido na NOTA TÉCNICA Nº 4/2022/DSEG/CIMTI/CGIS/DTI-INSS, que traz diretrizes para *hardening* em servidores Linux do INSS.

23.21.2. A implantação foca, além do *hardening*, na capacidade de monitoramento e utilização de Infraestrutura por Código para gerir o parque de servidores locais, o que possibilita versionamento e consequente gestão nas alterações realizadas pelo corpo técnico nas configurações dos servidores, além de centralização e automatização dos processos. Isso agrega melhoria no gerenciamento e consequentemente, na segurança.

23.21.3. Projeto formalizado através de Termo de Abertura de Projeto – TAP, cujo objetivo é definir e executar ações de hardening em todos os servidores Linux do parque tecnológico do INSS e conta com a participação das áreas de segurança e operações.

23.21.4. *Status:*

I - Definição dos procedimentos e criação das imagens Linux para instalação nos servidores.

II - A execução desse processo acompanhará o mesmo cronograma da implantação dos novos links de dados.

23.22. **AS20 - Implantar política de backup nas aplicações hospedadas em infraestrutura própria**

23.22.1. A política de backup e restauração de dados digitais objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pelo INSS e formalmente definidos como de necessária salvaguarda no INSS, para se manter a continuidade do negócio.

23.22.2. **Status**:

I - - Encontra-se em andamento a elaboração/validação do documento que explicita as diretrizes, regramentos e demais itens que nortearão a implementação da Política de Backup na instituição.

II - - A previsão para a publicação do referido documento é 31/10/2022.

23.23. **AS21 - Executar plano de ações operacionais de prevenção a incidentes de Segurança de TIC**

23.24. Promover ações de mitigação prévia de riscos relacionados a ameaças, mapeadas ou não, que podem explorar vulnerabilidades, conhecidas ou não, conforme a realidade dos incidentes enfrentada, avaliações de segurança e tendências externas.

23.25. **Status**:

I - Unificação dos campos E-mail Institucional e E-mail Particular no cadastro LDAP realizado.

II - Execução e acompanhamento do processo de monitoramento, auditoria e correção do campo de E-mail Particular no cadastro LDAP.

III - Estabelecimento da iniciativa sazonal de reset geral de senhas dos usuários do INSS.

IV - Consultoria de segurança à DGACO - Divisão de Gerenciamento de Acordos de Cooperação da DIRBEN - Diretoria de Benefícios e Relacionamento com o Cidadão, referente à educação e divulgação da POSIN e da NCAL junto aos credenciados dos entes que celebram Acordo de Cooperação Técnica - ACT junto ao INSS.

V - Apontamentos operacionais e cotidianos de fragilidades nos serviços e sistemas corporativos do INSS, sustentados pela DATAPREV ou pela Divisão de Operações em TI, à luz de incidentes de cibernéticos.

VI - Levantamento das possíveis causas raízes dos incidentes relacionados ao comprometimento de credenciais do INSS e execução das ações necessárias à mitigação de tais ameaças.

FORTALECIMENTO INSTITUCIONAL E NORMATIVO DA ÁREA DE SEGURANÇA DA INFORMAÇÃO

24. Diga-se, a área de Segurança da Informação recebeu atenção especial na nova Estrutura Regimental do INSS, aprovada pelo DECRETO Nº 10.995, DE 14 DE MARÇO DE 2022, notadamente na composição da Diretoria de Tecnologia da Informação.

25. Isso porque, no modelo antigo, a estrutura da área se limitava a **um Serviço** de Segurança da Informação (SSEG), passando agora a ser composta por **duas Divisões**: a Divisão de Segurança em TI (DSEG) e a Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (DTIR).

26. Esta última leva a efeito a instituição **regimental** da **ETIR**, atuando como Equipe desde a publicação da RESOLUÇÃO Nº 11 /CEGOV/INSS, DE 31 DE AGOSTO DE 2020.

26.1. Originalmente, dentre os modelos preconizados pela Norma Complementar (NC) nº 05 /IN01/DSIC/GSIPR - que disciplina a criação das ETIR nos órgãos e entidades da Administração Pública Federal - o INSS optou pelo **Modelo 1 – Utilizando a equipe de Tecnologia da Informação**, na qual não existia um grupo dedicado, agia reativamente e seu gestor atribuía responsabilidades para que os seus membros exercessem atividades proativas, em concorrência às demais demandas daquele profissional.

26.2. Quanto à autonomia da ETIR, esta nasceu na modalidade **Sem Autonomia**, quando a ETIR não possuía qualquer autonomia para a tomada de decisões ou adoção de ações, se limitando a recomendar os procedimentos a serem executados, sem direito a voto na decisão final.

26.3. Com a publicação da PORTARIA DTI/INSS Nº 75, DE 01 DE ABRIL DE 2022, a ETIR passou a ser dotada dos seguintes atributos:

> 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. 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 ultrapassarem 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.

26.4. A viabilização dessas alterações decorreram da decisão do CEGOV (Resolução CEGOV/INSS nº16, de 17 de março de 2022) no intuito de conferir à própria DTI autonomia para disciplinar as rotinas de Segurança da Informação em harmonia com a Política de Segurança da Informação do órgão, que segue sendo de alçada daquele Colegiado.

26.5. Na mesma esteira, foram alteradas a norma que disciplina o uso da Internet no INSS (PORTARIA DTI/INSS Nº 71, DE 16 DE MARÇO DE 2022) e a Norma de Controle de Acesso Lógico - NCAL (PORTARIA CONJUNTA DTI/DIRAT/INSS Nº 3, DE 01 DE ABRIL DE 2022), que 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.

27. Em se tratando de gestão de credenciais, objeto precípuo da presente Nota, tem-se na NCAL o norteador elementar. Dada sua crucialidade, valem os grifos abaixo:

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. 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. 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 à 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 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. 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.

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

(...)

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.

28. No intuito de aperfeiçoar e padronizar os requisitos de segurança adotados internamente, a DTI editou também a PORTARIA DTI/INSS Nº 79, DE 25 DE MAIO DE 2022 , que estabelece o processo de entrega de software, os padrões de desenvolvimento e obtenção segura de sistemas computacionais não finalísticos e as diretrizes para a utilização de rotinas de automação robótica de processos (RPA) no âmbito do INSS.

29. Anote-se a percepção, por esta Diretoria, de que há atual convergência da Dataprev no processo de amadurecimento e fortalecimento da Segurança da Informação.

AÇÃO TÉCNICA INTEGRADA INTERINSTITUCIONAL

30. Consoante propõe a NOTA TÉCNICA Nº 3/2022/CGIN/DTI-INSS, de 14/03/2022 (35014.068447/2022-25), foi instituída ação técnica integrada (interinstitucional) visando a apuração da causa primária do vazamento de credenciais de acessos a sistemas corporativos do INSS:

3. Não obstante tais diligências, o fato é que somente o trabalho repressivo não apresenta-se eficaz. Sendo certo que não há solução simples ou perfeitamente adequada a um problema tão complexo, apresenta-se imperiosa a colaboração técnica e de atividade de inteligência para que se efetivamente identifique e trate a causa raiz do vazamento das credenciais envolvidas em incidentes de segurança.

4. Nesse sentido, opina-se pela busca de apoio dos órgãos e setores elencados abaixo por meio da **indicação de um ponto focal titular e um suplente, preferencialmente com perfil técnico em cibersegurança, para a realização de reuniões regulares com o objetivo de buscar**

identificar a origem do vazamento das credenciais de acesso a sistemas do INSS comprometidas em incidentes de segurança da informação tratados pela Equipe de Prevenção, Tratamento e Reposta a Incidentes Cibernéticos do INSS (ETIR-INSS).

5. Os participantes sugeridos seguem abaixo.

5.1 Pelo INSS:

a) Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR

b) Coordenação-Geral de Infraestrutura e Operações;

c) Coordenação-Geral de Projetos e Soluções Digitais;

d) Diretoria de Integridade, Governança e Gerenciamento de Riscos - DIGOV;

e) Coordenação-Geral de Combate à Fraude - CGCF;

f) DPO - Data Protection Officer / INSS, especialmente designado para essa função;

5.2 Externos ao INSS:

a) Coordenação-Geral de Inteligência Previdenciária e trabalhista do Ministério do Trabalho e Previdência - CGINT;

b) Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov;

c) Divisão de Repressão a Crimes Previdenciários da Polícia Federal

d) Divisão de Repressão a Crimes Cibernéticos da Polícia Federal;

e) Diretoria de Tecnologia da Informação da Advocacia-Geral da União - AGU;

f) Diretoria de Privacidade e Segurança da Informação da Secretaria de Governo Digital do Min. Economia; e

g) Coordenação-Geral de Segurança de Informações da DATAPREV.

30.1. O grupo, sob coordenação da DTI/INSS, foi organizado em três frentes de trabalho:

Frente de Trabalho	Membros	Produto
I) Políticas de Gestão de Acesso	INSS – DSEG/DTI INSS – DIGOV INSS – DIRBEN INSS – PFE CTIR GOV AGU DATAPREV	Plano de Implementação das Políticas de Gestão de Acesso (medidas e ações a serem definidos pelo INSS a serem executadas por entes internos, pela Dataprev, ou entes externos que celebrem acordos com o Instituto).
II) Processos de Comunicação	INSS – DTIR/DTI INSS – CGCF INSS – DIGOV INSS – PFE DATAPREV AGU CTIR GOV CGINT	Criação de Fluxos de Comunicação e Gestão de Incidentes entre o INSS e entes internos e externos que celebrem acordos com o Instituto e que dele usufruam de aplicações, bases ou credenciais. Adesão à Rede Federal de Gestão de Incidentes Cibernéticos (DECRETO Nº 10.748, DE 16 DE JULHO DE 2021).
III) Estudos de Casos	INSS – DTIR/DTI INSS - CGCF AGU DATAPREV CGINT PF	Encaminhamentos necessários ante às discussões, análises e sugestões relacionadas aos incidentes apresentados. Documentação do conhecimento produzido e Elaboração de um Plano de Ação.

30.2. Dos trabalhos realizados, foi produzida a NOTA TÉCNICA Nº 6/2022/DTIR/COIM/CGIS/DTI-INSS (9151371), que em linhas gerais, trouxe os seguintes resultados e recomendações:

9. O produto final da frente de **Políticas de Gestão de Acesso** é o Plano de Implementação das Políticas e Gestão de Acesso que abrange as conclusões da Análise das Causas Raízes, as análises das respostas aos ofícios enviados à Dataprev, a discussão conduzida por esta frente e o cronograma de aprimoramentos de segurança nas aplicações, bases e infraestruturas corporativas

mantidas pela Dataprev, conforme estabelecido pelo Evento de Segurança (Dataprev x INSS) iniciado em junho de 2022, sintetizando possíveis sobreposições:

Medida	**Ação**	**Áreas responsáveis**	**STATUS**
Revisão da Norma de Controle de Acesso Lógico, visando melhor aplicabilidade da gestão do controle de acesso para não permitir concessão horizontal de gestão	Instituir GT, envolvendo a DTI, DGPI e áreas de negócio para consenso da redefinição das funções de gestão de acesso. Revisão das regras de negócios, dos papéis e permissões de gestores e das bases de usuários	DTI, DTIR, DSEG, DIRBEN	Sem demanda
Revisão da Política de Segurança da Informação	Instituir GT de revisão da POSIN-INSS.	CTGD, DTI, DSEG, DTIR	Sem demanda
Fortalecimento da política de senhas	Incrementar a quantidade e a complexidade de caracteres. Revisar os prazos de expiração de senhas e tokens de usuários internos e externos. Incluir item na revisão da NCAL de forma a abranger LDAP, Office 365 e Certificado Digital. Incluir no contrato com a Dataprev.	DTIR, DSEG	Sem demanda
Estabelecer um inventário de contas – sistemas mantidos pelo INSS	Realizar inventário das contas geridas pelo INSS.	DSEG, DIOP, CGDSI	Sem demanda
Estabelecer um inventário de contas - sistemas mantidos pela Dataprev	Solicitar à Dataprev realização de inventário de contas dos sitemas geridos pela empresa.	DSEG	Sem demanda
Desabilitar contas inativas – sistemas mantidos pelo INSS	Realizar a desabilitação e/ou exclusão de contas inativas há mais de 60 dias de sistemas geridos pelo INSS.	DSEG, DIOP, CGDIS	Sem demanda
Desabilitar contas inativas - sistemas mantidos pela Dataprev	Solicitar à Dataprev a desabilitação e/ou exclusão de contas inativas há mais de 60 dias de sistemas geridos pela empresa.	DSEG	Sem demanda
Restringir privilégios de administrador a contas de Administrador dedicadas	Criar constas específicas para usuários administradores, independentes das contas para uso em atividades comuns do dia-a-dia.	DSEG, DIOP, CGDSI	Sem demanda
Avaliar e revisar o ciclo de vida das contas de usuários que acessam os sistemas mantidos pelo INSS.	Criar ou revisar, caso já exista, processo de concessão e revogação de acesso aos sistemas mantidos pelo INSS Verificar com as áreas responsáveis pela concessão de acessos a existência de processo formal de concessão e revogação de acesso. Solicitar a revisão de papéis e de regras de negócio em busca da mitigação de flexibilizações e fragilidades. Execução de operação sazonal de reinicialização das senhas de todos os usuários internos do INSS	DSEG, DIOP, CGIS, Diretorias da Área Fim	Sem demanda

Medida	Ação	Áreas responsáveis	STATUS
Avaliar e revisar o ciclo de vida das contas de usuários que acessam os sistemas mantidos pela Dataprev.	Solicitar à Dataprev documento formal com o processo de concessão e revogação de acesso aos sistemas do INSS mantidos pela Dataprev. Criar ou revisar, caso já exista, processo de concessão e revogação de acesso aos sistemas mantidos pelo INSS Verificar com as áreas responsáveis pela concessão de acessos a existência de processo formal de concessão e revogação de acesso. Solicitar a revisão de papéis e de regras de negócio em busca da mitigação de flexibilizações e fragilidades. Revisar a possibilidade de atribuição de papéis em UF distintas da UF do gestor com mais controle, talvez de forma centralizada. Por exemplo, em Superintendências Regionais. Controlar, estabelecer rastreabilidade e visibilidade para a possibilidade de atribuição de papéis em UF distintas da UF do usuário, caso não exista serviço formalmente autorizado. Corrigir a possibilidade de duplicidade de papéis atribuídos. Por exemplo, caso um usuário receba um papel de consulta em um sistema, talvez não necessite receber papel similar no mesmo sistema, considerar UFs distintas.	DSEG, Dataprev	Sem demanda
Implementar o uso de *Single Sign-On* para acesso as aplicações web geridas pelo INSS	Verificar com as áreas responsáveis a existência/disponibilidade do recurso para as aplicações geridas pelo INSS.	DSEG, DIOP, CGDSI	Sem demanda
Implementar o uso de *Single Sign-On* para acesso as aplicações web geridas pela Dataprev	Solicitar implementação à Dataprev.	DSEG	Sem demanda
Implementar MFA nas aplicações mantidas pelo INSS	Verificar com as áreas responsáveis pela existência/disponibilidade do recurso para as aplicações geridas pelo INSS.	DSEG, DIOP, CGDSI	Sem demanda
Implementar MFA nas aplicações corporativas hospedadas pela Dataprev	Aplicar MFA (via Google Autenticator) no módulo de autenticação das aplicações	DSEG, Dataprev	Em andamento
Validar CPFs junto à base da Receita Federal durante o processo de credenciamento de usuários na árvore de diretórios LDAP do INSS.	Confirmar o andamento do desenvolvimento, pela Dataprev, da solução CDI, a qual, entre outras muitas funções, irá realizar validação de CPFs cadastrados no LDAP com a base da Receita Federal	DSEG, Dataprev	Em andamento
Segregar os grupos de usuários que usam certificado A1 e A3	Confirmar a conclusão da segregação dos grupos de usuários que usam certificado A1 e A3	DSEG, DGP, Dataprev	Em andamento

Medida	**Ação**	**Áreas responsáveis**	**STATUS**
Validar o status do usuário no LDAP durante o processo de autenticação no GERID via Certificado Digital.	Habilitar a validação do status do usuário no LDAP ao realizar login por Certificado Digital no GERID	DSEG, Dataprev	Implantado
Aplicação de MFA no processo de autenticação na VPN do INSS.	Acesso, exclusivo via Token A3, à VPN (exceto terceirizados, externos e estagiários)	DTI, Dataprev	Em andamento.
Concessão de Credenciais	Reavaliar a formalização da Concessão das Credenciais	DTI, DIRBEN, DGP, Dataprev	Em andamento.
Procedimento de reconhecimento de Token e de reinicialização de senha	Abolir o uso do email particular para o reconhecimento de Token e para a reinicialização de senha	Dataprev (Demanda DTP.71821)	Em homologação a ser realizada em Brasília-DF no dia 05/10.
Renovação de VPN	Implantar fluxo do processo de renovação automática da VPN (Nova ação).	Dataprev	Concluído.
Impedir eventos de *Impossible Travel* (acessos simultâneos) durante o uso de aplicações corporativas.	Implantar Bloqueio de Acesso Simultâneo	Dataprev	Em andamento.
Revisar a segurança dos sistemas legados	Aprimorar os controles e níveis de segurança dos sistemas legados (SUB/Plenus, Prisma, SABI e outros). Aplicação de controles de segurança mais robustos nos módulos de autenticação e de tráfego de dados nos sistemas corporativos legados	DTI, DIRBEN, Dataprev	Priorizado para 2023 e sem atualizações.
Revisão das políticas de identidade e acesso para usuários internos e externos	Aprimorar Processo de revisão de usários e seus privilegios	Dataprev	Priorizado para 2023 e sem atualizações.
Aprimorar o GERID	Elaborar Estudo de Evolução de Arquiterura Tecnologica do GERID. Implantar Versões Evolutivas do GERID (principais entregas). mplantar Versões de Manutenção Evolutiva do GERID.	DTI, Dataprev	Priorizado para 2023
Revisar os controles de acesso à Central 135	Revisar o fato de que durante o processo de gestão de acesso, não existe nenhuma regra de negócio relacionada às centrais 135. Desta forma, sim, é possível usar os papéis da central e acessar os sistemas (Internet ou intranet), mesmo estandofora da Central 135. Discutir a adoção de uma hierarquia de distribuição de papéis, autorizações e permissões de acesso mais robusta a fim de se contornar possibilidades atuais como a atribuição de perfil de acesso a qualquer usuário, inclusive aqueles alheios à Central 135.		

10. Os produtos finais da frente de **Processos de Comunicação** são:

10.1 A Revisão e a criação de fluxos de Comunicação e Gestão de Incidentes entre o INSS e entes internos e externos que celebrem acordos com o Instituto e que dele usufruam de aplicações, bases ou credenciais:

Revisão do fluxo básico de gestão de incidentes;

Criação de fluxo de tratamento de incidentes que envolvem entes que celebram acordos, contratos ou instrumentos congêneres (ACT) junto ao INSS por meio da DIRBEN, conforme formalizado no processo SEI 35014.277683/2022-31;

Criação de fluxo de registro e encaminhamento de incidentes de fraudes e vazamentos de dados pessoais, conforme formalizado no processo SEI 35014.434169/2022-17;

Criação de fluxo de investigação forense de equipamentos junto à PF com o apoio da CGINT;

Implantação de ferramenta de gestão de incidentes (TheHive4) após orientação do CTIR.gov;

Confirmar o fluxo de comunicação de incidentes com todos os atores da ação técnica integrada.

10.2 A adesão à REGIC (Rede Federal de Gestão de Incidentes Cibernéticos), nos termos do § 1º do art. 1º do Decreto nº 10.748, de 16 de julho de 2021, pela DTIR/INSS conforme estabelecido nos autos do processo SEI 35014.169878/2022-16.

11. O produto final da frente de **Estudo de Casos** é o Plano de Ação composto pelas conclusões da Análise das Causas Raízes, análises das respostas aos ofícios enviados à Dataprev, as análises dos incidentes tratados nesta frente e o cronograma de aprimoramentos de segurança nas aplicações, bases e infraestruturas corporativas mantidas pela Dataprev, conforme estabelecido pelo Evento de Segurança (Dataprev x INSS) iniciado em junho de 2022, sintetizando possíveis sobreposições:

Medida	**Ação**	**Áreas responsáveis**	**STATUS**

Medida	**Ação**	**Áreas responsáveis**	**STATUS**
Aprimorar os controles e níveis de segurança da árvore de diretórios LDAP do INSS.	Mapear o administrador e os gestores do GERID e iniciar, junto a eles, a mudança de comportamento e mudança de procedimentos impostas pelas políticas de segurança e das ferramenta estabelecidas. Solicitar a correção da fragilidade relacionada a acesso anônimo à árvore do LDAP e a hashes MD5. Revisar a qualidade cadastral dos dados da árvore LDAP. Validar e a aplicar controles de segurança no LDAP e em todas as aplicações corporativas e internas. Mapear todas as aplicações que se autenticam na base LDAP, além de realizar ajustes granulares de permissão. Validar o *backend* do LDAP e criar *playbooks* de testes de aplicações internas e corporativas a serem aplicados periodicamente. Solicitar à Dataprev a disponibilização de um painel de gerenciameto do LDAP e GERID. Limitar conexões ao LDAP dentro da Região de Acesso RII. Solicitar e avaliar o mapeamento do LDAP e o desenho de segurança do GERID. Agendar apresentação da pilha tecnológica que provê a segurança dos produtos do INSS sustentados pela DATAPREV e assim definir e detalhar melhorias a serem implementadas no produto GERID referentes a controle e à auditoria da distribuição de credenciais, papéis e permissões em conjunto com as áreas responsáveis. Controlar, estabelecer rastreabilidade e visibilidade para a possibilidade de gestores internos atribuírem papéis para usuários externos. Controlar, estabelecer rastreabilidade e visibilidade para a possibilidade de gestores atribuírem papéis para usuários no seu mesmo nível, na hierarquia de autorizações. Aplicar auditorias de segurança nas atribuições das permissões de acesso.	DTI, Dataprev	Priorizado para 2023 e sem atualizações.
Elaborar o Plano de Tratamento de Incidentes Cibernéticos (INSS x Dataprev)	Fluxo de Comunicação entre DTIR/INSS e CTIR/Dataprev. Completar o fluxo com retorno da DTIR/INSS. Solicitação de revisão de casos antigos e os testes na infraestrutura subjacente pela Dataprev	DTIR, CTIR Dataprev	Em andamento
Fluxo de Bloqueio e Desbloqueio de Credenciais no Pronto	Aprimorar a operacionalização do fluxo	DTIR, CTIR Dataprev	Concluído.

Medida	**Ação**	**Áreas responsáveis**	**STATUS**
Acessar, consumir e gerir logs de acessos em aplicações corporativas	Entrega de Arquivos de Logs - versão 1 Entrega de Arquivos de Logs - versão 1 / Viabilizando Nuvem. Evolução da Entrega de Logs / Definir forma de Disponibilização de Dados	DTIR, DIOP, CGDSI e Dataprev.	Em andamento.
Gerir vulnerabilidades em aplicações, protocolos e bases corporativos.	Definir serviços e escopo da gestão de vulnerabilidades. Executar o mapeamento de vulnerabilidades. Executar as correções das vulnerabilidades.	DTI, Dataprev	Não iniciado.
Discutir, decidir e deliberar a disciplina e regime de utilização ou existência de soluções RPA (*Robotic Process Automation*)	Implantação de APIs e desativação de Robôs	DTI, Dataprev	Em andamento
Executar testes de invasão	Definir serviço e escopo do pentest (reunião de kickoff INSS e DATAPREV). Elaborar cronograma das etapas de execução do pentest. Executar pentest no escopo definido e elaborar relatório. Implementar correções no serviço.	DTI, Dataprev	Não iniciado.
Hardening de servidores físicos do INSS.	Implantação da ferramenta inotify nos servidores GNU/Linux	DSEG, DIOP	Em andamento
Revisão da segurança de infraestrutura, de hosts, de borda e de nuvem.	Implantação de controles de segurança baseados em hosts e aplicação de uma solução de bloqueio, no firewall, de comunicações laterais na mesma zona de rede, de IPS, monitoramento de filesystem em servidores Linux e firewall de hosts. Contratação de monitoramento em aplicações hospedadas nas nuvens AWS e GovCloud. Implantação de controle de dispositivos e de redes no âmbito da infraestrutura de rede do INSS. Implantar segurança baseada em hosts e aplicar uma solução de bloqueio, no firewall, de comunicações laterais na mesma zona de rede, de IPS, monitoramento de filesystem em servidores Linux e firewall de hosts;	DSEG, DIOP, CGIS	Em andamento
Implantar modelo de desenvolvimento seguro de software no INSS	Revisar o modelo de desenvolvimento de software do INSS	DSEG, CGDSI	
Relacionamento com parceiros da DTIR.	Confirmar se os mecanismos de monitoramento de rede prometidos pela AGU foram implantados em sua rede, assim como a qualidade de tal controle;	DTI, AGU	Não iniciado
Campanhas de educação, treinamento e conscientização em segurança da informação.	Revisar e divulgar amplamento o curso de SIC.	DSEG	Em andamento
Gestão de segurança física no INSS	Aprimorar os controles de segurança física das unidades do INSS	DTI, DIROFL	Em andamento

Medida	**Ação**	**Áreas responsáveis**	**STATUS**
Disseminação controlada da DTIR/INSS.	Divulgar o ponto de contato da Divisão de Prevenção, Detecção, Tratamento e Resposta a Incidentes Cibernéticos do INSS para a comunidade interna (página na intranet) e externa (WHOIS).	DTIR, DSEG	Não iniciado
Gestão de pessoas no âmbito de segurança da informação	Apoio no estabelecimento de programas de políticas de gestão de pessoas para incentivo, educação, fomento à postura ética e divulgação de sanções relacionadas à infração às conformidades legais. Estabelecimento de programas de monitoramento de ambiente e de canais de denúncia anônima;	DTI, DGP	Não iniciado
Gestão de pessoas e tecnologias pertencentes às áreas de segurança da informação do INSS	Fortalecimento do quantitativo de pessoal e disponibilização de tecnologias (SOAR, XDR, Solução de Painel de Registros de Eventos e Ações, etc.) no time de gestão de incidentes de segurança da informação do INSS;	DTI, DGP	Em andamento
Gestão de projetos seguros no INSS	Priorizar as políticas e avaliações de segurança da informação em todos os projetos do Instituto. Implantação de princípios de design de segurança nos processos de negócio e na operação dos sistemas corporativos como: estabelecimento de least privileges (privilégios mínimos), de need to know (compartimentalização de ações), de separation of duties (separação de responsabilidades), de economy of mechanism (balanceamento entre segurança e complexidade), de complete mediation (mediação de cada ação); identificação de pontos mais fracos e de pontos únicos de falha em toda a cadeia de identidade e acesso do INSS; a prevenção de compartilhamento inadvertido e inadequado de informação e de separação de responsabilidades;	DTI, DIRBEN, DIGOV.	Não iniciado
Análise de ameaças às credenciais do INSS.	Modelagem das ameaças (atravessadores/vendedores) às credenciais do INSS. Incorporação do modelo de ameaças nos requsitos de segurança de todos os projetos do INSS.	DTI, DIGOV	Em andamento
Revisar os serviços da Central Service.	Avaliar o catálogo de serviços disponíveis em cada VIP da Central Service. Revisar o processos de autenticação, autorização e auditoria da Central Service. Reavaliar modelo, alinhar, junto com as áreas responsáveis, levantar requisitos e demandar a Dataprev, pois o acesso aos serviços em produção é realizado através usuário/senha exclusivos para os serviços do Central Service. Não há autenticação para usuário de LDAP.	DTI, Dataprev	Não iniciado
Revisão dos controles e níveis de segurança da API do Market Place	Confirmar a entrega parcial, pois a resposta não contemplou as data de expiração das credenciais autorizadas solicitadas. Verificar o que significa não associada à plano de consumo.	DTI, Dataprev	Não iniciado

Medida	**Ação**	**Áreas responsáveis**	**STATUS**
Revisão dos usuários e gestores associados a *usercodes* e seus respectivos *accesscodes* no CV3	Excluir/Inativar imediatamente todos os ACCESSCODE que tenham no campo DALASTLOGONTIME data anterior a 30/04/2022 Excluir/Inativar imediatamente todos os ACCESSCODE que o campo IDENTITY esteja em branco Excluir/Inativar imediatamente todos os ACCESSCODE que sejam iguais a matrículas de servidores com status EM QUARENTENA NO LDAP Excluir/Inativar imediatamente todos os ACCESSCODE que sejam iguais a números de CPFs Excluir/Inativar imediatamente todos os ACCESSCODE que sejam diferentes de matrícula SIAPE Confirmar datas e campos em branco Confirmar a descontinuação do Plenus CV3. Desenvolver forma de inativar ACCESSCODE de usuário com status EM QUARENTENA no LDAP, para casos de incidentes. Criar regra que não permita ACCESSCODE seja igual a número de CPF.	DTI, Dataprev	Não iniciado, mas priorizado no Plano de Segurança INSSxDataprev
Revisão do PROJETO INSS	Verificar necessidade com as áreas de negócio da lista de aplicações que usam mecanismo de autenticação junto à árvore de diretório LDAP do INSS e suas permissões	DTI, Áreas de Negócio e Dataprev	Não iniciado
Revisar a lista dos usuários com permissão de escrita na árvore de diretório LDAP do INSS.	Verificar quem são os OPs Numerados. Análisar necessidade com as áreas de negócio.	DTI, Áreas de Negócio e Dataprev	Não iniciado

Medida	Ação	Áreas responsáveis	STATUS
Avaliar o desenho de arquitetura de segurança dos ativos do INSS hospedados, sob contrato, na Dataprev, a saber: -controles de segurança de comunicação e de rede das implantados nas aplicações corporativas do INSS; -controles criptográficos de dados pessoais e das bases corporativas do INSS; -controles de segurança aplicados no ciclo de gerenciamento de identidade e acesso do INSS (LDAP e GERID); -Modelagem das ameaças aos ativos do INSS já mapeadas pela Dataprev; -análise de vulnerabilidades de aplicações, API's e protocolos corporativos do INSS; -Processo de desenvolvimento seguro das aplicações corporativasdo INSS; e -a natureza, a capacidade de retenção e de entrega dos logs das bases e aplicações corporativas do INSS gerenciados pela Dataprev.	Solicitar mais detalhamentos a respeito de como as camadas de segurança que foram apresentadas pela Dataprev estão configurada para o nosso ambiente. Solicitar novos documentos de modelagem de ameaça, pois os recebidos parecem estar incompletos e não fica claro se as recomendações para mitigar as ameaças já foram implementadas. Solicitar novos relatórios de análise de vulnerabilidades das aplicações são bastante suscintos e aparentemente incompletos, pois alguns sequer têm a data exata em que foi realizada a análise, ou não têm evidências reais. Solicitar um documento de diretrizes de desenvolvimento seguro, pois foram apresentadas Notas Técnicas com "padrões de segurança" para situações individuais e que deixam de abordar pontos essenciais de desenvolvimento seguro. Revisar os requisitos e políticas de *logs*.	DTI, Dataprev	Não iniciado
Grupos de VPN	Rediscutir a necessidade de tantos grupos de VPN existentes, suas permissões e ativos envolvidos (árvore de diretório, Firewall de Rede, WAF, Web Proxy, etc.) na cadeia de identidade e acesso da Dataprev;	DTI, Dataprev	Não iniciado
Implantatação de protocolo TLS/SSL nas aplicações web do INSS hospedadas na Dataprev.	Revisar as aplicações hospedadas na Dataprev que não utilizam mecanimos de autenticação MFA ou não estão hospedadas em ambientes configurados com protocolo HTTPS. Revisar o prazo para que as aplicações supracitadas sejam dotadas de mecanismo de MFA em seus módulos de autenticação. Solicitar a resposta ausente a respeito do prazo de implantação do protocolo HTTPS nos ambientes de hospedagem de aplicações do INSS que ainda não assim configurados		

31. Salienta-se que parte significativa das medidas propostas já foram implementadas ou encontram-se em andamento.

AÇÕES COMPLEMENTARES

32. Paralelamente a todas as iniciativas aqui descritas, vale menção às seguintes ações:

32.1. **Evoluções do GERID**, solução de gerenciamento de identidades provida pela Dataprev e responsável pela autenticação à maioria das aplicações críticas do INSS, conforme cronograma de priorização obtido junto à referida empresa para conclusão até 26/10/2022:

DEMANDAS DE EVOLUÇÃO DO SISTEMA DE GERENCIAMENTO DE IDENTIDADE – GERID		
Ideia	**Descrição**	**Status**
DM.092211	CDI - Central de Dados de Identidade	CONCLUÍDA
DM.083827	Gestão de identidade - consulta SIRC	CONCLUÍDA
DM.084646	Batimento com a base de dados da RFB	CONCLUÍDA
DM.083828	Ajuste no fluxo de gestão de identidade com validação no SIAPE (Sistema Integrado de Administração de Recursos Humanos)	CONCLUÍDA
DM.099033	Implantação do 2FA - Google Authenticator - Aplicações INSS integradas ao GERID	CONCLUÍDA
DM.087164	Notificação para usuários com gestor inválido	EM ANDAMENTO
DM.099552	Restrição de acesso dos usuários do INSS por CD da AC SERPRO	CONCLUÍDA
DM.095318	Rotina GERID - Credenciais de Estagiários e Terceirizados	EM ANDAMENTO
DM.090781	Perfis de Acesso para Estagiários no GERID	EM ANDAMENTO
DM.095855	Logs de acesso aos sistemas: GET, CONSIGWEB e TROCA SENHA	CONCLUÍDA
DM.094892	Logs de sistemas parceiros ao GERID	CONCLUÍDA
DM.086588	Carga de papeis em lote	EM ANDAMENTO
DM.096076	Criação de política (mensagens customizadas por tipo de bloqueio) de autenticação no CAS	EM ANDAMENTO
DM.090923	Formulário eletrônico com o Termo de Confidencialidade de Manutenção e Sigilo - TCMS	EM ANDAMENTO
DM.096279	Implementar regras sistêmicas no GERID em relação ao CNIS	EM ANDAMENTO
DM.096001	Exclusão do subsistema INTERNET_ADM do sistema SIBE	EM ANDAMENTO

32.2. **Disponibilização de novo curso de Segurança da Informação** na Escola Virtual do INSS, disponível para todos os colaboradores do INSS (servidores, estagiários e terceirizados) desde 30/06/22;

32.3. **Aperfeiçoamento do fluxo de bloqueio e desbloqueio de credenciais envolvidas em incidentes de segurança**, levado a efeito por meio da utilização da ferramenta "Pronto", otimizando a comunicação entre as equipes de segurança do INSS e da Dataprev;

32.4. **Elaboração/revisão das políticas de backup;**

32.5. Adesão ao **Programa de Privacidade e Segurança da Informação (PPSI) da Secretaria de Governo Digital (SGD/ME)**, constituido por um conjunto de ações de adequação nas áreas de privacidade e segurança da informação, desenvolvidas dentro do escopo das disciplinas de governança, pessoas, metodologia, tecnologia e gestão de maturidade, implementadas de forma concomitante e incremental. Tais ações são voltadas para aumento do grau de maturidade e de resiliência dos órgãos e das entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Poder Executivo Federal;

32.6. **Atualização da imagem (ISO) padrão de aplicações/configurações dos computadores**, como preparatório para a aquisição/entrega de novas máquinas, assim como para prover as últimas versões das aplicações em uso no INSS, dentre elas o agente de monitoramento (Grupo de Trabalho instituído pela PORTARIA DTI/INSS Nº 81, DE 15 DE JUNHO DE 2022);

32.7. **Ações de Gestão dos Ativos de Rede (Switches)**, por meio de Grupo de Trabalho instituído pela PORTARIA DTI/INSS Nº 36, DE 15 DE AGOSTO DE 2022, visando:

I - definir padrões e manuais de referência;

II - aferir se os ativos de rede (Switch) instalados nas Unidades do INSS estão acessíveis remotamente para equipe rede da DTI e supervisão;

III - averiguar se os usuários e estes ativos de rede (swicth) estão de acordo com a definição estabelecida pela equipe de rede da DTI e supervisão;

IV - verificar se as políticas de acesso (ACL) a esses ativos de rede (swicth) estão de acordo com a definição estabelecida pela equipe de rede da DTI e supervisão;

V - implementar correções nas configurações desses ativos de rede (switch), caso sejam encontradas em desacordo com os padrões definidos pela equipe de rede da DTI e supervisão; e

VI - realizar as configurações de todo ativo de rede (switch) novo ou ainda sem uso, antes de serem colocados em produção, de acordo com os padrões definidos pela equipe de rede da DTI e supervisão.

32.8. **Reinicialização geral de senhas** de todos os usuários administrativos do INSS, realizada em 28/07/2022;

32.9. **Aculturamento em Segurança da Informação, com apoio do Programa das Nações Unidas para o Desenvolvimento - PNUD (Projeto BRA/20/004)**, consistindo na contratação de serviços técnicos especializados para a elaboração e implantação de um Plano de Ação específico para essa finalidade;

32.10. **Restrição de acesso à intranet do INSS a partir da AGU**, com a implementação de regra para que todo acesso só seja feito por meio de VPN e mediante utilização de certificado digital A3;

32.11. **Aperfeiçoamento da temática segurança na relação contratual junto à Dataprev**, o que inclui:

I - Especificação dos componentes da solução de controle de acesso, autenticação, gestão de usuários e fornecimento de logs de auditoria;

II - Acesso aos registros de log de seus sistemas e dos acessos às suas bases de dados, sem custos, a fim de permitir a identificação dos responsáveis, data, hora e origem das transações realizadas;

III - Acesso direto por meio de ferramenta ou disponibilização, com intervalo máximo de 7 dias e em volumetria a ser pactuada entre as partes, os registros de logs do GERIDINSS, sem prejuízo das extrações e respectivos níveis de serviço;

IV - Verificação de segurança (PenTest) por ferramenta de mercado ou consultoria especializada, com disponibilização de relatório à área de Segurança da Informação do INSS, dos sistemas e demais soluções providas direta ou indiretamente pela Dataprev ao INSS, ou que permitam acesso a suas bases de dados, incluídos soluções ou módulos derivados de softwares livres ou de código aberto, tais quais Gerid, CAS, APIs, OpenLDAP, WSO2, VPN etc;

V - Implementação de rotina de verificação de segurança, em periodicidade no mínimo semestral, com escopo definido junto a contratada;

VI - Apresentação de relatório mensal das ações realizadas pela área de segurança da informação em relação a ativos do INSS bem como às soluções providas direta ou indiretamente ao INSS;

VII - Desativação dos VPNs sem acesso há mais de 60 dias, com anuência da gestão contratual;

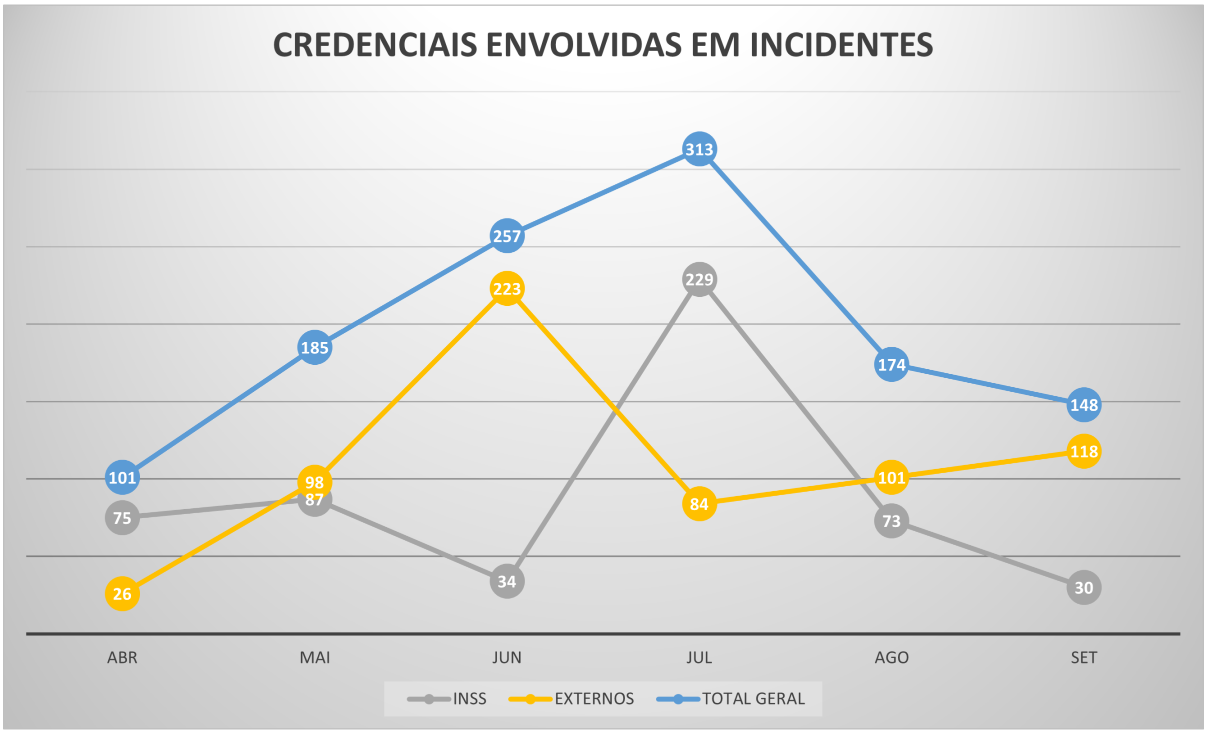
VIII - Fornecimento de APIs para coleta de incidentes de sistemas registrados pela CONTRATADA e API dos logs de proxy (Squid Report ou equivalente);

IX - Menções expressas de observância à Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) e à obrigação de aplicar e incorporar as normas afetas à Gestão de Segurança da Informação e Privacidade.

RESULTADOS

33. Como pontuado na Seção "IRREGULARIDADES EM BENEFÍCIOS" desta Nota Técnica, a PF recomendou providências urgentes em termos de segurança das credenciais dos servidores.

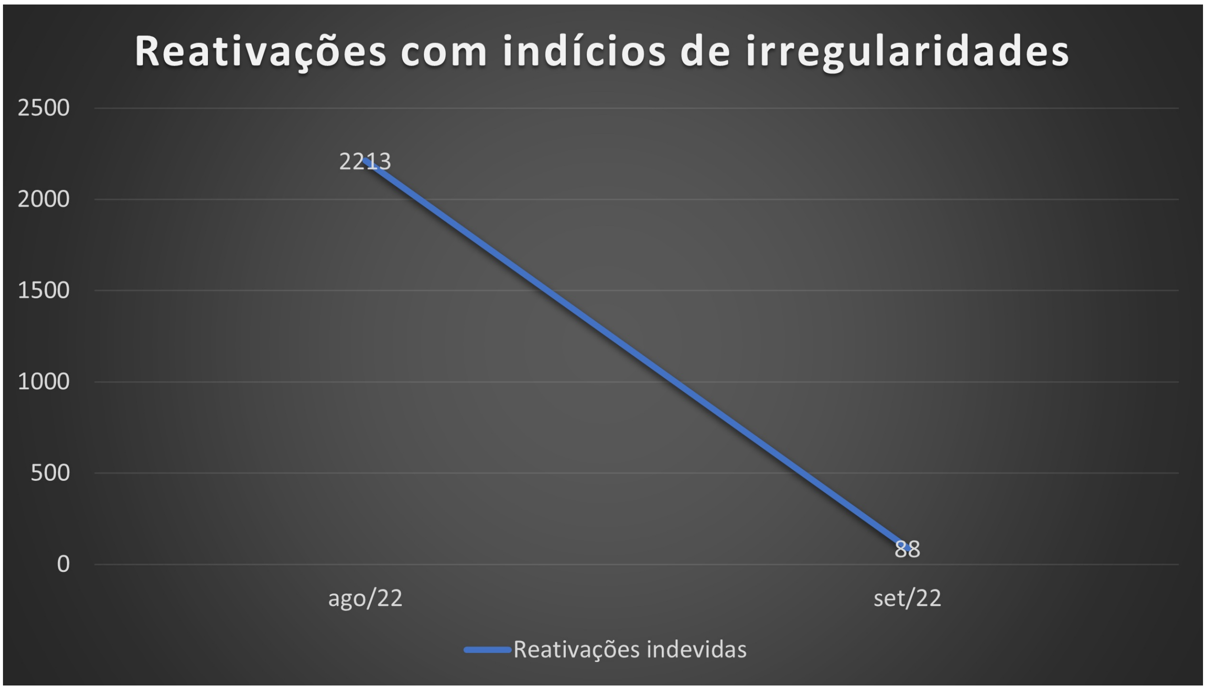
34. Para além das providências pontuais adotadas, como foi o caso do reset geral das senhas de todos os servidores do Instituto, é notório que todo um conjunto de ações estruturantes vêm sendo empreendidas e produzindo resultados práticos, tal qual demonstrado a seguir:



35. O gráfico acima demonstra que, após um pico de incidentes ocorrido em julho - ocasião em que foram encontrados os dispositivos clandestinos e que culminou com a reativação fraudulenta de benefícios - as medidas adotadas culminaram com a derrubada desses números, sendo que para credenciais de **usuários do INSS** (servidores e estagiários) envolvidas em incidentes de segurança, a quantidade caiu de 229 em julho para apenas 30 no mês de setembro.

36. Por outro lado, urge mencionar que o número de credenciais de usuários **externos** (Advocacia-Geral da União, cartórios e outras entidades decorrentes de Acordos de Cooperação Técnica, como a OAB, por exemplo) comprometidas vem sendo costumeiramente **maior** que o de usuários do próprio órgão, ensejando medidas urgentes em relação ao controle de acesso desse público.

37. No que tange à reativação de benefícios com indícios de irregularidades, a quantidade igualmente mostra resposta contundente entre a identificação dos incidentes, em agosto, e setembro (**de 2.213 para 88**), após a obrigatoriedade da utilização de certificado A3 implementada em 02/09/22:



RESTRIÇÃO ORÇAMENTÁRIA

38. Em que pese os esforços empreendidos pelo INSS, há limitações de caráter externo, já oportunamente mapeadas por ocasião do desenvolvimento do Plano Diretor de Segurança da Informação. É o caso, por exemplo, da justificada restrição orçamentária frente à inevitável necessidade de investimentos.

39. Em face desse fator, manifestou-se formalmente esta autarquia por meio dos seguintes documentos, exemplificativamente:

a) NOTA TÉCNICA Nº 4/2022/CGOFC/DGPA-INSS, de 16/02/2022;

b) NOTA TÉCNICA Nº 2/2022/DTI-INSS, de 22/02/2022;

c) NOTA TÉCNICA Nº 8/2022/CGOFC/DGPA-INSS, de 22/02/2022;

d) NOTA TÉCNICA Nº 10/2022/CGOFC/DGPA-INSS, de 15/03/2022;

e) NOTA TÉCNICA Nº 35/2022/CGOFC/DIROFL-INSS, de 15/07/2022;

f) NOTA TÉCNICA Nº 7/2022/CGIS/DTI-INSS, de 25/08/2022

CONCLUSÃO

40. Ante o exposto, se almeja ter restado evidenciado o empenho do Instituto no sentido de ampliar seus níveis de maturidade, técnico e tecnológico na área de segurança cibernética.

41. Assim, recomenda-se urgentemente à Presidência e demais Diretorias do INSS, assim como à Dataprev, em suas respectivas alçadas e sem prejuízo de todo o pontuado no decorrer da presente Nota Técnica, bem como nos documentos e normas referenciados:

I - implantação da exigência de certificado digital A3 para acesso aos sistemas do INSS por usuários externos, estagiários e terceirizados;

II - maximizar a priorização para a contratação de serviço de diretório, proteção contra ameaças e atualização do parque computacional;

III - desativação/migraçaõ ou, no mínimo, reforço da autenticação para acesso aos sistemas legados, notadamente CV3 e Prisma;

IV - revisão do PDSI visando dar encaminhamento às medidas propostas nesta Nota

Técnica, sobretudo aquelas decorrentes da Ação Técnica Interinstitucional;

V - pactuação de cronograma junto à Dataprev que permita a consecução do objetivo acima.

42. Ante o exposto, encaminhe-se:

I - no âmbito desta DTI:

a) Coordenação-Geral de Infraestrutura e Segurança em TI;

b) Coordenação-Geral de Dados e Sistemas de Informação;

c) Coordenação de Governança e Planejamento em TI

II - no âmbito do INSS:

a) Presidente;

b) Chefe de Gabinete da Presidência;

c) Diretora de Orçamento, Finanças e Logística;

d) Diretor de Governança, Planejamento e Inovação;

e) Diretor de Benefícios;

f) Diretor de Gestão de Pessoas;

g) Auditor-Geral;

h) Corregedor-Geral;

i) Procuradoria Federal Especializada;

j) Superintendentes Regionais;

III - em âmbito externo ao INSS:

a) Coordenação-Geral de Inteligência Previdenciária e Trabalhista (CGINT) do Ministério do Trabalho e Previdência;

b) Dataprev;

c) Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov);

d) Advocacia-Geral da União;

e) Departamento de Polícia Federal (mediante alinhamento com DIGOV/INSS, DIRBEN/INSS e CGINT/MTP).

43. Em tempo, **requer-se aos destinatários discrição no tratamento destas informações, observada a estrita necessidade de conhecer,** por força do disposto no Art. 15 do DECRETO Nº 10.748, DE 16 DE JULHO DE 2021:

> Art. 15. As informações específicas sobre os incidentes cibernéticos e sobre as configurações e características técnicas de ativos de informação de cada órgão ou entidade da administração pública federal direta, autárquica e fundacional são consideradas imprescindíveis à **segurança da sociedade e do Estado**.
>
> § 1º As informações de que trata o caput **somente poderão ser acessadas por profissionais autorizados** pelas autoridades responsáveis pelos ativos de informação dos órgãos ou das entidades da administração pública federal direta, autárquica e fundacional.

Brasília/DF, 7 de outubro de 2022.

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 07/10/2022, às 18:41, 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 **8737069** e o código CRC **ECF8B3B3**.

Referência: Processo nº 19955.102272/2022-14 SEI nº 8737069

INSTITUTO NACIONAL DO SEGURO SOCIAL

Superintendência Regional Sudeste II

DESPACHO

Superintendência Regional Sudeste II, em 10/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se da Nota Técnica nº 9/2022/DTI-INSS, que destina-se a prestar contas das atividades desenvolvidas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS, em seguimento ao exposto na NOTA TÉCNICA Nº 1/2021/CGIN/DTI-INSS (4651370), de 13/09/2021, em decorrência, sobretudo, do recebimento do DESPACHO Nº 314/2022/GMTP-MTP, de 11/08/2022 (8536675), oriundo do Gabinete do Sr. Ministro de Estado do Trabalho e Previdência.

2. Ciente nesta data dos termos do supracitado documento.

3. Restitua-se à Diretoria de Tecnologia da Informação para prosseguimento.

THIAGO ALBERTONI PRATA

Superintendência Regional Sudeste II

INSTITUTO NACIONAL DO SEGURO SOCIAL

Superintendência Regional Sudeste III

DESPACHO

Superintendência Regional Sudeste III, em 10/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Ciente quanto às manifestações da Diretoria de Benefícios e Relacionamento com o Cidadão e da Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos da Diretoria de Tecnologia da Informação - DTI (8823583).

2. Encerra-se o processo nesta unidade.

CAIO MAIA FIGUEIREDO

Superintendente

Superintendência Regional Sudeste III

Documento assinado eletronicamente por **CAIO MAIA FIGUEIREDO**, **Superintendente Regional Sudeste III**, em 10/10/2022, às 17:33, 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 **9265088** e o código CRC **5D8A52EE**.

INSTITUTO NACIONAL DO SEGURO SOCIAL

Presidência
Gabinete

DESPACHO

Gabinete, em 10/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDERAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Ciente e de acordo com os termos da Nota Técnica - NT nº 9/2022/DTI-INSS (8737069).

2. Considerando-se os encaminhamentos propostos no item 42 da referida NT e já providenciados pela Diretoria de Tecnologia da Informação - DTI, conforme se constata na movimentação do processo ora em análise, restitua-se à DTI para efetivo envio das informações pertinentes aos destinatários informados no inciso III do mesmo item 42, e após concluam-se os autos neste Gabinete.

SIDNEI CICERO COTTET

Chefe de Gabinete da Presidência

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação
Coordenação-Geral de Dados e Sistemas de Informação

DESPACHO

Coordenação-Geral de Dados e Sistemas de Informação, em 10/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se da Nota Técnica nº 9/2022/DTI-INSS, que destina-se a prestar contas das atividades desenvolvidas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS, em seguimento ao exposto na NOTA TÉCNICA Nº 1/2021/CGIN/DTI-INSS (4651370), de 13/09/2021, em decorrência, sobretudo, do recebimento do DESPACHO Nº 314/2022/GMTP-MTP, de 11/08/2022 (8536675), oriundo do Gabinete do Sr. Ministro de Estado do Trabalho e Previdência.
2. Ciente nesta data dos termos do supracitado documento.
3. Restitua-se à DTI

ISRAEL EDUARDO ZEBULON MARTINS DE SOUZA

Coordenador Geral de Dados e Sistemas de Informação

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Gestão de Pessoas

DESPACHO

Diretoria de Gestão de Pessoas, em 11/10/2022

Ref.: Processo nº 19955.102272/2022-14

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS

1. Trata-se da Nota Técnica nº 9/2022/DTI-INSS (8737069), que destina-se a prestar contas das atividades desenvolvidas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS, em seguimento ao exposto na Nota Técnica nº 1/2021/CGIN/DTI-INSS (4651370), de 13/09/2021, em decorrência, sobretudo, do recebimento do DESPACHO Nº 314/2022/GMTP-MTP, de 11/08/2022 (8536675), oriundo do Gabinete do Sr. Ministro de Estado do Trabalho e Previdência.

2. Ciente das informações contidas no supracitado documento.

3. Encaminhe-se às Coordenações-Gerais de Gestão de Pessoas (CGGP); de Centralização do Regime Próprio de Previdência da União (CGC-RPPU); e de Educação, Desenvolvimento e Carreiras (CGEDUC) para conhecimento.

JOBSON DE PAIVA SILVEIRA SALES

Diretor de Gestão de Pessoas

INSTITUTO NACIONAL DO SEGURO SOCIAL

Superintendência Regional Norte/Centro-Oeste

DESPACHO

Superintendência Regional Norte/Centro-Oeste, em 11/10/2022

Ref.: Processo nº 19955.102272/2022-14

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Ciente.

2. Trata-se de **NOTA TÉCNICA Nº 9/2022/DTI-INSS** (8737069), que discorre sobre as ações implementadas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS, em seguimento ao exposto na NOTA TÉCNICA Nº 1/2021/CGIN/DTI-INSS (4651370), de 13/09/2021, em decorrência, sobretudo, do recebimento do DESPACHO Nº 314/2022/GMTP-MTP, de 11/08/2022 (8536675), oriundo do Gabinete do Sr. Ministro de Estado do Trabalho e Previdência.

3. Feitas estas considerações, restituímos os autos à **COBEN-SRNCO**, em prosseguimento, para ciência e manifestação.

ANDRÉ PAULO FÉLIX FIDELIS

Superintendente Regional Norte/Centro-Oeste

SRNCO - Superintendência Regional Norte/Centro-Oeste
Setor de Autarquias Sul Q. 4
Asa Sul
Brasília - DF, 70297-400

INSTITUTO NACIONAL DO SEGURO SOCIAL

Auditoria-Geral

DESPACHO

Auditoria-Geral, em 11/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se do DESPACHO Nº 314/2022/GMTP-MTP (SEI 8536675), oriundo do Ministério de Trabalho e Previdência, cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, proveniente da Polícia Federal, comunicando a ocorrência de prováveis fraudes massivas contra o INSS.

2. Os autos foram encaminhados a esta Auditoria-Geral, sem indicação de providências, pela Diretoria de Tecnologia da Informação (DTI) por meio da NOTA TÉCNICA Nº 9/2022/DTI-INSS, de 07/10/2022 (SEI 8737069), que discorre "acerca da implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS".

3. Incumbiu-me o Auditor-Geral de encaminhar o presente processo à **Coordenação-Geral de Auditoria em Gestão Interna (CGAGIN)** para conhecimento e, caso haja, manifestação acerca da existência de eventuais recomendações emitidas pela Auditoria-Geral afetas ao tema "Segurança da Informação" ainda pendentes de implementação pela Gestão e que possam contribuir com os esforços de aperfeiçoamento de segurança cibernética da Autarquia já sinalizados no âmbito da referida Nota Técnica.

CÉSAR AUGUSTO MORAIS COSTA

Coordenador-Geral de Planejamento e Avaliação da Auditoria

Documento assinado eletronicamente por **CESAR AUGUSTO MORAIS COSTA**, **Analista do Seguro Social**, em 11/10/2022, às 09:19, 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 **9269185** e o código CRC **5DB87D02**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 9269185

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Governança, Planejamento e Inovação

DESPACHO

Diretoria de Governança, Planejamento e Inovação, em 11/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Discorre acerca da implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS.

1. Trata-se da Nota Técnica nº 9/2022/DTI-INSS (SEI nº 8737069), a qual destina-se a prestar contas das atividades desenvolvidas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS, em seguimento ao exposto na NOTA TÉCNICA Nº 1/2021/CGIN/DTI-INSS (4651370), de 13/09/2021, em decorrência, sobretudo, do recebimento do DESPACHO Nº 314/2022/GMTP-MTP, de 11/08/2022 (8536675), oriundo do Gabinete do Sr. Ministro de Estado do Trabalho e Previdência.

2. Encaminhe-se à Coordenação-Geral de Governança e Gerenciamento de Riscos - CGGOV e à Coordenação-Geral de Conformidade - CGCONF para conhecimento dos termos da Nota Técnica supracitada e providências que julgar cabíveis.

ALEXANDRE GUIMARÃES

Diretor de Governança, Planejamento e Inovação

Documento assinado eletronicamente por **ALEXANDRE GUIMARAES**, **Diretor(a) de Governança, Planejamento e Inovação**, em 11/10/2022, às 11:40, 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 **9272311** e o código CRC **EEEED73D**.

INSTITUTO NACIONAL DO SEGURO SOCIAL

Superintendência Regional Sudeste I

DESPACHO

Superintendência Regional Sudeste I, em 11/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDERAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se do DESPACHO Nº 314/2022/GMTP-MTP (SEI 8536675), oriundo do Ministério de Trabalho e Previdência, cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, proveniente da Polícia Federal, comunicando a ocorrência de prováveis fraudes massivas contra o INSS.

2. Os autos foram encaminhados a esta Superintendência Regional, sem indicação de providências, pela Diretoria de Tecnologia da Informação (DTI) por meio da NOTA TÉCNICA Nº 9/2022/DTI-INSS, de 07/10/2022 (SEI 8737069), que discorre "acerca da implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS".

3. Diante da relevância das informações elencadas na Nota Técnica nº 9/2022 DTI-INSS de 07/10/2022 sugiro que seja dado conhecimento à Coordenação de Gestão de Benefício;

4. À COBEN com trânsito pelo gabinete da Superintendência Regional Sudeste para ciência, manifestações e concordância.

FRANCISCO JOSÉ FORTE BARSOTTI

Assessor Técnico Especializado

Analista do Seguro Social

Gabinete da Superintendência Regional Sudeste I em 11/10/2022

1. Ciente e de acordo

VANDERLEI BARBOSA DOS SANTOS

SUPERINTENDENTE REGIONAL SUDESTE I

Documento assinado eletronicamente por **FRANCISCO JOSE FORTE BARSOTTI**, **Analista do Seguro Social**, em 11/10/2022, às 11:18, 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 **VANDERLEI BARBOSA DOS SANTOS**, **Superintendente Regional Sudeste I**, em 11/10/2022, às 12:45, 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 **9273422** e o código CRC **498E79C3**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 9273422

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Gestão de Pessoas
Coordenação-Geral de Educação, Desenvolvimento e Carreiras

DESPACHO

Coordenação-Geral de Educação, Desenvolvimento e Carreiras, em 11/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS

1. Trata-se da Nota Técnica nº 9/2022/DTI-INSS (SEI nº 8737069), a qual destina-se a prestar contas das atividades desenvolvidas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS, em seguimento ao exposto na NOTA TÉCNICA Nº 1/2021/CGIN/DTI-INSS (4651370), de 13/09/2021, em decorrência, sobretudo, do recebimento do DESPACHO Nº 314/2022/GMTP-MTP, de 11/08/2022 (8536675), oriundo do Gabinete do Sr. Ministro de Estado do Trabalho e Previdência.

2. Ciente das informações contidas no documento supracitado.

3. Encaminhe-se à Coordenação de Formação e Aperfeiçoamento e à Coordenação de Carreiras para conhecimento dos termos da Nota Técnica supracitada e providências que julgar cabíveis.

SANDRA CRISTINA CARDOSO DE SOUZA LUNA
Coordenadora-Geral de Educação, Desenvolvimento e Carreiras

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Gestão de Pessoas
Coordenação-Geral de Gestão de Pessoas

DESPACHO

Coordenação-Geral de Gestão de Pessoas, em 11/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS

1. Trata-se da Nota Técnica nº 9/2022/DTI-INSS (8737069), que destina-se a prestar contas das atividades desenvolvidas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS, em seguimento ao exposto na Nota Técnica nº 1/2021/CGIN/DTI-INSS (4651370), de 13/09/2021, em decorrência do recebimento do DESPACHO Nº 314/2022/GMTP-MTP, de 11/08/2022 (8536675), oriundo do Gabinete do Sr. Ministro de Estado do Trabalho e Previdência, que encaminhou o Ofício n° 146/2022/ASS/GAB/PF (8536675) à Presidência deste INSS para conhecimento e providências subsequentes.

2. Ciente da demanda e das providências tomadas pela Diretoria de Tecnologia da Informação.

3. Encaminhe-se o presente expediente s à COGEF, COLEMP, DGPI e DGCAF para ciência com destaque para a necessidade de discrição no tratamento das informações tratadas.

ANELIZIA GONÇALVES RODRIGUES

Coordenadora-Geral de Gestão de Pessoas - Substituta

Documento assinado eletronicamente por **ANELIZIA GONCALVES RODRIGUES**, **Coordenador(a)-Geral de Gestão de Pessoas Substituto(a)**, em 19/10/2022, às 19:38, 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 **9280250** e o código CRC **C05FD616**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 9280250

NOTA TÉCNICA Nº 9/2022/DTI-INSS

Diretoria De Tecnologia Da Informação <dti@inss.gov.br>

Ter, 11/10/2022 15:38

Para: Marcela Luci Formighieri <marcela.formighieri@dataprev.gov.br>;joao.augusto@presidencia.gov.br <joao.augusto@presidencia.gov.br>;ctir@ctir.gov.br <ctir@ctir.gov.br>;thiagomartins@agu.gov.br <thiagomartins@agu.gov.br>;macedo.nlkfm@pf.gov.br <macedo.nlkfm@pf.gov.br>;cassiana.csc@pf.gov.br <cassiana.csc@pf.gov.br>

Cc: JOAO RODRIGUES DA SILVA FILHO <joaorodrigues.filho@inss.gov.br>

1 anexos (2 MB)

NOTA TÉCNICA Nº 9_2022_DTI-INSS.pdf;

Prezados(as), boa tarde.

Com vistas ao atendimento de Despacho oriundo do Gabinete da Presidência deste Instituto Nacional do Seguro Social - INSS, Processo SEI 19955.102272/2022-14, esta Diretoria de Tecnologia da Informação - DTI, elaborou e traz ao conhecimento a **NOTA TÉCNICA Nº 9/2022/DTI-INSS**, que discorre acerca da implementação de medidas de segurança cibernética no âmbito do INSS.

O documento destina-se a prestar contas das atividades desenvolvidas pela área de Segurança da Informação do INSS, em decorrência, sobretudo, do recebimento do DESPACHO Nº 314/2022/GMTP-MTP, de 11/08/2022, proveniente do Gabinete do Sr. Ministro de Estado do Trabalho e Previdência.

De ordem do Diretor de Tecnologia da Informação, Sr. João Rodrigues da Silva Filho, segue a referida Nota Técnica, em anexo.

Gentileza nos confirmar o recebimento.

Atenciosamente,

--

Ana Lúcia Araújo Beserra

Analista de TI – 3204562

Apoio DTI

Teresina – PI

Teams | (86) 99806-7503

INSTITUTO NACIONAL DO SEGURO SOCIAL

Superintendência Regional Nordeste

DESPACHO

Superintendência Regional Nordeste, em 13/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se do DESPACHO Nº 314/2022/GMTP-MTP (SEI 8536675), oriundo do Ministério de Trabalho e Previdência, cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, proveniente da Polícia Federal, comunicando a ocorrência de prováveis fraudes massivas contra o INSS.

2. Os autos foram encaminhados a esta Superintendência Regional, sem indicação de providências, pela Diretoria de Tecnologia da Informação (DTI) por meio da NOTA TÉCNICA Nº 9/2022/DTI-INSS, de 07/10/2022 (SEI 8737069), que discorre "acerca da implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS".

3. Diante da relevância das informações elencadas na Nota Técnica nº 9/2022 DTI-INSS de 07/10/2022, encaminha-se à Coordenação de Gestão de Benefício - COBEN/SRNE para ciência, manifestações e concordância.

PAULA CALAZANS DE ARAÚJO TELES GOMES
Assistente da Superintendência Regional Nordeste

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Governança, Planejamento e Inovação
Coordenação-Geral de Governança e Gerenciamento de Riscos

DESPACHO

Coordenação-Geral de Governança e Gerenciamento de Riscos, em 14/10/2022

Ref.: 19955.102272/2022-14

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se de demanda recebida da Diretoria de Benefícios e relacionamento com o Cidadão proveniente da Coordenação Geral de Inteligência Previdenciária e Trabalhista versando sobre procedimentos de supostas reativações indevidas processadas em benefícios.

2. Considerando o teor do Despacho CGMOB (8575180) e NOTA TÉCNICA Nº 9/2022/DTI-INSS (8737069), informamos ciência e encaminhamos à DIGOV.

BRUNO BATISTA BARRETO
Coordenador-Geral de Governança e Gerenciamento de Riscos

Documento assinado eletronicamente por **BRUNO BATISTA BARRETO**, **Coordenador(a)-Geral de Governança e Gerenciamento de Riscos**, em 14/10/2022, 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 **9320853** e o código CRC **301C4085**.

INSTITUTO NACIONAL DO SEGURO SOCIAL
Diretoria de Governança, Planejamento e Inovação

MINUTA DE OFÍCIO SEI Nº 9320949/2022/DIGOV-INSS

Brasília, 14 de outubro de 2022.

A Sua Excelência o Senhor Ministro de Estado
JOSÉ CARLOS OLIVEIRA
Ministro do Trabalho e Previdência

Assunto: Resposta ao e-mail recebido em 15/08/2022 com assunto "ENC: Concessão de Aposentadoria constante no Processo SEI 19955.102272/2022-14

Referência: Caso responda este Ofício, indicar expressamente o Processo nº 19955.102272/2022-14.

Excelentíssimo Senhor Ministro do Trabalho e Previdência,

1. Em resposta ao e-mail datado de 12 de agosto de 2022 com o assunto "ENC: Concessão de Aposentadoria." que faz referência ao Ofício nº 146/2022/ASS/GAB/PF, de 18 de julho de 2022, temos o que segue.

2. O Ofício versa sobre a ocorrência de prováveis fraudes massivas contra o INSS, em tese, na reativação fraudulenta de benefícios, trazendo ainda que análises iniciais apontam para a massiva utilização indevida de senhas de servidores do INSS nos processos de reativação, informando a necessidade de providências urgentes em termos de segurança das credenciais dos servidores e beneficiários e/ou bloqueio cautelar desse tipo de atividade, além de solicitar prioridade máxima à CGINT para que a Polícia Federal adote as providências de suas atribuições.

3. Assim sendo, o processo foi encaminhado às áreas de negócio para manifestação que apresentam as informações abaixo.

4. A Coordenação-Geral de Monitoramento e Cobrança Administrativa de Benefícios - CGMOB informa que desenvolve atividades de monitoramento com o propósito de identificar procedimentos fraudulentos de reativações de benefícios possibilitando a atuação na cessação em bloco de benefícios que respondam a cenários de fraudes, além de apresentar o que citamos:

> 5. Atualmente está em andamento o tratamento de reativações indevidas operadas nos meses de junho e julho de 2022 - que estão inseridas dentro dos 60 dias mencionados no ofício da Direção da Polícia Federal. Por essa razão procedemos o batimento da lista de benefícios com aquela que é resultado dessa atividade de monitoramento. Aproveita-se para registrar de que o tema aqui trazido já vem sendo tratado no âmbito da Autarquia, por meio de processos SEI, ocasião em que foram identificados outros benefícios que passaram por semelhante modus operandi fraudulento.
>
> 6. Por meio desses processos vem sendo registradas as constatações e demandadas as providências no âmbito da Coordenação Geral de Monitoramento e Cobrança de Benefícios, sendo identificado que a fraude massiva contra o INSS tem acontecido por diversos meios como reativações indevidas de benefícios de espécies extintas, com renda mensal elevada e, em sua grande maioria, cessados por óbitos dos titulares; inclusão de empréstimos consignados, reativações de benefícios, e utilização de documentos fraudulentos; usurpação de acesso de servidores da Autarquia em diversas Unidades e a concessão indevida de benefícios com uso das referidas matrículas; fraudes em reativações de benefícios de pensão por morte concedidos irregularmente.

> 7. Impende salientar que os primeiros casos envolvendo reativações massivas de benefícios de forma irregular chegaram ao conhecimento desta Coordenação a partir do segundo semestre de 2021, ocasião em que as primeiras notas técnicas foram elaboradas no sentido de demandar cessações/suspensões em lote nos benefícios, desde então vem sendo tratado com as áreas competentes possíveis alterações nas regras de negócio das reativações nos sistemas de manutenção.
>
> 8. Assim como em trabalhos anteriores empreendidos pela Coordenação de Ações Corretivas e Cobrança Administrativa de Benefícios, o trabalho envolvendo o cenário das reativações se vale de algumas premissas que permitiram a identificação das fraudes e portanto conferem assertividade aos achados, elencamos de forma exemplificativa algumas dessas premissas:
>
> a) Volumetria de reativações concentradas em credenciais;
>
> b) Comportamento anômalo da credencial em relação a região geográfica e atividades diárias;
>
> c) Inexistência de instrução formal que justifique o procedimento;
>
> d) Variação do volume de reativação como um todo;
>
> e) Tempo decorrido entre a cessação e a reativação.
>
> (...)
>
> 11. A partir de uma primeira análise identificamos que 9.677 casos estão dentro do cenário mapeado pela CGMOB e foram alvo de atuação para cessar em lote e bloquear pagamentos que eventualmente ainda não tenha sido efetivados, por meio de demanda registrada na DATAPREV em 24/08/2022 que é a Empresa de Tecnologia responsável por estas ações junto ao INSS, cabendo, mas uma vez destacar, que a abertura da demanda é a conclusão do trabalho em desenvolvimento e já mencionado no presente relatório, isto é, tem como ponto de partida a ação de monitoramento que já vem sendo desenvolvida pela Coordenação.
>
> (...)

5. A CGMOB informa ainda resumo dos achados na ação de monitoramento, como o volume de reativações, locais de onde partiram as operações, locais de lotação dos servidores, locais de manutenção dos benefícios reativados após a reativação, características dos pagamentos emitidos após as reativações e distribuição das reativações por espécie, no item 19 do Despacho (8575180), bem como os casos identificados exclusivamente no mês 08/2022, nos itens 20 a 23 do referido Despacho e providências adotadas no item 24 do Despacho citado.

6. Em conseguinte, a Divisão de Manutenção de Direitos - DMAND se manifestou no Despacho (8802692) conforme citado abaixo.

> 4. Visando coibir as tentativas de fraude, foi criada a demanda DM.100261 em 11.07.2022, com o objetivo de alterar as regras de reativação de benefícios, para que os pagamentos sejam direcionados para cartão magnético, pois desta forma, para o recebimento dos valores gerados, há necessidade de identificação junto ao órgão pagador e implementada crítica (OPERAÇÃO NÃO PERMITIDA - MR TIPO 5) quando a alteração for feita para tipo de microrregião "5" (que só paga benefício em conta corrente), obrigando o servidor a efetuar a troca para microrregião tipo 1 ou 4, que destinará aquele benefício, obrigatoriamente, para cartão magnético.
>
> 5. Continuando, no comando efetuado no SIBE PU, quando finalizada a demanda, o sistema passará a exigir também, preenchimento de novo campo (NÚMERO DA TAREFA DO GERENCIADOR DE TAREFAS - GET) que após comunicação sistêmica verificará a existência ou não de tarefa de reativação no GET; .

7. Não obstante, a Diretoria de Tecnologia da Informação - DTI se manifestou através da NOTA TÉCNICA Nº 9/2022/DTI-INSS (8737069), apresentando a emissão de Notas Técnicas e outras providências que apresentamos um destaque nos próximos itens deste Ofício.

8. A DTI apresenta o histórico do registro, apuração, tratamento e resposta de incidentes cibernéticos, ações junto à Advocacia-Geral da União - AGU, ações junto à Dataprev e medidas preventivas estruturantes que elencamos abaixo:

a) instituição da Política de Segurança da Informação (POSIN-INSS);

b) instituição da Norma de Concessão de Acesso Lógico (NCAL-INSS);

c) instituição da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR-INSS);

d) Norma de Uso da Internet;

e) Programa Contínuo de conscientização em Segurança da Informação;

f) Squad Seg da Secretaria de Governo Digital (SGD);

g) Saneamento da base de usuários, duplo fator de autenticação (2FA) para acesso às aplicações parceiras ao GERID;

h) Solução de correio, comunicação, colaboração e produtividade;

i) mapeamento e gestão de "robôs" legítimos;

j) melhoria no monitoramento;

k) alocação de empregados públicos da Dataprev cedidos ao INSS em ações de SIC; e

l) Plano Diretor de Segurança da Informação (PDSI).

9. Além do exposto acima, a DTI apresenta recomendações contidas no item 4.6 da referida Nota Técnica.

10. Quanto a irregularidades em benefícios, a DTI apresenta informações diversas que são distribuídas nos tópicos abaixo:

I - Dispositivos de rede clandestinos;

II - Operação tarrafa;

III - Plano Diretor de Segurança da Informação (PDSI);

a) Implantação de sistema de registro de incidentes de segurança;

b) Construção de *dashboard* de segurança de TI;

c) Apresentação de diagnóstico de Segurança de TI nas reuniões de CTGD e do CEGOV;

d) Implantação de serviço de operação de infraestrutura e segurança em TI;

e) Assumir a gestão das políticas de segurança de TI na rede de dados do INSS;

f) Implantação de solução de proteção de *endpoints;*

g) Atualização do parque computacional do INSS;

h) Assumir a gestão das políticas de segurança do serviço de diretório do INSS;

i) Monitoramento da proteção de *endpoints;*

j) Monitoramento da rede de dados do INSS;

k) Monitoramento de Serviço de Diretório;

l) Monitoramento de ativos de TI;

m) Capacitação da equipe de segurança nas disciplinas de segurança de TIC e nas soluções disponibilizadas;

n) Revisão do processo de tratamento de incidentes de Segurança de TIC - interação com Dataprev;

o) Revisão do processo de tratamento de incidentes de Segurança de TIC - investigação interna;

p) Revisão do processo de tratamento de incidentes de Segurança de TIC - encaminhamentos externos;

q) Implantação de obrigatoriedade de certificado digital para acesso a sistemas críticos e para acesso à VPN;

r) Migração de aplicações hospedadas em infraestrutura própria para ambiente de nuvem;

s) Implantação de *hardening* nos servidores Linux de propriedade do INSS;

t) Implantação de política de backup nas aplicações hospedadas em infraestrutura própria; e

u) Execução de plano de ações operacionais de prevenção a incidentes de Segurança de TIC.

IV - Fortalecimento institucional e normativo da área de segurança da informação;

V - Ação técnica integrada interinstitucional;

VI - Ações complementares;

VII - Resultados; e

VIII - Restrição Orçamentária.

11. Destaca-se ainda as 26 medidas descritas na citação do item 9 da NOTA TÉCNICA Nº 6/2022/DTIR/COIM/CGIS/DTI-INSS (9151371) contida no item 30.2 da Nota Técnica referida no item 7 deste Ofício, e as 33 medidas da citação do item 11 da NOTA TÉCNICA Nº 6/2022/DTIR/COIM/CGIS/DTI-INSS (9151371) contida no item 30.2 da Nota Técnica referida no item 7 deste Ofício.

12. Segue em anexo o Despacho da CGMOB (8575180) e a Nota Técnica da DTI (8737069).

13. Por todo exposto, encaminhamos ao Ministério do Trabalho e Previdência.

Atenciosamente,

GUILHERME GASTALDELLO PINHEIRO SERRANO

Presidente

Documento assinado eletronicamente por **BRUNO BATISTA BARRETO**, **Diretor(a) de Governança, Planejamento e Inovação Substituto(a)**, em 14/10/2022, às 21:09, 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 **9320949** e o código CRC **99A6E2D2**.

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Governança, Planejamento e Inovação

DESPACHO

Diretoria de Governança, Planejamento e Inovação, em 14/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se de demanda recebida da Diretoria de Benefícios e relacionamento com o Cidadão proveniente da Coordenação Geral de Inteligência Previdenciária e Trabalhista versando sobre procedimentos de supostas reativações indevidas processadas em benefícios.

2. Considerando a temática e as manifestações no Despacho CGINT (8536675), Despacho CGMOB (8575180) e a NOTA TÉCNICA Nº 9/2022/DTI-INSS (8737069), sugerimos o envio de ofício com o teor da Minuta de Ofício (9320949).

3. Ao Gabinete da Presidência.

BRUNO BATISTA BARRETO

Diretor de Governança, Planejamento e Inovação - Substituto

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Benefícios e Relacionamento com o Cidadão
Coordenação-Geral de Pagamento de Benefícios
Coordenação De Pagamentos e Gestão De Benefícios
Divisão De Agentes Pagadores

DESPACHO

Divisão De Agentes Pagadores, em 14/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se do DESPACHO Nº 314/2022/GMTP-MTP, oriundo do Ministério de Trabalho e Previdência cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, no qual a Polícia Federal comunica a ocorrência de prováveis fraudes massivas contra o INSS e que veio a esta Divisão para prestar os esclarecimentos, abaixo transcritos, levantados pela Coordenação-Geral de Monitoramento e Cobrança Administrativa de Benefícios - CGMOB (ID 8575180).

2. Em atendimento a alínea "b", do inciso I, do item 25:

b) Dados sobre os pagamentos emitidos para os benefícios envolvidos (incluindo situação do crédito, instituição destinatária, modalidade de pagamento).

3. Cadastramos a demanda DM.101434 e a Dataprev atendeu à solicitação conforme planilha de relação de créditos (ID nº 9322104).

4. Encaminhe-se à CGPAG.

REINALDO CARLOS BARROSO DE ALMEIDA

Chefe da Divisão de Agentes Pagadores

Documento assinado eletronicamente por **REINALDO CARLOS BARROSO DE ALMEIDA**, **Técnico do Seguro Social**, em 14/10/2022, às 17:14, 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 **9322276** e o código CRC **828273AC**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 9322276

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Orçamento, Finanças e Logística

DESPACHO

Diretoria de Orçamento, Finanças e Logística, em 14/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: Diretoria de Tecnologia da Informação.

Ass.: Implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS.

1. Trata-se da Nota Técnica nº 9/2022/DTI-INSS (SEI nº 8737069), oriundo da Diretoria de Tecnologia da Informação, em que presta contas das atividades desenvolvidas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS.

2. Ciente do contido na supracitada Nota Técnica.

3. Pelo exposto, encaminhe-se à Coordenação-Geral de Recursos Logísticos - CGRLOG e Coordenação-Geral de Licitações e Contratos - CGLCO para verificar se há alguma providência a ser tomada, no âmbito de competência desta Diretoria, em relação às recomendações citadas no item 41, incisos I e II, observada a ressalva contida no item 43, quanto à discrição no tratamento das informações.

LARISSA ANDRADE MORA

Diretora de Orçamento, Finanças e Logística

INSTITUTO NACIONAL DO SEGURO SOCIAL

Superintendência Regional Sul

DESPACHO

Superintendência Regional Sul, em 14/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.:

1. Trata-se do DESPACHO Nº 314/2022/GMTP-MTP (SEI 8536675), oriundo do Ministério de Trabalho e Previdência, cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, proveniente da Polícia Federal, comunicando a ocorrência de prováveis fraudes massivas contra o INSS.

2. Os autos foram encaminhados a esta Superintendência Regional, sem indicação de providências, pela Diretoria de Tecnologia da Informação (DTI) por meio da NOTA TÉCNICA Nº 9/2022/DTI-INSS, de 07/10/2022 (SEI 8737069), que discorre "acerca da implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS"

3. Feitas as considerações, encaminhe-se à COBEN/SRSUL para ciência, manifestações.

KATHIA MARIA MOREIRA BRAGA

Superintendência Regional Sul

INSTITUTO NACIONAL DO SEGURO SOCIAL

Superintendência Regional Nordeste
Coordenação de Gestão de Benefícios

DESPACHO

Coordenação de Gestão de Benefícios, em 15/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: Serviço Público Federal MJSP - Polícia Federal.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se do **DESPACHO Nº 314/2022/GMTP-MTP**, oriundo do Ministério de Trabalho e Previdência, cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, proveniente da Polícia Federal, comunicando a ocorrência de prováveis fraudes massivas contra o INSS, conforme documento SEI 8536675.

2. Ciente.

3. Encaminhe-se à equipe da SERMOB da SR NE para análise e providências.

RODRIGO DIAS MEIRELES

Coordenador de Gestão de Benefícios da SR NE

Documento assinado eletronicamente por **RODRIGO DIAS MEIRELES**, **Coordenador(a) de Gestão de Benefícios**, em 17/10/2022, às 07:26, 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 **9323615** e o código CRC **BF5C0B8E**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 9323615

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Gestão de Pessoas
Coordenação-Geral de Centralização do Regime Próprio de Previdência da União

DESPACHO

Coordenação-Geral de Centralização do Regime Próprio de Previdência da União, em 17/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se do **DESPACHO Nº 314/2022/GMTP-MTP**, oriundo do Ministério de Trabalho e Previdência, cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, proveniente da Polícia Federal, comunicando a ocorrência de prováveis fraudes massivas contra o INSS.

2. Conforme trecho extraído do Despacho 8536675:

> O referido expediente relata que chegou ao conhecimento daquela Polícia Federal, por meio de análises de dados e via canal de inteligência, da ocorrência de prováveis fraudes massivas contra o INSS e que tais informes foram transmitidos, via canal de inteligência, à Coordenação-GeraI de Inteligência/MTP e às inteligências dos principais bancos afetados.
>
> Segundo o relato, as fraudes consistiriam, em tese, na reativação fraudulenta de benefícios, gerando pagamento de retroativos próximo ao limite de cinco anos, o que perfaria um valor estimado médio em torno de R$70.000,00, por beneficio fraudulentamente reativado.
>
> O Ofício complementa que análises iniciais apontam para a massiva utilização indevida de senhas de servidores do INSS nesses processos de reativação, o que demandaria, segundo preceitua, providências urgentes em termos de segurança das credenciais dos servidores e beneficiários e/ou bloqueio cautelar desse tipo de atividade.

3. Ciente ao contido no SEI 8536675.

4. Visto se tratar de matéria do Regime Geral de Previdência Social - RGPS, fundo que não se encontra nas competências dessa Coordenação Geral, concluímos o presente processo nesta unidade.

OLACIR LUCHETTA

Coordenação - Geral de Centralização do Regime Próprio de Previdência da União.

Documento assinado eletronicamente por **OLACIR LUCHETTA**, **Coordenador(a)-Geral de Centralização do Regime Próprio de Previdência da União**, em 20/10/2022, às 14:09, 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 **9335700** e o código CRC **658006BD**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 9335700

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Benefícios e Relacionamento com o Cidadão
Coordenação-Geral de Pagamento de Benefícios

DESPACHO

Coordenação-Geral de Pagamento de Benefícios, em 17/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se do DESPACHO Nº 314/2022/GMTP-MTP, oriundo do Ministério de Trabalho e Previdência cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, no qual a Polícia Federal comunica a ocorrência de prováveis fraudes massivas contra o INSS e que veio a esta Divisão para prestar os esclarecimentos, abaixo transcritos, levantados pela Coordenação-Geral de Monitoramento e Cobrança Administrativa de Benefícios - CGMOB (ID 8575180).

2. Ciente e de acordo com o despacho DAGPG (9322276).

3. Restitui-se à DIRBEN para prosseguimento.

VERÔNICA BRITO DE OLIVEIRA

Assistente Administrativo - CGPAG

INGRID AMBROZIO CAMILO

Coordenação-Geral de Pagamento de Benefícios.

INSTITUTO NACIONAL DO SEGURO SOCIAL

Superintendência Regional Sul
Coordenação de Gestão de Benefícios

DESPACHO

Coordenação de Gestão de Benefícios, em 17/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se do **DESPACHO Nº 314/2022/GMTP-MTP**, oriundo do Ministério de Trabalho e Previdência, cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, proveniente da Polícia Federal, comunicando a ocorrência de prováveis fraudes massivas contra o INSS, conforme documento SEI 8536675.

2. Cientes.

3. Ao Serviço de Monitoramento de Benefícios da Superintendência Regional Sul - SERMOB, para ciência, análise e manifestações cabíveis.

LÍVIA DA SILVA DE JESUS

ESTAGIÁRIA DE DIREITO - COBEN

ANDRÉ LUIS PONTES

COORDENADOR DE GESTÃO DE BENEFÍCIOS DA SUPERINTENDÊNCIA REGIONAL SUL

---

seil assinatura eletrônica

Documento assinado eletronicamente por **ANDRE LUIS PONTES**, **Técnico do Seguro Social**, em 18/10/2022, às 10:51, 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 **9339239** e o código CRC **06A5DACE**.

INSTITUTO NACIONAL DO SEGURO SOCIAL

Auditoria-Geral
Coordenação-Geral De Auditoria em Gestão Interna

DESPACHO

Coordenação-Geral De Auditoria em Gestão Interna, em 18/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se do DESPACHO Nº 314/2022/GMTP-MTP (SEI 8536675), oriundo do Ministério de Trabalho e Previdência, cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, proveniente da Polícia Federal, comunicando a ocorrência de prováveis fraudes massivas contra o INSS e da NOTA TÉCNICA Nº 9/2022/DTI-INSS, de 07/10/2022 (SEI 8737069), encaminhada à Auditoria-Geral pela Diretoria de Tecnologia da Informação (DTI) para conhecimento.

2. À Coordenação de Auditoria em Gestão Interna para providências, tendo em vista o disposto no item 3 do Despacho AUDGER (SEI 9269185).

MARIA INÊS DE MORAIS CARVALHO

Coordenadora-geral de Auditoria em Gestão Interna

Documento assinado eletronicamente por **MARIA INES DE MORAIS CARVALHO**, **Analista do Seguro Social**, em 18/10/2022, 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 **9351099** e o código CRC **302C7BAA**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 9351099

INSTITUTO NACIONAL DO SEGURO SOCIAL

Auditoria-Geral
Coordenação-Geral De Auditoria em Gestão Interna
Coordenação de Auditoria em Gestão Interna

DESPACHO

Coordenação de Auditoria em Gestão Interna, em 18/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Ciente do Despacho CGAGIN SEI nº 9351099.

2. Encaminha-se à DAGIN3, em observação ao item 2 do Despacho SEI 9351099 (CGAGIN), adote providências cabíveis.

ANA LUISA DA SILVA ROCHA

Coordenadora de Auditoria em Gestão Interna

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Gestão de Pessoas
Coordenação-Geral de Gestão de Pessoas
Divisão de Gerenciamento e Produção de Informações

DESPACHO

Divisão de Gerenciamento e Produção de Informações, em 20/10/2022

Referência: Processo nº 19955.102272/2022-14.

Interessada: MJSP - Polícia Federal.

Assunto: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Processo encaminhado a esta Divisão de Gerenciamento e Produção de Informações - DGPI em 19/10/2022 por meio do Despacho CGGP 9280250, da Coordenação-Geral de Gestão de Pessoas - CGGP.

2. Ciente do inteiro teor do Processo, e em especial do contido na Nota Técnica 9 (8737069), de 07/10/2022, da Diretoria de Tecnologia da Informação - DTI, que menciona **as atribuições e a participação da área de Gestão de Pessoas** no controle de acesso lógico Institucional.

3. Oportunamente, e enquanto partícipe junto à DTI em diversas rotinas e outras demandas pontuais de saneamento lógico de usuários internos do INSS, esta DGPI destaca os artigos 5º e 7º da Norma de Controle de Acesso Lógico - NCAL/INSS, instituída pela Portaria Conjunta DTI/DIRAT/INSS nº 3, de 01/04/2022:

> "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. 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." (Grifos nossos)

4. Em relação ao teor do artigo 5º da NCAL/INSS de 2022, esta DGPI tem atuado junto à área de TI do INSS e à DATAPREV **desde a publicação** da Política de Controle de Acesso Lógico - PCAL/INSS, **de 2014** (revogada pela NCAL/INSS de 2020), com o fornecimento de arquivos semanais de usuários internos do quadro de Pessoal **em atividade** do INSS cujos registros são extraídos do módulo extrator do SIAPE e em layout acordado com a DATAPREV, para saneamento automatizado do Sistema de Controle de Acessos - SCA, que gerencia usuários com acesso a **Sistemas Legados do INSS**.

5. Também sobre o artigo 5º da NCAL/INSS de 2022, esta DGPI tem fornecido à DATAPREV em rotina semanal e **desde 2020** (conforme NCAL/INSS de 2020, revogada pela NCAL/INSS vigente) relatórios gerados com dados do módulo extrator do SIAPE, de usuários internos **com ocorrência de desligamento** junto ao quadro de Pessoal do INSS para saneamento da **base do OpenLDAP**.

6. Posteriormente foram demandadas pela DTI à DGPI outras rotinas semanais, com fornecimento de relatórios específicos para saneamento lógico de usuários internos do INSS das categorias **Estagiário e Terceirizado em aplicações parceiras ao GERID**, sendo que, relativamente aos Terceirizados, os dados são obtidos junto à área de contratos da Diretoria de Orçamento Finanças e Logística e suas projeções, em razão da atribuição de gestão daquela área, e uma vez que os Terceirizados não compõem o quadro de Pessoal do INSS para validação por meio do SIAPE.

7. As rotinas dos itens 5 e 6 estão em fase de automação pela DATAPREV, abrangidas por demandas citadas na Nota Técnica 9 (8737069) da DTI.

8. Ainda, desde a implantação do Office365 (que dá acesso ao e-mail Outlook) como ferramenta Institucional esta DGPI também tem atuado junto à DTI em rotinas semanais, mensais e pontuais de saneamento de usuários licenciados.

9. Relativamente ao artigo 7º da NCAL/INSS, de 2022, esta DGPI **centraliza**, por meio de fluxo diário instituído desde 2020, as solicitações das unidades responsáveis em âmbito nacional relativas a usuários internos do quadro de Pessoal do INSS e usuários internos Terceirizados do INSS, para desativação, credenciamento, reativação ou alteração de contas de rede e de contas do Office365, nos termos do Ofício SEI Conjunto Circular nº 1/2022/DGP/DIROFL/DTI/INSS, de 22/06/2022, que revogou os Ofícios Circulares 56 e 62/2020/DGPA-INSS, e aprimorou o fluxo implementado à época.

10. O relato dos itens anteriores visa reforçar a **importância das atribuições afetas à área de Gestão de Pessoas previstas em normas de controle de acesso lógico Institucional desde 2014**, pelo que encaminho o feito ao conhecimento da Coordenação-Geral de Gestão de Pessoas - CGGP, com sugestão de encaminhamento à ciência pela Diretoria de Gestão de Pessoas - DGP.

MARLUCY INES TEIXEIRA DE AZEVEDO
Chefe da Divisão de Gerenciamento e Produção de Informações

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Gestão de Pessoas
Coordenação-Geral de Gestão de Pessoas

DESPACHO

Coordenação-Geral de Gestão de Pessoas, em 20/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS

1. Trata-se da Nota Técnica nº 9/2022/DTI-INSS (8737069), que destina-se a prestar contas das atividades desenvolvidas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS, em seguimento ao exposto na Nota Técnica nº 1/2021/CGIN/DTI-INSS (4651370), de 13/09/2021, em decorrência do recebimento do DESPACHO Nº 314/2022/GMTP-MTP, de 11/08/2022 (8536675), oriundo do Gabinete do Sr. Ministro de Estado do Trabalho e Previdência, que encaminhou o Ofício n° 146/2022/ASS/GAB/PF (8536675) à Presidência deste INSS para conhecimento e providências subsequentes.

2. Ciente do disposto no Despacho DGPI (9390950).

3. Encaminhe-se, conforme sugerido, à DGP para conhecimento.

ANELIZIA GONÇALVES RODRIGUES

Coordenadora-Geral de Gestão de Pessoas - Substituta

Documento assinado eletronicamente por **ANELIZIA GONCALVES RODRIGUES**, **Coordenador(a)-Geral de Gestão de Pessoas Substituto(a)**, em 21/10/2022, às 17:07, 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 **9392443** e o código CRC **6B418B42**.

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Gestão de Pessoas

DESPACHO

Diretoria de Gestão de Pessoas, em 24/10/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se da Nota Técnica nº 9/2022/DTI-INSS (8737069), que destina-se a prestar contas das atividades desenvolvidas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS, em seguimento ao exposto na Nota Técnica nº 1/2021/CGIN/DTI-INSS (4651370), de 13/09/2021, em decorrência do recebimento do DESPACHO Nº 314/2022/GMTP-MTP, de 11/08/2022 (8536675), oriundo do Gabinete do Sr. Ministro de Estado do Trabalho e Previdência, que encaminhou o Ofício n° 146/2022/ASS/GAB/PF (8536675) à Presidência deste INSS para conhecimento e providências subsequentes.

2. Ciente do disposto no Despacho DGPI (9390950).

3. Sem mais, arquiva-se.

LEONAM FERNANDES DA SILVA

Servidor - Matrícula 1348584

INSTITUTO NACIONAL DO SEGURO SOCIAL

Auditoria-Geral
Coordenação-Geral De Auditoria em Gestão Interna
Coordenação de Auditoria em Gestão Interna
Divisão de Auditoria em Gestão Interna III

DESPACHO

Divisão de Auditoria em Gestão Interna III, em 03/11/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDERAL MJSP - POLÍCIA FEDERAL.

1. Ciente do despacho (SEI 9351961), que solicitou adoção de providências com base no item 2 do despacho SEI 9351099 (CGAGIN).

2. Contudo, de acordo com nova ordem da CAGIN, encaminhamos o processo à DAGIN I para tratativas ao feito.

- **Alex Pires Moreira**
- DAGIN III- Substituto

Documento assinado eletronicamente por **ALEX PIRES MOREIRA**, **Chefe de Divisão de Auditoria em Gestão Interna Substituto(a)**, em 03/11/2022, às 14:50, 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 **9528917** e o código CRC **04E77BD7**.

INSTITUTO NACIONAL DO SEGURO SOCIAL

Auditoria-Geral
Coordenação-Geral De Auditoria em Gestão Interna
Coordenação de Auditoria em Gestão Interna
Divisão De Auditoria em Gestão Interna I

DESPACHO

Divisão De Auditoria em Gestão Interna I, em 07/11/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se de notícia de supostas "fraudes massivas" em benefícios, encaminhada pela Direção Geral da Polícia Federal ao Ministro de Estado do Trabalho e Previdência, por meio do Ofício nº 146/2022/ASS/GAB/PF, de 18/07/2022 - SEI 8536675, enviada a esta Divisão de Auditoria em Gestão Interna I – DAGIN I para tratativas, por meio do Despacho DAGIN3 9528917.

2. Diante do relatado pela Direção Geral da Polícia Federal ao Ministro do Trabalho e Previdência, as fraudes em investigação ocorreram por meio de reativação de benefícios, gerando pagamentos de retroativos aos últimos cinco anos, perfazendo um valor estimado em média de R$ 70.000,00 por benefício fraudulento reativado. Informa, ainda, o Diretor da Polícia Federal, que as análises iniciais apontam para a "*massiva utilização indevida de senhas de servidores do INSS nesses processos de reativação, o que demandaria, segundo preceitua, providências urgentes em termos de segurança das credenciais dos servidores e beneficiários e/ou bloqueio cautelar desse tipo de atividade*".

3. A Coordenação-Geral de Monitoramento e Cobrança Administrativa de Benefícios – CGMOB do INSS, por meio do Despacho SEI 8575180, informa que "*a fraude massiva contra o INSS tem acontecido por diversos meios como reativações indevidas de benefícios de espécies extintas, com renda mensal elevada e, em sua grande maioria, cessados por óbitos dos titulares; inclusão de empréstimos consignados, reativações de benefícios, e utilização de documentos fraudulentos; usurpação de acesso de servidores da Autarquia em diversas Unidades e a concessão indevida de benefícios com uso das referidas matrículas; fraudes em reativações de benefícios de pensão por morte concedidos irregularmente*." Relata ainda, a CGMOB que a área tem conhecimento de casos dessa natureza desde o segundo semestre de 2021 e que a partir de então tiveram início demandas para cessação/suspensão de benefícios em lote e tratativas de demandas junto à DATAPREV para retornar os benefícios identificados como irregulares para a situação de cessados e assim mitigar os efeitos das ações ilícitas.

4. Conforme o Despacho DMAND 8802692 e o Despacho DTIR 8823583, verifica-se que outras áreas técnicas do INSS também se manifestaram apresentando diagnósticos e demandas para tratar as irregularidades, bem como, medidas de tratamento para evitar que tais situações voltem a ocorrer.

5. A Diretoria de Tecnologia da Informação – DTI, por meio da Nota Técnica nº 09 DTI-INSS – SEI 8737069, encaminhada ao INSS, Ministério do Trabalho e Previdência e à Polícia Federal, discorre acerca da implementação de medidas de segurança cibernética no âmbito do INSS, registrando o cenário em que se encontra a área de segurança de informação do Instituto.

6. A Auditoria-Geral, em 07/11/2019, enviou à Presidência do INSS, a Nota de Auditoria nº 1/AUDGER/INSS - SEI 9567868, com o objetivo de alertar os gestores quanto a irregularidades a serem imediatamente sanadas, identificadas no curso da Auditoria Especial nº 5540/2019, que evidenciavam a existência de benefícios sendo reativados por meio de matrículas de estagiários ou mesmo ex-estagiários e ainda, detectou-se contas bancárias abertas com documentos falsos, por meio das quais houve recebimento de pagamentos de benefícios.

7. Ainda, na Nota de Auditoria, destacou-se o caso em que foi atribuído à estagiária perfis de acesso aos sistemas corporativos SIBE, GET e SAT em várias unidades (APS) do INSS, em desacordo com o §3º da Portaria nº 2.194/PRES/INSS, de 15 de agosto de 2019, o que permitiu a realização de operações nas bases de dados, com a matrícula de estagiária. Esta usuária, à época, constava lotada na Procuradoria Seccional em Manaus e foram identificadas para sua matrícula, reativações de benefícios em diversas APS (BA, SP, RJ, SC, CE, MT, PE, RS). O montante dessas reativações desde janeiro de 2017 foi calculado, na época, em R$ 3.086.463,42.

8. Dentro do processo de auditoria, sob o acompanhamento da Coordenação-Geral de Auditoria em Gestão Interna – CGAGIN, Coordenação de Auditoria em Gestão Interna - CAGIN e Divisões (DAGIN I, II e III), estão em andamento o monitoramento de recomendações exaradas em decorrência da publicação de diversos trabalhos de auditoria realizados sobre o tema "Segurança da Informação", conforme tabela a seguir:

Quadro I – Resumo recomendações em monitoramento – Segurança da Informação

#	Tarefa e-Aud	Recomendação de Auditoria	Unidade	Providências	Categoria	Data Limite	Avaliação dos Resultados
1	1123896	Revisar "Mapa de Gerenciamento de Riscos" do atual Contrato, ou do Contrato que venha a substitui-lo, para inclusão de riscos de incidentes relacionados à recepção e ao processamento dos arquivos do SIRC.	DTI	Evidenciada a implementação da recomendação por meio da apresentação de Mapa de Gerenciamento de Riscos, onde foi incluído o "Risco nº 13 - Interrupção dos serviços e as respectivas ações de tratamento", elaborado nos autos do processo da nova contratação de Prestação de Serviços de Tecnologia da Informação de Serviços Previdenciários, celebrado entre o INSS e a Dataprev.	Controles Internos	23/03/2022	Implementada

2	1123911	Exigir da contratada a elaboração dos Planos de Contingência previstos no Contrato em vigência, ou do Contrato que venha substitui-lo.	DTI	A unidade auditada informa que nos termos da nova contratação entre o INSS e a Dataprev consta a previsão de estabelecimento de planos de contingência. Após a avaliação da manifestação, a unidade de auditoria enviou posicionamento reiterando a implementação da recomendação, com alteração da data limite para 17/07/2022, tendo em vista que não foi apresentado pela área, o plano de contingência devidamente formalizado.	Controles Internos	17/07/2022	Em Implementação
3	1123916	Instaurar Processo Administrativo de apuração do descumprimento contratual relativo aos Contratos nº(s) 49/2018 e 20/2020, e aplicar as respectivas sanções, quando cabíveis, em relação às seguintes infrações cometidas: a) Ausência de planos de contingência; b) Desmobilização de equipamento servidor sem anuência do contratante; c) Ausência de comunicação tempestiva de incidente de indisponibilidade e instabilidade referente aos serviços contratados.	DTI	A unidade auditada apresenta manifestação contendo informações da adoção de providências as quais não têm relação com o teor da recomendação emitida no relatório de auditoria.	Controles Internos	21/02/2022	Em Implementação

4	1123922	Instaurar Processo Administrativo para apuração de danos ao erário causado pela contratada referente a pagamento indevido de benefícios em decorrência de falha na prestação do serviço, promovendo a respectiva ação de ressarcimento, quando for o caso.	DTI	A unidade auditada apresenta manifestação contendo informações da adoção de providências as quais não têm relação com o teor da recomendação emitida no relatório de auditoria.	Reposição de bens e valores	17/07/2022	Em Implementação
5	801015	Promover gestão junto à Dataprev para a elaboração de plano de recuperação de serviços, conforme disposição contratual, visando mitigar o risco de descontinuidade do processo de pagamento de benefícios (Constatação associada: subitem III.5).	DTI	Aguarda-se a aprovação de PDSI pelo CEGOV e publicação do referido documento.	Gestão de Riscos	30/11/2022	Em implementação
6	801016	Estabelecer com a Dataprev Acordo de Níveis Mínimos de Serviços para o sistema SISPAGBEN, em cumprimento a cláusula contratual. (Constatação associada: subitem III.6)	DTI	Com a assinatura do contrato nº 20/2020 em novembro, novo ANS foi aprovado o qual será utilizado para avaliar os níveis de serviços contratados, entre eles o SISPAGBEN.	Ajustes de objetos	31/12/2020	Implementada

7	850931	Cessar os acessos de estagiários ao sistema ConsigWeb, por este não ser essencial ao desempenho das atividades relacionadas à área de formação profissional do estagiário, conforme resposta da área auditada à Solicitação de Auditoria nº 34.825/2019.	DTI	A unidade auditada informa, em 30/09/2022, que a partir da publicação da Portaria PRES/INSS nº 1.474/2022, o acesso dos estagiários ao sistema CONSIGCWEB passou a ser autorizado formalmente pelo INSS. A manifestação está em análise pela unidade de auditoria.	Gestão de Riscos	13/07/2022	Em implementação
8	850932	Implantar um mecanismo de trava no sistema GERID que impeça a atribuição de perfil de acesso destinado a servidor para uso por estagiário.	DTI	A unidade auditada apresenta pedido de prorrogação de prazo para atendimento da recomendação até 30/11/2022, a qual foi acatada pela unidade de auditoria.	Gestão de Riscos	30/11/2022	Em implementação
9	850933	Promover a atualização contínua das bases de dados de usuários do LDAP, bem como a integração com a base de dados dos servidores do Instituto (SIAPE-INSS), conforme preceitua os itens 3.2 e 3.3 da PCAL – Resolução nº 413/PRES/INSS, de 20 de maio de 2014.	DTI	A unidade auditada apresenta pedido de prorrogação de prazo para atendimento da recomendação até 30/11/2022, o qual foi concedido pela unidade de auditoria.	Governança	30/11/2022	Em implementação
10	850934	Implementar mecanismo eletrônico e automatizado no GERID para notificação dos gestores de acesso e usuários visando informá-los a respeito dos cadastros e das permissões de acessos concedidas.	DTI	A área informa que a demanda (DM087164) correspondente ao atendimento desta recomendação será entregue até 11/11/2022.	Controles Internos	31/08/2022	Em implementação

11	850935	Disponibilizar solução tecnológica (módulo de auditoria) que permita à DTI, ou partes afins, consultar informações (logs) que demonstrem as ações efetuadas pelos usuários nos sistemas GERID e ConsigWeb.	DTI	A unidade auditada apresenta pedido de prorrogação de prazo para atendimento da recomendação até 30/11/2022, o qual foi concedida pela unidade de auditoria.	Gestão de Riscos	30/11/2022	Em implementação
12	850937	Garantir que o sistema GERID esteja aderente à nova Norma de Controle de Acesso (NCAL), que se encontra em fase de aprovação e publicação, quanto às regras estabelecidas para emissão de credenciais de acesso lógico no âmbito do INSS.	DTI	A unidade auditada apresenta pedido de prorrogação de prazo para atendimento da recomendação até 31/10/2022, o qual foi concedida pela unidade de auditoria.	Gestão de Riscos	31/10/2022	Em implementação
13	850939	Reavaliar o processo de autenticação de acesso ao GERID de forma que o mesmo esteja alinhado ao item 6.1.7 da Norma Complementar nº 07/IN01/DSIC/GSIPR, quanto a utilização de autenticação de multifatores.	DTI	A unidade auditada apresenta pedido de prorrogação de prazo para atendimento da recomendação. A unidade de auditoria prorrogou até 15/11/2022.	Gestão de Riscos	31/08/2022	Em implementação
14	850940	Revisar os requisitos de validação de senha entre os sistemas GERID e o LDAP, a fim de garantir as sincronizações com as devidas permissões.	DTI	A área informa que adotou providências para atendimento da recomendação. A unidade de auditoria está analisando as informações e documentos enviados para emitir o posicionamento referente aos documentos apresentados.	Gestão de Riscos	30/11/2022	Em implementação

15	850941	Implantar Equipe de Tratamento de Incidentes de Redes (ETIR), conforme Norma Complementar nº 08/IN 01/DSIC/GSI-PR/2010 para que os eventuais incidentes de segurança da informação sejam reportados ao CTIR-GOV.	DTI	A área informa o atendimento da recomendação ocorrido com a implantação da ETIR (Resolução nº 11/2020).	Governança	06/10/2020	Implementada
16	850942	Adequar a forma de autenticação e acesso de usuários no servidor ao nível de criticidade dos dados.	DTI	A unidade auditada apresenta pedido de prorrogação de prazo para atendimento da recomendação até 30/12/2022.	Gestão de Riscos	31/12/2021	Em implementação
17	850943	Avaliar periodicamente se o nível de segurança da aplicação e das plataformas que a sustentam são compatíveis com o risco que a administração definir como aceitável.	DTI	A área informa que adotou providências para atendimento da recomendação. A unidade de auditoria está analisando as informações e documentos enviados para emitir o posicionamento referente aos documentos apresentados.	Controles Internos	06/12/2021	Em implementação
18	850945	Suspender perfil alteração de dados nos sistemas corporativos de todos os usuários que não sejam servidores ativos.	DTI	A área apresenta pedido de prorrogação de prazo para atendimento da recomendação até 30/11/2022, o qual foi concedido pela unidade de auditoria.	Controles Internos	29/07/2022	Em implementação
19	850946	Providenciar troca de senhas de acesso de todos os usuários.	DTI	A área informa a alteração do período de troca de senha dos usuários para 90 dias.	Gestão de Riscos	09/07/2020	Implementada

20	917306	Adequar o cadastramento de demandas de extrações de dados, de modo a identificar e justificar os casos em que há tratamento de dados e os casos em que há extração de dados na forma bruta. (Achado nº 01)	DTI	A área apresenta pedido de prorrogação de prazo para atendimento da recomendação até 12/2021, a qual foi concedida pela unidade de auditoria.	Controles Internos	31/12/2021	Em implementação
21	917320	Apurar responsabilidade pelo atraso no cumprimento da Cláusula Sexta-B do 8º Termo Aditivo ao Contrato nº 49/2018, uma vez que não houve disponibilização de ferramenta suportada em Big Data que permitisse consultas e extrações a Datalake. (Achado nº 02)	DTI	A área informa que adotou providências para atendimento da recomendação. A unidade de auditoria está analisando as informações e documentos enviados para emitir o posicionamento referente aos documentos apresentados.	Controles internos	31/10/2021	Em implementação
22	917323	Reavaliar as demandas de extração de dados desde o início da vigência do 8º Termo Aditivo ao Contrato nº 49/2018, de modo a identificar as seguintes situações: a) extrações nas quais os dados deveriam ser tratados pela Dataprev, justificando a necessidade em cada caso; e b) extrações de dados tratados que foram solicitadas por não ter sido ainda disponibilizada, pela Dataprev, a ferramenta de Big Data mencionada no contrato e que permitiria extração de dados brutos e tratamento pela DTI. Nestes casos, providenciar o ressarcimento dos valores pagos. (Achado nº 03)	DTI	A área não apresentou documentos e/ou informações suficientes para comprovar a implementação da recomendação, de modo que a o posicionamento da unidade de auditoria foi pela reiteração da recomendação.	Controles Internos	30/10/2021	Em implementação

23	1011692	Disciplinar os procedimentos de prospecção de soluções de TIC para planejamento das contratações em observância às diretrizes da IN SGD/ME n° 01/2019 e do Acórdão n° 2.059/2017 – Plenário, visando garantir isonomia, impessoalidade e lisura dos procedimentos licitatórios.	DTI	Para atendimento da recomendação, a área informa a publicação da Portaria DTI/INSS nº 60, de 17/10/2021, que em conjunto com a Portaria e nº 60, de 18/10/2021, resultaram no posicionamento de atendimento da recomendação proferido pela unidade de auditoria.	Governança/Controles Internos	17/12/2021	Implementada
24	1011699	Desconsiderar os produtos resultantes de amostras do objeto já realizadas sem processo de planejamento de contratação instruído previamente.	DTI	A unidade auditada informou que todos os produtos resultantes das amostras foram desconsiderados e não serão aproveitados em contratações futuras.	Cessação de objetos	26/09/2021	Implementada

25	1011711	Regulamentar os procedimentos para realização de prospecção de produtos e testes de soluções de TIC no âmbito do INSS, observando as diretrizes da Política de Segurança da Informação - POSIN, incluindo avaliação de riscos e medidas para garantir proteção adequada das informações produzidas e custodiadas pelo INSS.	DTI	Com a publicação da Portaria DTI/INSS Nº 60, de 17 de outubro de 2021, a qual regulamentou os procedimentos para realização de prospecção de produtos e testes de soluções de TIC no âmbito do INSS, observando as diretrizes da Política de Segurança da Informação - POSIN, incluindo avaliação de riscos e medidas para garantir proteção adequada das informações produzidas e custodiadas pelo INSS, a recomendação foi implementada.	Governança/Gestão de Riscos	17/12/2021	Implementada

Fonte: Elaboração própria, com base em informações extraídas em 04/11/2022 do sistema e-Aud.

9. Assim, com base nas extrações realizadas do sistema e-Aud em 04/11/2022, foram implementadas 07 (sete) das 25 (vinte e cinco) recomendações propostas nos trabalhos de auditoria desde o ano de 2020, restando pendentes a implementação 18 (dezoito) recomendações, sob a responsabilidade da Diretoria de Tecnologia da Informação e Inovação - DTI.

10. Quanto às ações priorizadas pela Auditoria-Geral para o exercício de 2022, estão em andamento trabalhos de auditoria com o objetivo de avaliar processos de trabalho que incluem o tema de segurança de informação, dentre os quais, podemos destacar na área de gestão interna: **A avaliação do planejamento de aquisições relacionadas a TIC**, que dentre os riscos priorizados para realização de testes substantivos e de controle estão os seguintes: (i) a subjetividade no método de quantificação de demandas, (ii) a desconsideração de riscos existentes na contratação e (iii) a ausência de registro e acompanhamento das ações de tratamento; a ação de auditoria com o tema **Gestão de demandas por soluções de TIC** está na fase de planejamento dos trabalhos de auditoria e tem por objetivo, em especial, avaliar a gestão dos fluxos das demandas derivadas dos objetos dos Contratos nº 20/2020 e 30/2022 (DATAPREV); e a ação de auditoria de **Avaliação da aderência do Sistema de Atendimento (SAT)**, desenvolvido e mantido pela Empresa de Tecnologia e Informações da Previdência (DATAPREV), às normas e às boas práticas de segurança da informação, visando mitigar riscos de ataques cibernéticos e vazamento de dados.

11. Do exposto, conclui-se que as irregularidades informadas pela autoridade policial e as medidas de tratamento sugeridas pelas áreas técnicas e auditoria interna para tais inconformidades são de conhecimento da alta administração do INSS.

12. Dessa forma, propõe-se o encaminhamento do presente processo à CGABEN, Coordenações e Divisões de Auditoria em matéria de benefícios para pronunciamento, considerando a criticidade e materialidade envolvidas.

13. Feitas as considerações, encaminhe-se à CAGIN e CGAGIN em prosseguimento.

DAIANNY CRISTINA ZÁU DE OLIVEIRA NASCIMENTO

Chefe da Divisão de Auditoria em Gestão Interna I - Substituta

Documento assinado eletronicamente por **DAIANNY CRISTINA ZAU DE OLIVEIRA NASCIMENTO**, **Chefe de Divisão de Auditoria em Gestão Interna Substituto(a)**, em 08/11/2022, às 08:45, 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 **9565151** e o código CRC **42FCE0C8**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 9565151

AUDITORIA-GERAL

Nota de Auditoria nº: 1/AUDGER/INSS
Destinatário: Presidência do INSS
Unidade Auditada: Instituto Nacional do Seguro Social - INSS

Brasília, 7 de novembro de 2019.

Senhor Presidente,

Está em execução a Auditoria Especial nº 5540/2019 - Incidente de Segurança no Sistema ConsigWeb (protocolo nº 35014.003358/2019-38), cujo propósito é avaliar os controles relativos a segurança da informação. A ação teve início a partir de relatório produzido pela Diretoria de Tecnologia da Informação e Inovação – DTI dando notícia de falhas de segurança em sistemas e em computadores da rede do INSS. Estas falhas incluem concessão de acesso a sistemas de benefícios a pessoas não pertencentes ao quadro de servidores, roubo de identidade virtual (login/senha), robôs sendo executados clandestinamente para capturar dados, dentre outros apontamentos.

Durante o curso da auditoria, porém, foram constatados fatos com gravidade e abrangência suficientes para justificar atuação imediata da Administração, razão pela qual medidas estão sendo recomendadas por meio desta Nota de Auditoria.

Há evidências de benefícios sendo reativados por meio de matrículas de estagiários ou mesmo ex-estagiários. Além disso, uma instituição financeira informou ter detectado contas bancárias abertas com documentos falsos, por meio das quais houve recebimento de pagamentos de benefícios.

Em consulta realizada ao serviço de diretório LDAP em 05/11/2019, constatou-se que foram atribuídos à estagiária de matrícula nº 3.074.229 perfis de acesso aos sistemas corporativos SIBE, GET e SAT em várias unidades (APS) do INSS, o que permite realizar operações nas bases de dados. Esta usuária consta lotada na Procuradoria Seccional em Manaus.

Uma fragilidade evidenciada é que o Sistema de Gerenciamento de Identidade (GERID) permite conceder acesso a estagiário com perfil capaz de realizar operações de inclusão, alteração e exclusão de dados, em desacordo com o §3º da Portaria nº 2.194/PRES/INSS, de 15 de agosto de 2019.

No caso em análise tem-se o seguinte conjunto de fatos:

- Perfil concedido à estagiária no sistema GERID capaz de promover alterações nas bases de dados de benefícios.
- A servidora que consta como cadastradora nega ter executado tal concessão do acesso, e sugere ter havido roubo de senha ou falha no registro.
- Desde agosto de 2019 não consta registro de frequência no SISREF da referida estagiária, bem como no SIAPE não há registro de pagamento.

Após identificação dos indícios de irregularidade acima citados, verificou-se que a mesma matrícula da ex-estagiária consta como responsável pela reativação de benefícios em diversas APS (BA, SP, RJ, SC, CE, MT, PE, RS). O montante dessas reativações desde janeiro de 2017 é de R$ 3.086.463,42.

Diante deste quadro, a Auditoria-Geral recomenda que sejam adotadas as seguintes providências imediatas, sem prejuízo de ações estruturantes de mais longo prazo:

1. Suspender perfil alteração de dados nos sistemas corporativos de todos os usuários que não sejam servidores ativos;
2. Providenciar troca de senhas de acesso de todos os usuários;
3. Limitar o número de concessores de acesso aos sistemas de benefícios a um usuário por GEX e um usuário por Superintendência, até que nova política de segurança seja planejada e implantada;

4. Reavaliar as reativações de benefícios realizadas por servidores inativos, cedidos e estagiários nos últimos três meses, devendo-se estender este período a depender dos fatos que vierem a ser encontrados.

5. Monitorar os pagamentos alternativos de benefícios (PAB).

A Auditoria Especial nº 5540/2019 - Incidente de Segurança no Sistema ConsigWeb segue sendo executada e o relatório final será oportunamente divulgado.

Respeitosamente,

WILLIAM GUEDES
Auditor-Geral

Documento assinado eletronicamente por **WILLIAM GUEDES**, **Auditor-Geral**, em 07/11/2019, às 16:59, 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 **0002187** e o código CRC **2ADBE587**.

INSTITUTO NACIONAL DO SEGURO SOCIAL

Auditoria-Geral
Coordenação-Geral De Auditoria em Gestão Interna
Coordenação de Auditoria em Gestão Interna

DESPACHO

Coordenação de Auditoria em Gestão Interna, em 08/11/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Refere-se a Despacho nº 314/2022/GMTP-MTP, oriundo do Ministério de Trabalho e Previdência cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, no qual a Polícia Federal comunica a ocorrência de prováveis fraudes massivas contra o INSS e da NOTA TÉCNICA Nº 9/2022/DTI-INSS, de 07/10/2022 (SEI 8737069), encaminhada à Auditoria-Geral pela Diretoria de Tecnologia da Informação (DTI) para conhecimento.

2.Dada ciência às informações registradas no Despacho DAGIN1(9567868) e na Nota de Auditoria AUDGER/INSS nº 01/2019, encaminha-se à CGAGIN em prosseguimento.

ANA LUISA DA SILVA ROCHA

Coordenadora de Auditoria em Gestão Interna - CAGIN

INSTITUTO NACIONAL DO SEGURO SOCIAL

Auditoria-Geral
Coordenação-Geral De Auditoria em Gestão Interna

DESPACHO

Coordenação-Geral De Auditoria em Gestão Interna, em 08/11/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Ciente.

2. Trata-se do DESPACHO Nº 314/2022/GMTP-MTP (SEI 8536675), oriundo do Ministério de Trabalho e Previdência, cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, proveniente da Polícia Federal, comunicando a ocorrência de prováveis fraudes massivas contra o INSS e da NOTA TÉCNICA Nº 9/2022/DTI-INSS, de 07/10/2022 (SEI 8737069), encaminhado a esta Unidade para que se informe eventuais recomendações emitidas pela Auditoria-Geral afetas ao tema "Segurança da Informação", pendentes de implementação.

3. A Divisão de Auditoria em Gestão Interna I, por meio do Despacho SEI nº 9565151, informou as recomendações emitidas nos trabalhos de auditoria concluídos e as ações de auditoria em curso, relacionadas à "Segurança da Informação".

4. Em atenção ao solicitado (item 3 do Despacho AUDGER 9269185), enumera-se, abaixo, as recomendações pendentes de implementação, referentes ao tema.

Quadro I – Recomendações pendentes de implementação, relacionadas ao tema Segurança da Informação.
Unidade responsável pelo atendimento: Diretoria de Tecnologia da Informação.

Tarefa e-Aud	Recomendação de Auditoria
1123911	Exigir da contratada a elaboração dos Planos de Contingência previstos no Contrato em vigência, ou do Contrato que venha substitui-lo.
1123916	Instaurar Processo Administrativo de apuração do descumprimento contratual relativo aos Contratos nº(s) 49/2018 e 20/2020, e aplicar as respectivas sanções, quando cabíveis, em relação às seguintes infrações cometidas: a) Ausência de planos de contingência; b) Desmobilização de equipamento servidor sem anuência do contratante; c) Ausência de comunicação tempestiva de incidente de indisponibilidade e instabilidade referente aos serviços contratados.

1123922	Instaurar Processo Administrativo para apuração de danos ao erário causado pela contratada referente a pagamento indevido de benefícios em decorrência de falha na prestação do serviço, promovendo a respectiva ação de ressarcimento, quando for o caso.
801015	Promover gestão junto à Dataprev para a elaboração de plano de recuperação de serviços, conforme disposição contratual, visando mitigar o risco de descontinuidade do processo de pagamento de benefícios (Constatação associada: subitem III.5).
850931	Cessar os acessos de estagiários ao sistema ConsigWeb, por este não ser essencial ao desempenho das atividades relacionadas à área de formação profissional do estagiário, conforme resposta da área auditada à Solicitação de Auditoria nº 34.825/2019.
850932	Implantar um mecanismo de trava no sistema GERID que impeça a atribuição de perfil de acesso destinado a servidor para uso por estagiário.
850933	Promover a atualização contínua das bases de dados de usuários do LDAP, bem como a integração com a base de dados dos servidores do Instituto (SIAPE-INSS), conforme preceitua os itens 3.2 e 3.3 da PCAL – Resolução nº 413/PRES/INSS, de 20 de maio de 2014.
850934	Implementar mecanismo eletrônico e automatizado no GERID para notificação dos gestores de acesso e usuários visando informá-los a respeito dos cadastros e das permissões de acessos concedidas.
850935	Disponibilizar solução tecnológica (módulo de auditoria) que permita à DTI, ou partes afins, consultar informações (logs) que demonstrem as ações efetuadas pelos usuários nos sistemas GERID e ConsigWeb.
850937	Garantir que o sistema GERID esteja aderente à nova Norma de Controle de Acesso (NCAL), que se encontra em fase de aprovação e publicação, quanto às regras estabelecidas para emissão de credenciais de acesso lógico no âmbito do INSS.
850939	Reavaliar o processo de autenticação de acesso ao GERID de forma que o mesmo esteja alinhado ao item 6.1.7 da Norma Complementar nº 07/IN01/DSIC/GSIPR, quanto a utilização de autenticação de multifatores.
850940	Revisar os requisitos de validação de senha entre os sistemas GERID e o LDAP, a fim de garantir as sincronizações com as devidas permissões.
850942	Adequar a forma de autenticação e acesso de usuários no servidor ao nível de criticidade dos dados.
850943	Avaliar periodicamente se o nível de segurança da aplicação e das plataformas que a sustentam são compatíveis com o risco que a administração definir como aceitável.

850945	Suspender perfil alteração de dados nos sistemas corporativos de todos os usuários que não sejam servidores ativos.
917306	Adequar o cadastramento de demandas de extrações de dados, de modo a identificar e justificar os casos em que há tratamento de dados e os casos em que há extração de dados na forma bruta. (Achado nº 01)
917320	Apurar responsabilidade pelo atraso no cumprimento da Cláusula Sexta-B do 8º Termo Aditivo ao Contrato nº 49/2018, uma vez que não houve disponibilização de ferramenta suportada em Big Data que permitisse consultas e extrações a Datalake. (Achado nº 02)
917323	Reavaliar as demandas de extração de dados desde o início da vigência do 8º Termo Aditivo ao Contrato nº 49/2018, de modo a identificar as seguintes situações:
	a) extrações nas quais os dados deveriam ser tratados pela Dataprev, justificando a necessidade em cada caso; e
	b) extrações de dados tratados que foram solicitadas por não ter sido ainda disponibilizada, pela Dataprev, a ferramenta de Big Data mencionada no contrato e que permitiria extração de dados brutos e tratamento pela DTI. Nestes casos, providenciar o ressarcimento dos valores pagos. (Achado nº 03)

Fonte: Sistema e-Aud. Dados extraídos em 04.11.2022.

5. Feitas as considerações, encaminhe-se à Auditoria-Geral.

MARIA INÊS DE MORAIS CARVALHO

Coordenadora-Geral de Auditoria em Gestão Interna

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Orçamento, Finanças e Logística
Coordenação-Geral de Recursos Logísticos

DESPACHO

Coordenação-Geral de Recursos Logísticos, em 12/12/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: Diretoria de Tecnologia da Informação.

Ass.: Implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS.

1. Trata-se da Nota Técnica nº 9/2022/DTI-INSS (SEI nº 8737069), oriunda da Diretoria de Tecnologia da Informação, em que presta contas das atividades desenvolvidas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS.

2. Encaminhe-se à Divisão de Despesas Operacionais e Suprimentos para conhecimento e pronunciamento a respeito dos encaminhamentos sugeridos pela Diretoria de Tecnologia da Informação na Nota Técnica supracitada.

MANUELLA ANDRADE P. DE S. SILVA

Coordenadora-Geral de Recursos Logísticos

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Governança, Planejamento e Inovação
Coordenação-Geral de Conformidade

DESPACHO

Coordenação-Geral de Conformidade, em 28/12/2022

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se do DESPACHO Nº 314/2022/GMTP-MTP (SEI 8536675), oriundo do Ministério de Trabalho e Previdência, cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, proveniente da Polícia Federal, comunicando a ocorrência de prováveis fraudes massivas contra o INSS e da NOTA TÉCNICA Nº 9/2022/DTI-INSS, de 07/10/2022 (SEI 8737069), encaminhado a esta Unidade para que se informe eventuais recomendações emitidas pela Auditoria-Geral afetas ao tema "Segurança da Informação", pendentes de implementação.

2. Encaminho para as Coordenação de de Avaliação e Análise de Conformidade e para a Coordenação de Proteção de Dados Pessoais para conhecimento.

KLEYBER OLIVEIRA SILVA
Coordenador Geral de Conformidade - Substituto

---

sei! assinatura eletrônica

Documento assinado eletronicamente por **KLEYBER OLIVEIRA SILVA**, **Coordenador(a) Geral de Conformidade - Substituto(a)**, em 29/12/2022, às 14:13, 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 **10146415** e o código CRC **8D3F84D4**.

INSTITUTO NACIONAL DO SEGURO SOCIAL

Superintendência Regional Sudeste I
Coordenação de Gestão de Benefícios

DESPACHO

Coordenação de Gestão de Benefícios, em 23/01/2023

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se do **DESPACHO Nº 314/2022/GMTP-MTP**, oriundo do Ministério de Trabalho e Previdência, cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, proveniente da Polícia Federal, comunicando a ocorrência de prováveis fraudes massivas contra o INSS, conforme documento SEI 8536675.

2. Encaminhe-se à equipe da Serviço de Monitoramento e Cobrança Administrativa - SERMOB da SRSE-I, para CIÊNCIA, análise e providências cabíveis.

MARCELLE SEKIYA

Coordenadora de Gestão de Benefícios SRSE-I

Documento assinado eletronicamente por **MARCELLE SEKIYA**, **Coordenador(a) de Gestão de Benefícios**, em 23/01/2023, às 17:49, 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 **10352541** e o código CRC **7218EA72**.

INSTITUTO NACIONAL DO SEGURO SOCIAL

Superintendência Regional Sudeste I
Coordenação de Gestão de Benefícios
Serviço de Monitoramento e Cobrança Administrativa de Benefícios

DESPACHO

Serviço de Monitoramento e Cobrança Administrativa de Benefícios, em 24/01/2023

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Fraudes massivas de reativações de benefícios

1. Trata-se do **DESPACHO Nº 314/2022/GMTP-MTP**, oriundo do Ministério de Trabalho e Previdência, cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, proveniente da Polícia Federal, comunicando a ocorrência de prováveis fraudes massivas contra o INSS, conforme documento SEI 8536675, encaminhado pela Coordenação de Gestão de Benefícios desta Superintendência Regional para ciência, análise e providência cabíveis.

2. As fraudes aqui narradas possuem *"modus operandi"* já investigado pela Autarquia. As reativações apontam para indício de fraude estrutural o qual já é objeto de ação conjunta entre CGINT, CGMOB, CGPAG e DTI e, portanto, não serão apurados de forma individualizada.

3. Este Serviço aguarda o resultado da ação interinstitucional que poderá indicar os responsáveis pelo dano ao erário e, se assim for a decisão da Autarquia, instaurar o procedimento de cobrança administrativa em matéria de benefícios em face daqueles que se beneficiaram dos valores pagos indevidamente.

4. Portanto, neste momento, conclui-se que não será necessário cadastrar demanda de apuração ou de Recuperação de Créditos, porque não existe justa causa para instauração dos procedimentos individualizados por ausência de autoria. Um procedimento apuratório no âmbito administrativo já é conduzido por equipe especializada da CACB e espera-se que, tão logo se tenha a qualificação daqueles que deram causa ao dano do erário ou se beneficiaram dos ilícitos apontados.

5. Registra-se ciência à demanda, sem providências neste momento e conclui-se o processo nesta unidade.

MARCELO DE MEDEIROS PEREIRA
Chefe do Serviço de Monitoramento e Cobrança Administrativa de Benefícios
Superintendência Regional Sudeste I

Documento assinado eletronicamente por **MARCELO DE MEDEIROS PEREIRA**, **Chefe de Serviço de Monitoramento e Cobrança Administrativa de Benefícios**, em 24/01/2023, às 23:03, 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 **10368456** e o código CRC **B6DA55A4**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 10368456

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Benefícios e Relacionamento com o Cidadão

DESPACHO

Diretoria de Benefícios e Relacionamento com o Cidadão, em 17/02/2023

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Fraudes massivas de reativações de benefícios.

1. Ciente.
2. Retorne à CACB para conhecimento e acompanhamento.

ANDRÉ PAULO FELIX FIDELIS

Diretor de Benefícios e Relacionamento com o Cidadão

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Orçamento, Finanças e Logística
Coordenação-Geral de Recursos Logísticos
Coordenação de Acompanhamento de Logística
Divisão de Despesas Operacionais e Suprimentos

DESPACHO

Divisão de Despesas Operacionais e Suprimentos, em 26/04/2023

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS.

1. Dada ciência do teor da Nota Técnica nº 9/2022/DTI-INSS (SEI nº 8737069), oriunda da Diretoria de Tecnologia da Informação, que presta contas das atividades desenvolvidas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS.

2. No que se refere ao Sistema de Gestão de Contratos - GCWEB, informamos que a autenticação de usuários se dá por meio do serviço de LDAP disponibilizado pela Dataprev, o mesmo protocolo utilizado pelo Sistema Eletrônico de Informações - SEI. Deste modo, podemos afirmar que esta Divisão já vem seguindo as recomendações de segurança oriundas da Diretoria de Tecnologia da Informação - DTI.

3. Ademais, reforçamos que estamos comprometidos em adotar as melhores práticas de desenvolvimento, a fim de proteger as informações e garantir a confidencialidade dos dados, não só do sistema GCWEB, mas também de seus usuários. Assim, permanecemos à disposição para colaborar com a DTI em quaisquer ações necessárias para garantir a segurança da rede do INSS.

4. Feitas as considerações, restitua-se à Coordenação-Geral de Recursos Logísticos, com trâmite pela Coordenação de Acompanhamento de Logística, para o que couber.

ODIRLEI SILVA SANTOS
Chefe de Divisão

Documento assinado eletronicamente por **ODIRLEI SILVA SANTOS**, **Chefe da Divisão de Despesas Operacionais e Suprimentos**, em 26/04/2023, às 16:57, conforme horário oficial de Brasília, com o emprego de certificado digital emitido no âmbito da ICP-Brasil, com fundamento no art. 6º, caput, do Decreto nº 8.539, de 8 de outubro de 2015 .
Nº de Série do Certificado: 29951104499641863274733934898

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 **11475410** e o código CRC **7B6F5CD0**.

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Orçamento, Finanças e Logística
Coordenação-Geral de Recursos Logísticos

DESPACHO

Coordenação-Geral de Recursos Logísticos, em 27/04/2023

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS.

1. Ciente e de acordo com o contido o despacho da Divisão de Despesas Operacionais e Suprimentos - DDOS (SEI nº).

2. À Diretoria de Orçamento, Finanças e Logística - DIROFL para conhecimento e, se de acordo, encaminhamento à Diretoria de Tecnologia da Informação - DTI.

ANTONIO HAMAD JUNIOR
Coordenador de Acompanhamento de Logística

MANUELLA ANDRADE P. DE S. SILVA
Coordenadora-Geral de Recursos Logísticos

Documento assinado eletronicamente por **MANUELLA ANDRADE PEREIRA DE SOUZA SILVA**, **Coordenador(a) Geral de Recursos Logísticos**, em 27/04/2023, às 05:45, 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 **ANTONIO HAMAD JUNIOR**, **Coordenador(a)**, em 27/04/2023, às 06:58, 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 **11477646** e o código CRC **99838DAA**.

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Orçamento, Finanças e Logística

DESPACHO

Diretoria de Orçamento, Finanças e Logística, em 17/05/2023

Ref.: Processo nº 19955.102272/2022-14.

Int.: Diretoria de Tecnologia da Informação.

Ass.: Implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS.

1. Trata-se da Nota Técnica nº 9/2022/DTI-INSS (SEI nº 8737069), oriundo da Diretoria de Tecnologia da Informação, em que presta contas das atividades desenvolvidas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS, no qual recomenda:

> 41. Assim, recomenda-se urgentemente à Presidência e demais Diretorias do INSS, assim como à Dataprev, em suas respectivas alçadas e sem prejuízo de todo o pontuado no decorrer da presente Nota Técnica, bem como nos documentos e normas referenciados:
>
> I- implantação da exigência de certificado digital A3 para acesso aos sistemas do INSS por usuários externos, estagiários e terceirizados;
>
> II - maximizar a priorização para a contratação de serviço de diretório, proteção contra ameaças e atualização do parque computacional;
>
> III - desativação/migraçaõ ou, no mínimo, reforço da autenticação para acesso aos sistemas legados, notadamente CV3 e Prisma;
>
> IV - revisão do PDSI visando dar encaminhamento às medidas propostas nesta Nota Técnica, sobretudo aquelas decorrentes da Ação Técnica Interinstitucional;
>
> V - pactuação de cronograma junto à Dataprev que permita a consecução do objetivo acima.

2. Conforme despacho DIROFL (SEI nº 9277897), de 14/10/2022, o processo foi remetido às Coordenações-Gerais de Recursos Logísticos - CGRLOG e de Licitações e Contratos - CGLCO para verificar se havia alguma providência a ser tomada, no âmbito de competência da Diretoria de Orçamento, Finanças e Logística - DIROFL, em relação às recomendações citadas no item 41, incisos I e II, observada a ressalva contida no item 43 da referida Nota Técnica, quanto à discrição no tratamento das informações.

3. A CGRLOG manifestou-se nos termos do despacho SEI nº 11477646, no qual ratifica o contido no despacho da Divisão de Despesas Operacionais e Suprimentos - DDOS (SEI nº 11475410), o qual informa:

> 2. No que se refere ao Sistema de Gestão de Contratos - GCWEB, informamos que a autenticação de usuários se dá por meio do serviço de LDAP disponibilizado pela Dataprev, o mesmo protocolo utilizado pelo Sistema Eletrônico de Informações - SEI. Deste modo, podemos afirmar que esta Divisão já vem seguindo as recomendações de segurança oriundas da Diretoria de Tecnologia da Informação - DTI.
>
> 3. Ademais, reforçamos que estamos comprometidos em adotar as melhores práticas de desenvolvimento, a fim de proteger as informações e garantir a confidencialidade dos dados, não só do sistema GCWEB, mas também de seus usuários. Assim, permanecemos à disposição para colaborar com a DTI em quaisquer ações necessárias para garantir a segurança da rede do INSS.

4. Considerando, todavia, as soluções tecnológicas desenvolvidas no âmbito das Coordenações-Gerais de Orçamento, Finanças e Contabilidade - CGOFC e de Engenharia e Patrimônio Imobiliário - CGEPI, se faz necessário o envio dos autos para ciência das recomendações de segurança, em especial quanto aos requisitos de acesso e autenticação.

5. À CGOFC e CGEPI para ciência do contido na Nota Técnica nº 9/2022/DTI-INSS (SEI nº 8737069) e adoção das eventuais providências que sem façam necessárias.

BÁRBARA MACENA DE LIMA

Assessora da Diretoria de Orçamento, Finanças e Logística

Documento assinado eletronicamente por **BARBARA MACENA DE LIMA**, **Assessor(a) da Diretoria de Orçamento, Finanças e Logística**, em 17/05/2023, às 12:30, 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, informando o código verificador **11731281** e o código CRC **161CDEC5**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 11731281

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Orçamento, Finanças e Logística
Coordenação-Geral de Orçamento, Finanças e Contabilidade

DESPACHO

Coordenação-Geral de Orçamento, Finanças e Contabilidade, em 17/05/2023

Ref.: Processo nº 19955.102272/2022-14.

Int.: Diretoria de Tecnologia da Informação.

Ass.: Implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS.

1. Veio presente para ciência e adoção das eventuais providências que sem façam necessárias quanto à Nota Técnica nº 9/2022/DTI-INSS (SEI nº 8737069), oriundo da Diretoria de Tecnologia da Informação, em que presta contas das atividades desenvolvidas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS, no qual recomenda:

> 41. Assim, recomenda-se urgentemente à Presidência e demais Diretorias do INSS, assim como à Dataprev, em suas respectivas alçadas e sem prejuízo de todo o pontuado no decorrer da presente Nota Técnica, bem como nos documentos e normas referenciados:
>
> I- implantação da exigência de certificado digital A3 para acesso aos sistemas do INSS por usuários externos, estagiários e terceirizados;
>
> II - maximizar a priorização para a contratação de serviço de diretório, proteção contra ameaças e atualização do parque computacional;
>
> III - desativação/migraçaõ ou, no mínimo, reforço da autenticação para acesso aos sistemas legados, notadamente CV3 e Prisma;
>
> IV - revisão do PDSI visando dar encaminhamento às medidas propostas nesta Nota Técnica, sobretudo aquelas decorrentes da Ação Técnica Interinstitucional;
>
> V - pactuação de cronograma junto à Dataprev que permita a consecução do objetivo acima.

3. Encaminhe-se à Coordenação de Informação e Suporte à Gestão Orçamentária, Financeira e Contábil – COIS - OFC, para providências que couber.

SÉRGIO CHEQUE BERNARDO
Coordenador-Geral de Orçamento, Finanças e Contabilidade
do INSS, FRGPS e RPPU

Documento assinado eletronicamente por **SERGIO CHEQUE BERNARDO**, **Coordenador(a) Geral de Orçamento,Finanças e Contabilidade**, em 17/05/2023, às 13:22, 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 **11732165** e o código CRC **5EE44A4B**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 11732165

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 17/05/2023

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Minuta de Instrução Normativa que disciplina ….

1. Trata-se do DESPACHO Nº 314/2022/GMTP-MTP, oriundo do Ministério de Trabalho e Previdência cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, proveniente da Polícia Federal comunicando a ocorrência de prováveis fraudes massivas contra o INSS.

2. Ciente do Despacho DTI (8799248), destacando que já houve manifestação no Despacho CGIS (8800442).

3. O Despacho DTIR (8823583) prestou esclarecimentos cabíveis e, "no dia 06/09/2022, encaminhou o Ofício SEI Nº 23/2022/DTIR/COIM/CGIS/DTI-INSS (8823612), constante nos autos deste processo, à Dataprev para colher informações a respeito, haja vista que trata-se de prerrogativa daquela empresa a governança sobre os referidos apontamentos".

4. Como não consta resposta ao referido Ofício, necessário encaminhar o presente a DTIR para verificação quanto a esse ponto, com ciência da EFC Serviços Previdenciários, que deverá ser acionada caso não tenha havido resposta pela empresa.

5. Feitas as considerações, encaminhe-se à DTIR e à EFC Serviços Previdenciários.

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 17/05/2023, às 19:48, 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 **11739950** e o código CRC **1297FA9E**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 11739950

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Orçamento, Finanças e Logística
Coordenação-Geral de Engenharia e Patrimônio Imobiliário

DESPACHO

Coordenação-Geral de Engenharia e Patrimônio Imobiliário, em 18/05/2023

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS.

1. Ciente do Despacho da Diretoria de Orçamento, Finanças e Logística - DIROFL (11731281).

2. Encaminhe-se à Coordenação de Engenharia para análise e manifestação.

THIAGO REIS DO ESPIRITO SANTO

Coordenador-Geral de Engenharia e Patrimônio Imobiliário

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Orçamento, Finanças e Logística
Coordenação-Geral de Engenharia e Patrimônio Imobiliário
Coordenação de Engenharia

DESPACHO

Coordenação de Engenharia, em 24/05/2023

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDERAL MJSP - POLÍCIA FEDERAL.

Ass.: Implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS.

1. Ciente do contido na Nota Técnica 9 (8737069), de 07/10/2022, da Diretoria de Tecnologia da Informação - DTI, acerca da implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS.

2. Conforme apontado no despacho da Diretoria de Orçamento, Finanças e Logística-DIROFL, SEI nº 11731281, a Coordenação-Geral de Engenharia e Patrimônio Imobiliário- CGEPI, está, atualmente, conduzindo o desenvolvimento do sistema ENGWeb, cuja finalidade é a de permitir o armazenamento, manutenção, controle e gestão de dados relativos a infraestrutura, projetos, obras e serviços de engenharia das unidades operacionais do INSS, sendo este sistema a principal ferramenta de gestão das unidades operacionais do INSS quanto as condições físicas em que se apresentam os imóveis operacionais.

3. O sistema encontra-se hoje com:

3.1. autenticação de usuários através de consulta, por meio do protocolo LDAP, ao serviço de diretório institucional;

3.2. base de dados própria, não realizando consultas à outras bases do Instituto nem fornecendo ou consumindo dados através de APIs e

3.3. acesso somente através da rede interna da Autarquia ou com uso de VPN, não havendo exposição do sistema na internet.

4. Além das ações supracitadas, que contribuem para minorar exposição do sistema a eventuais incidentes de segurança da informação, tem-se buscado observar o contido na PORTARIA DTI/INSS Nº 79, DE 25 DE MAIO DE 2022, que estabelece o processo de entrega de software, os padrões de desenvolvimento e obtenção segura de sistemas computacionais não finalísticos e as diretrizes para a utilização de rotinas de automação robótica de processos (RPA) no âmbito do INSS, de forma a buscar meios de garantir a não existência de vulnerabilidades que possam comprometer o ambiente do Instituto.

5. Feitas as considerações, restitua-se à Coordenação-Geral de Engenharia e Patrimônio Imobiliário, para, se de acordo, proceder ao encaminhamento à Diretoria de Orçamento, Finanças e Logística.

WELERSON FERNANDES LOPES

Analista do Seguro Social

ALEXANDRE CIBIN RIBEIRO

Coordenador de Engenharia

Documento assinado eletronicamente por **ALEXANDRE CIBIN RIBEIRO**, **Coordenador(a) de Engenharia**, em 26/05/2023, às 18:11, 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 **WELERSON FERNANDES LOPES**, **Analista do Seguro Social**, em 26/05/2023, às 18:12, 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 **11826326** e o código CRC **9F4F70F2**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 11826326

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Orçamento, Finanças e Logística
Coordenação-Geral de Orçamento, Finanças e Contabilidade
Coordenação de Informação e Suporte à Gestão Orçamentária, Financeira e Contábil

DESPACHO

Coordenação de Informação e Suporte à Gestão Orçamentária, Financeira e Contábil, em 26/05/2023

Ref.: Processo nº 19955.102272/2022-14.

Int.: Diretoria de Tecnologia da Informação.

Ass.: Implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS.

1. Ciente.

2. Informamos que no âmbito da Coordenação-Geral de Orçamento, Finanças e Contabilidade, levantamos para o sistema OFCweb a necessidade de implantação da autenticação por certificado digital A3, demanda em desenvolvimento pela equipe técnica de suporte ao sistema. Os demais sistemas, geridos pela DATAPREV, como o GRU Cobrança e SISPAGBEN, já possuem autenticação pelo GERID atendendo assim as recomendações da Nota Técnica nº 9/2022/DTI-INSS (SEI nº 8737069).

3. Encaminhe-se à Coordenação-Geral de Orçamento, Finanças e Contabilidade - CGOFC em devolução.

RAFAEL DA SILVA FRANÇA

Coordenador de Informação e Suporte à Gestão Orçamentária, Financeira e Contábil

---

Documento assinado eletronicamente por **RAFAEL DA SILVA FRANCA**, **Coordenador(a) de Informação e Suporte à Gestão Orçamentária, Financeira e Contábil**, em 26/05/2023, às 11:02, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 11856873

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Orçamento, Finanças e Logística
Coordenação-Geral de Orçamento, Finanças e Contabilidade

DESPACHO

Coordenação-Geral de Orçamento, Finanças e Contabilidade, em 26/05/2023

Ref.: Processo nº 19955.102272/2022-14.

Int.: Diretoria de Tecnologia da Informação.

Ass.: Implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS.

1. Ciente do teor do Despacho COIS-OFC SEI nº 11856873, que informa a necessidade para o sistema OFCweb, de implantação da autenticação por certificado digital A3, demanda em desenvolvimento pela equipe técnica de suporte ao sistema. Os demais sistemas, geridos pela DATAPREV, como o GRU Cobrança e SISPAGBEN, já possuem autenticação pelo GERID atendendo assim as recomendações da Nota Técnica nº 9/2022/DTI-INSS (SEI nº 8737069).

2. Restitua-se à Diretoria de Orçamento, Finanças e Logística – DIROFL, para ciência e prosseguimento.

SÉRGIO CHEQUE BERNARDO
Coordenador-Geral de Orçamento, Finanças e Contabilidade
do INSS, FRGPS e RPPU

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Orçamento, Finanças e Logística
Coordenação-Geral de Engenharia e Patrimônio Imobiliário

DESPACHO

Coordenação-Geral de Engenharia e Patrimônio Imobiliário, em 29/05/2023

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS.

1. Ciente do Despacho da Coordenação de Engenharia - CENG (11826326).

2. Encaminhe-se, conforme o sugerido, à Diretoria de Orçamento, Finanças e Logística - DIROFL para conhecimento da supra manifestação em atendimento quanto ao solicitado no Despacho DIROFL (11731281).

THIAGO REIS DO ESPIRITO SANTO

Coordenador-Geral de Engenharia e Patrimônio Imobiliário

Documento assinado eletronicamente por **THIAGO REIS DO ESPIRITO SANTO**, **Coordenador(a) Geral de Engenharia e Patrimônio Imobiliário**, em 29/05/2023, 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 **11872320** e o código CRC **1268CAFD**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 11872320

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Orçamento, Finanças e Logística

DESPACHO

Diretoria de Orçamento, Finanças e Logística, em 31/05/2023

Ref.: Processo nº 19955.102272/2022-14.

Int.: Diretoria de Tecnologia da Informação.

Ass.: Implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS.

1. Trata-se da Nota Técnica nº 9/2022/DTI-INSS (SEI nº 8737069), oriundo da Diretoria de Tecnologia da Informação - DTI, em que presta contas das atividades desenvolvidas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS, e ainda apresenta recomendações, nos seguintes termos:

> 41. Assim, recomenda-se urgentemente à Presidência e demais Diretorias do INSS, assim como à Dataprev, em suas respectivas alçadas e sem prejuízo de todo o pontuado no decorrer da presente Nota Técnica, bem como nos documentos e normas referenciados:
>
> I- implantação da exigência de certificado digital A3 para acesso aos sistemas do INSS por usuários externos, estagiários e terceirizados;
>
> II - maximizar a priorização para a contratação de serviço de diretório, proteção contra ameaças e atualização do parque computacional;
>
> III - desativação/migraçaõ ou, no mínimo, reforço da autenticação para acesso aos sistemas legados, notadamente CV3 e Prisma;
>
> IV - revisão do PDSI visando dar encaminhamento às medidas propostas nesta Nota Técnica, sobretudo aquelas decorrentes da Ação Técnica Interinstitucional;
>
> V - pactuação de cronograma junto à Dataprev que permita a consecução do objetivo acima.

2. A CGRLOG manifestou-se nos termos do despacho SEI nº 11477646, no qual ratifica o contido no despacho da Divisão de Despesas Operacionais e Suprimentos - DDOS (SEI nº 11475410), o qual informa:

> 2. No que se refere ao Sistema de Gestão de Contratos - GCWEB, informamos que a autenticação de usuários se dá por meio do serviço de LDAP disponibilizado pela Dataprev, o mesmo protocolo utilizado pelo Sistema Eletrônico de Informações - SEI. Deste modo, podemos afirmar que esta Divisão já vem seguindo as recomendações de segurança oriundas da Diretoria de Tecnologia da Informação - DTI.
>
> 3. Ademais, reforçamos que estamos comprometidos em adotar as melhores práticas de desenvolvimento, a fim de proteger as informações e garantir a confidencialidade dos dados, não só do sistema GCWEB, mas também de seus usuários. Assim, permanecemos à disposição para colaborar com a DTI em quaisquer ações necessárias para garantir a segurança da rede do INSS.

3. Já a Coordenação de Informação e Suporte à Gestão Orçamentária, Financeira e Contábil - COIS-OFC (SEI nº 11856873), corroborada pela Coordenação-Geral de Orçamento, Finanças e Contabilidade - CGOFC (SEI nº 11858105), prestou informações quanto ao acesso ao sistema OFCWeb e

aos demais sistemas atualmente geridos pela Empresa de Tecnologia e Informações da Previdência - DATAPREV:

> 2. Informamos que no âmbito da Coordenação-Geral de Orçamento, Finanças e Contabilidade, levantamos para o sistema OFCweb a necessidade de implantação da autenticação por certificado digital A3, demanda em desenvolvimento pela equipe técnica de suporte ao sistema. Os demais sistemas, geridos pela DATAPREV, como o GRU Cobrança e SISPAGBEN, já possuem autenticação pelo GERID atendendo assim as recomendações da Nota Técnica nº 9/2022/DTI-INSS (SEI nº 8737069).

4. Por fim, a Coordenação de Engenharia - CENG (SEI nº 11826326) e Coordenação-Geral de Engenharia e Patrimônio Imobiliário - CGEPI (SEI nº 11872320) apresentaram informações acerca do acesso ao sistema ENGWeb:

> 2. Conforme apontado no despacho da Diretoria de Orçamento, Finanças e Logística- DIROFL, SEI nº 11731281, a Coordenação-Geral de Engenharia e Patrimônio Imobiliário- CGEPI, está, atualmente, conduzindo o desenvolvimento do sistema ENGWeb, cuja finalidade é a de permitir o armazenamento, manutenção, controle e gestão de dados relativos a infraestrutura, projetos, obras e serviços de engenharia das unidades operacionais do INSS, sendo este sistema a principal ferramenta de gestão das unidades operacionais do INSS quanto as condições físicas em que se apresentam os imóveis operacionais.
>
> 3.O sistema encontra-se hoje com:
>
> 3.1. autenticação de usuários através de consulta, por meio do protocolo LDAP, ao serviço de diretório institucional;
>
> 3.2. base de dados própria, não realizando consultas à outras bases do Instituto nem fornecendo ou consumindo dados através de APIs e
>
> 3.3. acesso somente através da rede interna da Autarquia ou com uso de VPN, não havendo exposição do sistema na internet.
>
> 4. Além das ações supracitadas, que contribuem para minorar exposição do sistema a eventuais incidentes de segurança da informação, tem-se buscado observar o contido na PORTARIA DTI/INSS Nº 79, DE 25 DE MAIO DE 2022, que estabelece o processo de entrega de software, os padrões de desenvolvimento e obtenção segura de sistemas computacionais não finalísticos e as diretrizes para a utilização de rotinas de automação robótica de processos (RPA) no âmbito do INSS, de forma a buscar meios de garantir a não existência de vulnerabilidades que possam comprometer o ambiente do Instituto.

5. Estando de acordo com as manifestações proferidas pelas áreas técnicas desta Diretoria de Orçamento, Finanças e Logística - DIROFL, restitua-se à DTI para ciência e prosseguimento.

ALESSANDRO ANTONIO STEFANUTTO

Diretor de Orçamento, Finanças e Logística

sei! assinatura eletrônica

Documento assinado eletronicamente por **ALESSANDRO ANTONIO STEFANUTTO**, **Diretor(a) de Orçamento, Finanças e Logística**, em 05/06/2023, 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 .

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 11924018

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Governança, Planejamento e Inovação
Coordenação-Geral de Conformidade
Coordenação de Proteção de Dados Pessoais

DESPACHO

Coordenação de Proteção de Dados Pessoais, em 08/08/2023

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se da Nota Técnica nº 9/2022/DTI-INSS, que destina-se a prestar contas das atividades desenvolvidas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS, em seguimento ao exposto na NOTA TÉCNICA Nº 1/2021/CGIN/DTI-INSS (4651370), de 13/09/2021, em decorrência, sobretudo, do recebimento do DESPACHO Nº 314/2022/GMTP-MTP, de 11/08/2022 (8536675), oriundo do Gabinete do Sr. Ministro de Estado do Trabalho e Previdência.

2. Informamos ciência e encaminhamos à DIGOV para verificar se há alguma providência a ser tomada no âmbito de competência desta COPDP, especialmente em relação às recomendações citadas no SEI (8823583), SEI (8737069), SEI (8575180).

3. Posteriormente à ciência da DIGOV e, se de acordo, encaminhar a Diretoria de Tecnologia da Informação (DTI) no sentido de consultar a Diretoria de Tecnologia da Informação para atualização do andamento das medidas que visam evitar o vazamento de credenciais de acessos a sistemas corporativos do INSS. Conforme o contido nos termos da:

a) NOTA TÉCNICA Nº 3/2022/CGIN/DTI-INSS, de 14/03/2022 - Proposta de ação técnica integrada que visa a apuração da causa primária do vazamento de credenciais de acessos a sistemas corporativos do INSS;

b) NOTA TÉCNICA Nº 9/2022/DTI-INSS, de 07/10/2022 - Discorre acerca da implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS; e

c) NOTA TÉCNICA Nº 6/2022/DTIR/COIM/CGIS/DTI-INSS, de 19/10/2022 - Relatório conclusivo sobre ação técnica integrada que visa a apuração da causa primária do vazamento de credenciais de acessos a sistemas corporativos do INSS.

d) E a respeito do acesso ao SAT Central se já houve relatório conclusivo sobre a implementação das medidas de segurança.

9. Encaminhe-se à DIGOV no sentido do item 3 para se de acordo encaminhar a DTI.

assinado digitalmente
ROBERTA DOS SANTOS LEMOS
Coordenadora de Proteção de Dados - COPDP
ENCARREGADA - DPO

assinado digitalmente
EDSON PINHEIRO ALVARISTA
ANALISTA DO SEGURO SOCIAL
Assessor Técnico Especializado - CGCONF

Documento assinado eletronicamente por **ROBERTA DOS SANTOS LEMOS**, **Analista do Seguro Social**, em 09/08/2023, às 11:46, 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 **EDSON PINHEIRO ALVARISTA**, **Analista do Seguro Social**, em 09/08/2023, às 12:52, 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 **12782179** e o código CRC **A52573FB**.

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Governança, Planejamento e Inovação

DESPACHO

Diretoria de Governança, Planejamento e Inovação, em 09/08/2023

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS.

1. Trata-se da Nota Técnica nº 9/2022/DTI-INSS (SEI nº 8737069), que destina-se a prestar contas das atividades desenvolvidas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS, em seguimento ao exposto na NOTA TÉCNICA Nº 1/2021/CGIN/DTI-INSS (SEI nº 4651370), de 13/09/2021, em decorrência, sobretudo, do recebimento do DESPACHO Nº 314/2022/GMTP-MTP, de 11/08/2022 (SEI nº 8536675), oriundo do Gabinete do Sr. Ministro de Estado do Trabalho e Previdência.

2. Ciente do Despacho COPDP SEI nº 12782179.

3. Em atendimento ao item 3 do referido despacho, encaminhe-se à Diretoria de Tecnologia da Informação - DTI para atualização do andamento das medidas que visam evitar o vazamento de credenciais de acessos a sistemas corporativos do INSS, conforme o contido nos termos dos seguintes documentos:

a) NOTA TÉCNICA Nº 3/2022/CGIN/DTI-INSS, de 14/03/2022 - Proposta de ação técnica integrada que visa a apuração da causa primária do vazamento de credenciais de acessos a sistemas corporativos do INSS;

b) NOTA TÉCNICA Nº 9/2022/DTI-INSS, de 07/10/2022 - Discorre acerca da implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS; e

c) NOTA TÉCNICA Nº 6/2022/DTIR/COIM/CGIS/DTI-INSS, de 19/10/2022 - Relatório conclusivo sobre ação técnica integrada que visa a apuração da causa primária do vazamento de credenciais de acessos a sistemas corporativos do INSS.

d) E a respeito do acesso ao SAT Central se já houve relatório conclusivo sobre a implementação das medidas de segurança.

ANA CAROLINA TIETZ

Diretora de Governança, Planejamento e Inovação

Documento assinado eletronicamente por **ANA CAROLINA TIETZ**, **Diretor(a) de Governança, Planejamento e Inovação**, em 09/08/2023, às 18:23, 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 **12801587** e o código CRC **B25E9C20**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 12801587

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação

DESPACHO

Diretoria de Tecnologia da Informação, em 17/08/2023

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS.

1. Trata-se da Nota Técnica nº 9/2022/DTI-INSS (SEI nº 8737069), que destina-se a prestar contas das atividades desenvolvidas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS, em seguimento ao exposto na NOTA TÉCNICA Nº 1/2021/CGIN/DTI-INSS (SEI nº 4651370), de 13/09/2021, em decorrência, sobretudo, do recebimento do DESPACHO Nº 314/2022/GMTP-MTP, de 11/08/2022 (SEI nº 8536675), oriundo do Gabinete do Sr. Ministro de Estado do Trabalho e Previdência.

2. Ciente do Despacho DIGOV (SEI nº 12801587).

3. De ordem do Diretor de Tecnologia da Informação, encaminhe-se à **CGTIS** - Coordenação-Geral de Tecnologia da Informação e Segurança, para ciência do despacho supra e atendimento na forma proposta em seu Item 3.

MÁRCIA SOARES SALGADO NUNES DE MATOS

Assessora DTI

Documento assinado eletronicamente por **MARCIA SOARES SALGADO NUNES DE MATOS**, **Assessor Técnico**, em 18/08/2023, às 15:10, 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 **12905389** e o código CRC **22325E65**.

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 25/08/2023

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS.

1. Trata-se da Nota Técnica nº 9/2022/DTI-INSS (SEI nº 8737069), que destina-se a prestar contas das atividades desenvolvidas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS, em seguimento ao exposto na NOTA TÉCNICA Nº 1/2021/CGIN/DTI-INSS (SEI nº 4651370), de 13/09/2021, em decorrência, sobretudo, do recebimento do DESPACHO Nº 314/2022/GMTP-MTP, de 11/08/2022 (SEI nº 8536675), oriundo do Gabinete do Sr. Ministro de Estado do Trabalho e Previdência.

2. Ciente do Despacho DTI (12905389).

3. O Despacho COPDP (12782179) , item 3 solicita atualização das medidas que visam evitar o vazamento de credenciais de acesso a sistemas corporativos do INSS . Conforme o contido nos termos da:

a) NOTA TÉCNICA Nº 3/2022/CGIN/DTI-INSS, de 14/03/2022 - Proposta de ação técnica integrada que visa a apuração da causa primária do vazamento de credenciais de acessos a sistemas corporativos do INSS;

c) NOTA TÉCNICA Nº 9/2022/DTI-INSS, de 07/10/2022 - Discorre acerca da implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS; e

e) NOTA TÉCNICA Nº 6/2022/DTIR/COIM/CGIS/DTI-INSS, de 19/10/2022 - Relatório conclusivo sobre ação técnica integrada que visa a apuração da causa primária do vazamento de credenciais de acessos a sistemas corporativos do INSS.

g) E a respeito do acesso ao SAT Central se já houve relatório conclusivo sobre a implementação das medidas de segurança.

4. Neste sentido, face à pertinência temática, encaminhe-se à Divisão de Segurança em Tecnologia da Informação - **DSEG**, para conhecimento e prosseguimento no que couber.

ISRAEL EDUARDO ZEBULON MARTINS DE SOUZA
Coordenador-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 25/08/2023, às 14:42, 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 **13010369** e o código CRC **78D083C5**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 13010369

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação
Coordenação-Geral de Tecnologia da Informação e Segurança
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 25/10/2023

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDERAL MJSP - POLÍCIA FEDERAL.

Ass.: Implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS.

1. Trata-se da Nota Técnica nº 9/2022/DTI-INSS (SEI nº 8737069), que destina-se a prestar contas das atividades desenvolvidas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS, em seguimento ao exposto na NOTA TÉCNICA Nº 1/2021/CGIN/DTI-INSS (SEI nº 4651370), de 13/09/2021, em decorrência, sobretudo, do recebimento do DESPACHO Nº 314/2022/GMTP-MTP, de 11/08/2022 (SEI nº 8536675), oriundo do Gabinete do Sr. Ministro de Estado do Trabalho e Previdência.

2. Ciente do Despacho 13010369, da Coordenação-Geral de Tecnologia da Informação e Segurança (CGTIS).

3. O item 3 de Despacho COPDP (12782179) solicita atualização das medidas que visam evitar o vazamento de credenciais de acesso a sistemas corporativos do INSS, conforme o contido nos termos da NOTA TÉCNICA Nº 3/2022/CGIN/DTI-INSS (6559716), de 14/03/2022 - Proposta de ação técnica integrada que visa a apuração da causa primária do vazamento de credenciais de acessos a sistemas corporativos do INSS, da NOTA TÉCNICA Nº 9/2022/DTI-INSS (8737069), de 07/10/2022 - Discorre acerca da implementação de medidas de segurança cibernética no âmbito do Instituto Nacional do Seguro Social - INSS, e da NOTA TÉCNICA Nº 6/2022/DTIR/COIM/CGIS/DTI-INSS (9151371), de 19/10/2022 - Relatório conclusivo sobre ação técnica integrada que visa a apuração da causa primária do vazamento de credenciais de acessos a sistemas corporativos do INSS, além de indagar se já houve relatório conclusivo sobre a implementação das medidas de segurança no acesso ao SAT Central.

4. Em relação ao acesso ao SAT Central, sugerimos oficiar à Dataprev para se manifestar sobre o solicitado.

5. Em relação a NOTA TÉCNICA Nº 3/2022/CGIN/DTI-INSS, tratava-se de proposta de ação técnica integrada que visava a apuração da causa primária do vazamento de credenciais de acessos a sistemas corporativos do INSS, tendo o seu objetivo sido atingido com a execução do trabalhos que deram origem a NOTA TÉCNICA Nº 6/2022/DTIR/COIM/CGIS/DTI-INSS, comentada a seguir.

6. A NOTA TÉCNICA Nº 6/2022/DTIR/COIM/CGIS/DTI-INSS tratou do relatório técnico conclusivo a respeito das atividades realizadas, respostas obtidas e propostas de intervenção ou de encaminhamentos referentes à apuração da causa primária do comprometimento de credenciais corporativas do INSS à luz das definições abordadas na NOTA TÉCNICA Nº 3/2022/CGIN/DTI-INSS.

6.1. Em relação as medidas definidas no item 9 da NOTA TÉCNICA Nº 6/2022/DTIR/COIM/CGIS/DTI-INSS, segue o status atual:

Medida	Ação	Áreas responsáveis	STATUS	Status em Outubro/2023	Próxima Ação

Medida	Ação	Áreas responsáveis	STATUS	Status em Outubro/2023	Próxima Ação
Revisão da Norma de Controle de Acesso Lógico, visando melhor aplicabilidade da gestão do controle de acesso para não permitir concessão horizontal de gestão	Instituir GT, envolvendo a DTI, DGPI e áreas de negócio para consenso da redefinição das funções de gestão de acesso. Revisão das regras de negócios, dos papéis e permissões de gestores e das bases de usuários	DTI, DTIR, DSEG, DIRBEN	Sem demanda	Não iniciado.	Encaminhar sugestão de revisão da NCAL-INSS no processo 35014.047735/2020-84
Revisão da Política de Segurança da Informação	Instituir GT de revisão da POSIN-INSS.	CTGD, DTI, DSEG, DTIR	Sem demanda	Não iniciado.	Encaminhar sugestão de revisão da POSIN-INSS no processo 35014.047735/2020-84
Fortalecimento da política de senhas	Incrementar a quantidade e a complexidade de caracteres. Revisar os prazos de expiração de senhas e tokens de usuários internos e externos. Incluir item na revisão da NCAL de forma a abranger LDAP, Office 365 e Certificado Digital. Incluir no contrato com a Dataprev.	DTIR, DSEG	Sem demanda	Dependente da revisão da NCAL.	Após revisão e publicação da nova NCAL, oficiar à Dataprev para que os sistemas mantidos por ela se adaptem a nova política de senhas.
Estabelecer um inventário de contas – sistemas mantidos pelo INSS	Realizar inventário das contas geridas pelo INSS.	DSEG, DIOP, CGDSI	Sem demanda	Consultar áreas envolvidas para poder atualizar status.	Solicitar manifestação da DIOP e da CADS sobre a existência desse inventário ou sobre alguma iniciativa iniciada, ou prevista, nesse sentido.
Estabelecer um inventário de contas - sistemas mantidos pela Dataprev	Solicitar à Dataprev realização de inventário de contas dos sitemas geridos pela empresa.	DSEG	Sem demanda	Consultar Dataprev para poder atualizar status.	Oficiar à Dataprev solicitando manifestação sobre a existência desse inventário ou sobre alguma iniciativa iniciada, ou prevista, nesse sentido.
Desabilitar contas inativas – sistemas mantidos pelo INSS	Realizar a desabilitação e/ou exclusão de contas inativas há mais de 60 dias de sistemas geridos pelo INSS.	DSEG, DIOP, CGDIS	Sem demanda	**Concluído**.	Medida atendida conforme fluxo estabelecido por meio do OFÍCIO SEI CONJUNTO CIRCULAR Nº 1/2023/DGP/DIROFL/DTI/INSS
Desabilitar contas inativas - sistemas mantidos pela Dataprev	Solicitar à Dataprev a desabilitação e/ou exclusão de contas inativas há mais de 60 dias de sistemas geridos pela empresa.	DSEG	Sem demanda	**Concluído**.	Medida atendida conforme fluxo estabelecido por meio do OFÍCIO SEI CONJUNTO CIRCULAR Nº 1/2023/DGP/DIROFL/DTI/INSS
Restringir privilégios de administrador a contas de Administrador dedicadas	Criar constas específicas para usuários administradores, independentes das contas para uso em atividades comuns e cotidianas.	DSEG, DIOP, CGDSI	Sem demanda	Não iniciado.	Despachar à DIOP encaminhando o tema para ser implementado no Microsoft Office e na AWS

Medida	Ação	Áreas responsáveis	STATUS	Status em Outubro/2023	Próxima Ação
Avaliar e revisar o ciclo de vida das contas de usuários que acessam os sistemas mantidos pelo INSS.	Criar ou revisar, caso já exista, processo de concessão e revogação de acesso aos sistemas mantidos pelo INSS Verificar com as áreas responsáveis pela concessão de acessos a existência de processo formal de concessão e revogação de acesso. Solicitar a revisão de papéis e de regras de negócio em busca da mitigação de flexibilizações e fragilidades. Execução de operação sazonal de reinicialização das senhas de todos os usuários internos do INSS	DSEG, DIOP, CGIS, Diretorias da Área Fim	Sem demanda	Parcialmente atendido. Os processos de concessão e revogação de acesso aos sistemas já definido pela NCAL.	Solicitar manifestação da DIOP e da CADS sobre o procedimento da concessão de acessos aos sistemas mantidos pelo INSS e o ciclo de vida das contas dos usuários

Medida	Ação	Áreas responsáveis	STATUS	Status em Outubro/2023	Próxima Ação
Avaliar e revisar o ciclo de vida das contas de usuários que acessam os sistemas mantidos pela Dataprev.	Solicitar à Dataprev documento formal com o processo de concessão e revogação de acesso aos sistemas do INSS mantidos pela Dataprev. Criar ou revisar, caso já exista, processo de concessão e revogação de acesso aos sistemas mantidos pelo INSS Verificar com as áreas responsáveis pela concessão de acessos a existência de processo formal de concessão e revogação de acesso. Solicitar a revisão de papéis e de regras de negócio em busca da mitigação de flexibilizações e fragilidades. Revisar a possibilidade de atribuição de papéis em UF distintas da UF do gestor com mais controle, talvez de forma centralizada. Por exemplo, em Superintendências Regionais. Controlar, estabelecer rastreabilidade e visibilidade para a possibilidade de atribuição de papéis em UF distintas da UF do usuário, caso não exista serviço formalmente autorizado. Corrigir a possibilidade de duplicidade de papéis atribuídos. Por exemplo, caso um usuário receba um papel de consulta em um sistema, talvez não necessite receber papel similar no mesmo sistema, considerar UFs distintas.	DSEG, Dataprev	Sem demanda	Não iniciado.	Oficiar à Dataprev solicitarndo manifestação sobre o procedimento da concessão de acessos aos sistemas mantidos por aquela empresa e o ciclo de vida das contas dos usuários
Implementar o uso de *Single Sign-On* para acesso as aplicações web geridas pelo INSS	Verificar com as áreas responsáveis a existência/disponibilidade do recurso para as aplicações geridas pelo INSS.	DSEG, DIOP, CGDSI	Sem demanda	Em andamento.	Despachar à DIOP solicitando manifestação a respeito do atual status de implementação e uso da conta office como Single Sign-On para acesso as aplicações web geridas pelo INSS
Implementar o uso de *Single Sign-On* para acesso as aplicações web geridas pela Dataprev	Solicitar implementação à Dataprev.	DSEG	Sem demanda	Não iniciado.	Oficiar à Dataprev solicitando manifestação a respeito iniciativa em andamento ou prevista de implementação de solução Single Sign-On para acesso as aplicações web geridas do INSS geridas pela Dataprev

Medida	Ação	Áreas responsáveis	STATUS	Status em Outubro/2023	Próxima Ação
Implementar MFA nas aplicações mantidas pelo INSS	Verificar com as áreas responsáveis pela existência/disponibilidade do recurso para as aplicações geridas pelo INSS.	DSEG, DIOP, CGDSI	Sem demanda	Em andamento.	Despachar à DIOP solicitando manifestação a respeito do atual status de implementação e uso da conta office como Single Sign-On para acesso as aplicações web geridas pelo INSS, com consequente uso de MFA já existente no Office 365
Implementar MFA nas aplicações corporativas hospedadas pela Dataprev	Aplicar MFA (via Google Autenticator) no módulo de autenticação das aplicações	DSEG, Dataprev	Em andamento	Ação constante no plano de segurança criado no Evento de Segurança INSS x Dataprev.	Despachar ao Administrador do GERID para manifestação.
Validar CPFs junto à base da Receita Federal durante o processo de credenciamento de usuários na árvore de diretórios LDAP do INSS.	Confirmar o andamento do desenvolvimento, pela Dataprev, da solução CDI, a qual, entre outras muitas funções, irá realizar validação de CPFs cadastrados no LDAP com a base da Receita Federal	DSEG, Dataprev	Em andamento	Discussão levantada nas análises sobre políticas de gestão de acesso	Despachar ao Administrador do GERID para manifestação.
Segregar os grupos de usuários que usam certificado A1 e A3	Confirmar a conclusão da segregação dos grupos de usuários que usam certificado A1 e A3	DSEG, DGP, Dataprev	Em andamento	**Concluída**.	Atualmente todos os servidores do INSS utilizam apenas certificado digital do tipo A3.
Validar o status do usuário no LDAP durante o processo de autenticação no GERID via Certificado Digital.	Habilitar a validação do status do usuário no LDAP ao realizar login por Certificado Digital no GERID	DSEG, Dataprev	Implantado	Ação constante no plano de segurança criado no Evento de Segurança INSS x Dataprev.	Despachar ao Administrador do GERID para manifestação.
Aplicação de MFA no processo de autenticação na VPN do INSS.	Acesso, exclusivo via Token A3, à VPN (exceto terceirizados, externos e estagiários)	DTI, Dataprev	Em andamento.	**Concluída.**	Atualmente todos os servidores do INSS utilizam apenas certificado digital do tipo A3 para acesso à VPN corporativa.
Concessão de Credenciais	Reavaliar a formalização da Concessão das Credenciais	DTI, DIRBEN, DGP, Dataprev	Em andamento.	Ação constante no plano de segurança criado no Evento de Segurança INSS x Dataprev. Demandas DM.095318 e DM. 090781	Despachar ao Administrador do GERID para manifestação.
Procedimento de reconhecimento de Token e de reinicialização de senha	Abolir o uso do email particular para o reconhecimento de Token e para a reinicialização de senha	Dataprev (Demanda DTP.71821)	Em homologação a ser realizada em Brasília-DF no dia 05/10.	**Concluída.**	Atualmente o token para reinicilização de senha é enviado apenas para o e-mail institucional do servidor.
Renovação de VPN	Implantar fluxo do processo de renovação automática da VPN (Nova ação).	Dataprev	Concluído.	**Concluída.**	Conforme PORTARIA CONJUNTA DTI/DIRAT/INSS Nº 1, DE 23 DE MARÇO DE 2022.
Impedir eventos de *Impossible Travel* (acessos simultâneos) durante o uso de aplicações corporativas.	Implantar Bloqueio de Acesso Simultâneo	Dataprev	Em andamento.	Ação constante no plano de segurança criado no Evento de Segurança INSS x Dataprev. Homologação na data prevista (30/09/2022), porém, foi suspensa em função de problema identificado.	Despachar ao Administrador do GERID para manifestação.

Medida	Ação	Áreas responsáveis	STATUS	Status em Outubro/2023	Próxima Ação
Revisar a segurança dos sistemas legados	Aprimorar os controles e níveis de segurança dos sistemas legados (SUB/Plenus, Prisma, SABI e outros). Aplicação de controles de segurança mais robustos nos módulos de autenticação e de tráfego de dados nos sistemas corporativos legados	DTI, DIRBEN, Dataprev	Priorizado para 2023 e sem atualizações.	Em andamento.	Despachar à CGAUT para se manifestar sobre essa medida.
Revisão das políticas de identidade e acesso para usuários internos e externos	Aprimorar Processo de revisão de usários e seus privilegios	Dataprev	Priorizado para 2023 e sem atualizações.	Não iniciado.	O tema deve ser tratado durante as revisões da POSIN-INSS e da NCAL-INSS.
Aprimorar o GERID	Elaborar Estudo de Evolução de Arquiterura Tecnologica do GERID. Implantar Versões Evolutivas do GERID (principais entregas). mplantar Versões de Manutenção Evolutiva do GERID.	DTI, Dataprev	Priorizado para 2023	Em andamento.	Despachar ao Administrador do GERID para manifestação.
Revisar os controles de acesso à Central 135	Revisar o fato de que durante o processo de gestão de acesso, não existe nenhuma regra de negócio relacionada às centrais 135. Desta forma, sim, é possível usar os papéis da central e acessar os sistemas (Internet ou intranet), mesmo estandofora da Central 135. Discutir a adoção de uma hierarquia de distribuição de papéis, autorizações e permissões de acesso mais robusta a fim de se contornar possibilidades atuais como a atribuição de perfil de acesso a qualquer usuário, inclusive aqueles alheios à Central 135.			Ação decorrente de resposta ao OFÍCIO SEI Nº 17/2022/DTIR/CIMTI/CGIS/DTI-INSS constante no MEMO/CGSI/008/2022 anexo nos autos deste processo. Alinhar, junto às áreas responsáveis, a avaliação de impacto da implementação proposta e demandar à DATAPREV.	Despachar à CGREC/DIRBEN para se manifestar sobre essa medida.

6.2. Em relação as medidas definidas no item 10 da NOTA TÉCNICA Nº 6/2022/DTIR/COIM/CGIS/DTI-INSS, como são todos de competência da DTIR, iremos despachar àquela Divisão para manifestação sobre.

6.3. Em relação as medidas definidas no item 11 da NOTA TÉCNICA Nº 6/2022/DTIR/COIM/CGIS/DTI-INSS, segue o status atual:

Medida	Ação	Áreas responsáveis	STATUS	Status em Outubro/2023	Próxima Ação
	Mapear o administrador e os gestores do GERID e iniciar, junto a eles, a mudança de comportamento e mudança de				

Medida	Ação	Áreas responsáveis	STATUS	Status em Outubro/2023	Próxima Ação
Aprimorar os controles e níveis de segurança da árvore de diretórios LDAP do INSS.	procedimentos impostas pelas políticas de segurança e das ferramenta estabelecidas. Solicitar a correção da fragilidade relacionada a acesso anônimo à árvore do LDAP e a hashes MD5. Revisar a qualidade cadastral dos dados da árvore LDAP. Validar e a aplicar controles de segurança no LDAP e em todas as aplicações corporativas e internas. Mapear todas as aplicações que se autenticam na base LDAP, além de realizar ajustes granulares de permissão. Validar o *backend* do LDAP e criar *playbooks* de testes de aplicações internas e corporativas a serem aplicados periodicamente. Solicitar à Dataprev a disponibilização de um painel de gerenciameto do LDAP e GERID. Limitar conexões ao LDAP dentro da Região de Acesso RII. Solicitar e avaliar o mapeamento do LDAP e o desenho de segurança do GERID. Agendar apresentação da pilha tecnológica que provê a segurança dos produtos do INSS sustentados pela DATAPREV e assim definir e detalhar melhorias a serem implementadas no produto GERID referentes a controle e à auditoria da distribuição de credenciais, papéis e permissões em conjunto com as áreas responsáveis. Controlar, estabelecer rastreabilidade e visibilidade para a possibilidade de gestores internos atribuírem papéis para usuários externos. Controlar, estabelecer rastreabilidade e visibilidade para a possibilidade de gestores atribuírem papéis para usuários no seu mesmo nível, na hierarquia de autorizações. Aplicar auditorias de segurança nas atribuições	DTI, Dataprev	Priorizado para 2023 e sem atualizações.	Em Andamento.	Despachar ao Administrador do GERID para manifestação.

Medida	Ação	Áreas responsáveis	STATUS	Status em Outubro/2023	Próxima Ação
	das permissões de acesso.				
Elaborar o Plano de Tratamento de Incidentes Cibernéticos (INSS x Dataprev)	Fluxo de Comunicação entre DTIR/INSS e CTIR/Dataprev. Completar o fluxo com retorno da DTIR/INSS. Solicitação de revisão de casos antigos e os testes na infraestrutura subjacente pela Dataprev	DTIR, CTIR Dataprev	Em andamento	Em Andamento.	Despachar à DTIR para manifestação.
Fluxo de Bloqueio e Desbloqueio de Credenciais no Pronto	Aprimorar a operacionalização do fluxo	DTIR, CTIR Dataprev	Concluído.	Ação constante no plano de segurança criado no Evento de Segurança INSS x Dataprev.	Despachar à DTIR para manifestação.
Acessar, consumir e gerir logs de acessos em aplicações corporativas	Entrega de Arquivos de Logs - versão 1 Entrega de Arquivos de Logs - versão 1 / Viabilizando Nuvem. Evolução da Entrega de Logs / Definir forma de Disponibilização de Dados	DTIR, DIOP, CGDSI e Dataprev.	Em andamento.	Ação constante no plano de segurança criado no Evento de Segurança INSS x Dataprev.	Despachar ao Administrador do GERID para manifestação.
Gerir vulnerabilidades em aplicações, protocolos e bases corporativos.	Definir serviços e escopo da gestão de vulnerabilidades. Executar o mapeamento de vulnerabilidades. Executar as correções das vulnerabilidades.	DTI, Dataprev	Não iniciado.	Não Iniciado.	Oficiar à Dataprev para se manifestar sobre essa medida.
Discutir, decidir e deliberar a disciplina e regime de utilização ou existência de soluções RPA (*Robotic Process Automation*)	Implantação de APIs e desativação de Robôs	DTI, Dataprev	Em andamento	Em Andamento.	Despachar à CADS para manifestação sobre essa medida.
Executar testes de invasão	Definir serviço e escopo do pentest (reunião de kickoff INSS e DATAPREV). Elaborar cronograma das etapas de execução do pentest. Executar pentest no escopo definido e elaborar relatório. Implementar correções no serviço.	DTI, Dataprev	Não iniciado.	Não Iniciado.	Oficiar à Dataprev para se manifestar sobre essa medida.
Hardening de servidores físicos do INSS.	Implantação da ferramenta inotify nos servidores GNU/Linux	DSEG, DIOP	Em andamento	Em Andamento.	Despachar à DIOP para manifestação sobre essa medida.

Medida	Ação	Áreas responsáveis	STATUS	Status em Outubro/2023	Próxima Ação
Revisão da segurança de infraestrutura, de hosts, de borda e de nuvem.	Implantação de controles de segurança baseados em hosts e aplicação de uma solução de bloqueio, no firewall, de comunicações laterais na mesma zona de rede, de IPS, monitoramento de filesystem em servidores Linux e firewall de hosts. Contratação de monitoramento em aplicações hospedadas nas nuvens AWS e GovCloud. Implantação de controle de dispositivos e de redes no âmbito da infraestrutura de rede do INSS. Implantar segurança baseada em hosts e aplicar uma solução de bloqueio, no firewall, de comunicações laterais na mesma zona de rede, de IPS, monitoramento de filesystem em servidores Linux e firewall de hosts;	DSEG, DIOP, CGIS	Em andamento	Em Andamento.	Despachar à DIOP para se manifestar sobre controles de segurança aplicados à AWS e demais itens dessa medida. Oficiar à Dataprev para se manifestar sobre controles de segurança aplicados à GovCloud.
Implantar modelo de desenvolvimento seguro de software no INSS	Revisar o modelo de desenvolvimento de software do INSS	DSEG, CGDSI		**Concluído**.	Medida atendida conforme PORTARIA DTI/INSS Nº 79, DE 25 DE MAIO DE 2022.
Relacionamento com parceiros da DTIR.	Confirmar se os mecanismos de monitoramento de rede prometidos pela AGU foram implantados em sua rede, assim como a qualidade de tal controle;	DTI, AGU	Não iniciado	Em Andamento.	Despachar à DTIR para manifestação.
Campanhas de educação, treinamento e conscientização em segurança da informação.	Revisar e divulgar amplamento o curso de SIC.	DSEG	Em andamento	Em Andamento.	Em tramitação a NOTA TÉCNICA Nº 34/2023/DSEG/COIM/CGTIS/DTI-INSS (Processo SEI 35014.224576/2023-91) com Recomendação para criação do Programa de Conscientização em Segurança da Informação do INSS, denominado Programa SSIN-INSS (Simplifica Segurança da INformação no INSS).
Gestão de segurança física no INSS	Aprimorar os controles de segurança física das unidades do INSS	DTI, DIROFL	Em andamento	Em Andamento.	Despachar à DIROFL para manifestação sobre essa medida.
Disseminação das competências, da gestão de incidentes e contatos da DTIR/INSS.	Divulgar o ponto de contato da Divisão de Prevenção, Detecção, Tratamento e Resposta a Incidentes Cibernéticos do INSS para a comunidade interna (página na intranet) e externa (WHOIS). Criar página de divulgação na intranet.	DTIR, DSEG	Não iniciado	Em Andamento.	Despachar à DTIR para manifestação.

Medida	Ação	Áreas responsáveis	STATUS	Status em Outubro/2023	Próxima Ação
Gestão de pessoas no âmbito de segurança da informação	Apoio no estabelecimento de programas de políticas de gestão de pessoas para incentivo, educação, fomento à postura ética e divulgação de sanções relacionadas à infração às conformidades legais. Estabelecimento de programas de monitoramento de ambiente e de canais de denúncia anônima;	DTI, DGP	Não iniciado	Não iniciado.	Despachar à DGP para manifestação sobre essa medida.
Gestão de pessoas e tecnologias pertencentes às áreas de segurança da informação do INSS	Fortalecimento do quantitativo de pessoal e disponibilização de tecnologias (SOAR, XDR, Solução de Painel de Registros de Eventos e Ações, etc.) no time de gestão de incidentes de segurança da informação do INSS;	DTI, DGP	Em andamento	Em Andamento.	Despachar à DTIR para manifestação.
Gestão de projetos seguros no INSS	Priorizar as políticas e avaliações de segurança da informação em todos os projetos do Instituto. Implantação de princípios de design de segurança nos processos de negócio e na operação dos sistemas corporativos como: estabelecimento de least privileges (privilégios mínimos), de need to know (compartimentalização de ações), de separation of duties (separação de responsabilidades), de economy of mechanism (balanceamento entre segurança e complexidade), de complete mediation (mediação de cada ação); identificação de pontos mais fracos e de pontos únicos de falha em toda a cadeia de identidade e acesso do INSS; a prevenção de compartilhamento inadvertido e inadequado de informação e de separação de responsabilidades;	DTI, DIRBEN, DIGOV.	Não iniciado	Não Iniciado.	Despachar à DIRBEN e DIGOV para manifestação sobre essa medida.
Análise de ameaças às credenciais do INSS.	Modelagem das ameaças (atravessadores/vendedores) às credenciais do INSS. Incorporação do modelo de ameaças nos requsitos de segurança de todos os projetos do INSS.	DTI, DIGOV	Em andamento	Em Andamento.	Despachar à DIGOV para manifestação sobre essa medida.

Medida	Ação	Áreas responsáveis	STATUS	Status em Outubro/2023	Próxima Ação
Revisar os serviços da Central Service.	Avaliar o catálogo de serviços disponíveis em cada VIP da Central Service. Revisar o processos de autenticação, autorização e auditoria da Central Service. Reavaliar modelo, alinhar, junto com as áreas responsáveis, levantar requisitos e demandar a Dataprev, pois o acesso aos serviços em produção é realizado através usuário/senha exclusivos para os serviços do Central Service. Não há autenticação para usuário de LDAP.	DTI, Dataprev	Não iniciado	Não Iniciado.	Despachar à CGAUT e CADS para manifestação sobre esse medida. Oficiar à Dataprev para manifestação sobre esse medida.
Revisão dos controles e níveis de segurança da API do Market Place	Confirmar a entrega parcial, pois a resposta não contemplou as datas de expiração das credenciais autorizadas solicitadas. Verificar o que significa não associada à plano de consumo.	DTI, Dataprev	Não iniciado	Não Iniciado.	Oficiar à Dataprev para manifestação sobre esse medida.

Medida	Ação	Áreas responsáveis	STATUS	Status em Outubro/2023	Próxima Ação
Revisão dos usuários e gestores associados a *usercodes* e seus respectivos *accesscodes* no CV3	Excluir/Inativar imediatamente todos os ACCESSCODE que tenham no campo DALASTLOGONTIME data anterior a 30/04/2022 Excluir/Inativar imediatamente todos os ACCESSCODE que o campo IDENTITY esteja em branco Excluir/Inativar imediatamente todos os ACCESSCODE que sejam iguais a matrículas de servidores com status EM QUARENTENA NO LDAP Excluir/Inativar imediatamente todos os ACCESSCODE que sejam iguais a números de CPFs Excluir/Inativar imediatamente todos os ACCESSCODE que sejam diferentes de matrícula SIAPE Confirmar datas e campos em branco Confirmar a descontinuação do Plenus CV3. Desenvolver forma de inativar ACCESSCODE de usuário com status EM QUARENTENA no LDAP, para casos de incidentes. Criar regra que não permita ACCESSCODE seja igual a número de CPF.	DTI, Dataprev	Não iniciado, mas priorizado no Plano de Segurança INSSxDataprev	Não iniciado.	Oficiar à Dataprev para manifestação sobre esse medida.
Revisão do PROJETO INSS	Verificar necessidade com as áreas de negócio da lista de aplicações que usam mecanismo de autenticação junto à árvore de diretório LDAP do INSS e suas permissões	DTI, Áreas de Negócio e Dataprev	Não iniciado	Não Iniciado.	Despachar à CADS e CGAUT para manifestação sobre essa medida.
Revisar a lista dos usuários com permissão de escrita na árvore de diretório LDAP do INSS.	Verificar quem são os OPs Numerados. Analisar necessidade com as áreas de negócio.	DTI, Áreas de Negócio e Dataprev	Não iniciado	Não Iniciado.	Despachar à CADS e CGAUT para manifestação sobre essa medida.

Medida	Ação	Áreas responsáveis	STATUS	Status em Outubro/2023	Próxima Ação
Avaliar o desenho de arquitetura de segurança dos ativos do INSS hospedados, sob contrato, na Dataprev, a saber: -controles de segurança de comunicação e de rede das implantados nas aplicações corporativas do INSS; -controles criptográficos de dados pessoais e das bases corporativas do INSS; -controles de segurança aplicados no ciclo de gerenciamento de identidade e acesso do INSS (LDAP e GERID); -Modelagem das ameaças aos ativos do INSS já mapeadas pela Dataprev; -análise de vulnerabilidades de aplicações, API's e protocolos corporativos do INSS; -Processo de desenvolvimento seguro das aplicações corporativas do INSS; e -a natureza, a capacidade de retenção e de entrega dos logs das bases e aplicações corporativas do INSS gerenciados pela Dataprev.	Solicitar mais detalhamentos a respeito de como as camadas de segurança que foram apresentadas pela Dataprev estão configuradas para o nosso ambiente. Solicitar novos documentos de modelagem de ameaça, pois os recebidos parecem estar incompletos e não fica claro se as recomendações para mitigar as ameaças já foram implementadas. Solicitar novos relatórios de análise de vulnerabilidades das aplicações são bastante suscintos e aparentemente incompletos, pois alguns sequer têm a data exata em que foi realizada a análise, ou não têm evidências reais. Solicitar um documento de diretrizes de desenvolvimento seguro, pois foram apresentadas Notas Técnicas com "padrões de segurança" para situações individuais e que deixam de abordar pontos essenciais de desenvolvimento seguro. Revisar os requisitos e políticas de *logs*.	DTI, Dataprev	Não iniciado	Não Iniciado.	Oficiar à Dataprev para manifestação sobre esse medida.
Grupos de VPN	Rediscutir a necessidade de tantos grupos de VPN existentes, suas permissões e ativos envolvidos (árvore de diretório, Firewall de Rede, WAF, Web Proxy, etc.) na cadeia de identidade e acesso da Dataprev;	DTI, Dataprev	Não iniciado	Não Iniciado.	Oficiar à Dataprev para manifestação sobre esse medida.

Medida	Ação	Áreas responsáveis	STATUS	Status em Outubro/2023	Próxima Ação
Implantação de protocolo TLS/SSL nas aplicações web do INSS hospedadas na Dataprev.	Revisar as aplicações hospedadas na Dataprev que não utilizam mecanismos de autenticação MFA ou não estão hospedadas em ambientes configurados com protocolo HTTPS. Revisar o prazo para que as aplicações supracitadas sejam dotadas de mecanismo de MFA em seus módulos de autenticação. Solicitar a resposta ausente a respeito do prazo de implantação do protocolo HTTPS nos ambientes de hospedagem de aplicações do INSS que ainda não assim configurados	DTI, Dataprev	Não iniciado	Não Iniciado.	Oficiar à Dataprev para manifestação sobre esse medida.

7. Observando-se as informações constantes na coluna **Próxima Ação** das tabelas do item 6 desta nota técnica, sugerimos os seguintes encaminhamentos:

7.1. À DIOP para se manifestar sobre as medidas em que é incitada;

7.2. À DTIR para se manifestar sobre as medidas em que é incitada;

7.3. À CADS para se manifestar sobre as medidas em que é incitada;

7.4. Ao Administrador do GERID, para se manifestar sobre as medidas em que é incitado;

7.5. À CGAUT para se manifestar sobre as medidas em que é incitada;

7.6. À DIGOV para se manifestar sobre as medidas em que é incitada;

7.7. À DGP para se manifestar sobre as medidas em que é incitada;

7.8. À DIROFL para se manifestar sobre as medidas em que é incitada;

7.9. À DIRBEN para se manifestar sobre as medidas em que é incitada;

7.10. À Dataprev, via ofício, para se manifestar sobre as medidas em que é incitada;

8. Feitas as considerações, encaminhe-se à (ao) COIM para conhecimento e andamento conforme julgar necessário.

LUZIVAN DE MOURA GOIS

Técnico do Seguro Social

GIULIANO FUCULO MACHADO

Chefe da Divisão de Segurança em Tecnologia da Informação

INSTITUTO NACIONAL DO SEGURO SOCIAL

Superintendência Regional Norte/Centro-Oeste
Coordenação de Gestão de Benefícios
Serviço de Monitoramento e Cobrança Administrativa de Benefícios

DESPACHO

Serviço de Monitoramento e Cobrança Administrativa de Benefícios, em 31/10/2023

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Ciência do processo.

1. Ciente.

2. Trata-se do DESPACHO Nº 314/2022/GMTP-MTP, oriundo do Ministério de Trabalho e Previdência, cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, proveniente da Polícia Federal, comunicando a ocorrência de prováveis fraudes massivas contra o INSS, conforme documento SEI 8536675.

4. As fraudes aqui narradas possuem *"modus operandi"* já investigado pela Autarquia. As reativações apontam para indício de fraude estrutural o qual já é objeto de ação conjunta entre CGINT, CGMOB, CGPAG e DTI e, portanto, não serão apurados de forma individualizada.

5. Este Serviço aguarda o resultado da ação interinstitucional que poderá indicar os responsáveis pelo dano ao erário e, se assim for a decisão da Autarquia, instaurar o procedimento de cobrança administrativa em matéria de benefícios em face daqueles que se beneficiaram dos valores pagos indevidamente.

7. Portanto, neste momento, conclui-se que não será necessário cadastrar demanda de apuração ou de Recuperação de Créditos, porque não existe justa causa para instauração dos procedimentos individualizados por ausência de autoria. Um procedimento apuratório no âmbito administrativo já é conduzido por equipe especializada da CACB e espera-se que, tão logo se tenha a qualificação daqueles que deram causa ao dano do erário ou se beneficiaram dos ilícitos apontados.

9. Registra-se ciência à demanda, sem providências neste momento e conclui-se o processo nesta unidade.

LUCIANO ACEDO MARTINS

Chefe de Monitoramento e Cobrança de Benefício da SRNCO.

Documento assinado eletronicamente por **LUCIANO MACEDO MARTINS**, **Chefe de Serviço de Monitoramento e Cobrança Administrativa de Benefícios**, em 31/10/2023, às 10:59, 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 **13816953** e o código CRC **5328CAEA**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 13816953

INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Benefícios e Relacionamento com o Cidadão
Coordenação-Geral de Monitoramento e Cobrança Administrativa de Benefícios

DESPACHO

Coordenação-Geral de Monitoramento e Cobrança Administrativa de Benefícios, em 23/11/2023

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Ciência do processo.

1. Ciente do despacho SEI (13816953).

2. Nos termos do art. 210 do Regimento Interno do INSS, aprovado pela Portaria PRES/INSS nº 1.532, de 08/12/2022, compete a Coordenação de Ações Corretivas e Cobrança Administrativa de Benefícios - CACB promover o direcionamento das apurações de indícios de irregularidades, em articulação com os demais órgãos externos e entidades envolvidas., quanto a forma de operacionalização das apurações de irregularidades e cobrança administrativa em benefícios.

3. Feitas as considerações, encaminha-se à CACB para tratamento e resposta ao demandante.

FERNANDA CRISTINA DOERL DOS SANTOS

Coordenadora Geral de Monitoramento e Cobrança Administrativa de Benefícios

INSTITUTO NACIONAL DO SEGURO SOCIAL

Superintendência Regional Sudeste III
Coordenação de Gestão de Benefícios
Serviço de Monitoramento e Cobrança Administrativa de Benefícios

DESPACHO

Serviço de Monitoramento e Cobrança Administrativa de Benefícios, em 15/03/2024

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDERAL MJSP - POLÍCIA FEDERAL.

Ass.: Fraudes massivas de reativações de benefícios.

1. Trata-se do **DESPACHO Nº 314/2022/GMTP-MTP**, oriundo do Ministério de Trabalho e Previdência, cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, proveniente da Polícia Federal, comunicando a ocorrência de prováveis fraudes massivas contra o INSS, conforme documento SEI 8536675, encaminhado pela Superintendência Regional Sudeste III para ciência.

2. As fraudes aqui narradas possuem *"modus operandi"* já investigado pela Autarquia. As reativações apontam para indício de fraude estrutural o qual já é objeto de ação conjunta entre CGINT, CGMOB, CGPAG e DTI e, portanto, não serão apurados de forma individualizada.

3. Este Serviço aguarda o resultado da ação interinstitucional que poderá indicar os responsáveis pelo dano ao erário e, se assim for a decisão da Autarquia, instaurar o procedimento de cobrança administrativa em matéria de benefícios em face daqueles que se beneficiaram dos valores pagos indevidamente.

4. Portanto, neste momento, conclui-se que não será necessário cadastrar demanda de apuração ou de Recuperação de Créditos, porque não existe justa causa para instauração dos procedimentos individualizados por ausência de autoria. Um procedimento apuratório no âmbito administrativo já é conduzido por equipe especializada da CACB e espera-se que, tão logo se tenha a qualificação daqueles que deram causa ao dano do erário ou se beneficiaram dos ilícitos apontados.

5. Registra-se ciência à demanda, sem providências neste momento e conclui-se o processo nesta unidade.

ELAINA BARCELLOS PEREIRA

Chefe do Serviço de Monitoramento e Cobrança Administrativa de Benefícios

---

Documento assinado eletronicamente por **ELAINA BARCELLOS PEREIRA**, **Chefe de Serviço de Monitoramento e Cobrança Administrativa de Benefícios**, em 15/03/2024, às 12:22, 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 **15339277** e o código CRC **5F3455EB**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 15339277

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 25/04/2024

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDERAL MJSP - POLÍCIA FEDERAL.

Ass.: Fraudes massivas de reativações de benefícios.

1. Trata-se do **DESPACHO Nº 314/2022/GMTP-MTP**, oriundo do Ministério de Trabalho e Previdência, cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, proveniente da Polícia Federal, comunicando a ocorrência de prováveis fraudes massivas contra o INSS, conforme documento SEI 8536675, encaminhado pela Superintendência Regional Sudeste III para ciência.

2. Ciente.

3. Tendo em vista a matéria estar vinculada à incidência de dispositivos desconhecidos inseridos na rede do INSS nos 2 últimos anos e, tal fato, já estar sob mapeamento da Presidência do INSS e Diretorias afetas ao problema - DTI, DIRBEN e DIGOV -, arquive-se.

FRANCISCO HUMBERTO MENDONÇA DE ARAUJO

Chefe da Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos

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 **15859682** e o código CRC **CC34B0F6**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 15859682

INSTITUTO NACIONAL DO SEGURO SOCIAL

Superintendência Regional Nordeste
Coordenação de Gestão de Benefícios
Serviço de Monitoramento e Cobrança Administrativa de Benefícios

DESPACHO

Serviço de Monitoramento e Cobrança Administrativa de Benefícios, em 27/08/2024

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Fraudes massivas de reativações de benefícios.

1. Trata-se do **DESPACHO Nº 314/2022/GMTP-MTP**, oriundo do Ministério de Trabalho e Previdência, cujo propósito é o encaminhamento, ao INSS, do OFÍCIO Nº 146/2022/ASS/GAB/PF, proveniente da Polícia Federal, comunicando a ocorrência de prováveis fraudes massivas contra o INSS, conforme documento SEI 8536675, encaminhado pela Superintendência Regional Sudeste III para ciência.

2. As fraudes aqui narradas possuem *"modus operandi"* já investigado pela Autarquia. As reativações apontam para indício de fraude estrutural o qual já é objeto de ação conjunta entre CGINT, CGMOB, CGPAG e DTI e, portanto, não serão apurados de forma individualizada.

3. Este Serviço aguarda o resultado da ação interinstitucional que poderá indicar os responsáveis pelo dano ao erário e, se assim for a decisão da Autarquia, instaurar o procedimento de cobrança administrativa em matéria de benefícios em face daqueles que se beneficiaram dos valores pagos indevidamente.

4. Portanto, neste momento, conclui-se que não será necessário cadastrar demanda de apuração ou de Recuperação de Créditos, porque não existe justa causa para instauração dos procedimentos individualizados por ausência de autoria. Um procedimento apuratório no âmbito administrativo já é conduzido por equipe especializada da CACB e espera-se que, tão logo se tenha a qualificação daqueles que deram causa ao dano do erário ou se beneficiaram dos ilícitos apontados.

5. Registra-se ciência à demanda, sem providências neste momento e conclui-se o processo nesta unidade.

GIORGI ALEXANDRE DE ALENCAR MODESTO

Chefe do Serviço de Monitoramento e Cobrança Administrativa de Benefícios - SERMOB/SRNE

Documento assinado eletronicamente por **GIORGI ALEXANDRE DE ALENCAR MODESTO**, **Chefe de Serviço de Monitoramento e Cobrança Administrativa de Benefícios**, em 02/09/2024, às 13:14, 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 **17433589** e o código CRC **B6E79426**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 17433589

INSTITUTO NACIONAL DO SEGURO SOCIAL

Superintendência Regional Sul
Coordenação de Gestão de Benefícios
Serviço de Monitoramento e Cobrança Administrativa de Benefícios

DESPACHO

Serviço de Monitoramento e Cobrança Administrativa de Benefícios, em 18/03/2025

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se de processo encaminhado ao Serviço de Monitoramento e Cobrança Administrativa da SR Sul conforme despacho SEI 9339239.

2. Por meio do despacho nº 314/2022/GMTP-MTP de origem do Ministério de Trabalho e Previdência, foi encaminhado ao INSS o ofício nº 146/2022/ASS/GAB/PF, proveniente da Polícia Federal, comunicando a ocorrência de prováveis fraudes massivas contra o INSS, conforme documento SEI 8536675, que consistem na reativação fraudulenta de benefícios.

3. Conforme despacho 8575180 a demanda já é monitorada pela Coordenação-Geral de Monitoramento e Cobrança Administrativa de Benefícios.

4. Neste sentido, considerando que inexistem providências a serem adotadas neste momento, concluo o processo nesta Unidade.

DÉBORA PORTELLA
Chefe do Serviço de Monitoramento e Cobrança Administrativa de Benefícios
Superintendência Regional Sul

Documento assinado eletronicamente por **DEBORA PORTELLA**, **Técnico do Seguro Social**, em 18/03/2025, às 14:01, 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 **19917424** e o código CRC **8799A445**.

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 Segurança em Tecnologia da Informação

DESPACHO

Divisão de Segurança em Tecnologia da Informação, em 27/11/2025

Ref.: Processo nº 19955.102272/2022-14.

Int.: SERVIÇO PÚBLICO FEDEAL MJSP - POLÍCIA FEDERAL.

Ass.: Comunica ocorrência de prováveis fraudes massivas contra o INSS.

1. Trata-se da Nota Técnica nº 9/2022/DTI-INSS (SEI nº 8737069), que destina-se a prestar contas das atividades desenvolvidas pela área de Segurança da Informação no âmbito do Instituto Nacional do Seguro Social - INSS, em seguimento ao exposto na NOTA TÉCNICA Nº 1/2021/CGIN/DTI-INSS (SEI nº 4651370), de 13/09/2021, em decorrência, sobretudo, do recebimento do DESPACHO Nº 314/2022/GMTP-MTP, de 11/08/2022 (SEI nº 8536675), oriundo do Gabinete do Sr. Ministro de Estado do Trabalho e Previdência.

2. Considerando o lapso temporal transcorrido sem novas manifestações ou pendências a serem sanadas, e não havendo outras diligências identificadas por esta unidade, concluo o presente processo.

3. Ressalvo que, caso surjam novos elementos ou necessidade superveniente relacionada ao objeto tratado, o processo poderá ser reaberto para prosseguimento, conforme cabível.

SALACIER M. NASSER JR.
Analista do Seguro Social

NELSON ANTONIO PIMENTEL JACINTO
Chefe da Divisão de Segurança em Tecnologia da Informação

Documento assinado eletronicamente por **SALACIER MANHAES NASSER JUNIOR**, **Analista do Seguro Social**, em 28/11/2025, às 09:50, 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 **23361210** e o código CRC **8A34043A**.

Referência: Caso responda este Despacho, indicar expressamente o Processo nº 19955.102272/2022-14 SEI nº 23361210