INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria de Tecnologia da Informação
Coordenação-Geral de Tecnologia da Informação
Coordenação de Infraestrutura e Monitoramento de Tecnologia da Informação
Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos

NOTA TÉCNICA Nº 14/2025/DTIR/COIM/CGTI/DTI-INSS
PROCESSO Nº 35014.431841/2025-57
INTERESSADO: SENADO FEDERAL

Nota Técnica destinada a apresentar informações detalhadas solicitadas pela Comissão Parlamentar Mista de Inquérito (CPMI do INSS), contemplando: (i) a relação completa de senhas bloqueadas no Sistema SUIBE, contendo identificação dos titulares, função, lotação, data de criação e autoridade responsável pela autorização; (ii) a quantidade, localização, possível período de instalação e natureza dos dados potencialmente capturados por equipamento vulgarmente denominados de "chupa-cabras" instalados no mês de junho de 2024 no edifício-sede da Administração Central do INSS; (iii) relatório circunstanciado das providências administrativas, operacionais e tecnológicas adotadas pelo órgão após a identificação do vazamento de credenciais, acompanhado da documentação comprobatória; (iv) informações quanto à eventual instauração de investigação criminal, com envio dos autos ou documentos correlatos; e (v) o quantitativo atualizado de senhas ativas no Sistema SUIBE, com indicação da lotação dos servidores titulares.

INTRODUÇÃO

1. A presente Nota Técnica tem por finalidade atender às solicitações (SEI nº 23205925) formuladas pela CPMI do INSS – Comissão Parlamentar Mista de Inquérito do INSS (2025), no tocante a aspectos operacionais, de segurança da informação e de gestão de acessos no âmbito do Instituto Nacional do Seguro Social (INSS). Este documento apresenta, de forma resumida e consolidada, os esclarecimentos referentes ao incidente cibernético envolvendo múltiplas tentativas de acesso à aplicação SUIBE, aos incidentes envolvendo dispositivos de captura clandestina de dados ("chupa-cabras") identificados no edifício-sede do INSS, às medidas adotadas para mitigação de riscos e prevenção de novos eventos, bem como às informações disponíveis sobre eventual instauração de procedimentos investigativos pelas autoridades competentes.

2. As respostas são expostas de maneira objetiva, com fundamento nos processos administrativos instaurados para apuração dos eventos relacionados à aplicação SUIBE e ingresso de dispositivo não autorizados na rede de dados do edifício-sede do INSS, respeitadas as competências legais de cada unidade envolvida. **Quando determinado dado está sob a guarda ou responsabilidade de outra área de negócio do Instituto, o respectivo encaminhamento é indicado de forma expressa.**

DA REQUISIÇÃO CONTIDA NO OFÍCIO Nº 1065/2025 – CPMI INSS

3. O documento inaugural (SEI nº 23205925, páginas 3/4) cuida em requisitar desta Autarquia previdenciária, *in verbis*:

> a) O número exato de senhas bloqueadas do Sistema SUIBE, bem como sua identificação: titulares, com função e lotação, data de criação de cada uma e quem as

autorizou;

b) Informações sobre os "chupa-cabras" encontrados no INSS: **quantos eram**, **onde estavam localizados**, **se foi possível descobrir quando foram instalados** e **quais dados foram capturados**;

c) Relatório sobre as providências tomadas pelo órgão diante do vazamento das senhas, para que não aconteça novamente, com remessa da documentação pertinente a esta comissão;

d) Se houve abertura de investigação criminal, com remessa da documentação pertinente a esta comissão;

e) Atualmente, quantas senhas e qual a lotação dos servidores titulares destas.

4. Motiva a presente requisição de acordo com o exposto na peça inaugural, a notícia publicada pelo portal CNN Brasil acerca da drástica redução de servidores com acesso aos dados do INSS, e o teor do depoimento prestado pelo senhor Alessandro Steffanuto, ex-presidente da autarquia, perante a CPMI do INSS.

4.1. Em apertada síntese, a reportagem noticia que o Instituto bloqueou mais de 3 mil senhas que permitiam acesso a informações sensíveis, concentrando tal controle nas mãos de apenas seis servidores.

4.2. Em oitiva realizada nesta CPMI em 13 de outubro de 2025, o ex-presidente da autarquia, Alessandro Steffanuto, confirmou que, ao assumir a gestão, identificou que mais de 3 mil servidores possuíam credenciais ativas para o Sistema Único de Informações de Benefícios (SUIBE), sem controle efetivo, além da existência de equipamentos de captura de senhas ("chupa-cabras") instalados no edifício do INSS — inclusive próximo ao seu gabinete.

5. Pois bem. Aportam os autos nesta Divisão para conhecimento e atendimento, no que couber (SEI nº 23231909).

ACERCA DO NÚMERO EXATO DE CREDENCIAIS BLOQUEADAS NO SISTEMA SUIBE À ÉPOCA DO INCIDENTE CIBERNÉTICO QUE ENVOLVEU MÚLTIPLAS TENTATIVAS DE ACESSO ANÔMALOS

6. De início, cumpre esclarecer que o incidente envolvendo a aplicação SUIBE, mencionado na reportagem que fundamenta a requisição desta CPMI, foi inicialmente identificado por meio de monitoramento ativo, o qual registrou um volume atípico de tentativas de autenticação malsucedidas — caracterizado como ataque de força bruta —, entre os dias 8 e 14/04/2024, utilizando a credencial PAULO RICARDO BRITO CERQUEIRA, matrícula SIAPE 1639175, lotado na Agência da Previdência Social em Santo Estêvão, Bahia**.**

7. **Adicionalmente, constatou-se que a origem do ataque de força bruta estava vinculada a um sistema legítimo de tradução de endereços (NAT) — responsável por converter endereços IP privados em públicos e vice-versa — utilizado pelo MDS (Ministério do Desenvolvimento Social), a partir do qual foram realizadas as tentativas de acesso utilizando credenciais do INSS (Sei nº 23251933).**

8. Noutro giro, à época dos eventos que afetaram o sistema SUIBE — e, ainda, na estrutura regimental atual do Instituto — cabe a Divisão de Gerenciamento de Informações - DGINF, vinculada à Coordenação-Geral de Suporte ao Atendimento - CGSAT, alocada na DIRBEM-INSS, o monitoramento da disponibilização de acessos aos sistemas de informações gerenciais para servidores internos, bem como os acessos para externos, nos termos do art. 232, inciso VI, do Regimento Interno do INSS, aprovado pela Portaria PRES/INSS nº 1.678, de 29 de abril de 2024.

9. Nessa esteira, em atendimento à solicitação referente **à relação completa de senhas bloqueadas no Sistema SUIBE — incluindo a identificação dos titulares, função, lotação, data de criação e autoridade responsável pela autorização** — a DTIR/COIM/CGTI/DTI-INSS informa que tal informação granular é de competência da área de negócio responsável pela gestão de acessos da aplicação SUIBE, Dieretoria de Benefício do INSS (DIRBEN-INSS). **Assim, recomenda-se o redirecionamento da demanda à unidade gestora, por ser o setor detentor e administrador direto dessas informações**.

ACERCA DE QUANTAS SENHAS E QUAL A LOTAÇÃO DOS SERVIDORES TITULARES DESTAS

10. *Data venia*, interpretamos que se refere às senhas ativas no sistema SUIBE, dado o contexto no qual se insere o questionamento. Por isso, em atendimento **à solicitação referente ao quantitativo atualizado de senhas ativas no Sistema SUIBE, com indicação da lotação dos servidores titulares,** a DTIR/COIM/CGTI/DTI-INSS informa que **tais dados são de competência da área de negócio responsável pela gestão de acessos da aplicação SUIBE, a DIRBEN-INSS**. **Assim, recomenda-se o redirecionamento da demanda à unidade gestora, por ser o setor detentor e administrador direto dessas informações.**

ACERCA DAS INFORMAÇÕES SOBRE OS "CHUPA-CABRAS" ENCONTRADOS NO INSS

11. Internamente, entende-se por "chupa-cabras", nos termos do Ofício SEI Conjunto Circular nº 2/2022/DTI/DIROFL/INSS, de 04 de julho de 2022 (SEI nº 23248830), os dispositivos ou equipamentos eletrônicos de origem desconhecida instalados nas unidades operacionais do INSS. Esses equipamentos mal-intencionados são comumente compostos por dois equipamentos interconectados e amarrados ou colados entre si: um Access Point ou Roteador (conforme indicado pelo número 1 na figura abaixo) ou um modem 4G (conforme indicado pelo número 2 na figura abaixo):

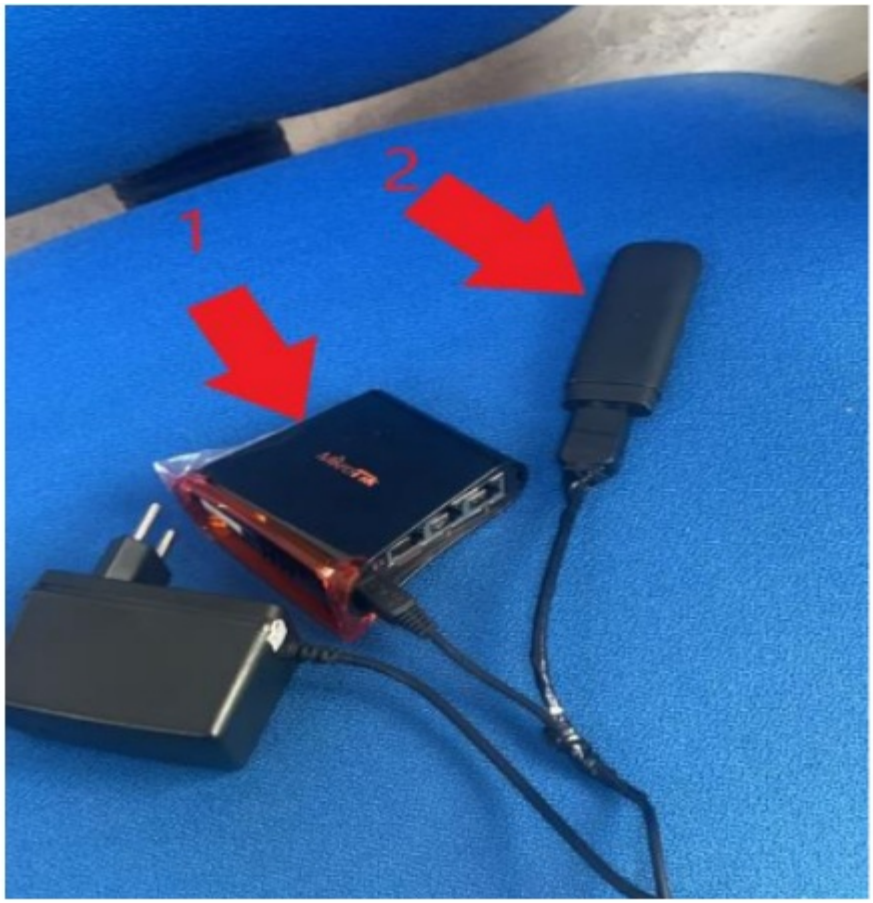

Figura 1. Exemplo de um conjunto de equipamentos eletrônicos mal-intencionados (imagens meramente ilustrativas. Os modelos podem variar.). Fonte: Ofício SEI Conjunto Circular nº 2/2022/DTI/DIROFL/INSS, de 04 de julho de 2022.

12. Apresentado os contornos dos dispositivos vulgarmente denominados de "Chupa-Cabras", passa-se a responder aos questionamentos aduzidos pela CPMI do INSS acerca dos equipamentos de origem desconhecida instalados no edifício da Administração Central do INSS, localizado no SAUS Quadra 02, Bloco O, Edifício sede, Brasília - DF, com CEP 70070-946, no interstício de 20/06/2024 à 26/06/2024:

12.1. As equipe de rede, segurança da informação e cibernética do INSS localizou 7 (sete) "chupa-cabras" distribuídos por 6 (seis) andares e 7 (sete) *racks switches* que atendem a 6 setores

administrativos e o gabinete da presidência do INSS:

- ✓ 1º = ALA SUL = APOIO DA DIRETORIA DE GESTÃO DE PESSOAS = **1 dispositivo**
- ✓ 2º = ALA SUL = COORD.FORMAÇAO E APERFEIÇOAMENTO (CFAI) = **1 dispositivo**
- ✓ 4º = ALA SUL = DIV.ADM.PREDIAL E DIV.GESTÃO MATERIAIS = **1 dispositivo**
- ✓ 5º = ALA SUL = COORD.GERAL ORÇAM. E FINANÇAS = **1 dispositivo**
- ✓ 9º = ALA SUL E ALA NORTE = DIRETORIA DE BENEFÍCIOS = **2 dispositivos (um em cada ala)**
- ✓ 10º = ALA NORTE = OUVIDORIA E GABINETE DA PRESIDÊNCIA = **1 dispositivo**

12.2. Quanto à data exata da instalação dos equipamentos e ao volume de dados eventualmente exfiltrados, esta divisão não realizou análise forense nos dispositivos mencionados. Isso porque, tão logo tomou conhecimento dos fatos, a autoridade policial federal recolheu os referidos equipamentos, conforme comprovam os documentos acostados sob o nº 21770759.

12.2.1. Confeccionado os laudos forenses, registrou a autoridade policial sobre a localização dos dispositivos:

> "Os dispositivos foram **localizados em salas específicas de racks**, distribuídas entre os **andares 10º, 9º (dois dispositivos neste andar), 5º, 4º, 2º e 1º do prédio**. Esses equipamentos estavam **conectados à energia elétrica e camuflados entre cabos de rede, indicando que sua instalação foi realizada por alguém com conhecimento técnico sobre o ambiente e os sistemas do INSS.**"

12.2.2. Sobre a análise preliminar, sustentou a autoridade em comento:

> "A análise preliminar indicou que os dispositivos, possivelmente do tipo 'Raspberry Pi',**tinham potencial para interceptar dados sensíveis, como credenciais de login e informações confidenciais de beneficiários**, e poderiam ser utilizados para reativar benefícios indevidamente ou para acessar remotamente a rede do INSS"

12.2.3. Sobre os os dados extraídos dos dispositivos clandestinos apreendidos no INSS, pontuou:

> "...a presente análise busca descrever os dados extraídos dos dispositivos clandestinos apreendidos no INSS, especialmente detalhando as informações que o hacker estava obtendo e as ações que estava realizando a partir dos dispositivos"

12.2.4. De acordo com os Laudos (SEI nº 23251692), foram identificados, em todos os equipamentos analisados, dados de usuários da Previdência Social. Constatou-se que arquivos contendo documentos pessoais desses usuários se repetem em diferentes dispositivos. Ao todo, foram encontrados documentos referentes a 45 pessoas. Dentre elas, apenas quatro não possuem qualquer tipo de benefício registrado no Sistema Integrado de Benefícios (SIBE), enquanto 33 possuem benefícios ativos, conforme consulta ao próprio SIBE.

ACERCA DAS DAS PROVIDÊNCIAS TOMADAS PELO ÓRGÃO DIANTE DO VAZAMENTO DAS SENHAS

13. Quanto **às providências adotadas pelo órgão diante do vazamento de senhas, com vistas a impedir a reincidência do ocorrido**, informa-se que o documento SEI nº 16723401 detalha as medidas implementadas para prevenir novos incidentes, especificamente aqueles registrados no edifício-sede do INSS.

14. Por derradeiro, no âmbito do incidente relacionado à aplicação SUIBE, foram adotadas e implementadas diversas medidas de reforço à segurança lógica, conforme consignado no despacho SEI nº 16156168 e 23230465. Dentre as principais ações, destacam-se:

a) a segmentação da aplicação, restringindo seu acesso exclusivamente por meio de conexão VPN institucional, assegurando o isolamento do tráfego e mitigando riscos de interceptação;

b) a exigência de autenticação reforçada mediante utilização de certificado digital A3 (token criptográfico), elevando o nível de garantia quanto à identidade do agente autenticado; e

c) a limitação do número de credenciais autorizadas a acessar a plataforma, associada à implementação de controle centralizado para autorização, criação e revisão de novas credenciais, assegurando rastreabilidade, governança e aderência aos princípios de mínimo privilégio e segregação de funções.

15. Tais medidas, em conjunto, compõem um pacote de endurecimento de segurança voltado à mitigação de vulnerabilidades previamente identificadas, à redução da superfície de ataque e ao fortalecimento da gestão de acessos no ambiente institucional.

ACERCA DA ABERTURA DE INVESTIGAÇÃO CRIMINAL

16. No tocante às informações relativas à eventual instauração de investigação criminal, inclusive quanto ao envio de autos ou documentos correlatos, esta divisão informa que não detém conhecimento sobre tais procedimentos — excetuando-se o que consta no SEI nº 23251692 — por se tratar de matéria que extrapola sua competência legal. Ressalte-se, contudo, que as autoridades de persecução penal federal foram tempestivamente comunicadas, conforme registrado no documento SEI nº 23251816.

17. Quanto à comprovação da instauração de investigação criminal em razão da descoberta de equipamento do tipo "chupa-cabra" nas dependências do edifício da Administração Central do INSS, esta divisão recebeu os laudos periciais referentes à análise dos sete equipamentos encontrados, produzidos no âmbito do Inquérito Policial nº 2024.0059553-SR/PF/DF, conforme demonstra o documento SEI nº 23251692.

DOS ENCAMINHAMENTOS

18. Encaminhe-se à CGTI.

Brasília/DF, 18 de novembro de 2025.

Documento assinado eletronicamente por **FRANCISCO HUMBERTO MENDONCA DE ARAUJO**, **Chefe da Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos** , em 18/11/2025, às 17:44, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **23234337** e o código CRC **27A16627**.

FRANCISCO HUMBERTO MENDONÇA DE ARAÚJO

Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos

Referência: Processo nº 35014.431841/2025-57 SEI nº 23234337