INSTITUTO NACIONAL DO SEGURO SOCIAL

OFÍCIO SEI CONJUNTO CIRCULAR Nº 2/2022/DTI/DIROFL/INSS

Brasília, 04 de julho de 2022.

Aos Senhores
Diretores de Benefícios e Relacionamento com o Cidadão, de Gestão de Pessoas, de Governança, Planejamento e Inovação, Superintendentes Regionais, Gerentes Executivos, Gerentes de Agências da Previdência Social, Chefes de Serviço de Tecnologia da Informação e de Setores de Demandas de Tecnologia da Informação
Instituto Nacional do Seguro Social - INSS

Assunto: Orientações e procedimentos em casos de incidentes envolvendo a identificação de equipamentos eletrônicos de origem desconhecida nas unidades do INSS.

Senhores Diretores,

1. A Resolução nº 9/CEGOV/INSS, de 31 de agosto de 2020 aprova e institui a POSIN-INSS – Política de Segurança da Informação do Instituto Nacional do Seguro Social:

> "Art. 1º A POSIN-INSS tem por objetivo estabelecer e difundir diretrizes e princípios de Segurança da Informação – SI, com vistas à orientação para uso e proteção adequados das informações produzidas e custodiadas pelo Instituto, preservando sua disponibilidade, integridade, confidencialidade e autenticidade."

2. Nesse sentido, em caso de identificação de dispositivos eletrônicos de origem desconhecida nas unidades operacionais do INSS, esta Diretoria de Tecnologia da Informação - DTI recomenda a adoção das seguintes medidas:

I - **Detecção:** Conforme o Anexo I, 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).

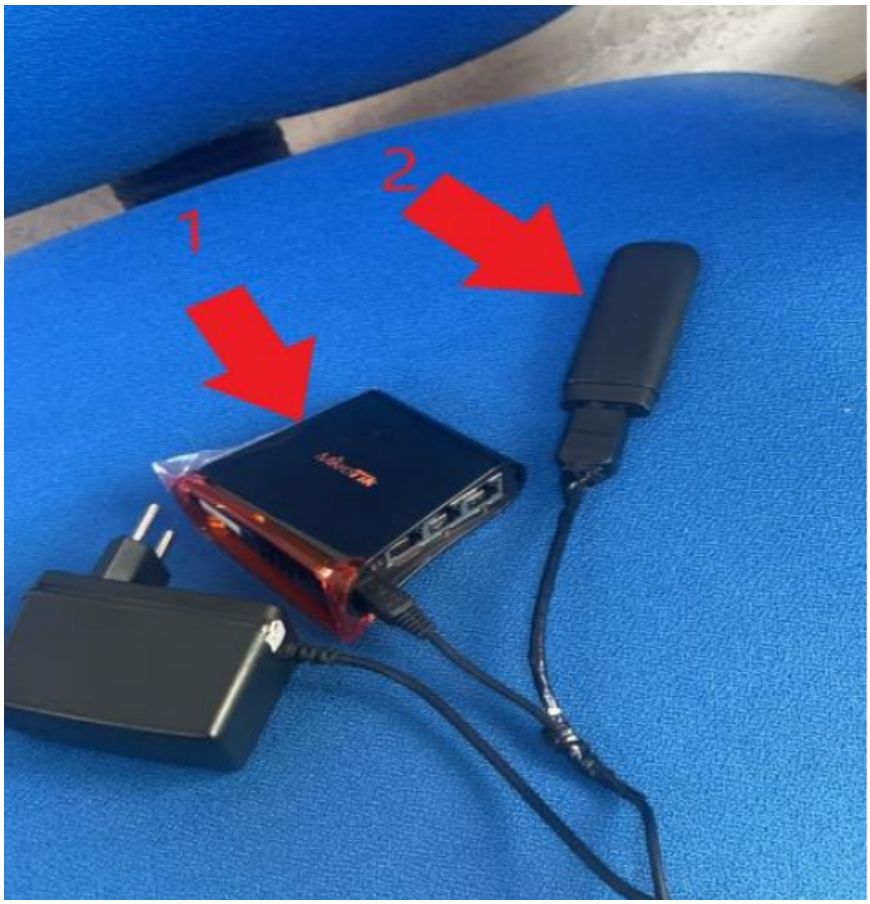

Figura 1 – Exemplo de um conjunto de equipamentos eletrônicos mal-intencionados (imagens meramente exemplificadoras. Os modelos podem variar.)

A identificação visual de equipamento eletrônico de origem desconhecida na unidade poderá ser realizada por qualquer servidor, terceirizado ou estagiário; Caso a identificação não tenha sido efetuada pelo Gestor da Unidade, este deve ser comunicado imediatamente.

II - **Contenção** (ações de contenção do incidente e preservação das evidências):

a) Sem tocar no equipamento ou em suas conexões, o GESTOR deve documentar em fotos e em vídeos, quando for possível visualizar: o modelo e fabricante do equipamento (etiquetas, textos, selos, etc.); os pontos de conexão no equipamento (cabo de rede, cabo USB, etc.); os LEDs (aceso, piscando ou apagado) e; a visão panorâmica do local instalação do equipamento e das conexões elétricas e de rede;

b) o GESTOR deve desconectar os cabos de alimentação elétrica, os cabos de conexão de rede e as conexões entre os equipamentos suspeitos encontrados. Utilizar luvas descartáveis de látex ao manusear os equipamentos a fim de preservar impressões digitais originais;

c) a partir de então, não tocar no equipamento e em suas conexões, bem como mudá-lo ou retirá-lo do local onde foi encontrado;

d) não limpar ou aplicar nenhum produto nos equipamentos ou no ambiente próximo; e

e) evitar o acesso ao local onde foi encontrado o equipamento. Observação: quando não for possível isolar a área, manter as pessoas afastadas do equipamento suspeito.

III - **Resposta:**

a) Imediatamente após, de forma sigilosa, providenciar as seguintes comunicações:

- à unidade do Departamento de Polícia Federal mais próxima do local dos fatos (https://www.gov.br/pf/pt-br/acesso-ainformacao/institucional/quem-e-quem/superintendencias-edelegacias); e

- à Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do INSS (ETIR-INSS), vinculada à DTI, através do e-mail: etir@inss.gov.br.

- A comunicação deverá vir acompanhada de relatório do incidente, conforme Anexo III.
- Após a identificação de um equipamento eletrônico de origem desconhecida, o GESTOR deverá realizar varredura física (inspeção visual baseada em um checklist, conforme Anexo II) de equipamentos suspeitos ao longo da infraestrutura de rede (rack e pontos de dados) e das estações de trabalho da unidade.
- Em caso de invasão, furto ou arrombamento da unidade, o GESTOR deve adotar os procedimentos cabíveis junto à área de Orçamento, Finanças e Logística de vinculação.

b) A ETIR-INSS, por sua vez, providenciará as seguintes comunicações:

- à Divisão de Segurança da Informação - DSEG da DTI, para avaliação e sugestão relativas a controles de segurança da informação);
- à Coordenação-Geral de Inteligência Previdenciária e Trabalhista do Ministério do Trabalho e Previdência - CGINT, para providências a seu cargo;
- à Coordenação-Geral de Monitoramento Operacional de Benefícios - CGMOB, vinculada à Diretoria de Benefícios e Relacionamento com o Cidadão - DIRBEN, para avaliação de impactos na concessão e manutenção de benefícios ou outros comportamentos anômalos executados em sistemas corporativos a partir da localidade ou envolvendo as credenciais de usuários ali lotados;
- à DIGOV – Diretoria de Governança, Planejamento e Inovação, para providências relativas à prevenção de fraudes e proteção de dados;
- à CTIR - Coordenação de Resposta a Incidentes Cibernéticos e Violações à Privacidade - da Dataprev (para avaliação e sugestão relativas a controles de segurança da informação); e
- ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo – CTIR Gov, para registro de incidentes no âmbito da Rede Federal de Incidentes Cibernéticos.

IV - **PREVENÇÃO:**

a) As Superintendências Regionais, em conjunto com a DTI e a Diretoria de Orçamento, Finanças e Logística - DIROFL deverão promover ações de aculturamento e conscientização, bem como o planejamento da varredura física (inspeção visual) periódica das descentralizadas sob sua vinculação, bem como a revisão de procedimentos relacionados à manutenção das unidades, dentre eles a disposição e funcionamento dos dispositivos de CFTV (Circuito Fechado de TV); e

b) Sugere-se que todos os servidores do INSS, estagiários e terceirizados realizem o novo curso de Segurança da Informação disponível na Escola Virtual do INSS.

3. O Anexo I apresenta modelos de equipamentos como referência e auxílio para a inspeção visual na unidade.

4. Adicionalmente, o Anexo IV descreve o procedimento básico de verificação lógica em estações de trabalho do INSS.

5. Todas as ações descritas neste documento devem ser realizadas, se possível ou necessário, com o apoio do setor ou seção de TI de vinculação (SDTI-Setor de Demandas de Tecnologia da Informação).

6. A DTI ressalta que contatos telefônicos, via email ou via serviços de mensageria (SMS, *Whatsapp*, *Telegram*, *Signal*, *Teams*, etc.) não formalizados, que visem a instalação lógica de aplicativos nas estações de trabalho ou a instalação física de equipamentos e que sejam considerados suspeitos devem ser imediatamente reportados ao setor ou seção de TI de vinculação (SDTI-Setor de Demandas de Tecnologia da Informação) que buscará orientações junto à área de segurança da informação da DTI.

7. O Anexo V descreve as orientações de acesso físico de terceirizados e prestadores de serviço nas unidades do INSS.

8. Essa ação conjunta irá contribuir para melhoria do desempenho da rede de dados das unidades e redução dos riscos e incidentes cibernéticos.

Atenciosamente,

JOÃO RODRIGUES DA SILVA FILHO
Diretor de Tecnologia da Informação

LARISSA ANDRADE MORA
Diretora de Orçamento, Finanças e Logística

Anexos: I - Procedimento de inspeção visual periódica em busca de equipamento eletrônica de origem desconhecida na infraestrutura elétrica e de rede da unidade (SEI nº 8023978).
II - Procedimento de inspeção visual periódica em busca de equipamento eletrônica de origem desconhecida na infraestrutura elétrica e de rede da unidade (SEI nº 8023980).
III - Modelo de Relatório de Incidente (SEI nº 8023982).
IV - Procedimento Básico de Verificação Lógica em Estações de Trabalho do INSS (SEI nº 8023974)
V - Orientações de acesso físico de terceirizados e prestadores de serviço nas unidades do INSS (SEI n° 8023976)

Documento assinado eletronicamente por **JOAO RODRIGUES DA SILVA FILHO**, **Diretor(a) de Tecnologia da Informação**, em 04/07/2022, às 15:45, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **LARISSA ANDRADE MORA**, **Diretor(a) de Orçamento, Finanças e Logística**, em 04/07/2022, às 15:53, 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 **8018446** e o código CRC **FF2C5A7D**.