INSTITUTO NACIONAL DO SEGURO SOCIAL

AUDITORIA-GERAL

RELATÓRIO DE AVALIAÇÃO

Avaliação da Gestão de Respostas a Incidentes e as Implicações na Continuidade dos Negócios do INSS

Exercício 2025

29 de dezembro de 2025

INSTITUTO NACIONAL DO SEGURO SOCIAL

AUDITORIA-GERAL

RELATÓRIO DE AVALIAÇÃO

Unidade Auditada: **Diretoria de Tecnologia da Informação**

Município/UF: **Brasília/DF**

Relatório de Avaliação: **#1769248**

INSTITUTO NACIONAL DO SEGURO SOCIAL
AUDITORIA-GERAL

MISSÃO DA AUDITORIA-GERAL

A missão da Auditoria-Geral é aumentar e proteger o valor organizacional do INSS por meio da prestação de serviços de avaliação e consultoria baseada em riscos.

AVALIAÇÃO

O trabalho de avaliação, como parte da atividade de auditoria interna, consiste na obtenção e na análise de evidências com o objetivo de fornecer opiniões ou conclusões independentes sobre um objeto de auditoria. Objetiva também avaliar a eficácia dos processos de governança, de gerenciamento de riscos e de controles internos relativos ao objeto e à Unidade Auditada, e contribuir para o seu aprimoramento.

RESUMO

1. QUAL FOI O TRABALHO REALIZADO PELA AUDITORIA?

A realização deste trabalho teve como objetivo avaliar a eficácia da gestão de respostas a incidentes cibernéticos no âmbito da Autarquia, considerando suas implicações diretas nos negócios e na continuidade dos serviços prestados à sociedade. A ação contemplou toda a cadeia de resposta a incidentes, abrangendo desde a notificação e o tratamento até as etapas de prevenção e monitoramento gerencial, incluindo o gerenciamento e monitoramento do processo.

2. POR QUE A AUDITORIA REALIZOU ESSE TRABALHO?

A auditoria realizou este trabalho por considerar que a gestão de respostas a incidentes cibernéticos é um tema estratégico e essencial para garantir a continuidade dos negócios da Autarquia, especialmente diante do crescente número de ameaças digitais que podem comprometer a integridade, disponibilidade e confidencialidade das informações institucionais. O tema foi proposto pela Diretoria de Governança, Planejamento e Inovação (DIGOV), para compor o Plano Anual de Auditoria Interna do INSS (PAINT) para o exercício de 2025, reforçando a importância de avaliar e aprimorar os mecanismos de prevenção, detecção e resposta a incidentes no ambiente tecnológico da instituição.

3. QUAIS AS CONCLUSÕES ALCANÇADAS PELA AUDITORIA? QUAIS AS RECOMENDAÇÕES QUE DEVERÃO SER ADOTADAS?

A auditoria concluiu que a gestão de incidentes cibernéticos na Autarquia apresenta fragilidades significativas que comprometem a capacidade institucional de prevenir, detectar e responder adequadamente a ameaças digitais. Foi constatada a desatualização e a inobservância do Plano de Gestão de Incidentes Cibernéticos do INSS (PGIC/INSS), falhas no monitoramento e na supervisão do processo de trabalho.

Diante desse cenário, a auditoria recomenda medidas para a atualização do PGIC/INSS, para o acompanhamento dos resultados e dos procedimentos relacionados à gestão de incidentes cibernéticos, bem como a revisão contratual para inclusão de cláusulas específicas acerca dos incidentes cibernéticos que envolvam redes, serviços, sistemas e/ou informações do INSS que são tratados por empresas terceirizadas.

LISTA DE SIGLAS E ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
APF	Administração Pública Federal
CEGOV	Comitê Estratégico de Governança
CGCONF	Coordenação-Geral de Conformidade
CGGOV	Coordenação-Geral de Governança e Gerenciamento de Riscos
CGSAT	Coordenação-Geral de Suporte ao Atendimento
CGTIS	Coordenação-Geral de Infraestrutura e Segurança em Tecnologia da Informação
CISC	Centro Integrado de Segurança Cibernética do Governo Digital
COIM	Coordenação de Infraestrutura e Monitoramento de Tecnologia da Informação
CTIRgov	Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo
DATAPREV	Empresa de Tecnologia e Informações da Previdência S.A
DGP	Diretoria de Gestão de Pessoas
DIGOV	Diretoria de Governança, Planejamento e Inovação
DIRBEN	Diretoria de Benefícios e Relacionamento com o Cidadão
DSC	Departamento de Segurança de Cibernética
DTI	Diretoria de Tecnologia da Informação
DTIR/DTI	Divisão de Tratamento de Incidentes Cibernéticos
ENISA	*European Union Agency for Cybersecurity*
ETIR	Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos
GI	Grupo de Implantação
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
INSS	Instituto Nacional do Seguro Social
MGI	Ministério da Gestão e da Inovação em Serviços Públicos
PAINT	Plano Anual de Auditoria Interna
PCN	Plano de Continuidade de Negócios
PDTIC	Plano Diretor de Tecnologia da Informação
PGIC/INSS	Plano de Gestão de Incidentes Cibernéticos

PLANGIC	Plano de Gestão de Incidentes Cibernéticos para a Administração Federal
POSIN-INSS	Política de Segurança da Informação do Instituto Nacional do Seguro Social
PPSI	Programa de Privacidade e Segurança da Informação
PRES	Presidência do INSS
REGIC	Rede Federal de Gestão de Incidentes Cibernéticos
RIC	Relatório de Incidente Cibernético
RSIT	*Reference Security Incident Taxonomy*
SEI	Sistema Eletrônico de Informações
SGD	Secretaria do Governo Digital
SI	Segurança da informação
SISP	Sistema de Administração dos Recursos de Tecnologia da Informação
SSIC	Secretaria de Segurança da Informação e Cibernética
TELEBRAS	Telecomunicações Brasileiras S.A.
TIC	Tecnologia da Informação e Comunicação
WAN	Solução corporativa de rede de dados de longa distância

SUMÁRIO

INTRODUÇÃO

O objeto de auditoria desta ação, previsto no Plano Anual de Auditoria Interna do INSS de 2025 – PAINT/2025, foi proposto pela Diretoria de Governança, Planejamento e Inovação (DIGOV) e pela Diretoria de Tecnologia da Informação (DTI) em vista à importância do tema relacionado a incidentes cibernéticos para a segurança da informação na organização e para a sociedade brasileira, uma vez considerados os riscos envolvidos para as operações do INSS e a relevância da resposta da instituição a esses eventos de forma a minimizar os prejuízos, sejam eles materiais ou de cunho reputacional.

Diante desse contexto, foram realizados testes de auditoria para responder às seguintes questões de auditoria:

1. A gestão de incidentes cibernéticos do INSS mostra-se efetiva para mitigar eventuais impactos na continuidade dos negócios?
2. Os mecanismos utilizados para a comunicação, conscientização e acompanhamento dos incidentes cibernéticos no INSS são eficientes?

O escopo da ação incluiu a avaliação do processo de trabalho atinente ao fluxo e procedimentos relacionados à gestão de respostas a incidentes cibernéticos ocorridos no período de janeiro de 2023 a maio de 2025, que envolveram a rede, os serviços, os sistemas e as informações do INSS.

Salienta-se que não fizeram parte do escopo a avaliação qualitativa das ferramentas e dos procedimentos adotados pela equipe responsável pelo tratamento de incidentes cibernéticos no Instituto.

A gestão de incidentes cibernéticos no Governo Federal está estruturada sob um modelo centralizado de coordenação e descentralizado na execução, com base nas diretrizes da Política Nacional de Segurança da Informação (PNSI), instituída pelo Decreto nº 10.748, de 16.07.2021, e as normas complementares editadas pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

Para apoiar a atuação descentralizada, foi estabelecida uma rede composta por Equipes de Tratamento e Resposta a Incidentes (ETIRs) nos diversos órgãos e entidades da Administração Pública Federal. Essas equipes são responsáveis pela gestão local dos incidentes, incluindo as etapas de identificação, análise, contenção, erradicação e recuperação, bem como comunicação ao CTIR Gov sobre as ocorrências.

Além disso, o Plano de Gestão de Incidentes Cibernéticos para a Administração Pública Federal (PLANGIC) orienta as ações estratégicas de proteção cibernética e define metas para aprimoramento contínuo da capacidade de resposta, abrangendo as fases de prevenção, detecção, tratamento, resposta e pós-incidente, visando a melhoria contínua das capacidades de cibersegurança do governo federal.

Contemporaneamente, o Ministério da Gestão e Inovação em Serviços Públicos (MGI), por meio da Secretaria de Governo Digital (SGD), lançou o PPSI 2.0, nova versão do programa

institucional voltado à privacidade e segurança da informação para os órgãos e entidades federais.

No âmbito interno, por meio da Resolução n° 9 /CEGOV/INSS, de 31.08.2020, foi instituída no INSS a Política de Segurança da Informação da Autarquia (POSIN-INSS), que prevê a implementação de mecanismos garantidores da segurança da informação, tendo como objetivo proteger a disponibilidade, integridade, autenticidade, confidencialidade e salvaguarda das informações do Instituto. Dentre as diretrizes gerais da POSIN-INSS estão o tratamento de incidentes cibernéticos e a gestão de continuidade.

Como instrumento operacional para aplicação das diretrizes previstas na POSIN, o INSS, através a Diretoria de Tecnologia da Informação (DTI), instituiu o seu Plano de Gestão de Incidentes Cibernéticos (PGIC/INSS), estabelecendo os procedimentos padronizados para detecção, tratamento, comunicação e registro de incidentes cibernéticos no âmbito da autarquia.

O plano define a estrutura de governança de resposta a incidentes, o fluxo de comunicação interna e externa, os níveis de severidade dos eventos e as etapas do ciclo de tratamento (identificação, análise, contenção, erradicação, recuperação e lições aprendidas). Também regulamenta a obrigatoriedade de comunicação tempestiva ao CTIR Gov, em conformidade com os normativos federais e com o PLANGIC.

No âmbito do INSS, a DTI é responsável pelo objeto da ação, competindo à referida diretoria a gestão de Tecnologia da Informação e Comunicação – TIC do INSS, sendo responsável por coordenar a execução da política de segurança de TI e comunicação.

O normativo que instituiu a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do INSS (ETIR-INSS) define-a como uma equipe técnica especializada, composta por profissionais designados para receber, analisar, monitorar e responder a notificações e ocorrências relacionadas a incidentes cibernéticos. Sua finalidade é atuar de forma proativa e coordenada na identificação, investigação e tratamento de incidentes, bem como propor medidas corretivas e preventivas voltadas à mitigação de riscos e à preservação da confidencialidade, integridade, disponibilidade e autenticidade das informações no âmbito do INSS.

Com o objetivo de avaliar se a gestão de incidentes cibernéticos do INSS é efetiva para mitigar impactos na continuidade dos negócios, a auditoria estruturou um conjunto de testes voltados à análise da capacidade institucional de prevenir, detectar, tratar e acompanhar esses eventos.

Ainda, com vistas à avaliação da eficiência dos mecanismos de comunicação, conscientização e acompanhamento da gestão de respostas aos incidentes cibernéticos no INSS, a auditoria estruturou um conjunto de testes que buscaram identificar se há ferramentas adequadas para o registro, monitoramento e supervisão dos incidentes, bem como se as informações são utilizadas de forma estratégica para apoiar a tomada de decisão e a adoção de medidas preventivas. Também foi verificada a regularidade da comunicação com instâncias externas.

RESULTADOS DOS EXAMES

1. Não atualização do Plano de Gestão de Incidentes Cibernéticos do INSS – PGIC/INSS.

Para a administração pública federal foi publicado o Plano de Gestão de Incidentes Cibernéticos (PLANGIC), normativo que objetiva apoiar os órgãos e entidades na prevenção, tratamento e resposta aos incidentes cibernéticos.

O PLANGIC, aprovado pela Portaria GSI/PR nº 120, de 21.12.2022, do Gabinete de Segurança Institucional da Presidência da República, estabeleceu os procedimentos de gestão de incidentes cibernéticos para os participantes da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC)[1].

Com o objetivo de disciplinar os procedimentos e diretrizes a serem tomados nas fases de detecção, tratamento, resposta e prevenção da ocorrência de incidentes cibernéticos no âmbito do INSS, foi estabelecido o Plano de Gestão de Incidentes Cibernéticos do INSS (PGIC/INSS)[2] a partir da Portaria DTI/INSS nº 88, de 27.12.2022.

O PGIC/INSS define os objetivos, o público-alvo, os requisitos tecnológicos, as bases legais e as normativas, a identificação de papéis e responsabilidades dos atores envolvidos, determinação do escopo, da caracterização e do risco dos incidentes. Indica ainda o relacionamento com outras políticas, faz a definição da metodologia e das orientações do processo de gestão de incidentes cibernéticos, concluindo com os procedimentos e requisitos de comunicação dos resultados e riscos às partes interessadas, bem como a documentação dos relatórios.

Cabe destacar que o PGIC/INSS instituído abarcou diversos aspectos relacionados à prevenção e resposta dos incidentes cibernéticos, como os serviços proativos, serviços reativos, prospecção ou monitoração de novas tecnologias; serviços de qualidade, avaliação de resultados e lições aprendidas, atribuídos à ETIR/INSS, unidade vinculada à DTIR/DTI.

De acordo com o item 25 do PGIC/INSS, a Divisão de Tratamento de Incidentes Cibernéticos (DTIR/DTI), unidade vinculada à Coordenação de Infraestrutura e Monitoramento de Tecnologia da Informação (COIM), da Coordenação-Geral de Tecnologia da Informação (CGTI), da Diretoria de Tecnologia e Informação (DTI), é responsável pelos testes, revisões, atualizações e manutenção do plano.

O PGIC/INSS prevê no item 25 a revisão trimestral do plano, bem como atualizações semestrais para os testes. Ainda, previa uma série de atualizações, de modo a contemplar:

> a) Adesão aos futuros: plano de recuperação de desastres e plano de continuidade de negócios.

[1] Instituída pelo Decreto nº 10.748, de 16. 07.2021, estabelece participação obrigatória aos órgãos e entidades da administração pública federal direta, autárquica e fundacional (art.1º, §1º).
[2] Anexo I da Portaria DTI/INSS nª 88/2022, de 27.12.2022.

b) Atualização do Cadernos de Serviços (PORTARIA DTI/INSS Nº 60, DE 18 DE OUTUBRO DE 2021 que aprova o Caderno de Serviços e Fluxo Operacional da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos).

c) Apoio na realização e estabelecimento do mapeamento de ameaças e riscos junto às áreas de negócio.

d) Execução do projeto de classificação das informações do INSS é disciplinado por força-tarefa a ser criada e executada pela DIGOV, DIRBEN e DTI.

e) Criação ou revisão de fluxos de incidentes relacionados a usuários do Ministério da Economia, do Ministério do Trabalho e Emprego, da Subsecretaria de Perícia Médica Federal (SPMF), do Conselho de Recursos da Previdência Social (CRPS), de Cartórios e Serventias e do Ministério da Justiça que utilizem serviços ou sistemas do INSS.

f) Criação e execução de fluxos relacionados a comprometimento de dados pessoais do cidadão junto ao Encarregado de Dados do INSS e à ANPD; análise de vulnerabilidades, de segurança e forense ativos de rede (*endpoints* e servidores); bloqueio/remoção de endereços web junto à DIOP; retirada de ativos da rede junto à DIOP; escalada interna e externa no tratamento de incidentes de segurança cibernética; comunicação padronizada de incidentes (internos e externos) de segurança cibernética; solicitação de dados para a DATAPREV; fornecimento de informações para órgãos internos (Auditoria, Corregedoria, PFE, DIRBEN, DIGOV, etc.); e fornecimento, conforme alinhamento com normativos institucionais, de informações para órgãos externos (CTIR.gov, DPF, Judiciário, Órgãos de Controle, AGU, OAB, Cartórios e Serventias etc.);

g) Revisão do fluxo de bloqueio e desbloqueio de credenciais (internas e externas) junto à Dataprev.

Na avaliação realizada, ficou constatado que, apesar da previsão normativa, o PGIC/INSS, desde sua implementação em dezembro de 2022, não passou por atualizações, mantendo-se vigente e inalterado desde sua publicação.

Inexistem no PGIC/INSS procedimentos referentes aos incidentes que são tratados por empresas terceirizadas e que envolvam as redes, sistemas, serviços e informações do INSS, assim como não são especificados controles para a avaliação, por parte do INSS, se os procedimentos adotados por essas empresas em resposta ao incidente cibernético estão de acordo com as diretrizes estabelecidas pelo órgão.

Como causas, tem-se que não há uma definição estratégica de controle para avaliar, direcionar e monitorar a atuação da gestão para implementação das atualizações em razão das alterações normativas e para revisar os pontos que já haviam sido definidos na constituição do PGIC/INSS.

Quanto às consequências de o PGIC/INSS não estar atualizado e revisto, além das desconformidades verificadas, poderá ocorrer aumento de incidentes registrados, do número de vazamentos de dados sob a responsabilidade do INSS e uma maior vulnerabilidade a novos ataques, visto que as revisões necessárias a serem efetuadas no PGIC/INSS não estão implementadas, diminuindo a segurança necessária para salvaguarda das informações sob responsabilidade do INSS. A falta de atualizações e revisões trimestrais previstas nas normas instituídas impacta diretamente na realização das atividades da ETIR-INSS.

Ressalta-se também que, em razão da desatualização dos documentos citados, as equipes acabam se utilizando, de forma subsidiária, de material de apoio não formalizado, como o documento “Procedimento Operacional ETIR-INSS".

2. Carência de cláusulas contratuais que permitam ao INSS monitorar as ocorrências de incidentes cibernéticos.

A terceirização na Administração Pública Federal é disciplinada pelo Decreto nº 9.507, de 21.09.2018, que estabelece limites expressos quanto à delegação de competências. Embora seja permitida a contratação de serviços de apoio técnico ou especializado, é vedada a transferência a terceiros de atividades estratégicas, como aquelas que envolvem tomada de decisão, posicionamento institucional, planejamento, coordenação, supervisão e controle, ou outras funções típicas da Administração, incluindo a manifestação final de vontade administrativa.

Nesse contexto, são passíveis de execução indireta os serviços de disponibilização de software, computação em nuvem e as atividades de operação e gerenciamento desses serviços, desde que seus padrões de desempenho e qualidade estejam objetivamente definidos por meio de especificações consagradas e usualmente adotadas pelo mercado.

O modelo de contratação Software como Serviço (SaaS) está previsto no art. 6º, III, da Portaria SGD/MGI nº 5.950, de 26.10.2023, que institui diretrizes para aquisição de soluções de software e serviços de computação em nuvem no âmbito da Administração Pública Federal. Conforme disposto em seu Anexo I, esse modelo é de adoção obrigatória pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Poder Executivo Federal, devendo observar parâmetros técnicos e de governança que assegurem supervisão contratual, disponibilidade, segurança e conformidade com as políticas públicas de tecnologia da informação.

Para a contratação de SaaS, a prestadora fornece uma solução completa hospedada em data center próprio, incluindo infraestrutura, middleware, software aplicativo e dados, sendo responsável pela gestão de hardware e software, garantindo disponibilidade e segurança do serviço.

A análise evidenciou fragilidades relevantes nos contratos firmados pelo INSS com empresas terceirizadas. O contrato com a Telebrás, relativo à solução corporativa de rede WAN, contempla cláusulas específicas sobre monitoramento contínuo, identificação tempestiva de eventos de segurança e reporte imediato de incidentes ao INSS, com prazos, fluxos e responsabilidades claramente definidos, conferindo ao Instituto meios efetivos de supervisão e controle.

Em contraste, o contrato firmado com a Dataprev não contém cláusulas que assegurem ao INSS mecanismos adequados para repasse de informações sobre incidentes cibernéticos detectados e tratados pela contratada, como plano de comunicação, prazos de notificação, parâmetros de desempenho ou obrigações relacionadas à análise, contenção, erradicação e

recuperação. Também não prevê fluxo formal de reporte nem obriga a disponibilização de evidências técnicas que permitam ao INSS validar os procedimentos adotados.

Essa lacuna contratual reduz substancialmente a capacidade de supervisão do INSS, condiciona a gestão de incidentes à atuação da contratada e compromete a visibilidade institucional sobre eventos que impactam a confidencialidade, integridade e disponibilidade dos sistemas e dados do Instituto. Ademais, prejudica a cadeia interna de gestão de incidentes, uma vez que informações relevantes deixam de subsidiar o Plano de Conformidade conduzido pela CGCONF e o envio de dados consolidados ao CTIR Gov, em desacordo com as diretrizes federais de segurança cibernética.

A ausência de requisitos mínimos de reporte, transparência e disponibilização de evidências técnicas fragiliza a atuação da ETIR-INSS e contraria o Decreto nº 9.507/2018 e as normas federais aplicáveis à gestão de segurança cibernética.

Como causa da situação encontrada, destaca-se a deficiência nos mecanismos contratuais das atividades terceirizadas no tratamento de incidentes cibernéticos, podendo haver como consequência o comprometimento dos controles e da regularidade do processo de gestão de incidentes.

3. Insuficiência de informações para o acompanhamento de resultados e monitoramento do processo.

O monitoramento de dados gerenciais de incidentes cibernéticos consiste na coleta, análise e acompanhamento sistemático de informações relacionadas a eventos que comprometem a segurança digital dos sistemas e processos do INSS, de modo que se identifique os quantitativos, os locais de ocorrência, as responsabilidades, as vulnerabilidades mais recorrentes, mensurem impactos, indisponibilidade de sistemas, interrupção das prestações de serviços do INSS, entre outras informações.

O Decreto nº 9.203, de 22.11.2017, que dispôs sobre a política de governança da administração pública federal direta, autárquica e fundacional, conceituou em seu art. 2º, I, que governança pública é o "conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade".

O mesmo decreto estabeleceu, como uma das diretrizes para governança pública, o monitoramento do desempenho e a avaliação dos resultados das políticas e ações prioritárias, de modo a assegurar a observação das diretrizes estratégicas[3], determinando que compete a alta administração implementar e manter mecanismos de governança, devendo ser incluídas, minimamente, formas de acompanhamento de resultados[4].

O PGIC/INSS indicou, em seu item 10.2, a utilização de um painel para demonstração de indicadores e de uma ferramenta de gestão de incidentes cibernéticos.

[3] Art. 4º, III do Decreto n°9.203, de 22.11.2017.
[4] Art. 6º, parágrafo único, I, Decreto n°9.203, de 22.11.2017.

O painel, denominado Painel de Incidentes de Segurança Cibernética, apresentaria indicadores aptos a mensurar os quantitativos, médias, status e tipificação de incidentes cibernéticos que envolvam os dados, sistemas, serviços e rede do INSS, com atualização semanal[5]. O referido painel estaria alojado no endereço *www-dadosinss.prevnet*.

Para a gestão dos incidentes cibernéticos, de acordo com o previsto no subitem 18.2 do PGIC/INSS, a DTIR/DTI dispõe da ferramenta *TheHive*, atualmente mantida pela empresa *StrangeBee*, concebida para organizar, registrar e acompanhar todo o ciclo de vida dos incidentes cibernéticos, desde a detecção até a resolução, bem como armazenar lições aprendidas, promovendo colaboração estruturada, rastreabilidade e eficiência no tratamento de eventos de segurança.

O Caderno de Serviços da ETIR-INSS, aprovado pela Portaria DTI/INSS nº 60, de 18.10.2021, prevê a catalogação dos incidentes detectados em ferramenta própria a ser indicada pela DTI[6].

Dentre as atividades previstas no subitem 17.3 do PGIC/INSS, consta o cadastro do suposto incidente no sistema informatizado, denominada como "Registrar Relatos de Incidente Cibernético - Alertas", na qual o responsável deverá incluir o registro das informações iniciais de um possível incidente de segurança em sistema informatizado.

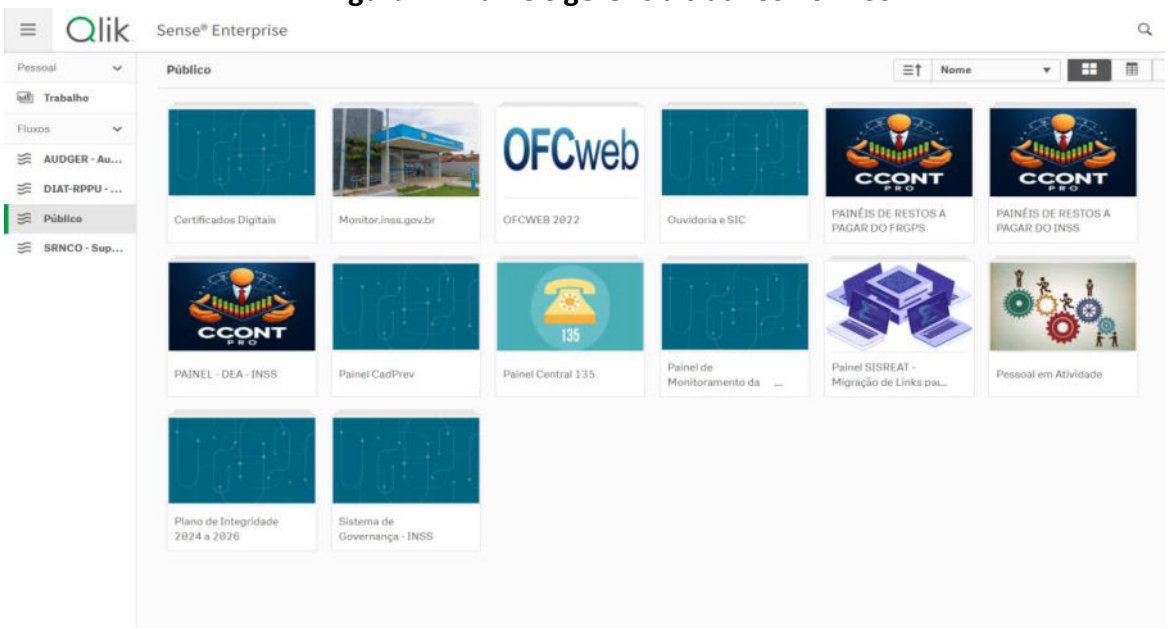
Em atividade posterior denominada "Registrar Incidente Cibernético", o colaborador registrará a classificação quanto ao nível de severidade e impacto, e demais parâmetros relacionados ao incidente no referido sistema.

Os exames realizados pela equipe constataram que o INSS não dispõe das informações estruturadas sobre os incidentes ocorridos e sobre os registros e procedimentos adotados no seu tratamento.

Em relação ao Painel de Incidentes de Segurança Cibernética, foi observada a sua inexistência na plataforma em que estão armazenados os painéis públicos do INSS[7], como demonstrado na figura 1.

[5] Item 20 do Plano de Gestão de Incidentes Cibernéticos (PGIC/INSS).
[6] Subitem 4.1.1 Tratamento de Incidentes, Item 4. Serviços, do Caderno de Serviços da ETIR-INSS.
[7] Disponível para consulta em <https://www-dadosinss.prevnet>

Figura 1 – Painéis gerenciais ativos no INSS



Fonte: Portal www-dadosinss.prevnet, acessado em 27.11.2025.
(https://www-dadosinss.prevnet/custom/hub/stream/aaec8d41-5201-43ab-809f-3063750dfafd)

Em resposta ao questionamento efetuado sobre o painel de indicadores, a unidade auditada informou que o painel foi descontinuado em 2023, tendo sido atualizado até fevereiro daquele ano[8].

Segundo explicações apresentadas pela Coordenação-Geral de Infraestrutura e Segurança em Tecnologia da Informação (CGTIS), a unidade optou por não dar publicidade aos números acerca dos incidentes cibernéticos e às medidas tomadas para combate aos incidentes, pois considera que a divulgação acarreta maior vulnerabilidade à Autarquia, considerando esta nova decisão, um protocolo de segurança[9]. Apesar do esclarecimento em reunião, a descontinuidade da publicidade não foi precedida de processo formal de decisão, não tendo sido normatizada. Não foi definida substituição à ferramenta ou qualquer outro instrumento oficial que assegure transparência e rastreabilidade à mudança adotada.

A fim de se verificar se o INSS era detentor das informações relacionadas aos incidentes ocorridos no período de janeiro de 2023 a maio de 2025, foi solicitada pela equipe a disponibilização dos registros dos incidentes de segurança cibernética ocorridos nesse período.

Em resposta, inicialmente a unidade auditada informou[10] que,

> com base na análise dos relatórios de gerenciamento de incidentes fornecidos pela DATAPREV e dos alertas recebidos por meio da caixa postal institucional [...] verificou-se que, no período de 2023 a 2025, a ETIR-INSS recebeu um total de 317 (trezentas e

[8] Despacho DTIR/DTI, em 16/06/2025, Documento SEI nº *1155***, item 2.2, letra 'b'.
[9] Entrevista com o gestor da CGTIS em 22.08.2025, Documento SEI nº *2179*** - Processo SEI nº 35014.03****/2025-**
[10] Despacho DTIR/DTI, em 16/06/2025, Documento SEI nº *1155***, item 2.2, letra 'a'.

dezessete) notificações de incidentes cibernéticos envolvendo ativos de informação do INSS.

Posteriormente, por meio da Nota Técnica nº 7/2025/DTIR/DTI/COIM/CGTIS/DTI-INSS[11], apresentou novos dados para o mesmo período, retificando o anteriormente informado com relação ao quantitativo de incidentes tratados envolvendo o INSS e indicando um total de 564 incidentes, cuja ocorrência por ano se encontra demonstrada na tabela 1.

Tabela 1– Incidentes Cibernéticos ocorridos no período de janeiro de 2023 a maio de 2025

ANO	Ocorrências registradas
2023	334
2024	211
2025	19
Total	564

Fonte: elaboração Própria com base nos dados apresentados em Nota Técnica nº 7/2025/DTIR/DTI/COIM/CGTIS/DTI-INSS.

Contudo, quando solicitado o encaminhamento das informações relacionadas a esses incidentes, durante a reunião de esclarecimentos, a DTIR/DTI informou que o INSS não realiza a compilação dos dados dos incidentes cibernéticos detectados, de modo a reunir os informados e tratados pela Dataprev e pela Telebrás, prejudicando a consolidação das informações, a análise integrada dos riscos e a tomada de decisão baseada em evidências. Ainda, conforme exposto pela DTIR/DTI, a quantidade de e-mails recebidos e armazenados na caixa institucional da ETIR-INSS é extremamente elevada, o que inviabilizaria, na prática, a identificação manual dos e-mails relacionados especificamente aos incidentes cibernéticos. Segundo a Divisão, esse esforço demandaria tempo e recursos significativos, acarretando prejuízos à rotina operacional da equipe. Ainda, ressalta-se que conforme relatado pela DTIR/DTI, não há um controle sobre a quantidade de mensagens que constam na caixa[12].

Diante da inexistência do Painel com os indicadores e de informações gerenciais consolidadas e estruturadas, a equipe de auditoria solicitou uma amostra aleatória das ocorrências, para as quais deveriam ser apresentados os e-mails de comunicação, bem como os respectivos RIC relacionados. Assim, a partir dos 564 registros de incidentes de segurança cibernética ou alertas do período, a auditoria elaborou uma amostra com um total de 145 incidentes. Desses, foram disponibilizados 117 (80,69%) dos registros solicitados.

Para a amostra disponibilizada, não foram encontrados pela unidade auditada 29 comunicados de incidentes cibernéticos encaminhados à caixa da ETIR-INSS, 20% do total da amostra.

Quanto ao registro do incidente no sistema de gestão *TheHive*, constatou-se que da amostra disponibilizada pela unidade auditada, não havia registro de 73 dos 145 incidentes tratados,

[11] Note Técnica nº 7/2025/DTIR/DTI/COIM/CGTIS/DTI-INSS - Documento SEI nº *1303***, item 4 - Processo SEI nº 35014.03****/2025-**.

[12] Reunião com DTIR/DTI e ETIR-INSS, em 03.07.2025 – Documento SEI *1853***, Processo SEI nº 35014.03****/2025-**.

50,34%. Ou seja, não estavam registrados no sistema de gestão mais de 50% dos incidentes tratados.[13]

A tabela 2 apresenta o resultado do cruzamento entre as informações constantes no sistema de gestão *TheHive* com as ocorrências listadas no documento encaminhado pela unidade auditada, indicando os alertas e incidentes detectados ou informados ao INSS relacionados aos sistemas, redes, serviços e informações do órgão.

Tabela 2 – Comparativo entre os incidentes e alertas detectados ou informados ao INSS e os registros cadastrados no sistema de gestão *TheHive* no período de 01/2023 a 05/2025

Situação no sistema de gestão The Hive	Incidentes ou alertas informados ou detectados pelo INSS	%
Registrados	278	49,29%
Não registrados	286	50,71%
Total	564	100,00%

Fonte: elaboração própria com base nas informações dOS incidentes e alertas detectados ou informados ao INSS as extraídas do sistema de gestão *TheHive*.

Constata-se que 50,71% dos incidentes e alertas informados ou detectados não estavam registrados no sistema de gestão do INSS.

De acordo com as justificativas da área aos questionamentos efetuados pela equipe, o sistema é utilizado apenas para registrar as informações de incidentes cibernéticos que, encaminhados à ETIR/INSS, são tratados por eles, não sendo cadastradas no sistema informações de incidentes oriundas do tratamento efetuado por empresa terceirizadas (DATAPREV e Telebrás)[14].

Em contrapartida, quando analisados os incidentes e alertas registrados no sistema de gestão *TheHive* em comparação com os constantes no documento disponibilizado pela área, constatou-se que 166 registros não constavam na relação indicada pela área quanto aos incidentes ou alertas detectados ou comunicados ao INSS. O resultado do cruzamento é apresentado na tabela 3.

[13]Em manifestação ao relatório preliminar, por meio da Nota Técnica nº 23/2025/CGTIS/DTI-INSS, a CGTIS informa que seria "*mais consistente restringir o escopo de avaliação a partir do segundo semestre de 2023, quando o uso do sistema passou a ser adotado de forma sistemática pela ETIR-INSS*". Entretanto, uma vez que não foram encaminhados pela unidade auditada o total mensal de registros de incidentes no ano de 2023, inviabiliza-se a avaliação de período parcial daquele ano. Assim, considerados os dados a partir de 2024, tem-se que, de 61 registros de incidentes, 25 não constavam do TheHive, indicando que 40,98% dos incidentes tratados não estavam registrados no referido sistema de gestão, ratificando-se a insuficiência de informações para o acompanhamento de resultados como achado de auditoria.

[14] Reunião com DTIR/DTI e ETIR-INSS, em 03.07.2025 – Documento SEI *1853***, Processo SEI nº 35014.03****/2025-**.

Tabela 3 – Comparativo entre os registros cadastrados no sistema de gestão TheHive e os incidentes e alertas detectados ou informados ao INSS no período de 01/2023 a 05/2025

Situação em relação aos incidentes e alertas detectados ou informados ao INSS	Registros no sistema de Gestão de TheHive	%
Informado	285	63,19%
Não informado	166	36,81%
Total	451	100,00%

Fonte: elaboração própria com base nas informações dOS incidentes e alertas detectados ou informados ao INSS as extraídas do sistema de gestão TheHive.

Dessa forma, observa-se que não constam no sistema de gestão TheHive incidentes computados pela unidade, assim como foram observados incidentes informados pela unidade e que não foram registrados no sistema de gestão, denotando que não são disponibilizadas, de modo seguro, informações fidedignas para a gestão de incidentes.

Os exames revelaram também que o sistema de gestão utilizado não possui ferramenta para geração de relatórios gerenciais. Os dados consolidados utilizados para o cruzamento de informações foram compilados pela equipe de auditoria, de forma autônoma, em outro aplicativo por meio da manipulação de dados. Ou seja, não é possível se obter, de forma gerencial e consolidada, os dados necessários à gestão a partir do sistema de gestão utilizado pelo INSS.

Essa situação foi reforçada em reunião pela equipe da ETIR-INSS que indicou que o sistema possui limitações gerenciais, sendo adequado para o registro e demais atividades relacionadas ao tratamento do incidente cibernético[15].

Ademais, como restou evidenciado, as informações de posse do Instituto apresentam distorções entre os registros repassados pela área e os constantes no sistema de gestão.

Desse modo, considerando a descontinuidade do Painel de Incidentes de Segurança Cibernética e a ausência dos indicadores previstos, associado à dificuldade de levantamento dos registros por parte da unidade auditada, e à ausência de registros da totalidade dos incidentes cibernéticos, seja no sistema de gestão adotado pelo INSS seja dos emails comunicando a ocorrência dos incidentes, conclui-se que o órgão não dispõe de mecanismo e ferramenta para acompanhamento e monitoramento dos resultados relacionados ao tratamento de incidentes que envolvam as redes, sistemas, serviços e informações institucionais.

Embora a Portaria DTI/INSS nº 88/2022 esteja vigente e, em seu item 20.1 determine a divulgação de indicadores com quantitativos, médias, monitoramento de *status* e tipificação de incidentes, com atualizações semanais, o INSS descontinuou o Painel desde fevereiro de 2023.

[15] Reunião com DTIR/DTI e ETIR-INSS, em 03.07.2025 – Documento SEI *1853***, Processo SEI nº 35014.03****/2025-**.

Do mesmo modo, não registra a totalidade de alertas comunicados, bem como de incidentes tratados por terceiros que afetam seus ativos de informações no sistema de gestão adotado pelo órgão, em desacordo ao item 18.1 do PGIC/INSS.

A descontinuidade do Painel de Indicadores de Incidentes Cibernéticos, sem substituição formal por outro mecanismo alternativo de consolidação de dados, assim como a falta de registro de todos os incidentes no sistema de gestão evidencia o descumprimento de normativos vigentes e a ausência de transparência na gestão.

Tem-se como causas para as constatações observadas a deficiência na governança que afeta os mecanismos de controle e monitoramento dos incidentes cibernéticos bem como a deficiência nos fluxos de informação e comunicação para produção e/ou disponibilização de informações, que tenham como finalidade apoiar a tomada de decisão.

Como consequência direta da ausência das informações gerenciais no Painel de Incidentes de Segurança Cibernética e de registro no sistema de gestão dos incidentes em que estiveram envolvidos redes, sistemas, serviços, informações do INSS está a impossibilidade de estudos visando a avaliação e identificação das vulnerabilidades, com limitação de atuação da alta administração pela falta de avaliação dos resultados do processo de trabalho, com prejuízo ao monitoramento do processo de trabalho e, consequentemente, à governança.

A ausência de informações gerenciais no Painel e no sistema de gestão impossibilita identificar tendências, falhas e vulnerabilidades, bem como gerar estatísticas para análise. Essa lacuna limita a avaliação dos resultados e compromete o monitoramento do processo e a governança.

4. Ausência de Relatórios de Incidentes Cibernéticos para todos os incidentes cibernéticos.

Os Relatórios de Incidentes Cibernéticos (RIC) constituem um instrumento essencial para a gestão estruturada dos incidentes de segurança da informação, permitindo que a organização registre, análise e aprimore continuamente suas ações de prevenção, detecção, resposta e recuperação frente a eventos cibernéticos.

De acordo com o descrito no Plano de Gestão de Incidentes Cibernéticos do INSS (PGIC/INSS), tal "artefato deverá ser preenchido por toda cadeia de gestão de incidentes de segurança cibernética e será utilizado como insumo para análises históricas e estatísticas[16].

Dentre as atividades previstas de serem executadas pela ETIR no subitem 17.3 do PGIC/INSS, consta a geração do relatório de incidente cibernético (RIC), o qual deverá conter as informações produzidas no transcorrer do incidente de segurança, bem como as fases em que ocorreram. Ainda, o item 22, que trata da documentação de relatórios, versa que os incidentes serão revisados *post-mortem* para avaliar se o processo de investigação foi bem-sucedido e

[16] Item 1 do Apêndice D - Relatório de Incidentes Cibernéticos, do Plano de Gestão de Incidentes Cibernéticos (PGIC/INSS).

eficaz. Ajustes subsequentes podem ser feitos a partir da avaliação dos métodos e procedimentos usados, objetivando a melhoria do processo de resposta a incidentes.

Ainda, no que tange ao RIC, de acordo com o PGIC/INSS, o incidente de segurança poderá produzir uma grande quantidade de informações, necessárias durante suas fases de tratamento, de acordo com seu impacto e extensão. Essas informações, assim como as fases em que ocorrerão, conforme descrito no Plano, serão registradas em um modelo de relatório específico que deverá ser utilizado pela DTIR/DTI[17], e fomentarão a aquisição de conhecimentos necessários em futuros tratamentos de casos similares, cujo modelo se encontra instituído no Apêndice D do PGIC/INSS.

Assim, com vistas à avaliação dos relatórios de incidentes cibernéticos emitidos pela ETIR, solicitou-se a disponibilização dos RIC elaborados a partir da amostra de 145 incidentes de segurança cibernética registrados no período compreendido entre janeiro de 2023 e maio de 2025.

Do total de 145 registros da amostra, foram disponibilizados 10 RIC, dos quais 5 deles (50%) mostraram correlação com o registro efetuado no sistema de gestão *TheHive*, sendo que outros 2 não foram registrados e 3 apresentavam divergências entre as informações constantes no relatório e o registro constante no sistema de gestão, como demonstrado no quadro 1.

Quadro 1 - Correlação de Informações entre os registros dos Relatórios de Incidente Cibernético (RIC) e os constantes no Sistema de Gestão (TheHive)

ID	RIC Descrição e/ou código do incidente	TheHive Descrição ou código do incidente	Situação de correlação
RIC nº 01-20**	Computador que virtualiza servidor SAT Infectado	-	Sem registro no sistema
RIC - Relatório de Incidentes Cibernéticos nº 1*	Roteadores MIKROTIK e os conceitos de segurança cibernética no INSS	-	Sem registro no sistema
RIC nº 020-20**	Atividades suspeitas analisadas pela SGD no Balcão de Atendimento Govbr	#20 - 20******43** - Credencial conectada na VPN diferente da credencial autenticada no Suibe	Divergente
Relatório de Incidente	Relatório de Incidente na APS ****/PE	#1** - APS ****	Convergente
RIC Nº 3*4	Case # 3*4 – 17***2* - Acesso volumétricos e possivelmente maliciosos na janela SISBEN	#3*4 – 17***2* - Acesso volumétricos e possivelmente maliciosos na janela SISBEN	Convergente
RIC Nº 3*2	Equipamentos de origem desconhecida instalado na APS ****/BA	#3*2 - Incidente Cibernético no Programa de Despacho e Recursos - PDR	Divergente
RIC Nº 3*6	Case #3*6 Vulnerabilidade POODLE [inss.gov.br]. CTIR Gov [43***3]	#3*6 - [#42***5] - 2ª Notificação - Vulnerabilidade POODLE [inss.gov.br]	Divergente

[17] Art.7º da Portaria DTI/INSS nº 88, de 27.12.2022.

ID	RIC Descrição e/ou código do incidente	TheHive Descrição ou código do incidente	Situação de correlação
RIC Nº 4*2	Case # 4*2 - [#43***9] - 1ª Notificação - [TLP:AMBER] Possível comprometimento de credenciais [inss.gov.br]	#472 - [#43***9] - 1ª Notificação - [TLP:AMBER] Possível comprometimento de credenciais [inss.gov.br]	Convergente
RIC Nº 4*7	[INC-1764150] Acessos volumétricos e automatizados à API MeuINSS	#4*7 - [TLP:AMBER+STRICT][INSS][INC-17***5*] Acessos volumétricos e automatizados à API MeuINSS	Convergente
RIC Nº 5*8	17***5* : Exportação de informações de forma automatiza por vulnerabilidade explorada	#5*8 – 17***5* : Exportação de informações de forma automatiza por vulnerabilidade explorada	Convergente

Fonte: elaboração própria com base nos RIC disponibilizados e pesquisa no *TheHive*.

Considerando a amostra de 145 alertas ou incidentes, não foram elaborados ou disponibilizados relatórios para 140 incidentes (96,56% do total de registros da amostra).

Ademais, utilizando o número do incidente como base para pesquisa, dos 10 RIC disponibilizados, 30% não possuem correlação com o registro no *TheHive*, conforme demonstrado no quadro 1.

Questionada sobre os Relatórios, em reunião, a DTIR/DTI informa que não são confeccionados relatórios para cada um dos incidentes detectados, diferente daquilo que determina a norma. Conforme padrão instituído pela Equipe, são produzidos relatórios apenas referentes a incidentes inéditos, de grande impacto ou que envolvam vazamento de dados, não sendo feitos, por exemplo, relatórios para incidentes que se repetem. Complementarmente, registram não ter conhecimento de quantos relatórios foram elaborados no período de avaliação da ação[18].

No que se refere à revisão *post-mortem* dos documentos produzidos durante o processo de investigação dos incidentes, verifica-se que essa atividade está comprometida em razão da inexistência das informações mantidas pela unidade auditada, o que inviabiliza o cumprimento do disposto no item 22 do PGIC/INSS.

Pelo exposto, constatou-se que não são elaborados RIC para 96,56% dos incidentes ou dos alertas componentes da amostra, configurando o descumprimento da norma em relação a sua elaboração.

Importante ressaltar que a ausência de Relatórios observada para a quase totalidade de incidentes reduz o aprendizado organizacional e dificulta o aperfeiçoamento dos controles de segurança, tais como os relacionados ao Plano de Conformidade.

As causas para a ausência de RIC estão relacionadas à falta de definição estratégica de controle para monitorar e avaliar a atuação da gestão, aliado à falta de mecanismos de supervisão sobre os procedimentos adotados.

[18] Reunião com DTIR/DTI e ETIR-INSS, em 03.07.2025 – Documento SEI *1853***, Processo SEI nº 35014.03****/2025-**.

Como consequências, têm-se a falta de informações relacionadas aos incidentes cibernéticos tratados e concluídos, essenciais para que a gestão possa acompanhar os resultados advindos das respostas e dos tratamentos realizados sobre os sistemas, serviços, bases de dados e redes do INSS, assim como para avaliar a correção e a amplitude das medidas tomadas na contenção do incidente cibernético, fornecendo subsídios para atuação futura e em medidas preventivas.

5. O INSS não realiza a supervisão dos procedimentos adotados para o tratamento de resposta aos incidentes cibernéticos que envolvam seus ativos informacionais.

O processo de supervisão compreende o acompanhamento, orientação, controle e avaliação das atividades realizadas, com o objetivo de garantir que essas ações estejam alinhadas com normas, metas e padrões de qualidade estabelecidos.

No setor público, a supervisão tem um papel estratégico na promoção da legalidade e da eficiência ao processo de trabalho. A supervisão tem como objetivo orientar servidores sobre suas atribuições e a confecção de documentação, detectando falhas e propondo as correções devidas.

De acordo com o art. 127, 'c', do Regimento Interno do INSS[19], compete à DTIR/DTI supervisionar a execução das fases do gerenciamento de incidentes, em articulação com as demais unidades organizacionais.

O exame demonstrou que não são realizados atestes sobre a completude e a correção dos procedimentos adotados para a resposta dada aos incidentes que envolvam os ativos de informação do INSS, tanto pela ETIR-INSS quanto pelas equipes responsáveis pelo tratamento junto às empresas.

Não foram disponibilizados pela unidade auditada documentos ou processos com as rotinas e/ou fluxos operacionais relativos à supervisão e avaliação da correção dos procedimentos adotados tanto pelos colaboradores da ETIR-INSS ou quanto aos executados pelas empresas terceirizadas no tratamento dos incidentes cibernéticos.[20]

Conforme reforçado pela unidade auditada[21], a supervisão de incidentes cibernéticos não é estruturada ou institucionalizada, não dispondo de documentos decorrentes da supervisão. A unidade declarou ainda que, nos casos de incidentes cibernéticos já conhecidos, não considera necessária a realização de supervisão específica.

---

[19] Aprovado pela Portaria PRES/INSS nº 1.678, de 19.04.2024

[20] Item 5, ii), da Solicitação de Auditoria nº 001/2025, Tarefa e-CGU #1819567 – Documento SEI nº *1090*** - Processo SEI nº 35014.03****/2025-**.

[21] 1. Despacho DTIR/DTI, em 16/06/2025, Documento SEI nº *115**** item 2.3, letra b - Processo SEI nº 35014.03****/2025-**.

2. Reunião com DTIR/DTI e ETIR-INSS, em 03.07.2025 – Documento SEI *1853***, Processo SEI nº 35014.03****/2025-**.

3. Reunião com DTIR/DTI e ETIR-INSS, em 05.08.2025 – Documento SEI *1856***, Processo SEI nº 35014.03****/2025-**.

As causas para a ausência de supervisão do processo de gestão de incidentes no INSS estão relacionadas à deficiência no controle e monitoramento da atuação da gestão.

A ausência de processo de supervisão formalizado e aplicado demonstra fragilidade na gestão do processo de trabalho avaliado, que resulta na falta de uniformidade, baixa qualidade dos procedimentos adotados, conforme observado, além do descumprimento do PGIC/INSS.

6. Ausência de comunicação de incidentes cibernéticos ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo (CTIR Gov).

O repasse e o compartilhamento de informações relacionadas a incidentes cibernéticos fazem parte dos mecanismos estabelecidos para controle de diferentes instâncias e órgãos públicos que se utilizam desses dados para o desenvolvimento de ações que visam à mitigação e à prevenção de tais eventos.

O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov)[22] é integrante do Departamento de Segurança de Cibernética (DSC) da Secretaria de Segurança da Informação e Cibernética (SSIC)[23] do Gabinete de Segurança Institucional (GSI) da Presidência da República (PR).

O CTIR Gov tem por objetivo coordenar e integrar as ações destinadas à gestão de incidentes computacionais em órgãos ou entidades da Administração Pública Federal, bem como: prevenir, monitorar, analisar e mitigar os incidentes de segurança da informação; promover o intercâmbio científico-tecnológico; participar da articulação para o estabelecimento de diretrizes sobre gestão de incidentes computacionais; e criar processo de inteligência de ameaças cibernéticas para subsidiar a criação de políticas públicas e tomada de decisão.

Segundo o art. 12, IV, do Decreto nº 10.748/2021, compete aos órgãos e às entidades da administração pública federal direta, autárquica e fundacional comunicar imediatamente o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, por meio de suas equipes de prevenção, tratamento e resposta a incidentes cibernéticos, sobre a existência de vulnerabilidades ou incidentes de segurança cibernética que impactem ou que possam impactar os serviços prestados ou contratados.

De acordo com o item 5.3 da Portaria GSI/PR nº 120, de 21.12.2022, que aprova o Plano de Gestão de Incidentes Cibernéticos da Administração Pública Federal, após a conclusão do processo de recuperação, os participantes da ReGIC devem encaminhar ao Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) um relatório detalhado do incidente, contendo, no mínimo, as seguintes informações:

- identificação dos atores atacantes e atacados;
- atores envolvidos nas atividades de tratamento e resposta ao incidente;
- evidências coletadas durante a apuração;

[22] Disponível em <https://www.gov.br/ctir/pt-br>
[23] Disponível em <https://www.gov.br/gsi/pt-br/composicao/SSIC>

- indicadores de comprometimento (IoCs) e as respectivas táticas, técnicas e procedimentos (TTPs) observados;
- ativos de infraestrutura, serviços e número total de usuários afetados;
- volume de dados exfiltrados;
- cronologia dos eventos relacionados ao incidente;
- medidas de contenção, erradicação e recuperação adotadas; e
- ações preventivas propostas para evitar a reincidência de ocorrências similares.

Da análise dos RIC encaminhados para os exames, em 6 deles constava o item “Comunicações Realizadas”, como demonstrado no quadro 2.

Quadro 2 - Informações do RIC sobre comunicações realizadas

ID	Data do incidente	Comunicações realizadas
RIC Nº 3*4	21.08.2025	1. DTIR/DTI - Divisão de Prevenção, Resposta e Tratamento de Incidentes 2. CGTIS - Coordenação Geral de Sistemas de Informação e Segurança 3. DTI.CRPS - Divisão de Tecnologia da Informação Conselho de Recursos da Previdência Social 4. ETIR MPS - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos MPS 5. ETIR MTE - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos MTE
RIC Nº 3*2	19.01.2025	1. Encarregado pelo Tratamento de Dados Pessoais do INSS e para: 2. DTIR/DTI - Divisão de Prevenção, Resposta e Tratamento de Incidentes. 3. CGTIS - Coordenação Geral de Sistemas de Informação e Segurança.
RIC Nº 3*6	11.02.2025	1.Comissão de Tratamento e Resposta a Incidentes Cibernéticos – CTIR. 2. Divisão de Prevenção, Resposta e Tratamento de Incidentes – DTIR/DTI. 3. Divisão de Operações em TI – DIOP. 4. Divisão de Segurança em TI – DSEG. 5. Coordenação de Infraestrutura e Mon. de TI – COIM. 6. Coordenação-Geral de Tecnologia da Informação e Segurança – CGTIS
RIC Nº 4*2	24.02.2025	1. Comissão de Tratamento e Resposta a Incidentes Cibernéticos – CTIR Gov.
RIC Nº 4*7	07.03.2025	1. Encarregado pelo Tratamento de Dados Pessoais do INSS e para: 2. DTIR/DTI - Divisão de Prevenção, Resposta e Tratamento de Incidentes. 3. CGTIS - Coordenação Geral de Sistemas de Informação e Segurança.
RIC Nº 5*8	25.04.2025	1. Encarregado pelo Tratamento de Dados Pessoais do INSS e para: 2. DTIR/DTI - Divisão de Prevenção, Resposta e Tratamento de Incidentes. 3. CGTIS – Coordenação-Geral de Sistemas de Informação e Segurança. 4. CGAUT – Coordenação-Geral de Sistemas e Automação.

Fonte: elaboração própria com base nos RIC disponibilizados pela unidade auditada.

Como observa-se do quadro, para os incidentes relatados nos RIC 3*4; 3*2; 4*7 e 5*8 não houve comunicação à CTIR Gov, como estabelecido pelo art. 12, IV, do Decreto nº 10.748/2021.

A unidade auditada informou, em resposta à equipe, desconsiderar a obrigação normativa de comunicar de imediato a ocorrência de todos os incidentes de segurança na sua área de atuação ao CTIR Gov, em que pese a obrigatoriedade imposta pelas normas federais.

A ausência de comunicação tempestiva dos incidentes por parte dos órgãos compromete a capacidade de resposta coordenada da ReGIC, além de fragilizar o monitoramento nacional de ameaças e vulnerabilidades.

A falta de definição de estratégia de controle para monitorar a atuação da gestão, associado a deficiências no fluxo de comunicação e informação e a falta de um processo de supervisão instituído e aplicado periodicamente sobre os procedimentos adotados pelos colaboradores que identificaria as falhas e lacunas são as causas para os achados relacionados às falhas de repasse dos dados relacionados aos incidentes cibernéticos ao CTIR Gov.

Consequentemente, os dados que serviriam de subsídios para análises estatísticas e históricas do Governo Federal não chegam ao conhecimento da área, causando prejuízos à transparência e à gestão de informação relacionada às ocorrências de incidentes no INSS e no Governo Federal.

Conclui-se que ocorrem falhas no envio das informações relacionadas aos incidentes cibernéticos por parte do INSS, devendo ser adequado o fluxo e os procedimentos para o envio de todas as informações para os órgãos que as utilizam como subsídio.

RECOMENDAÇÕES

Recomendação nº 1

Atualizar o Plano de Gestão de Incidentes Cibernéticos para contemplar o monitoramento, avaliação e supervisão dos procedimentos relacionados ao tratamento de incidentes, buscando a sua adequação aos objetivos de segurança cibernética.

Achados nº 1; 3; 4; 5 e 6

Recomendação nº 2

Aprimorar os mecanismos e as rotinas para o registro, acompanhamento, armazenamento e comunicação das informações relacionadas a todos os incidentes cibernéticos, de modo a fornecer as informações quantitativas e qualitativas para a cadeia de gestão.

Achados n° 3; 4 e 6.

Recomendação nº 3

Revisar o contrato firmado com a Dataprev, com vistas a incluir cláusulas específicas que assegurem ao INSS mecanismos adequados de comunicação, transparência e supervisão das atividades relacionadas ao tratamento de incidentes cibernéticos efetuados pela empresa.

Achado nº 2

CONCLUSÃO

A ação buscou avaliar a gestão de incidentes cibernéticos no INSS, sua aderência às normas do Governo Federal e às necessidades internas do órgão decorrentes das informações relacionadas ao processo de trabalho.

Assim, com base nos resultados da avaliação realizada, identificou-se que o processo de gestão de incidentes cibernéticos do INSS possui limitações significativas, com descumprimento de normativos e ausência de mecanismos adequados para a execução do PGIC/INSS.

Conforme verificado, o Instituto não atua em demandas que o incidente cibernético é tratado por empresas terceirizadas, mesmo que envolvam sistemas, serviços, informações e redes do INSS. Essa situação, contudo, não exime o INSS de acompanhar, monitorar, registrar e avaliar os procedimentos adotados, de modo a verificar sua adequação as diretrizes do Instituto e avaliar o impacto nos seus negócios.

O PGIC/INSS atualmente vigente está desatualizado, não sendo alterado desde sua publicação, não tendo sido revisto de modo a contemplar as alterações procedimentais previstas de serem realizadas desde a sua publicação e das novas rotinas procedimentais em uso, tal como o tratamento de incidentes cibernéticos pelas empresas terceirizadas.

Em termos de avaliação dos resultados obtidos pelo processo de tratamento e resposta aos incidentes no INSS, observou-se que o órgão não dispõe das informações necessárias para o acompanhamento do processo de trabalho, com prejuízos ao monitoramento e à governança. Em relação à execução dos procedimentos adotados, não constam rotinas de supervisão e nem a possibilidade de avaliar os procedimentos pelos dados armazenados no sistema de gerenciamento. Também não se adota mecanismos para supervisão e monitoramento das ações e procedimentos adotados pelas empresas terceirizadas envolvidas no tratamento de incidentes nos ativos de informação do órgão, não avaliando a sua adequação aos objetivos Institucionais. Ainda relativo às empresas terceirizadas, observou-se a falta de cláusulas contratuais necessárias para atender as necessidades do órgão.

Pelo exposto, conclui-se que a gestão do processo de trabalho se mostra inefetiva para avaliar os impactos para os negócios do Instituto dos incidentes cibernéticos ocorridos nos sistemas, serviços, rede e informações do INSS, visto que não dispõe de informações de todos os incidentes ocorridos, o que prejudica a avaliação real do impacto no órgão, ficando restrita aos incidentes que são tratados pela ETIR-INSS. De forma consequente, os mecanismos utilizados para o monitoramento e a comunicação restam prejudicados pelo mesmo motivo, visto não disporem, de forma completa, transparente e com qualidade, das informações relativas aos incidentes cibernéticos que envolvem o INSS.

Além disso, o PGIC/INSS normatizado não está sendo executado na forma prevista, e em que pese sua desatualização, sua subutilização prejudica sobremaneira a estruturação do Plano e da gestão sobre os incidentes cibernéticos que envolvam o INSS.

Em termos gerais, observa-se como principal causa dos achados a falta de definição estratégica da gestão para acompanhar a implementação do PGIC/INSS, assim como para monitorar os resultados do plano e para avaliar a execução das atividades propostas à ETIR-INSS.

A fim de proporcionar ao INSS a governança sobre o processo de trabalho, foram propostas recomendações para revisão do PGIC/INSS, contemplando as atualizações já previstas anteriormente, assim como a incorporação de rotinas para a supervisão e monitoramento dos procedimentos adotados por empresas terceirizadas; a implementação de mecanismos e rotinas para o registro, acompanhamento, armazenamento e compartilhamento das informações relacionadas aos incidentes cibernéticos que envolvam sistemas, serviços, redes e informações do órgão; e a revisão contratual com inclusão de cláusulas específicas para reporte ao INSS de incidentes tratados por empresas terceirizadas

ANEXOS

I – MANIFESTAÇÃO DA UNIDADE AUDITADA E ANÁLISE DA EQUIPE DE AUDITORIA

Em resposta à versão preliminar deste relatório, a Diretoria de Tecnologia da Informação por meio de despacho SEI 23714302, encaminhou Nota Técnica (NT) nº 23/2025/CGTIS/DTI-INSS (SEI 23710036) elaborada pela Coordenação-Geral de Tecnologia da Informação e Segurança, em que apresenta manifestação técnica acerca da Auditoria realizada, seus achados e recomendações.

Conforme consta na referida NT, a área informa que a implementação efetiva de ações referentes à gestão de incidentes cibernéticos requer investimentos financeiros, reforço de pessoal e amadurecimento institucional, além do envolvimento e colaboração de outras áreas do INSS, tanto no âmbito da gestão quanto da infraestrutura tecnológica, e argumenta que:

> a ETIR-INSS não detém competência institucional nem capacidade operacional para atuar isoladamente em todas as frentes relacionadas à segurança da informação, sendo imprescindível o envolvimento das áreas técnicas, das áreas de negócio e das instâncias decisórias.

No que concerne às manifestações referentes aos achados e recomendações de auditoria, conforme descrito no item “QUESTIONAMENTOS DA AUDITORIA” da NT, registra-se:

Achado nº 1

Manifestação da unidade auditada

> A Unidade Auditada reconhece a necessidade de atualização do Plano de Gestão de Incidentes Cibernéticos do INSS (PGIC/INSS). Contudo, esclarece que a publicação do referido plano ocorreu em contexto no qual ainda não havia estrutura organizacional, tecnológica e orçamentária plenamente consolidada para atendimento integral das diretrizes nele previstas.
>
> [...]
>
> A Unidade Auditada destaca que, mesmo na ausência de revisão formal do PGIC/INSS, as atividades de prevenção, detecção, análise e tratamento de incidentes vêm sendo executadas pela ETIR-INSS, com base em práticas técnicas consolidadas, orientações emanadas de instâncias centrais de governança digital e frameworks reconhecidos de governança e gestão de TI, como o COBIT 2019, que preconiza a evolução progressiva da capacidade de processos conforme o nível de maturidade organizacional.
>
> Nesse sentido, a ausência de atualização formal do plano não implica paralisação das atividades da ETIR-INSS, tampouco inviabiliza o tratamento de incidentes. O que se verifica é a necessidade de maior formalização e consolidação documental de práticas que já vêm sendo executadas de forma operacional, em um contexto de amadurecimento institucional.
> [...]
> Assim, a ausência de atualização formal do PGIC não decorre de omissão gerencial, mas de processo de amadurecimento institucional, que demanda tempo e investimentos, os quais vêm sendo buscados junto às instâncias competentes.

Achado nº 2

Manifestação da unidade auditada

Ressalta-se que a ETIR não detém competência para alterar unilateralmente cláusulas contratuais, sendo tais ajustes dependentes de processos formais de revisão contratual. Não obstante, a gestão reconhece a oportunidade de aprimoramento e vem avaliando a inclusão de cláusulas específicas relacionadas à segurança da informação em futuras contratações e revisões, em alinhamento às orientações normativas vigentes.

Achado nº 3

Manifestação da unidade auditada

Quanto à alegada insuficiência de informações gerenciais e indicadores, a Unidade Auditada esclarece que a decisão de não manter painéis públicos de incidentes decorreu de avaliação técnica de risco, considerando a sensibilidade das informações e o potencial de exploração adversa.

[...]

A Unidade Auditada esclarece que o sistema de gestão de incidentes *TheHive* não se encontrava em produção no início do período analisado pela auditoria, tendo sua implantação ocorrido de forma gradual, após fase de configuração, testes e capacitação da equipe técnica.

[...] a Unidade Auditada esclarece que tal percentual reflete, majoritariamente, incidentes tratados em período anterior à consolidação do *TheHive* como ferramenta oficial, não caracterizando falha de controle ou de registro no período em que o sistema já se encontrava em produção e operacionalmente estabilizado.

Ressalta-se, ainda, que durante o período de transição, os registros dos incidentes foram mantidos por meio de outros instrumentos internos de controle, tais como planilhas, registros de chamados, e-mails institucionais e procedimentos operacionais internos, os quais permitiram o acompanhamento, a rastreabilidade mínima e a gestão dos incidentes, ainda que fora da plataforma *TheHive*.

A Unidade Auditada reconhece que a centralização dos registros em sistema único de gestão representa avanço relevante de maturidade e, nesse sentido, reafirma que, a partir da efetiva entrada em produção do *TheHive*, os incidentes passaram a ser registrados de forma sistemática, reforçando a governança, a rastreabilidade e a capacidade de análise histórica.

Achado nº 4

Manifestação da unidade auditada

No tocante à ausência de Relatórios de Incidente Cibernético (RIC) para todos os eventos tratados, a Unidade Auditada esclarece que deveria ser adotada avaliada em risco e materialidade. Dessa forma, a elaboração de RIC detalhado é priorizada para incidentes relevantes, inéditos ou com impacto significativo, não sendo considerada proporcional sua produção individualizada para incidentes repetitivos ou de baixo impacto.

A revisão do PGIC/INSS contemplará a formalização de critérios objetivos para definição da necessidade de elaboração de RIC.

Achado nº 5

Manifestação da unidade auditada

> Quanto à supervisão dos incidentes, a Unidade Auditada esclarece que o acompanhamento ocorre predominantemente de forma técnica e integrada aos fluxos operacionais da área, ainda que nem sempre formalizado em registros específicos. A inexistência de determinados documentos não implica ausência de supervisão, mas indica oportunidade de aprimoramento dos mecanismos formais de controle e registro.
>
> [...]
> Nesse sentido, a gestão avalia a instituição de rotinas formais de supervisão e validação, de modo a fortalecer a rastreabilidade das ações e atender às recomendações da auditoria.

Achado nº 6

Manifestação da unidade auditada

> No que se refere à comunicação ao CTIR Gov, a Unidade Auditada reconhece a necessidade de aperfeiçoamento do fluxo de notificação. Contudo, esclarece que há distinção técnica entre alertas, tentativas e incidentes cibernéticos efetivos, sendo que nem todos os eventos tratados possuem impacto ou criticidade que justifiquem comunicação imediata.
>
> A gestão pretende revisar e formalizar critérios de notificação, alinhando-os às diretrizes vigentes, de forma a assegurar conformidade normativa sem comprometer a eficiência operacional da ETIR.

Análise da equipe de auditoria

Após análise da manifestação apresentada pela unidade auditada, conclui-se que não foram identificados elementos que justifiquem a revisão dos achados ou das recomendações constantes no relatório preliminar.

As justificativas apresentadas, embora contextualizem as dificuldades enfrentadas pela unidade, não afastam as fragilidades apontadas nem comprovam a adoção efetiva de medidas corretivas capazes de mitigar os riscos identificados. Assim, mantêm-se os achados de auditoria e as respectivas recomendações.

Diante do exposto e, considerando a ausência de manifestação da área auditada quanto aos prazos para implementação das medidas propostas, estabelece-se o prazo de 180 dias para atendimento das recomendações constantes neste Relatório Final, contado a partir da data de cadastramento no sistema e-CGU.

INSTITUTO NACIONAL DO SEGURO SOCIAL
AUDITORIA-GERAL

AUDITORIA-GERAL
Setor de Autarquias Sul, Quadra 2, Bloco O
Edifício-Sede do Instituto Nacional do Seguro Social
6° andar, Sala 619
70070-946 - Brasília/DF
(61) 3313-4587
audger@inss.gov.br

INSTITUTO NACIONAL DO SEGURO SOCIAL

AUDITORIA-GERAL