INSTITUTO NACIONAL DO SEGURO SOCIAL
Auditoria-Geral

RELATÓRIO DE AVALIAÇÃO

Avaliação da aderência do Sistema de Atendimento (SAT) às normas de segurança da informação

Diretoria de Tecnologia da Informação

Brasília/DF, dezembro de 2022

Instituto Nacional do Seguro Social
Auditoria-Geral
Coordenação-Geral de Auditoria em Gestão Interna
Coordenação de Auditoria em Gestão Interna
Auditoria Regional Salvador

Unidade Examinada: Diretoria de Tecnologia da Informação.

Missão

Aumentar e proteger o valor organizacional, fornecendo avaliações, assessoria e conhecimento objetivos, baseados em risco, a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de governança, gerenciamento de riscos e controles.

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?

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.

O sistema SAT é constituído do módulo Central, um portal de sistemas e serviços previdenciários para auxiliar ao atendimento na obtenção de informações previdenciárias, e do módulo Local, uma solução de atendimento presencial que vai do gerenciamento da fila de atendimentos, à chamada ao balcão, à realização do atendimento e sua finalização.

2. POR QUE A AUDITORIA REALIZOU ESSE TRABALHO?

A presente ação de auditoria está prevista no Plano de Auditoria Interna (PAINT) 2022, cuja elaboração foi baseada nos riscos de cada processo de trabalho, e abordou especificamente o processo de atendimento ao cidadão.

A motivação para a realização do trabalho considerou aspectos relativos à materialidade, criticidade e relevância do tema para o Instituto. Em 2021, foram realizados mensalmente, em média, 1.252.526 atendimentos presenciais.

3. QUAIS AS CONCLUSÕES ALCANÇADAS? QUAIS RECOMENDAÇÕES DEVERÃO SER ADOTADAS?

Na análise realizada, esta ação de auditoria constatou:

1. Ausência de controles que possibilitem a confirmação dos dados produzidos pelo Painel Monitoramento do Acordo dos Níveis de Serviços (ANS), nos casos de possíveis divergências identificadas pela Fiscalização do Contrato.
2. Plano de contingência do sistema SAT não aborda o tratamento de incidentes de segurança e não inclui o SAT Local.
3. Ausência da avaliação dos requisitos de segurança da informação, por parte da DTI, das demandas de desenvolvimento relacionadas ao sistema SAT.
4. Ausência de processo de gestão de riscos de segurança da informação.

Nesse sentido, foram emitidas as seguintes recomendações:

1. Instituir controles e monitoramentos que sejam capazes de identificar de forma automatizada paradas e indisponibilidades do sistema SAT e suas respectivas causas, de modo a confirmar ou contrapor os dados fornecidos pela Contratada relacionados ao ANS.
2. Estabelecer padrão técnico a ser seguido pela Contratada na elaboração do Plano de Recuperação de Desastres (PRD) do sistema SAT (Central e Local), incluindo minimamente cenários de incidentes e indisponibilidades por motivo de segurança da informação,

conforme disposto no tópico de Gestão da continuidade do negócio da ABNT NBR ISO/IEC 27001.

3. Estabelecer rotina de supervisão técnica relacionada aos requisitos de segurança da informação, no que diz respeito às demandas de desenvolvimento do sistema SAT e suas respectivas homologações.
4. Instituir o processo de gestão de riscos de segurança da informação do INSS, de que trata o art. 12 da IN nº 3/2021 GSI/PR, abrangendo:
    a. O Plano de Gestão de Riscos de Segurança da Informação (PGRSI), de acordo com o art. 13 da IN nº 3/2021 GSI/PR.
    b. O Relatório de Identificação, Análise e Avaliação dos Riscos de Segurança da Informação (RIAARSI), de acordo com o art. 14 da IN nº 3/2021 GSI/PR.
    c. O Relatório de Tratamento de Riscos de Segurança da Informação (RTRSI), de acordo com o art. 15 da IN nº 3/2021 GSI/PR.

LISTA DE SIGLAS E ABREVIATURAS

ANS	Acordo de Níveis de Serviço
AUDGER	Auditoria-Geral
AUDSAL	Auditoria Regional em Salvador
Clarity	CA Clarity PPM (aplicação de Gestão de Projetos e Portfólios)
Dataprev	Empresa de Tecnologia e Informações da Previdência
DIGOV	Diretoria de Governança, Planejamento e Inovação
DTI	Diretoria de Tecnologia da Informação
GSI	Gabinete de Segurança Institucional
IN	Instrução Normativa
INSS	Instituto Nacional do Seguro Social
Neo POSIN	Nova Política de Segurança da Informação do INSS
NT	Nota Técnica
PAINT	Plano de Auditoria Interna
POSIN	Política de Segurança da Informação do INSS
PR	Presidência da República
PRD	Plano de Recuperação de Desastres
SAT	Sistema de Atendimento
SDM	CA Service Desk Manager (aplicação de registro e consulta de chamados)
SI	Segurança da Informação
SI	Segurança da Informação
TIC	Tecnologia da Informação e Comunicações

SUMÁRIO

1 INTRODUÇÃO

A presente Ação de Auditoria teve como objetivo a 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. Foram analisadas as informações presentes na contratação da Dataprev, como empresa provedora de soluções de tecnologia da informação previdenciárias para o INSS, no que tange ao sistema SAT. Foram também analisadas as demandas de desenvolvimento referentes ao sistema SAT no ano de 2021.

A Segurança da Informação (SI) é definida pelo Gabinete de Segurança Institucional (GSI) da Presidência da República (PR) como um conjunto de ações que objetiva viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações[1] (princípios de SI). Essas ações abrangem: a segurança cibernética; a defesa cibernética; a segurança física; a proteção de dados organizacionais; e as ações destinadas a assegurar os citados princípios de SI[2].

No Governo Federal, a SI é normatizada pelas Instruções Normativas (IN) nºs 1, 2 e 3, do GSI/PR, de 27 de maio e 24 de julho de 2020 e de 28 de maio de 2021, respectivamente.

Nesse contexto, o Instituto Nacional do Seguro Social (INSS) utiliza o sistema SAT, módulos Central e Local, como ferramenta computacional para gerir e auxiliar no atendimento ao cidadão. Esse sistema é desenvolvido e mantido pela Empresa de Tecnologia e Informações da Previdência (Dataprev), empresa pública criada para atender as necessidades de Tecnologia da Informação e Comunicações (TIC) da Previdência Social. As diretrizes do ambiente relacionadas à SI são definidas contratualmente, bem como os níveis de serviço são pactuados entre as partes por Acordo de Níveis de Serviço (ANS). Como ferramenta de gestão de demandas de desenvolvimento, o INSS utiliza a ferramenta Clarity, definida e mantida pela Contratada.

Assim, para realizar o atendimento à população, o Instituto conta com uma rede de aproximadamente 1.700 unidades de atendimento, distribuídas em 1.443 municípios no território nacional. Nessas unidades, o Sistema de Atendimento (SAT) módulo Local é utilizado para a recepção do cidadão, triagem, controle da fila e realização do atendimento, coletando e registrando informações inerentes ao processo. Sua execução e utilização é realizada na própria unidade.

Em paralelo, o Sistema de Atendimento (SAT) módulo Central é utilizado como um agregador de sistemas previdenciários, provendo informações a serem utilizadas durante o atendimento do cidadão na unidade. Esse sistema também é utilizado, de forma remota, por órgãos externos visando disponibilização de informações previdenciárias aos entes públicos.

A tabela a seguir lista o total de atendimentos/requerimentos nos quais foi utilizado o sistema SAT (Central ou Local) como plataforma de agendamento, atendimento e/ou consulta.

[1] SEGURANÇA DA INFORMAÇÃO, Glossário de Segurança da Informação, Anexo, Portaria GSI/PR nº 93, de 18 de outubro de 2021
[2] Art. 3, Instrução Normativa nº 1 /GSI/PR, de 27 de maio de 2020.

Tabela 1: Média mensal de atendimentos em 2021

Item	Descrição	Quantitativo médio mensal
Atendimento Presencial	Atendimentos presenciais	1.252.526
Requerimento Central135	Requerimentos solicitados pelo canal Central 135 a serem atendidos à distância	343.312
	Requerimentos solicitados pelo canal Central 135 a serem atendidos presencialmente (agendamento)	120.027
Requerimento Internet	Requerimentos solicitados pelo canal Internet a serem atendidos à distância	841.615
	Requerimentos solicitados pelo canal Internet a serem atendidos presencialmente (agendamento)	88.618
Requerimento Intranet	Requerimentos solicitados pelo canal Intranet a serem atendidos à distância	317.836
	Requerimentos solicitados pelo canal Intranet a serem atendidos presencialmente (agendamento)	21.414
Agendamento via PMF	Quantidade de agendamento	294.404
Requerimento via SABI/SABIweb	Quantidade de requerimento	299.560
Acesso MEU INSS	Quantidade de Acessos ao MEU INSS	36.743.705
Assistente Virtual	Quantidade de Utilizações da Assistente Virtual do Meu INSS	1.836.062

Fonte: INSS (SEI 6619482).

Considerando o acima exposto, e o objetivo da presente Ação de Auditoria, buscou-se respostas às seguintes questões e subquestões de auditoria:

1. O sistema SAT mantém aderência aos princípios de disponibilidade, integridade, confidencialidade e autenticidade das informações?
    a. Houve paradas/indisponibilidades do sistema SAT superiores ao definido no Acordo de Níveis de Serviços (princípio da disponibilidade)?
    b. As ferramentas de acompanhamento/monitoramento e os procedimentos de contingência mitigam os efeitos causados por incidentes/indisponibilidades, físico ou lógico (princípio da integridade)?
    c. As medidas adotadas no sistema SAT para prevenir acessos indevidos asseguram que pessoas desautorizadas não acessem o sistema SAT e suas informações (princípio da confidencialidade)?
    d. As medidas adotadas no sistema SAT para comprovação de autenticidade da informação garantem a veracidade da sua autoria (princípio da autenticidade)?
2. As solicitações e aceites de demandas de desenvolvimento cadastradas no sistema Clarity da Dataprev, concernentes ao sistema SAT, atendem aos princípios de segurança da informação definidos pela Neo POSIN INSS e NC nº 07 /IN01/DSIC/GSIPR?
3. Foi definido processo de gestão de riscos de segurança da informação para o sistema SAT, de acordo com os arts. 12 a 15 da IN nº 3/2021 GSI/PR?
    a. Foi elaborado Plano de Gestão de Riscos de Segurança da Informação, de acordo com o art. 13 da IN nº 3/2021 GSI/PR?
    b. Foi elaborado Relatório de Identificação, Análise e Avaliação dos Riscos de Segurança da Informação, de acordo com o art. 14 da IN nº 3/2021 GSI/PR?

c. Foi elaborado Relatório de Tratamento de Riscos de Segurança da Informação, de acordo com o art. 15 da IN nº 3/2021 GSI/PR?

Os exames foram realizados utilizando as técnicas de indagação à área auditada, análise documental e correlação das informações obtidas.

2 RESULTADOS DOS EXAMES

2.1 Ausência de controles que possibilitem a confirmação dos dados produzidos pelo Painel Monitoramento do Acordo dos Níveis de Serviços (ANS), nos casos de possíveis divergências identificadas pela Fiscalização do Contrato.

A IN nº 1/2019 SGD/ME define mecanismos de controle do fornecimento de solução de TIC[3], procedimentos de teste e inspeção[4] e a necessidade da avaliação da qualidade dos serviços realizados ou dos bens entregues, com suas devidas justificativas[5]. Nesse sentido, o Contrato nº 30/2022 prevê que o INSS receba mensalmente relatórios de disponibilidade do sistema SAT[6], monitore os serviços prestados e meça os níveis mínimos de serviço entregues pela Contratada[7].

O Regimento Interno do INSS, por sua vez, atribui à DTI o papel de planejar e monitorar a estrutura de tecnologia da informação do Instituto[8].

O INSS utiliza ferramenta de monitoramento disponibilizada pela Contratada (Painel de Monitoramento), que afere mensalmente, de forma automatizada, registros de paradas/ indisponibilidades do sistema SAT. Os relatórios obtidos pela referida ferramenta, em todas as competências referentes ao período auditado, de 2021, não apontaram ocorrências de indisponibilidade fora dos níveis acordados no ANS do Sistema SAT. Os relatórios extraídos dessa ferramenta são utilizados como base para o faturamento mensal apresentado pela Contratada ao INSS.

O INSS utiliza, paralelamente, sistemas de monitoramento próprios e de registros de chamados, que apontam paradas/indisponibilidades no sistema SAT, entre eles os sistemas CASA, SDM, Suporte INSS e controle de metas do GET.

Embora de forma não automatizada, o sistema CASA apresenta uma fotografia em tempo real da disponibilidade do sistema SAT nas unidades de atendimento, independentemente do monitoramento apresentado pela Contratada.

Os sistemas SDM e Suporte INSS são utilizados para a abertura de chamados referentes a indisponibilidades e paradas do sistema SAT, registrados por usuários, também de maneira independente do monitoramento apresentado pela Contratada.

A aferição e controle de metas do GET realizado pelo INSS disponibiliza relatórios mensais que evidenciam a impossibilidade de realização de atendimentos devido a paradas do sistema SAT, implicando em redução de metas de servidores.

[3] Alínea d, inciso III, art. 17 da IN nº 1/2019 SGD/ME, de 4 de abril de 2019.
[4] Itens 1 e 2, alínea a, inciso II, art. 19 da IN nº 1/2019 SGD/ME, de 4 de abril de 2019.
[5] Alínea b, inciso II, art. 33 da IN nº 1/2019 SGD/ME, de 4 de abril de 2019.
[6] Alíneas XIII, XVI, XXXIV, XXXV, subitem 5.2 do Projeto Básico do Contrato nº 30/2022 INSS/Dataprev
[7] Alínea 7.2.4, subitem 7.2; do Projeto Básico do Contrato nº 30/2022 INSS/Dataprev
[8] Incisos I, III, VII e VIII, art. 12 do Decreto nº 10.995/2022, de 14 de março de 2022.

Todavia, o Instituto não dispõe de um sistema que realize, de forma automatizada e independente, a coleta de dados de disponibilidade do sistema SAT, o que tornaria possível ao Instituto confrontar as informações prestadas pelo citado Painel de Monitoramento. Desse modo, os referidos dados obtidos pela gestão e fiscalização do contrato não são reconhecidos como tendo acuracidade técnica pela Contratada, prevalecendo as informações de disponibilidade do sistema obtidas do Painel.

Inclusive, através dos Ofícios nºs 05/2019 e 14/2019, a DTI relacionou possíveis divergências das informações de indisponibilidades obtidas pelo sistema de monitoramento da Contratada e registros próprios. Verifica-se a existência de questionamentos acerca da confiabilidade dos dados produzidos pelo citado Painel por parte da área gestora do contrato, conforme descrito no Ofício citado.

O referido Ofício nº 05/2019, por exemplo, emitido em 01 de novembro de 2019, relata:

> 2. Complementarmente, informo que o Relatório de Gerenciamento de Níveis de Serviço encaminhado mensalmente para o INSS não nos atende para este fim, visto que os incidentes de indisponibilidades relacionados não batem com os incidentes registrados no SDM e tampouco os registros de reclamações dos usuários de toda a rede INSS.

Considerando os fatos apresentados, percebe-se que o Instituto carece de controles automatizados para o efetivo monitoramento da disponibilidade do sistema SAT, visando obter informações que sejam tecnicamente corretas e válidas como fundamento a ser apresentado à Contratada quando das tratativas sobre eventuais divergências.

Questionada acerca do tema, a DTI informou que está engajando esforços na implantação de ferramenta em software livre que possibilite o monitoramento da disponibilidade do sistema SAT de forma automatizada e independente do monitoramento oferecido pela Contratada, como forma de corroborar ou contestar os dados fornecidos pelo Painel de Monitoramento. Trata-se da ferramenta Zabbix[9], que se encontra em testes no INSS, já em coleta inicial de dados.

Ante o exposto, devido à ausência de uma estratégia própria de controle para monitoramento de aplicações do INSS, buscando avaliar, direcionar e monitorar o sistema SAT (Central e Local), capaz de contrapor ou confirmar as informações relatadas pela Contratada, identificou-se a impossibilidade de o Instituto confirmar a veracidade dos dados apresentados pela Contratada referentes ao ANS do sistema SAT.

2.2 Plano de contingência do sistema SAT não aborda o tratamento de incidentes de segurança e não inclui o SAT Local.

Conforme previsão do Contrato nº 30/2022, a Contratada deve manter planos de contingência que garantam a disponibilidade dos sistemas e dados implantados e armazenados nas suas dependências e disponibilizados à DTI quando solicitados[10]. Estes planos devem estar em

[9] Zabbix monitoring system (https://www.zabbix.com), da Zabbix LLC, é um software livre e de código aberto, que utiliza a licença GNU General Public License (GPL) version 2.
[10] Item XXXIX da Cláusula 5.2. do Contrato nº 30/2022.

consonância com a Política de Segurança da Informação do INSS (Neo POSIN INSS), a qual dispõe que todo incidente de segurança da informação deve ser imediatamente relatado à DTI.

A Neo POSIN INSS dispõe, ainda, que os ativos de informação que suportam as atividades críticas do Instituto devem ser amparados por ambiente de alta disponibilidade e ter capacidade de recuperação em prazos e condições previamente definidos para situações de contingência, devendo ser itens contratuais[11]. Finalmente, o gerenciamento de continuidade de serviço também são práticas amplamente embasadas tanto pelo ITIL v4[12] quanto pelo COBIT 2019[13].

Complementarmente, de acordo com o disposto no tópico A.14 Gestão da continuidade do negócio da ABNT NBR ISO/IEC 27001:2006, temos:

A.14.1 Aspectos da gestão da continuidade do negócio, relativos à segurança da informação
Objetivo: Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso.

A.14.1.1	Incluindo segurança da informação no processo de gestão da continuidade de negócio	Controle Um processo de gestão deve ser desenvolvido e mantido para assegurar a continuidade do negócio por toda a organização e que contemple os requisitos de segurança da informação necessários para a continuidade do negócio da organização.
A.14.1.2	Continuidade de negócios e análise/avaliação de risco	Controle Devem ser identificados os eventos que podem causar interrupções aos processos de negócio, junto à probabilidade e impacto de tais interrupções e as conseqüências para a segurança de informação.
A.14.1.3	Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação	Controle Os planos devem ser desenvolvidos e implementados para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio.
A.14.1.4	Estrutura do plano de continuidade do negócio	Controle Uma estrutura básica dos planos de continuidade do negócio deve ser mantida para assegurar que todos os planos são consistentes, para contemplar os requisitos de segurança da informação e para identificar prioridades para testes e manutenção.
A.14.1.5	Testes, manutenção e reavaliação dos planos de continuidade do negócio	Controle Os planos de continuidade do negócio devem ser testados e atualizados regularmente, de forma a assegurar sua permanente atualização e efetividade.

Adicionalmente, a publicação Boas Práticas em Segurança da Informação[14], do TCU, salienta que o Plano de Continuidade de Negócios (PCN) consiste em um conjunto de estratégias e procedimentos que devem ser adotados quando a instituição ou uma área, depara-se com problemas que comprometem o andamento normal dos processos e a consequente prestação de serviços. Tem como objetivo, dentre outros, garantir que o funcionamento dos sistemas informatizados seja restabelecido no menor tempo possível a fim de reduzir os impactos causados por fatos imprevistos.

[11] Incisos II e IV, Art 5º, Resolução nº 9/2020 CEGOV/INSS, de 31 de agosto de 2020.
[12] Gerenciamento de continuidade de serviço, Práticas de gerenciamento de serviços, ITIL v4 (2019).
[13] DS4. Assegurar Continuidade de Serviços, Processo Entregar e Suportar, COBIT 2019.
[14] Capítulo 3 Plano de Continuidade do Negócio, Boas Práticas em Segurança da Informação, 4ª edição, TCU.

Também o Acórdão nº 1603/2008 - TCU-Plenário, no item 9.2, recomenda ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR), que oriente os órgãos/entidades da Administração Pública Federal sobre a importância da segurança da informação, promovendo, inclusive, mediante orientação, ações que visem estabelecer e/ou aperfeiçoar a gestão de continuidade do negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos de TI, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso.

Por fim, a Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021 estabelece em seu art. 22 que o plano de continuidade de negócios em segurança da informação tem por objetivo definir como serão realizadas a gestão dos incidentes em caso de desastres ou de outras interrupções das operações de negócios e a maneira como deverão ser recuperadas as atividades nos prazos estabelecidos.

Entretanto, o Plano de Recuperação de Desastres (PRD) do sistema SAT que se equivale ao plano de continuidade de negócios, elaborado pela Contratada e apresentado à DTI, não trata da recuperação do sistema SAT Central no caso de incidentes e/ou indisponibilidades relacionados à segurança da informação, bem como não apresenta situações de recuperação para o sistema SAT Local. O PRD limita-se a tratar de situações de "Servidor de aplicação do SAT Central corrompido" e de "Perda do balanceamento - VIP do SAT". Ambas as situações, relacionadas ao SAT Central.

Ressalte-se que, por meio de Nota Técnica (NT), destinada à Presidência e Diretorias, a DTI expôs medidas e propôs ações de tratamento e resposta a incidentes cibernéticos no âmbito do INSS[15], incluindo o sistema SAT como possível alvo de ataques cibernéticos, principalmente quanto à tentativa de obtenção de credenciais de usuários e perfis de acesso.

Diante do exposto, verifica-se a inexistência de um ambiente de controle, com processos definidos no que tange a controle de falhas e acompanhamento da execução de sistemas corporativos, falhas na disponibilização de informações e comunicações claras acerca dos requisitos de segurança da informação necessários ao INSS, e ausência do monitoramento da continuidade do negócio do Instituto no que tange ao mapeamento de riscos. Estes fatores têm como consequência direta a possibilidade de indisponibilidade do sistema SAT em níveis superiores ao tolerável em caso de incidente de segurança.

2.3 Ausência da avaliação dos requisitos de segurança da informação, por parte da DTI, das demandas de desenvolvimento relacionadas ao sistema SAT.

Segundo o disposto no Regimento Interno do INSS[16], a DTI deve planejar, coordenar, normatizar e supervisionar os projetos de desenvolvimento e manutenção de sistemas, infraestrutura tecnológica entre outras atividades de tecnologia da informação e comunicação, bem como exercer as funções de unidade de planejamento, monitoramento e avaliação da estratégia de tecnologia da

[15] Nota Técnica nº 1/2021 /CGIN/DTI-INSS, de 13 de setembro de 2021.
[16] Itens I, III, IV, VII e VIII, Art. 12 do Decreto nº 10.995, de 14 de março de 2022.

informação e da comunicação. A DTI deve, ainda, coordenar as atividades de ciência de dados e de análises estruturadas, e também estabelecer diretrizes, normas e padrões técnicos de implantação, utilização e modernização dos sistemas corporativos, em articulação com as demais unidades organizacionais.

Nessa linha, o Contrato nº 30/2022, prevê que a Contratada deverá definir, em conjunto com a DTI, todos os requisitos não funcionais envolvidos, principalmente os de integração, sustentação e de segurança da informação[17]. Do mesmo modo, a Neo POSIN INSS[18] define diretrizes para a aplicação da Política de Segurança da Informação do Instituto, tendo por objetivo estabelecer e difundir diretrizes e princípios de SI.

Todavia, verificou-se que a DTI não está efetivamente envolvida no fluxo de análise de requisitos de segurança da informação no processo de execução de demandas para o sistema SAT, conforme relatos da área (em resposta a Solicitações de Auditoria – SA) e análises de demandas de desenvolvimento. A decisão acerca de funcionalidades para o sistema fica a cargo da própria área solicitante e da Contratada. Dessa forma, o papel da DTI encontra-se restrito ao controle da fila de demandas e de decisão orçamentária.

Ao analisar as demandas de desenvolvimento registradas no sistema Clarity para o sistema SAT, no ano de 2021, verificou-se ausência de avaliação ou direcionamento da DTI sobre quesitos de segurança da informação.

No detalhamento do processo de gestão de demandas de desenvolvimento do sistema SAT, observou-se o desempenho do papel de aprovação financeira e análise de fila das demandas por parte da DTI. Não foram obtidas, todavia, evidências da análise de demandas sob a ótica de segurança da informação.

Devido à inobservância da competência regimental da DTI e do seu papel na gestão contratual, aplicações são desenvolvidas pela Contratada sem a devida supervisão técnica da DTI em relação aos requisitos de segurança da informação, sendo o desenvolvimento de funcionalidades, no caso do sistema SAT, realizado sem planejamento e supervisionamento no contexto da estratégia de tecnologia da informação do Instituto, ficando este suscetível a ser realizado sem diretrizes, normas e padrões técnicos de segurança da informação.

2.4 Ausência de processo de gestão de riscos de segurança da informação.

Conforme disposto na Instrução Normativa nº 3/2021 /GSI/PR, de 28 de maio de 2021, a gestão de segurança da informação deve ser mantida e implementada de forma contínua, buscando manter o alinhamento com a evolução da tecnologia e de seus riscos, identificando os fatores internos e externos que podem impactar no alcance dos objetivos do Instituto.

[17] Item 6.3.1.5 do Projeto Básico do Contrato INSS/Dataprev nº 30/2022.
[18] Resolução nº 9/2020 CEGOV/INSS, de 31 de agosto de 2020.

Nesse sentido, em relação ao processo de gestão de riscos de segurança da informação, o referido normativo, em seu art. 12, prevê:

> Art. 12. O processo de gestão de riscos de segurança da informação deverá fornecer à organização os seguintes documentos:
> I - plano de gestão de riscos de segurança da informação;
> II - relatório de identificação, análise e avaliação dos riscos de segurança da informação; e
> III - relatório de tratamento de riscos de segurança da informação.

Do mesmo modo, os arts. 13 a 15 da mesma norma disciplinam acerca do conteúdo e forma de apresentação dos citados documentos.

Todavia, verificou-se durante os exames, que não foram elaborados os citados documentos. Questionada a respeito, a DTI informou ser de responsabilidade da Contratada sua elaboração e que a Diretoria de Governança, Planejamento e Inovação (DIGOV) é a responsável pelos parâmetros afetos ao tema.

Entretanto, a referida IN prevê, no art. 16, que cabe ao gestor de segurança da informação de cada órgão ou entidade a coordenação da gestão de riscos de segurança da informação, a designação de servidor efetivo do órgão como agente responsável pela gestão de riscos de segurança da informação, a aprovação dos documentos citados e a proposição de medidas preventivas à alta administração. Além disso, cabe ao agente designado a elaboração dos documentos do processo de gestão de riscos de segurança da informação, conforme art. 17 da mencionada IN.

Desse modo, observou-se a ausência de uma definição de estratégia de controle para avaliar, direcionar e monitorar os riscos da segurança de informação implantada no Instituto, impactando na possibilidade de suscetibilidade a incidentes de segurança da informação e na ausência de identificação e tratamento de riscos.

3 RECOMENDAÇÕES

Objetivando o tratamento dos achados relatados, recomendamos a adoção das medidas elencadas a seguir:

Recomendação nº 1: Instituir controles e monitoramentos que sejam capazes de identificar de forma automatizada paradas e indisponibilidades do sistema SAT e suas respectivas causas, de modo a confirmar ou contrapor os dados fornecidos pela Contratada relacionados ao ANS.

Achado nº 2.1

Recomendação nº 2: Estabelecer padrão técnico a ser seguido pela Contratada na elaboração do Plano de Recuperação de Desastres (PRD) do sistema SAT (Central e Local), incluindo cenários de incidentes e indisponibilidades por motivo de segurança da informação, conforme disposto no tópico de Gestão da continuidade do negócio da ABNT NBR ISO/IEC 27001.

Achado nº 2.2

Recomendação nº 3: Estabelecer rotina de supervisão técnica relacionada aos requisitos de segurança da informação, no que diz respeito às demandas de desenvolvimento do sistema SAT e suas respectivas homologações.

Achado nº 2.3

Recomendação nº 4: Instituir o processo de gestão de riscos de segurança da informação do INSS, de que trata o art. 12 da IN nº 3/2021 GSI/PR, abrangendo:

4.1: O Plano de Gestão de Riscos de Segurança da Informação (PGRSI), de acordo com o art. 13 da IN nº 3/2021 GSI/PR.

4.2: O Relatório de Identificação, Análise e Avaliação dos Riscos de Segurança da Informação (RIAARSI), de acordo com o art. 14 da IN nº 3/2021 GSI/PR.

4.3: O Relatório de Tratamento de Riscos de Segurança da Informação (RTRSI), de acordo com o art. 15 da IN nº 3/2021 GSI/PR.

Achado nº 2.4

4 CONCLUSÃO

Após a realização dos testes de auditoria, embora as principais diretrizes referentes à segurança da informação estejam abarcadas contratualmente, foi identificada a ausência de controles automatizados relacionados à obtenção de dados referentes à disponibilidade do sistema SAT (Central e Local), que possibilitem ao INSS a aferição das às informações fornecidas pelo Painel Monitoramento do Acordo dos Níveis de Serviços (ANS). Foi também identificado que o plano de contingência do sistema SAT, elaborado pela Contratada, não aborda o tratamento de incidentes de segurança da informação e não inclui cenários para o módulo Local.

Constatou-se também a ausência da avaliação dos requisitos de segurança da informação, por parte da DTI, nas demandas de desenvolvimento relacionadas ao sistema SAT, tanto para novas funcionalidades quanto para melhorias ou correções no sistema. Identificou-se também a ausência do Plano de Gestão de Riscos de Segurança da Informação, do Relatório de Identificação, Análise e Avaliação dos Riscos de Segurança da Informação e do Relatório de Tratamento de Riscos de Segurança da Informação, definidos como essenciais pela IN 3/2021 /GST/PR.

Buscando sanar as irregularidades evidenciadas, bem como aprimorar o processo de trabalho examinado, foram emitidas recomendações visando: a possibilidade de o INSS aferir e gerenciar paradas/ indisponibilidades do sistema SAT, de forma efetiva e automatizada, e a possibilidade de contraprova aos dados apresentados pela Contratada por meio do Painel de Monitoramento, aumentando os controles e agregando valor a gestão; a recuperação do sistema SAT de forma controlada e otimizada, com o mínimo de custo e impacto, em caso de incidentes e indisponibilidades por motivo de segurança; uma maior observância dos requisitos de segurança da informação no desenvolvimento e homologação de funcionalidades para o sistema SAT e o aprimoramento do processo de desenvolvimento do sistema SAT; e a identificação e tratamento de riscos de segurança da informação relacionados ao sistema SAT e a mitigação de riscos de indisponibilidade do sistema SAT.

5 ANEXO I - MANIFESTAÇÃO DA UNIDADE AUDITADA E ANÁLISE DA EQUIPE DE AUDITORIA

Considerando a manifestação da Diretoria de Tecnologia da Informação e suas respectivas Coordenações-Gerais e Coordenação de Governança e Planejamento em TI, por meio do Despacho SEI nº 9998566, em 20.12.2022, apresenta-se a seguir a análise realizada pela equipe de auditoria:

Inicialmente, a DTI elenca atividades em andamento relevantes ao tema auditado:

> *2. Inicialmente esclarecemos as atividades em andamento nesta diretoria:*
> - *A Divisão de Operações - DIOP, vem trabalhando na modernização do ambiente local das unidades de atendimento do INSS, onde o sistema auditado está inserido;*
> - *Entre as recomendações de melhoria, está a proposta de redesenho do sistema para que ele possa funcionar em nuvem e/ou ser totalmente remodelado, tanto em relação a integração com a ferramenta SAT Central, quanto ao modelo de registro e integração com os sistemas de autenticação da Dataprev/GERID. Muito em razão do SAT já ser um sistema legado.*
> - *A fim de mitigar algumas características atuais do sistema que comprometem a estabilidade da aplicação, elencamos no Plano de Ação 2023 da DIOP o Projeto de Automação de Backup e Restauração dos SATs locais. Contudo, a característica do sistema atual não permite que possamos garantir que esse backup seja 100% efetivo. O projeto prevê o armazenamento em nuvem, diário, das informações de configurações dos painéis locais, bem como a chave de registro da aplicação. Em caso de desastre, seria possível restaurar a aplicação sem necessidade de reconfiguração.*
> - *Outrossim, também no Plano de Ação 2023 DIOP, há previsão do Projeto de Administração dos Servidores SAT Locais com Infraestrutura por Código Automatizada. Trazendo padronização e celeridade nas ações de manutenções dos referidos equipamentos que sustentam o sistema SAT.*
> - *Contudo, cabe reportar que estes projetos serão adotados concomitantemente com a migração para os novos links SDWAN, pois carecem de maior banda de dados para execução.*
> - *Por fim, o monitoramento dos sistemas já é previsto no sistema Zabbix, atualmente em fase final de adequação, pois nem todos os servidores SATs atuais suportam os Agentes Zabbix de monitoramento, por serem sistemas operacionais antigos, mas que serão atualizados em conjunto com implantação dos projetos supracitados.*

Achado nº 1: Ausência de controles que possibilitem a confirmação dos dados produzidos pelo Painel Monitoramento do Acordo dos Níveis de Serviços (ANS), nos casos de possíveis divergências identificadas pela Fiscalização do Contrato.

Recomendação nº 1: Instituir controles e monitoramentos que sejam capazes de identificar de forma automatizada paradas e indisponibilidades do sistema SAT e suas respectivas causas, de modo a confirmar ou contrapor os dados fornecidos pela Contratada relacionados ao ANS.

Manifestação da Unidade Auditada:

> *Proposta de Tratamento: Quanto ao SAT Central atividade já em execução pela equipe de fiscalização do contrato com apoio da equipe técnica da DIOP, porém sem obrigação contratual formalizada. Proporemos aditivo qualitativo ao contrato para formalizar a ferramenta em operação na DTI, discorrendo sobre a forma de apresentação de relatórios e contraprovas pela contratada. Conforme sinalizado no item 2, quanto ao SAT Local, as atividades estão em andamento, porém demandam as ativações dos novos links para que sejam tecnicamente viáveis.*
>
> *Prazo: Dezembro de 2023*

Análise da Equipe de Auditoria:

A unidade auditada apresenta um rol de providências que tem adotado visando à instituição de controles no que se refere ao sistema SAT. Na explanação inicial, citada acima, apresenta maiores detalhes relacionados aos projetos para implementação desses controles e, na manifestação relacionada à proposta de tratamento, quanto ao SAT Central, informa que há atividade já em execução pela equipe de fiscalização do contrato, contudo sem obrigação contratual instituída. A unidade gestora ressalta, neste caso, que irá propor aditivo qualitativo ao contrato para formalizar a ferramenta em operação na DTI. No que se refere ao e o SAT Local, a área auditada informa que existem atividades ainda em andamento, restando ativação de novos links.

Considerando que as implementações foram justificadas com atividades continuadas e conclusão aprazada para o exercício de 2023, especificamente no mês de dezembro, essa auditoria considera razoável o prazo solicitado, para implementação da recomendação, observando-se, contudo, o monitoramento desses controles que deverão ser instituídos. Dessa forma, conclui-se pela manutenção do achado e da recomendação, a qual será registrada no sistema e-Aud, sendo possível futuras manifestações, em fase de monitoramento.

Achado nº 2: Plano de contingência do sistema SAT não aborda o tratamento de incidentes de segurança e não inclui o SAT Local.

Recomendação nº 2: Estabelecer padrão técnico a ser seguido pela Contratada na elaboração do Plano de Recuperação de Desastres (PRD) do sistema SAT (Central e Local), incluindo cenários de incidentes e indisponibilidades por motivo de segurança da informação, conforme disposto no tópico de Gestão da continuidade do negócio da ABNT NBR ISO/IEC 27001.

Manifestação da Unidade Auditada:

> *Proposta de Tratamento: A DTI em parceria com a DIGOV está finalizando a elaboração da metodologia de continuidade de negócios e apresentará os artefatos às suas contratadas para que se adequem aos artefatos propostos em aderências às boas práticas. Espera-se consolidar esta metodologia no primeiro trimestre de 2023 e no segundo trimestre de 2023 priorizaremos a formalização dos ativos da informação relacionados ao sistema SAT.*
>
> *Prazo: Julho de 2023*

Análise da Equipe de Auditoria:

Apesar da unidade auditada informar que está em andamento a finalização da elaboração de metodologias de continuidade de negócio e artefatos para aderência às boas práticas e redução dos impactos que poderão comprometer os ativos da informação, relacionados ao sistema SAT, não detalha quais os artefatos compatíveis com o disposto na ABNT NBR ISO/IEC 27001 serão propostos à contratada, para a correspondente adequação às boas práticas estabelecidas, assim como não deixa claro quais as boas práticas adotadas. Estipula um prazo para adequação até julho de 2023.

Nesse sentido, há necessidade de um maior detalhamento quanto a elaboração dessa metodologia em correspondência com a Norma supramencionada. No entanto, tendo em vista que que as atividades já estão em andamento, considera-se o prazo sugerido pela unidade gestora razoável para atendimento do recomendado. Sendo assim, mantém-se o achado e a recomendação, a qual será registrada e monitorada no sistema e-Aud, sendo possível futuras manifestações e interações entre as unidades envolvidas no processo e equipe de auditoria.

Achado nº 3: Ausência da avaliação dos requisitos de segurança da informação, por parte da DTI, das demandas de desenvolvimento relacionadas ao sistema SAT.

Recomendação nº 3: Estabelecer rotina de supervisão técnica relacionada aos requisitos de segurança da informação, no que diz respeito às demandas de desenvolvimento do sistema SAT e suas respectivas homologações.

Manifestação da Unidade Auditada:

> *Proposta de Tratamento: Inicialmente cumpre destacar que o sistema SAT e respectivas demandas por atualizações, homologação de versões, arquitetura e modelagem utilizada pelo sistema, bem como contato e tomada de decisões com a Dataprev estão atualmente sob gestão da DIRBEN, onde atua o Product Owner da solução. Porém haja vista a publicação do regimento interno que publicou as competências da Coordenação-Geral de Dados e Sistemas de Informação - CGDSI, unidade técnica desta diretoria, iniciaremos tratativas para que requisitos não funcionais sejam observados, principalmente requisitos relacionadas à segurança da informação.*
>
> *Prazo: Julho de 2023.*

Análise da Equipe de Auditoria:

Observa-se que a presente recomendação especifica o estabelecimento de “supervisão técnica” que é de competência da área auditada, conforme mencionado no art.115, I da Portaria PRES/INSS nº 1.532 de dezembro de 2022, portanto, diz respeito às atividades inerentes à sua área de atuação. Porém, nesse sentido, a área informa que serão iniciadas “tratativas” para que os requisitos não funcionais sejam “observados”, principalmente àqueles relacionados à segurança da informação. No entanto, não detalha quais os procedimentos efetivos, que serão adotados para o estabelecimento das rotinas de supervisão relacionadas às demandas de desenvolvimento do sistema SAT.

O prazo estipulado pela unidade gestora, julho de 2023, para implantação dos procedimentos recomendados é considerado razoável pela equipe de auditoria, porém, saliente-se que a supervisão é uma atividade continuada. Diante o exposto, conclui-se pela manutenção do achado e da recomendação, a qual será registrada no sistema e-Aud, sendo possível futuras manifestações, em fase de monitoramento.

Achado nº 4: Ausência de processo de gestão de riscos de segurança da informação.

Recomendação nº 4: Instituir o processo de gestão de riscos de segurança da informação do INSS, de que trata o art. 12 da IN nº 3/2021 GSI/PR, abrangendo:

4.1: O Plano de Gestão de Riscos de Segurança da Informação (PGRSI), de acordo com o art. 13 da IN nº 3/2021 GSI/PR.

4.2: O Relatório de Identificação, Análise e Avaliação dos Riscos de Segurança da Informação (RIAARSI), de acordo com o art. 14 da IN nº 3/2021 GSI/PR.

4.3: O Relatório de Tratamento de Riscos de Segurança da Informação (RTRSI), de acordo com o art. 15 da IN nº 3/2021 GSI/PR.

Manifestação da Unidade Auditada:

> *Proposta de Tratamento: a DTI foi reestruturada pelo Decreto 10.995, de 14 de março de 2022, regimento interno do INSS - portaria PRES/INSS nº 1.532, de 8 de dezembro de 2022, resultando no redesenho de suas competências através do mapeamento de sua cadeia de valor (portaria DTI/INSS nº 85, de 25 de novembro de 2022). A partir desses referênciais estratégicos iniciamos o mapeamento dos processos de TI da Diretoria, entre eles os afetos à área de segurança da informação. O primeiro desafio da IN nº 3/2021 GSI/PR é mapear os ativos de informação, entre eles os afetos ao sistema SAT. Após os ativos mapeados documentaremos o Plano de Gestão de Riscos com apoio da DIGOV e unidade de negócio gestora do ativo (DIRBEN).*
>
> *Prazo: Agosto de 2023*

Análise da Equipe de Auditoria:

Considerando o estabelecido na IN nº 3/2021 GSI/PR:

> *Art. 14, § 1º O relatório de identificação, análise e avaliação dos riscos de segurança da informação deverá ser atualizado anualmente e sempre que houver alteração em algum dos fatores de risco ou em algum contexto interno ou externo, devendo ser posteriormente enviado ao gestor de segurança da informação para aprovação.*
>
> *Art. 15. O relatório de tratamento de riscos de segurança da informação deve ser resultante do relatório de identificação, análise e avaliação dos riscos de segurança da informação.*

Apesar da unidade auditada informar que a DTI foi reestruturada pelo Decreto 10.995 de março de 2022 e que com isso a área tem iniciado ações no sentido de mapear os processos da Diretoria de Tecnologia da Informação observa-se que a Norma, publicada em 2021, ou seja, o critério vigente, dentre outros aspectos, estabelece a necessidade de atualização anual do relatório de identificação e registra que o relatório de tratamento de riscos deve ser resultante do relatório de identificação, análise e avaliação dos riscos de segurança da informação, portanto, trata-se de atividade cíclica e continuada e mister se faz que as ações sejam iniciadas e tão logo implementadas, bem como acompanhadas. Quanto ao prazo sugerido pela unidade auditada para implementação da ação

recomendada, essa equipe de auditoria o considera razoável. Dessa forma, conclui-se pela manutenção do achado e da recomendação, a qual será registrada no sistema e-Aud, sendo possível futuras manifestações, em fase de monitoramento.