Diretoria de Tecnologia da Informação - DTI
Coordenação de Governança e Planejamento de TI - COGPL
Divisão de Planejamento e Projetos de TI - DPP

2023-2025

Plano Diretor de Segurança da Informação

30 de Novembro de 2022

INSS
INSTITUTO NACIONAL DO SEGURO SOCIAL

Comitê Estratégico de Governança - CEGOV

Presidente do Instituto Nacional do Seguro Social
Guilherme Gastaldello Pinheiro Serrano

Diretor de Tecnologia da Informação
João Rodrigues da Silva Filho
Diretora de Orçamento Finanças e Logística
Larissa Andrade Mora
Diretor de Governança Planejamento e Inovação
Alexandre Guimarães
Diretor de Benefícios e Relacionamento com o Cidadão
Edson Akaio Yamada
Diretor de Gestão de Pessoas
Eva Lorena Alves Ferreira

Comitê Temático de Governança Digital - CTGD

Coordenador do Comitê:
João Rodrigues da Silva Filho

Representante Diretoria de Orçamento Finanças e Logística
André Rocha Marinho

Representante Diretoria de Governança Planejamento e Inovação
Bruno Batista Barreto

Representante Diretoria de Benefícios e Relacionamento com o Cidadão
Ailton Nunes de Matos Junior

Representante Diretoria de Gestão de Pessoas
Anelizia Gonçalves Rodrigues

Equipe responsável pelo Plano Diretor de Segurança da Informação

Nome	Papel	E-mail
João Rodrigues da Silva Filho	Diretor de Tecnologia da Informação	joaorodrigues.filho@inss.gov.br
João Henrique Mourão de Marco	Coordenador-Geral de Infraestrutura e Segurança em Tecnologia da Informação	joaodemarco@inss.gov.br
Jullyano Lino da Silva	Oficial de Segurança da Informação	jullyano.silva@inss.gov.br
Hugo Rafael Torma de Lima	Chefe de Divisão de Operações de Tecnologia da Informação	hugo.lima@inss.gov.br
Luzivan de Moura Gois	Chefe da Divisão de Segurança em Tecnologia da Informação	luzivan.gois@inss.gov.br
Francisco Humberto Mendonça de Araújo	Chefe da Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos	francisco.haraujo@inss.gov.br

Gestores de Tecnologia da Informação - Consultados

CGDIS - Coordenação-Geral de Dados e Sistema de Informação

Israel Eduardo Zebulon Martins de Souza

CCD - Coordenação de Ciência de Dados

Marcelo Albuquerque Sette

CADS - Coordenação de Análise e Desenvolvimento de Sistemas

Rodrigo Gomes Rodrigues

COGPL - Coordenação de Governança e Planejamento de Tecnologia da Informação

Marcelo Genu Beserra

DPP - Divisão de Planejamento e Projetos de TI

Rodolfo Luis Couy de Araujo Costa

DSC - Divisão de Suporte a Contratações de TI

Rafael Roque Leite

HISTÓRICO DE ALTERAÇÕES

Data	Versão	Descrição	Autor
30/11/2022	1.0	PDSI 2023-2025	COGPL, DPP e CGIS

Sumário

1 - Introdução

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

Este plano diretor descreve, em relação à segurança da informação, onde a organização está, onde precisa chegar, visando promover adequada infraestrutura, suporte logístico, recursos tecnológicos, humanos e financeiros para segurança da informação. Busca definir objetivos de curto e médio prazo com o foco específico em SI e sua elaboração envolve o gestor da segurança da informação e uma equipe interdisciplinar, em um processo de planejamento participativo.

É um planejamento que deve estar alinhado ao Planejamento Estratégico da Organização, principalmente aos seus objetivos e ao Plano Diretor de Tecnologia da Informação - PDTI. Neste sentido, adotou-se para o presente documento o mesmo prazo de vigência do PDTI que se estenderá até 2022.

Este documento está estruturado em partes assim distribuídas:

- **Apresentação:** descreve a distribuição do conteúdo do documento.
- **Documentos de referência:** lista dos documentos que podem ser utilizados como referências sobre os assuntos tratados neste documento.
- **Siglas:** apresenta os significados das siglas utilizadas na elaboração do documento.
- **Termos e definições:** apresenta os significados dos termos utilizados na elaboração do documento.
- **Metodologia aplicada:** introduz a forma de levantamento das informações, condução dos trabalhos e elaboração do documento.
- **Situação inicial:** descreve o retrato das condições do INSS no que diz respeito à segurança de suas informações quando da realização do projeto.
- **Desenvolvimento do PDSI:** detalhamento do levantamento das necessidades, metas e ações e sua priorização.
- **Plano de Gestão de Riscos:** Riscos identificados relacionados a eventos que podem comprometer a execução do plano e suas ações;
- **Conclusão: Fatores:** críticos de sucesso e considerações finais.

2 - Documentos de Referência

- **Acórdão 1603/2008 - Plenário** – Levantamento de auditoria, situação da governança de tecnologia da informação na administração pública federal. Ausência de planejamento estratégico institucional. Deficiência na estrutura de pessoal. Tratamento inadequado à confidencialidade, integridade e disponibilidade das informações. Recomendações.
- **Decreto Nº 9.637, de 26 de dezembro de 2018** - Institui a Política Nacional de Segurança da Informação.
- **Lei nº 12.527, de 18 de novembro de 2011** – Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências.
- **Instrução Normativa GSI/PR Nº 01/2020, de 27 de maio de 2020** - Dispõe sobre a Estrutura de Gestão de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal.
- **INSTRUÇÃO NORMATIVA Nº 2, DE 24 DE JULHO DE 2020** - Altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.
- **Instrução Normativa GSI/PR Nº 3, de 28 de maio de 2021** - Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.
- **Norma Complementar nº 04/IN01/DSIC/GSIPR** – Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal.
- **Resolução nº 9/CEGOV/INSS, de 31 de agosto de 2020** - Atualiza a Política de Segurança da Informação do Instituto Nacional do Seguro Social – POSIN-INSS.
- **Resolução nº 10/CEGOV/INSS, de 31 de agosto de 2020** - Define as regras para emissão de credenciais de acesso lógico (NCAL).
- **RESOLUÇÃO Nº 11/CEGOV/INSS, DE 31 DE AGOSTO DE 2020** - Institui a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR do Instituto Nacional do Seguro Social.
- **RESOLUÇÃO Nº 12/CEGOV/INSS, DE 31 DE AGOSTO DE 2020** - Disciplina o uso da Internet no INSS, regulamenta e define o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.
- **PORTARIA Nº 93, DE 26 DE SETEMBRO DE 2019** - Aprova o Glossário de Segurança da Informação.
- **PDTIC 2023/2025** – Plano Diretor de Tecnologia da Informação e Comunicações do INSS.

- **RESOLUÇÃO Nº 5 /CEGOV/INSS, DE 28 DE MAIO DE 2020** - Institui a Política de Gestão de Riscos do Instituto Nacional do Seguro Social - INSS.
- **PORTARIA Nº 1.191/PRES/INSS, DE 3 DE OUTUBRO DE 2016** - Regulamenta o uso e acesso de dispositivos móveis à rede corporativa do INSS.
- **LEI Nº 12.965, DE 23 DE ABRIL DE 2014 -** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
- **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018** - Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).
- **DECRETO Nº 10.046, DE 9 DE OUTUBRO DE 2019** - Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

3 - Termos e abreviações

TERMO	DESCRIÇÃO
ABNT	Associação Brasileira de Normas Técnicas
APF	Administração Pública Federal
CTGD	Comitê Temático de Governança Digital
DTI	Diretoria de Tecnologia da Informação
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
INSS	Instituto Nacional do Seguro Social
PDTI	Plano Diretor de Tecnologia da Informação
PDSI	Plano Diretor de Segurança da Informação
SI	Segurança da Informação
TCU	Tribunal de Contas da União

Tabela 1: Termos e Abreviações

4 - Definições

Para fins deste documento, consideram-se as seguintes definições:

Ativo de Informação: Os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e os recursos humanos que a eles têm acesso.

Ativo de Rede: Equipamento que centraliza, interliga, roteia, comuta, transmite ou concentra dados em uma rede de computadores.

Autoridade Certificadora (AC): entidade responsável por emitir e gerenciar certificados digitais.

Autoridade Certificadora Raiz (AC-Raiz): se situa no topo da hierarquia da cadeia de certificação, sendo a primeira autoridade. Sua função é executar as normas técnicas e operacionais e as políticas de certificados estabelecidas pelo Comitê Gestor da ICP Brasil. Isso significa que a AC-Raiz pode emitir, distribuir, expedir, revogar e gerenciar os certificados das autoridades que estão abaixo de seu nível hierárquico, que são as autoridades certificadoras. A Autoridade Certificadora Raiz da ICP Brasil é o Instituto Nacional de Tecnologia da Informação (ITI)

Autoridade de Registro (AR): estabelece a interface entre o usuário e a Autoridade Certificadora. A AR se vincula à AC e tem como principal objetivo ser o intermediário presencial entre a AC e o interessado pelo certificado digital, recebendo, validando e encaminhando as solicitações de emissão ou revogação dos certificados digitais, além de identificar seus solicitantes de forma presencial.

Certificado Digital: conjunto de dados de computador, gerados por uma Autoridade Certificadora, em observância à Recomendação Internacional ITU-T X.509, que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre uma chave criptográfica e uma pessoa física, jurídica, máquina ou aplicação.

Computação em Nuvem: modelo computacional que permite acesso por demanda, e independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou de interação com o provedor de serviços.

Conscientização: atividade que tem por finalidade orientar sobre o que é SI levando os participantes a obterem um nível adequado de conhecimento sobre segurança, além de um senso apropriado de

responsabilidade. O objetivo dessa atividade é proteger o ativo de informações do órgão ou entidade para garantir a continuidade dos negócios, minimizar os danos e reduzir eventuais prejuízos financeiros;

Dashboard: ferramenta de gerenciamento de informações que permite acompanhar visualmente, analisar e exibir indicadores de desempenho (KPI), métricas e outros dados importantes para monitorar a saúde de um negócio, departamento ou processo específico.

Segurança de Endpoint: realiza o gerenciamento de todos os dispositivos conectados à rede da empresa, controlando cada um dos acessos e evitando que pessoas não autorizadas consigam alcançar determinados dados.

Parque Computacional: corresponde a toda a estrutura de TI disponível para a empresa. Ela inclui desde computadores e periféricos, como impressoras e monitores, até servidores e outras soluções de tecnologia.

Serviço de diretório: Serviço que fornece os métodos para armazenar dados de diretório e disponibilizar esses dados para usuários e administradores de rede. Tem-se como exemplo o *Active Directory* que armazena informações sobre contas de usuário, como nomes, senhas, e-mail, e permite que outros usuários autorizados na mesma rede acessem essas informações.

Rede de dados: é um conjunto de dois ou mais dispositivos eletrônicos de computação (ou módulos processadores ou nós da rede) interligados por um sistema de comunicação digital (ou link de dados), guiados por um conjunto de regras (protocolo de rede) para compartilhar entre si informação, serviços e, recursos físicos e lógicos.

Incidente: evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

Hardening: é um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, com foco na infraestrutura e objetivo principal de torná-la preparada para enfrentar tentativas de ataque.

Política de backup: consiste em um documento que engloba as normas e regras para guiar todo o ciclo do gerenciamento de dados corporativos – desde a concepção até o descarte.

5 - Metodologia Aplicada

A metodologia a ser utilizada para a elaboração do PDSI é a mesma do Modelo de Referência de PDTIC do SISP, versão 2.0. Para sua elaboração será adotado o Guia Prático de Elaboração de PDTIC do SISP que disponibiliza o fluxo do processo, templates de documentos a serem usados pelos órgãos da Administração Pública Federal.

Aproveitando o trabalho da equipe que elabora o PDTIC 2023-2025, desdobramos na etapa de planejamento as metas e ações do PDSI, ou seja, uma equipe, uma etapa de preparação, uma etapa de diagnóstico e dois planos: PDTIC 2023-2025 e PDSI 2023-2025.

O macroprocesso para elaboração do PDSI é subdivido nos seguintes processos:

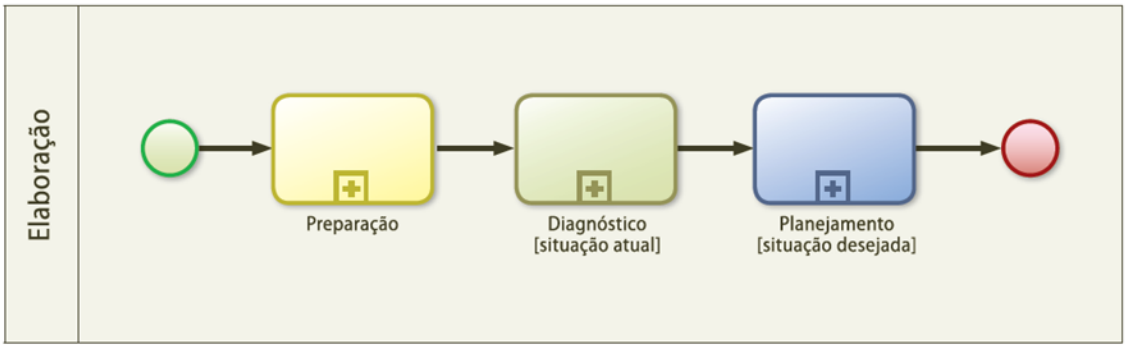

FIgura 2

Processo de Preparação: é a primeira fase de elaboração do plano de trabalho. Para este processo será aproveitado o trabalho do PDTIC 2023-2025;
Processo de Diagnóstico: nesta fase serão verificadas as necessidades ou demandas de TI e identificada a situação atual. Para este processo será aproveitado o trabalho do PDTIC 2023-2025;
Processo de Planejamento: nesta fase as necessidades serão priorizadas e planejadas e as ações para execução, representam a busca da situação desejada. Neste processo destacaremos as atividades relacionadas à identificação de riscos, metas e ações específicas relacionadas à segurança da informação.

As atividades que compõem o subprocesso de Preparação são: (serão identificadas no PDTIC)

- Definir abrangência e período do PDTIC;
- Definir a Equipe de Elaboração do PDTIC – EqEPDTIC;

- Descrever a metodologia de elaboração;
- Consolidar documentos de referência;
- Identificar estratégias da organização;
- Identificar princípios e diretrizes;
- Elaborar o Plano de Trabalho do PDTIC – PT-PDTIC;
- Aprovar o PT-PDTIC.

As atividades que compõem o subprocesso de Diagnóstico são:

- Analisar resultados do PDSI anterior;
- Analisar o referencial estratégico de TIC;
- Analisar a organização da TIC;
- Realizar Análise SWOT da TIC;
- Estimar a capacidade da execução da TIC;
- Planejar o levantamento das necessidades;
- Identificar necessidades de Informação;
- Identificar necessidades de Serviços de TIC;
- Identificar necessidades de Infraestrutura de TIC;
- Identificar necessidades de Contratação de TIC;
- Identificar necessidades de Pessoal de TIC;
- Consolidar o Inventário de Necessidades;
- Alinhar as necessidades de TIC às estratégias da organização;
- Aprovar o Inventário de Necessidade.

As atividades que compõem o subprocesso de Planejamento são:

- Atualizar critérios de priorização;
- Priorizar as necessidades inventariadas;
- Definir metas e ações;
- Planejar ações de pessoal (serão identificadas no PDTIC);
- Planejar orçamento das ações do PDSI (serão identificadas no PDTIC);
- Identificar os fatores críticos de sucesso;
- Planejar o gerenciamento de riscos;
- Consolidar a Minuta do PDSI;
- Aprovar a Minuta do PDSI;
- Publicar o PDSI.

6 - Referencial Estratégico de TIC

Figura 1 - Mapa Estratégico INSS

Objetivos Estratégicos de TIC

OETIC01: Entregar soluções de TIC que agregam valor estratégico para o INSS.

OETIC02: Aumentar o nível de satisfação dos usuários de TIC do INSS.

OETIC03: Viabilizar o Uso de Inteligência de Negócio nas soluções de TIC.

OETIC04: Promover a cultura de SIC.

OETIC05: Promover um ambiente seguro de TIC.

OETIC06: Aprimorar a governança e a gestão de serviços de TIC.

OETIC07: Priorizar a transformação digital na entrega de soluções de TIC

OETIC08: Promover a inovação e a modernização da infraestrutura e serviços de TIC

OETIC09: Fortalecer o quadro de colaboradores de TIC

OETIC10: Ampliar a capacidade e a qualidade da entrega dos serviços de TIC

6.1 - Análise SWOT

A análise SWOT realizada tem como alinhamento o Mapa Estratégico da DTI, esta ferramenta foi adotada como base para gestão e planejamento estratégico institucional, podendo ser utilizada em qualquer tipo de análise de cenário.

Essa análise ajuda a ter clareza do negócio, possibilitando que se identifiquem quais pontos ajudam a determinar a posição atual da organização e antecipar seu futuro, visando o aproveitamento das oportunidades e a mitigação dos riscos.

Em seu processo de planejamento, a DTI construiu a seguinte análise de seu ambiente de atuação na esfera de segurança da informação:

AMBIENTE INTERNO	AMBIENTE EXTERNO
FORÇAS	OPORTUNIDADES
. Patrocínio da PR e Diretorias do INSS; . POSIN, NCAL, Norma de Acesso à Internet publicadas; . Gestão de Segurança da Informação institucionalizada; . ETIR institucionalizada e atuando; . Equipe técnica experiente e conhecedora do ambiente interno; . Existência de estruturas de disseminação do conhecimento em segurança da informação; . Ferramentas de colaboração mais seguras; . Política e práticas de segurança da informação institucionalizadas	. Repercussão pública da necessidade do enfrentamento aos frequentes ataques Hackers à Administração Pública Federal . Publicações de normativos pelo GSI e outros entes externos; . Apontamentos de Auditoria por órgãos de controle externo . Existência de empresa contratada para apoio à instituição nas ações de segurança; . Integração com outras instâncias de investigação; . Criação da Rede Federal de Gestão de Incidentes Cibernéticos; . Exigência legal e fiscalização do controle interno e externo; . Destaque à segurança da informação por diferentes entidades, contra-ataques cibernéticos

	na administração pública; . Novas tendências e inovações na área de segurança da informação.
FRAQUEZAS	AMEAÇAS
. Alterações nas prioridades estratégicas; . Infraestrutura de segurança da informação ineficiente; . Não observância de competências regimentais e normativos relativos à segurança da informação (conformidade), e falta de responsabilização . Falta de maturidade da cultura de segurança; . Estrutura da área de segurança insuficiente (porte, equipe, capacitação, ferramentas) . Falta de conscientização dos usuários em segurança da informação.	. Restrição orçamentária; . Intensificação de incidentes de segurança da informação; . Compartilhamento de informações com outras instituições; . Descontinuidade nas estratégias e políticas governamentais; . Institucionalização de sistemas de informação não geridos pela DTI.

Tabela 2- Análise SWOT

Nos próximos tópicos serão realizados alguns comentários a respeito de cada ponto levantado através da análise SWOT.

A. Forças

Um fator fundamental identificado corresponde ao patrocínio da alta gestão do INSS em relação às atividades relacionadas à segurança, o que permite o desenvolvimento das ações necessárias identificadas através deste plano diretor. Apenas com a chancela, e reconhecimento da importância dessa matéria por todos, é que será possível avançar com as ações vistas como necessárias.

Patrocínio da Presidência e da Diretoria do INSS:

Um fator fundamental identificado corresponde ao patrocínio da alta gestão do INSS em relação às atividades relacionadas à segurança, o que permite o desenvolvimento das ações necessárias

identificadas através deste plano diretor. Apenas com a chancela, e reconhecimento da importância dessa matéria por todos, é que será possível avançar com as ações vistas como necessárias.

POSIN, NCAL, Norma de Acesso à Internet Publicadas, entre outras:

A publicação de normativos é uma das maiores forças identificadas. Visando atender aos normativos federais que disciplinam requisitos mínimos de segurança e de tratamento de incidentes no âmbito da administração pública federal, em agosto de 2020 o INSS publicou três resoluções sobre a temática de segurança.

Em acordo com a determinação contida na Política Nacional de Segurança da Informação (PNSI), que dispõe sobre a governança da segurança da informação, em 31/08/2020 o INSS apresentou, através da Resolução n. 9 CEGOV/INSS, a sua Política de Segurança da Informação (POSIN), a qual elencou algumas diretrizes relacionadas à segurança da informação, quais sejam: tratamento da informação; tratamento de incidentes de SI; gestão de riscos de segurança; gestão de continuidade; controles de acesso; recursos computacionais; auditoria e conformidade; responsabilidade pela gestão das informações; segurança física e do ambiente e, gestão de ativos da informação;

Também em 31 de agosto de 2020 o INSS estabeleceu, por meio da Resolução n.10 CEGOV/INSS, as regras para emissão de credenciais de acesso lógico (NCAL) a qual trouxe como diretrizes regras para o acesso à rede e aos sistemas corporativos do INSS, atribuição de credenciais e previsão de penalidades no caso de uso indevido de informações dos sistemas corporativos.

Quanto ao uso efetivo da internet no INSS, foi emitida a Resolução n. 12 de 31 de agosto de 2020 que disciplinou o uso da internet e definiu o conjunto de perfis de acesso, competências e conteúdo de acesso para cada perfil.

Gestão de Segurança da Informação institucionalizada:

Existe na DTI uma área de segurança da informação institucionalizada. Em 06 de setembro de 2019, através da Resolução n. 702, foi criado o Serviço de Segurança em Tecnologia da Informação e Comunicação na instituição estando vinculada diretamente à CSIT e fazendo parte da Diretoria de Tecnologia da Informação e Inovação - DTI. Este serviço visa dar suporte às atividades de segurança da informação de competência da DTI. Embora a estrutura deste serviço seja insuficiente e incompatível com a importância que ele tem, é ainda uma das forças, haja vista sua existência e institucionalização.

ETIR institucionalizada e atuando:

Em conformidade com a Instrução Normativa n. 1 GSI, o INSS instituiu a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR através da Resolução n. 11 de 31 de agosto de 2020, a qual tem como objetivo agir proativamente, receber, analisar, monitorar, coordenar e propor

respostas a notificações e atividades relacionadas a incidentes de segurança da informação e comunicações no âmbito do INSS. A ETIR revela-se, hoje, como uma outra grande força na medida em que, além de institucionalizada, já está atuando, recebendo e respondendo às demandas de incidentes de segurança.

Equipe técnica experiente e conhecedora do ambiente interno:

A equipe técnica formada para atuar na DTI e, especialmente, no Serviço de Segurança da Informação e Inovação

SSEG e na Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR é experiente e conta com amplo conhecimento da estrutura e funcionamento da Instituição, de tal forma que possui capacidade de bem executar as atividades que lhe incumbe. Esta é, sem dúvidas, uma força, haja vista que o conhecimento dos integrantes que compõem uma equipe de segurança está fortemente vinculado ao sucesso em suas atividades desempenhadas.

Existência de estruturas de disseminação do conhecimento em segurança da informação:

Atualmente, o INSS possui estruturas para disseminação de informações sobre segurança. A Assessoria de Comunicação Social vem realizando a divulgação de campanhas NEOPOSIN e de cuidados a serem tomados em relação a *phishing* e outros tipos de ataques cibernéticos. Essas campanhas institucionalizadas são determinantes para a disseminação da cultura de segurança dentro da organização e para a redução de incidentes de segurança.

Ferramentas de colaboração mais seguras:

Foi contratada pelo INSS uma solução integrada de colaboração, comunicação e produtividade que vem permitindo garantir mais segurança às atividades da organização, principalmente no que se refere ao uso do correio eletrônico e no armazenamento e compartilhamento de informações e documentos.

Política e práticas de segurança da informação institucionalizadas

B. Fraquezas

Alterações nas prioridades estratégicas

A principal fraqueza identificada relaciona-se com as alterações que podem ocorrer nas prioridades estratégicas do INSS, inviabilizando a execução de ações previamente planejadas e, consequentemente, a consecução de suas finalidades.

Infraestrutura de segurança da informação insuficiente

Foram identificadas várias fraquezas que se referem à infraestrutura de segurança, dentre elas a ausência de segurança de *endpoint*, ausência de atualização de software, insuficiência de certificados A3 implantados, ferramenta de acesso remoto sem implementação de certificado A3, falta de gestão da rede de dados (a qual é provida por empresa contratada), inexistência de gestão de ativos de informação, ausência de serviço de sustentação à infraestrutura (a exemplo de um *Security Operations Center* – SOC), ausência de serviço de diretório e de solução integrada para trabalho remoto (desktop virtual, por exemplo). São vários pontos a serem tratados a fim de que se alcance uma infraestrutura de segurança adequada.

Não observância de competências regimentais e normativos relativos à segurança da informação (conformidade), e falta de responsabilização

Atualmente, embora existam normas específicas de segurança que prevejam responsabilidades formais para gestores de sistema, gestores de acesso, usuários da DTI, área de proteção de dados, área de combate à fraude, áreas de benefícios, entre outras áreas, cada uma tendo sua responsabilidade correspondente no ecossistema de segurança, na prática, ocorre a inobservância de fato dessas responsabilidades formalmente estabelecidas. A ausência de responsabilização no caso de descumprimento de normativos acentua ainda mais a inobservância às regras e responsabilidades previamente determinadas.

Falta de maturidade da cultura de segurança na instituição

Apesar de existirem trabalhos que procuram promover a disseminação de orientações e informações a respeito de segurança da informação dentro do INSS, a cultura de segurança da informação é ainda muito incipiente, inclusive com medidas que visam favorecer a segurança sendo vistas como obstáculos. Esta falta de maturidade é uma grande fraqueza que precisa ser combatida através do aumento da conscientização de todos.

Estrutura da área de segurança insuficiente (porte, equipe, capacitação, ferramentas)

Verificou-se que a área da segurança da informação, no cenário atual, possui uma série de deficiências tais como insuficiência de força de trabalho, de capacitação da equipe, de ferramentas para fazer uso e de porte apropriado para o tamanho e necessidades da organização.

Falta de conscientização dos usuários em segurança da informação

C. Oportunidades

Repercussão pública da necessidade do enfrentamento aos frequentes ataques *Hackers* à Administração Pública Federal:

A crescente preocupação relacionada à segurança da informação, haja vista a frequente ocorrência de ataques, pode ser vista como uma grande oportunidade na medida em que as organizações têm compreendido cada vez mais a importância de ações que visam garantir segurança da informação, priorizando recursos para o desenvolvimento de ações planejadas. Além disso, essa preocupação desencadeia uma série de movimentos que dão mais força às equipes de se dedicam a área.

Publicações de Normativos pelo GSI e outros entes externos:

O Gabinete de Segurança Institucional da Presidência da República, vem emitindo normativos que disciplinam processos relacionados à gestão de segurança da informação, elencando processos de realização obrigatória aos órgãos e entidades da Administração Pública Federal além de diretrizes para implementação de controles relacionados à temática. Esses normativos, são essenciais para que o INSS emita os seus próprios normativos internos disciplinando questões relacionadas à área.

Apontamentos de Auditoria por órgãos de controle externo

Através de apontamentos realizados por auditorias, principalmente pelo TCU e CGU, o INSS tem a oportunidade de melhorar seus processos e sistemas em adequação aos seus próprios normativos ou corrigindo fragilidades identificadas.

Existência de empresa contratada para apoio à instituição nas ações de segurança:

Atualmente o INSS conta com uma empresa externa que dá apoio nas ações de segurança da informação. A Dataprev, empresa pública vinculada ao Ministério da Economia, é responsável hoje pela gestão da base de dados do INSS e também por outras atividades tais como gestão de vários de seus sistemas. As atividades atualmente suportadas pela Dataprev são imprescindíveis para a manutenção das ações de segurança da forma como a área de segurança da informação está operacionalizada na organização.

Desde 18/09/2020 está em vigor a Lei Geral de Proteção de Dados a qual dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Ao mesmo tempo em que a LGPD pode

representar uma ameaça, ela também propicia a consolidação da maturidade em tratamento de dados pessoais e provoca a implementação de procedimentos e medidas adicionais direcionadas a fortalecer a proteção em torno dos dados que coleta e trata, de forma geral.

Integração com outras instâncias de investigação

A integração com outras instâncias de investigação como o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), a Polícia Federal e a Coordenação-Geral de Inteligência Previdenciária e Trabalhista (CGINT) da Secretaria Especial de Previdência e Trabalho do Ministério da Economia é um fator externo positivo que pode ser proveitoso para o INSS no que se refere à sua atuação em Segurança da Informação.

Criação da Rede Federal de Gestão de Incidentes Cibernéticos

O Decreto nº 10.748 criou em julho de 2021, a Rede Federal de Gestão de Incidentes Cibernéticos, com o fim de proporcionar prevenção contra ameaças cibernéticas e de elevar o nível de resiliência em segurança cibernética dos ativos de informação dos órgãos e das entidades da administração pública federal. Apesar da instituição desta rede ser recente, ela poderá ser uma grande oportunidade e apoio para as ações do INSS relacionadas a incidentes.

Exigência legal e fiscalização do controle interno e externo

Destaque à segurança da informação por diferentes entidades, contra-ataques cibernéticos na administração pública

Novas tendências e inovações na área de segurança da informação

D. Ameaças

Restrição orçamentária:

As ações necessárias na área de segurança dependem de investimento. A ausência de recursos impacta a concretização das ações e, por consequência, o alcance dos objetivos de segurança previstos pela Organização.

Intensificação de incidentes de segurança da informação:

Se por um lado a ocorrência de incidentes e ataques mais frequentes trouxe à tona a importância que o tema exige, por outro lado, os ataques continuam sendo uma grande ameaça e o motivo pelo qual ações devem ser tomadas e equipes dedicadas à segurança devem existir.

Compartilhamento de informações com outras instituições:

O INSS compartilha informações com outras instituições, seja através de acordos de cooperação técnica, pregão de folha de pagamento ou outros. Esse compartilhamento permite com que dados dos segurados e servidores estejam hoje em poder de bancos ou de outras entidades, fugindo ao controle estrito do INSS.

Descontinuidade nas estratégias e políticas governamentais

Institucionalização de sistemas de informação não geridos pela DTI

7 - Alinhamento com a estratégia da organização

Para atingimento de sua finalidade o INSS utiliza como ferramenta de planejamento e acompanhamento o Mapa Estratégico, construído com base na metodologia do Balanced Scorecard – BSC e que atualmente abrange o período de 2022-2023, alinhado ao plano plurianual vigente. Este mapa proporciona maior alinhamento do Instituto aos seus objetivos estratégicos institucionais.

O Mapa Estratégico do INSS está organizado da seguinte forma:

Figura 2

8 - Inventário de Necessidades

8.1 - Plano de Levantamento das Necessidades

As necessidades de TIC identificadas neste PDSI foram mapeadas a partir de reuniões e relatórios consolidados de demandas das unidades finalísticas e das áreas de atividades meio do Instituto. Também foram consideradas as necessidades pactuadas no PDTIC.

De forma geral, as necessidades identificadas se referem a demandas de contratação de bens ou serviços de TIC, como também aquelas relacionadas aos pontos fracos definidos na análise SWOT.

A seguir são apresentadas as necessidades, que serão executadas pela DTI, identificando as unidades responsáveis pela execução, juntamente com o alinhamento aos Objetivos Estratégicos do INSS e Objetivos Estratégicos da DTI.

8.2 – Necessidades Identificadas

ID	Necessidades de SI	OE INSS	OE DTI	Unidade Responsável
NSI1	Prover Infraestrutura de Segurança da Informação	Promover a modernização tecnológica e a cultura de segurança da informação	OETIC05; OETIC06; OETIC08	CGIS
NSI2	Monitorar a Segurança da Informação	Promover a modernização tecnológica e a cultura de segurança da informação	OETIC05; OETIC06	COIM
NSI3	Aprimorar Normas e Processos de Negócio de Segurança da Informação	Promover a modernização tecnológica e a cultura de segurança da informação	OETIC05; OETIC06; OETIC08; OETIC10	DSEG
NSI4	Prevenir incidentes de Segurança da Informação	Promover a modernização tecnológica e a cultura de segurança da informação	OETIC05; OETIC06; OETIC09	CGIS
NSI5	Executar ações de Detecção, Tratamento e Resposta a Incidentes de Segurança da Informação	Promover a modernização tecnológica e a cultura de segurança da informação	OETIC05; OETIC06; OETIC08	DTIR

Tabela 4 - Necessidades de SI

8.3 - Plano de Metas e Ações

Com a finalidade de atender às necessidades identificadas no inventário, foram definidas metas e ações. As metas definem marcos monitoráveis com o propósito de indicar o atingimento das ações. Sendo assim, o Plano de Metas e Ações foi elaborado com a intenção de resultar em ações para atendimento das necessidades levantadas, com estimativas preliminares, a fim de mensurar o atingimento das metas estabelecidas.

As metas estabelecidas para a DTI dizem respeito à sua conclusão, dentro do triênio 2023-2025, atendendo aos critérios de prazo, custo e qualidade, desde que todas as premissas do planejamento se mantenham e as dependências externas sejam observadas dentro dos prazos. Após a aplicação do critério de priorização e validadas pelo Comitê Temático de Governança Digital (CTGD) será possível selecionar os itens que irão compor o Plano de Metas da área de Tecnologia que serão executadas durante a vigência deste PDSI.

NSI1 - Prover Infraestrutura de Segurança da Informação					
Id Ação	**Ação**	**Indicador**	**2023**	**2024**	**2025**
AInf-01	Disponibilizar solução de segurança de endpoints	Taxa da Solução disponibilizada	100%	-	-
AInf-02	Atualiar sistema operacional dos ativos de TIC	Taxa de ativos de TIC atualizados	100%	-	-
AInf-03	Implantar serviço de operação de infraestrutura e segurança de TIC	Taxa de serviço implantado	-	-	100%
NSI2 - Gerir e Monitorar a Segurança da Informação					
AGM-01	Implantar serviço de monitoramento	Taxa de serviço implantado	100%	-	-
Amon-02	Gerenciar as políticas de segurança de TIC na rede de dados do INSS	Taxa de políticas gerenciadas	100%	-	-
Amon-03	Gerenciar as políticas de segurança de TIC no serviço de diretório do INSS	Taxa de políticas gerenciadas	100%	-	-
Amon-04	Construir dashboard de segurança da informação	Taxa de dashboard construído	100%	-	-

Amon-05	Monitorar proteção de endpoint	Taxa de endpoints monitorados	100%	-	-
Amon-06	Monitorar rede de dados do INSS	Taxa de unidades monitoradas	100%	-	-
Amon-07	Monitorar serviço de Diretório	Taxa de serviços monitorados	100%	-	-
Amon-08	Monitorar ativos de TIC	Taxa de ativos monitorados	100%	-	-
Amon-09	Executar Pentest em aplicações críticas	Taxa de aplicações testadas	-	100%	-
NSI3 - Aprimorar Normas e Processos de Negócio de Segurança da Informação					
ANP-01	Revisar a POSIN	Política revisada	1	-	-
ANP-02	Revisar a NCAL, funções de gestão de acesso e política de perfis	Norma revisada	1	-	-
ANP-03	Normativar a utilização de redes sem fio (wi-fi)	Norma publicada	1	-	-
ANP-04	Implantar ações do Programa de Privacidade e Segurança da Informação (PPSI)	Taxa de implantação de ações	-	100%	-
ANP-05	Revisar os serviços e processos da Central Service	Taxa de serviços e processos revisados	-	100%	-
ANP-06	Revisar os serviços e processos da API do Market Place	Taxa de serviços e processos revisados	-	100%	-
NSI4 - Prevenir incidentes de Segurança da Informação					
API-01	Aprimorar controles de segurança física nas unidades do INSS	Taxa de controles aprimorados	-	-	100%
API-02	Inventariar e Classificar ativos da informação	Taxa de ativos inventariados e classificados	100%	-	-

API-03	Sersibilizar os colaboradores do INSS	Taxa de colaboradores sensibiliados	60%	100%	-
API-04	Revisar e fortalecer políticas de senha	Taxa de revisão da política de senha	100%	-	-
API-05	Ampliar a adoção de duplo fator de autenticação	Taxa de adoção	100%	-	-
API-06	Disponibilizar inventário de contas de sistemas do INSS e Dataprev	Inventário disponibilizado	1	-	-
API-07	Avaliar e revisar o ciclo de vida das contas INSS	Taxa de avaliação e revisão	100%	-	-
API-08	Avaliar/revisar ciclo de vida das contas Dataprev	Taxa de avaliação e revisão	100%	-	-
API-09	Executar evoluções GERID	Taxa de evoluções concluídas	100%	-	-
API-10	Disponibilizar módulo de consumo de logs da Dataprev	Módulo disponibiliado	1	-	-
API-11	Implantar gestão de vulnerabilidades	Gestão de vulnerabilidades implantadas	-	1	-
API-12	Efetuar desabilitação automática de contas sem acesso há mais de 60 dias	Desabilitação efetuada	1	-	-
API-13	Restringir privilégios de administrador às contas de Administrador.dedicadas	Privilégios restringidos	1	-	-
API-14	Avaliar e implementar Single Sign-On – Dataprev	Taxa de implantação	-	-	100%
API-15	Desativar/migrar ou reforçar a autenticação para acesso aos sistemas legados, notadamente CV3 e Prisma	Taxa de migração	100%	-	-
API-16	Revisar controles de acesso Central 135	Taxa de revisão	-	100%	-
API-17	Aprimorar controles e níveis de segurança da árvore LDAP	Taxa de controles aprimorados	100%	-	-

API-18	Revisar lista de usuários com permissão de escrita no LDAP	Taxa de usuários revisados	100%	-	-
API-19	Apurar reutilização de hash de sessão – sistemas Dataprev	Taxa de apuração executada	100%	-	-
API-20	Executar demandas remanescentes GERID/LDAP 2022	Taxa de execução	100%	-	-
API-21	Implantar obrigatoriedade de certificado digital para acesso a sistemas críticos (sistemas e usuários internos e externos)	Taxa de implantação	50%	80%	100%
API-22	Migrar aplicações hospedadas em infraestrutura própria para ambiente de nuvem	Taxa de aplicações migradas	100%	-	-
API-23	Implantar hardening nos servidores Linux de propriedade do INSS	Taxa de implantação	100%	-	-
API-24	Implantar política de back-up nas aplicações hospedadas em infraestrutura própria	Taxa de implantação	-	100%	-
API-25	Padronizar a configuração dos switches nacionalmente	Taxa de equipamentos configurados	100%	-	-
NSI5 - Executar ações de Detecção, Tratamento e Resposta a Incidentes de Segurança da Informação					
ADTR-01	Revisar processo de tratamento de incidentes de segurança de TIC – interação com DATAPREV	Taxa de Processo revisado	-	-	100%
ADTR-02	Revisar processo de tratamento de incidentes de segurança de TIC – investigação interna	Taxa de Processo revisado	-	-	100%
ADTR-03	Revisar processo de tratamento de incidentes de segurança de TIC – encaminhamentos externos	Taxa de Processo revisado	-	-	100%

Tabela 5 - Metas e Ações

8.4 – Critérios de Priorização

A ferramenta utilizada na análise das priorizações foi a matriz de priorização, ou Matriz GUT, que considera a gravidade, a urgência e a tendência do problema:

- **GRAVIDADE** - é o impacto do problema sobre coisas, pessoas, resultados, processos ou organizações e efeitos que surgirão no longo prazo, caso o problema não seja resolvido;
- **URGÊNCIA** - é a relação com o tempo disponível ou necessário para resolver o problema;
- **TENDÊNCIA** - é o potencial de crescimento do problema, a avaliação da tendência de crescimento, redução ou desaparecimento do problema.

A cada ação identificada será atribuída uma pontuação entre 1 e 5 aos parâmetros Gravidade, Urgência e Tendência, conforme definição na Matriz GUT, e, em seguida, obtêm-se a priorização em ordem decrescente por meio da multiplicação dessas notas, G x U x T.

Nota	Gravidade	Urgência	Tendência
1	Sem gravidade	Pode esperar	Não irá mudar
2	Pouco grave	Pouco urgente	Irá piorar a longo prazo
3	Grave	O mais rápido possível	Irá piorar
4	Muito grave	É urgente	Irá piorar a curto prazo
5	Extremamente grave	Precisa de ação imediata	Irá piorar rapidamente

Tabela 6 - Critérios de Priorização

Id Ação	Ação	Indicador	G	U	T	Priorização
AInf-01	Disponibilizar solução de segurança de endpoints	Taxa da Solução disponibilizada	5	5	5	**125**
AInf-02	Atualizar sistema operacional dos ativos de TIC	Taxa de ativos de TIC atualizados	5	5	5	**125**
API-01	Aprimorar controles de segurança física nas unidades do INSS	Taxa de controles aprimorados	5	5	5	**125**
API-02	Inventariar e Classificar ativos da informação	Taxa de ativos inventariados e classificados	5	5	5	**125**
API-11	Implantar gestão de vulnerabilidades	Gestão de vulnerabilidades implantadas	5	4	4	**80**
API-21	Implantar obrigatoriedade de certificado digital para acesso a sistemas críticos e a VPN	Taxa de implantação	5	4	4	**80**
API-22	Migrar aplicações hospedadas em infraestrutura própria para ambiente de nuvem	Taxa de aplicações migradas	5	4	4	**80**
API-23	Implantar hardening nos servidores Linux de propriedade do INSS	Taxa de implantação	5	4	4	**80**
API-25	Padronizar a configuração dos switches nacionalmente	Taxa de equipamentos configurados	5	4	4	**80**
API-05	Aderir à rede federal de gestão de incidentes cibernéticos	Taxa de adesão	4	4	4	**64**
API-09	Executar evoluções GERID	Taxa de evoluções concluídas	4	4	4	**64**
API-12	Efetuar desabilitação automática de contas sem acesso há mais de 60 dias	Desabilitação efetuada	4	4	4	**64**
API-13	Restringir privilégios de administrador às contas de Administrador.dedicadas	Privilégios restringidos	4	4	4	**64**
API-15	Desativar/migrar ou reforçar a autenticação para acesso aos sistemas legados, notadamente CV3 e Prisma	Taxa de migração	4	4	4	**64**
API-16	Revisar controles de acesso Central 135	Taxa de revisão	4	4	4	**64**
API-17	Aprimorar controles e níveis de segurança da árvore LDAP	Taxa de controles aprimorados	4	4	4	**64**
API-18	Revisar lista de usuários com permissão de	Taxa de usuários	4	4	4	**64**

	escrita no LDAP	revisados				
API-19	Apurar reutilização de hash de sessão – sistemas Dataprev	Taxa de apuração executada	4	4	4	**64**
API-20	Executar demandas remanescentes GERID/LDAP 2022	Taxa de execução	4	4	4	**64**
API-24	Implantar política de backup nas aplicações hospedadas em infraestrutura própria	Taxa de implantação	5	4	3	**60**
AGM-01	Implantar serviço de monitoramento	Taxa de serviço implantado	3	3	3	**27**
Amon-02	Gerenciar as políticas de segurança de TIC na rede de dados do INSS	Taxa de políticas gerenciadas	3	3	3	**27**
Amon-03	Gerenciar as políticas de segurança de TIC no serviço de diretório do INSS	Taxa de políticas gerenciadas	3	3	3	**27**
Amon-08	Monitorar ativos de TIC	Taxa de ativos monitorados	3	3	3	**27**
Amon-09	Executar Pentest em aplicações críticas	Taxa de aplicações testadas	3	3	3	**27**
API-03	Sensibilizar os colaboradores do INSS	Taxa de colaboradores sensibilizados	3	3	3	**27**
API-04	Revisar e fortalecer políticas de senha	Taxa de revisão da política de senha	3	3	3	**27**
API-06	Disponibilizar inventário de contas de sistemas do INSS e Dataprev	Inventário disponibilizado	3	3	3	**27**
API-07	Avaliar e revisar o ciclo de vida das contas INSS	Taxa de avaliação e revisão	3	3	3	**27**
API-08	Avaliar/revisar ciclo de vida das contas Dataprev	Taxa de avaliação e revisão	3	3	3	**27**
API-10	Disponibilizar módulo de consumo de logs da Dataprev	Módulo disponibilizado	3	3	3	**27**
API-14	Avaliar e implementar Single Sign-On – Dataprev	Taxa de implantação	3	3	3	**27**
ADTR-01	Revisar processo de tratamento de incidentes de segurança de TIC – interação com DATAPREV	Taxa de Processo revisado	3	3	3	**27**
ADTR-02	Revisar processo de tratamento de incidentes de segurança de TIC – investigação interna	Taxa de Processo revisado	3	3	3	**27**

ADTR-03	Revisar processo de tratamento de incidentes de segurança de TIC – encaminhamentos externos	Taxa de Processo revisado	3	3	3	**27**
Amon-04	Construir dashboard de segurança da informação	Taxa de dashboard construído	3	3	2	**18**
Amon-05	Monitorar proteção de endpoint	Taxa de endpoints monitorados	3	3	2	**18**
Amon-06	Monitorar rede de dados do INSS	Taxa de unidades monitoradas	3	3	2	**18**
Amon-07	Monitorar serviço de Diretório	Taxa de serviços monitorados	3	3	2	**18**
AInf-03	Implantar serviço de operação de infraestrutura e segurança de TIC	Taxa de serviço implantado	3	2	2	**12**
ANP-01	Revisar a POSIN	Política revisada	2	2	2	**8**
ANP-02	Revisar a NCAL, funções de gestão de acesso e política de perfis	Norma revisada	2	2	2	**8**
ANP-03	Normatizar a utilização de redes sem fio (wi-fi)	Norma publicada	2	2	2	**8**
ANP-04	Implantar ações do Programa de Privacidade e Segurança da Informação (PPSI)	Taxa de implantação de ações	2	2	2	**8**
ANP-05	Revisar os serviços e processos da Central Service	Taxa de serviços e processos revisados	1	1	1	**1**
ANP-06	Revisar os serviços e processos da API do Market Place	Taxa de serviços e processos revisados	1	1	1	**1**

Tabela 7 - Ações

Legenda:

AInf - Ação de Estruturação de infraestrutura

AGM - Ação de Gestão e Monitoramento

ANP - Ação de Normatização e Mapeamento de Processos

API - Ação de Prevenção a Incidentes

ADTR - Ação de Detecção, Tratamento e Resposta a Incidentes.

9 – Plano de Gestão de Riscos

O plano de gestão de riscos está disponibilizado no anexo deste documento.

Este plano segue a Política de Gestão de Riscos do INSS, instituída pela Resolução nº 5/PRES/INSS, de 28 de maio de 2020 e a Metodologia de Gerenciamento de Riscos do INSS, aprovada pela Resolução CGOV/INSS, nº 20, de 20 de maio de 2022, em vigor desde 01 de junho de 2022.

Conforme a metodologia acima mencionada, são apresentadas a seguir as Escalas de Probabilidade, Impacto, Nível de risco e a Descrição do nível de risco:

Define como a probabilidade de um evento ocorrerá e será medida, analisando as causas ou o evento de risco considerando aspectos como a frequência observada e esperada.

A Probabilidade (P) é pontuada de 1 a 5, conforme tabela abaixo:

PROBABILIDADE	POSSIBILIDADE DE OCORRÊNCIA DO RISCO
5- Muito Alta	Evento esperado que ocorra na maioria das circunstâncias >90%
4- Alta	Evento provavelmente ocorra na maioria das circunstâncias >=50% <= 90%
3- Média	Evento deve ocorrer em algum momento >=30% <= 50%
2- Baixa	Evento pode ocorrer em algum momento >=10% <= 30%
1- Muito Baixa	Evento pode ocorrer apenas em circunstâncias excepcionais <10%

Tabela 9 - Escala de probabilidade

Define como o impacto será mensurado, em função da análise das consequências de um evento de risco com relação às dimensões (custo, prazo, escopo e qualidade) no caso de projetos/processos/iniciativa, e com relação à severidade que avalia o comprometimento do desempenho, confiabilidade ou qualidade do processo de trabalho ou do serviço provido tanto para o público interno ou externo.

O Impacto (I) é pontuado de 1 a 5, conforme demonstra a tabela abaixo:

IMPACTO	A OCORRÊNCIA DO RISCO CAUSARÁ
5- Catastrófico	Evento com potencial para levar o negócio/serviço ao colapso.
4- Grande	Evento crítico, mas com a devida gestão pode ser suportado.
3- Moderado	Evento significativo que pode ser gerenciado em circunstâncias normais.
2- Pequeno	Evento cujas consequências podem ser absorvidas, mas carece do esforço da gestão para minimizar o impacto.
1- Insignificante	Evento cujo impacto pode ser absorvido por meio de atividades normais.

Tabela 10 - Escala de impacto

Define o grau de risco para avaliação da intensidade dos quais (riscos) uma instituição está exposta.

ESCALA DE NÍVEL DE RISCO	
NÍVEIS	**PONTUAÇÃO**
RC - Risco Crítico	13 a 25
RA - Risco Alto	7 a 12
RM - Risco Moderado	4 a 6
RP - Risco Pequeno	1 a 3

Tabela 11 - Escala de Nível de risco

Nível de Risco	Descrição do Nível de Risco	Parâmetro de Análise para Adoção de Resposta	Tipo de Resposta	Ação de Controle
Risco Crítico	Indica que nenhuma opção de resposta foi identificada para reduzir a probabilidade e o impacto a nível aceitável. Nível de risco muito além do apetite a risco	Custo desproporcional, capacidade limitada diante do risco identificado	**Evitar**	Promover ações que evitem/eliminem as causas e/ou efeitos
Risco Alto	Indica que o risco residual será reduzido a um nível compatível com a tolerância a riscos. Nível de risco além do apetite a riscos	Nem todos os riscos podem ser transferidos. Exemplo: Risco de Imagem, Risco de Reputação	**Reduzir**	Adotar medidas para reduzir a probabilidade ou impacto dos riscos, ou ambos
Risco Moderado	Indica que o risco residual será reduzido a um nível compatível com a tolerância a riscos. Nível de risco dentro do apetite a risco	Reduzir probabilidade ou impacto, ou ambos	**Compartilhar ou Transferir**	Reduzir a probabilidade ou impacto pela transferência ou compartilhamento de uma parte do risco. (seguro, transações de hedge ou terceirização da atividade).
Risco Pequeno	Indica que o risco inerente já está dentro da tolerância a risco. Nível de risco dentro do apetite a risco	Verificar a possibilidade de retirar controles considerados desnecessários	**Aceita**	Conviver com o evento de risco mantendo práticas e procedimentos existentes

Tabela 12 - Descrição do Nível de Risco

		Matriz de Riscos				
I M P A C T O	Catastrófico	5	10	15	20	25
	Grande	4	8	12	16	20
	Moderado	3	6	9	12	15
	Pequeno	2	4	6	8	10
	Insignificante	1	2	3	4	5
		Muito Baixa	Baixa	Média	Alta	Muito Alta
		menor que 10%	de 10% a 30%	de 30% a 50%	de 50% a 90%	maior que 90%

PROBABILIDADE

Tabela 13 - Matriz de Risco

10 – Processo de Revisão do PDSI

O PDSI é um plano dinâmico e, portanto, poderá sofrer alterações no decorrer da sua vigência. O processo de revisão possibilita a implementação de procedimentos que orientem a atuação dos responsáveis pela execução do PDSI, possibilitando maximizar o alcance das ações planejadas com maior eficiência e eficácia.

O acompanhamento do PDSI permite a análise de mudanças no ambiente interno ou externo que impactem na sua execução. Dessa forma, mantém-se atualizado e adaptado aos novos cenários.

A revisão do PDSI e seus anexos será realizada trimestralmente ou conforme a necessidade. Revisões deverão ser submetidas à avaliação do CTGD sempre que impactarem o cumprimento de metas estabelecidas no plano, que incluírem ou excluírem ações, ou que modificarem o orçamento de TI.

11 – Fatores Críticos de Sucesso

Com o intuito de que o PDSI alcance a efetividade esperada, e se torne um importante instrumento para o aperfeiçoamento da segurança da informação, os fatores críticos de sucesso são condições que devem, necessariamente, ser satisfeitas. A ausência de um ou de vários fatores críticos identificados, ou mesmo sua presença de forma precária, gerará impacto na estratégia proposta no PDSI.

Os principais fatores críticos identificados:

- Patrocínio e participação ativa do CTGD no monitoramento do PDSI;
- Fortalecimento e participação ativa da Equipe de Acompanhamento do PDSI na execução das ações de monitoramento e avaliações previstas, incluindo suas possíveis revisões;
- Comprometimento das áreas responsáveis pela execução das ações na prestação tempestiva à DTI de informações sobre o seu andamento;
- Disponibilidade de recursos orçamentários e humanos proporcionais ao desafio proposto neste PDSI; e
- Apoio e comprometimento da alta direção do INSS.

12 – Conclusão

O PDSI 2023-2025 elenca um conjunto de ações mapeadas para solucionar problemas, aperfeiçoar serviços e implementar novas soluções, bem como os recursos orçamentários necessários para viabilizá-lo, o que é fundamental para que a Diretoria de Tecnologia da Informação do INSS, em harmonia com o Sistema de Governança Institucional, possam deliberar sobre os investimentos de TIC, baseados em análise de riscos e seus impactos.

Este plano pode e deve ser atualizado e complementado durante sua vigência para adequar-se às novas necessidades, diretrizes ou correções que se fizerem necessárias, através de monitoramento trimestral conduzido pela Coordenação de Governança e Planejamento de TI - COGPL e suas unidades subordinadas.

Anexo - Plano de Gestão de Riscos

Anexo III - Tabela 6 – Plano de Gerenciamento do Risco

ID	Evento de Risco	Probabilidade	Impacto	Criticidade	Escala	Tipo de resposta	Ação Preventiva	Ação Contingência	Responsável
1	Contingenciamento orçamentário	3	4	12	Alto	Reduzir	- Consultar a previsão de disponibilidade orçamentária diante da expectativa de custo de aquisição da solução. - Priorizar projetos segundo as maiores necessidades da Autarquia. - Rever os itens e quantitativos com o objetivo de tentar reduzir os custos de aquisição.	- Priorizar unidades que tenham maior necessidade da solução. - Verificar a prioridade deste projeto em relação aos demais projetos da Autarquia. - Elaborar estratégia de aquisição de ativos, contendo percentuais a serem adquiridos a cada ano.	Ação Preventiva: Ação Contingência:
2	Perda de recursos humanos	2	3	6	Moderado	Reduzir	-Melhorar a qualidade do ambiente de trabalho. -Capacitar gestores para melhoria do relacionamento com seus colaboradores.	-Criar Banco de Talentos para substituição de eventuais perdas de colaboradores.	

							-Incentivar a capacitação de seus colaboradores.		
3	Descontinuidade de planos e projetos por mudança de gestão	4	4	16	Crítico	Aceitar	- Elaborar o PDSI com base nos normativos legais vigentes. -Sensibilizar os novos gestores sobre a importância dos projetos.	-Prever no PDSI as revisões para atender as mudanças nas políticas por novos gestores.	
4	Demandas fora do planejamento do PDSI	3	3	9	Alto	Aceitar	-Envolver de forma mais efetiva os gestores no levantamento de necessidades. - Difundir o PDSI em toda à instituição.	-Envolver de forma mais efetiva os gestores no levantamento de necessidades.	

5	**Descontinuidade do fornecimento de bens ou serviços de TIC, relacionados a segurança da informação.**	**1**	**4**	**4**	**Moderado**	**Mitigar**	**Verificar constantemente a execução dos serviços, apontando as não conformidades.** **Observar as recomendações da área jurídica do órgão/entidade.** **- Prever aplicação de multas em caso de impactos à instituição.**	**- Estudar possível contratação de nova empresa para garantia e suporte técnico para os itens que perderam o suporte.** **-Verificar possibilidade legal de chamar a próxima colocada.** **- Renovar de forma provisória o contrato.**	
6	**Escassez de colaboradores para execução do PDSI**	**5**	**4**	**20**	**Crítico**	**Aceitar**	**-Aumentar a equipe de colaboradores.**	**-Desenvolver os projetos, conforme critérios de priorização.**	
7	**Mudanças nas normas legais**	**3**	**2**	**6**	**Moderado**	**Aceitar**	**-Participação efetiva da alta gestão da DTI nas mudanças dos normativos internos.** **-Acompanhar possíveis alterações em normativos legais que impactam a Segurança da Informação no âmbito do INSS.**	**-Revisão do PDSI em observância a novos dispositivos legais.**	

8	**Alteração de requisitos ou de escopo de projetos**	**3**	**4**	**12**	**Alto**	**Reduzir**	**-Definir de forma precisa com os demandantes o escopo do projeto e seus requisitos.** **- Identificar, analisar e validar os requisitos.** **- Formalizar documento de identificação, análise e validação dos requisitos.**	**Elaborar novo documento de levantamento dos requisitos.**	
9	**Monitoramento e controle da execução do PDSI inadequados**	**3**	**4**	**12**	**Alto**	**Reduzir**	**-Rever a sistemática de monitoramento e controle do PDSI.**	**-Acompanhar de forma contínua a execução do PDSI.**	

10	**Infraestrutura tecnológica inadequada para suportar as ações e projetos do PDSI**	**2**	**4**	**8**	**Alto**	**Evitar**	**- Avaliar a infraestrutura necessária às necessidades técnicas da solução.** **-Adaptar a infraestrutura tecnológica aos projetos previstos no PDSI.** **- Verificar a viabilidade da implantação da solução técnica desejada.** **- Analisar os requisitos do bem ou serviço que compõe a solução**	**-Disponibilizar de forma emergencial os recursos de infraestrutura necessários para continuidade do negócio.**	
11	**Processos de governança e gestão do PDSI com baixa maturidade**	**2**	**3**	**6**	**Moderado**	**Reduzir**	**-Definir e implementar os processos de gestão do PDSI.** **-Capacitar servidores responsáveis pelo monitoramento e controle do PDSI.** **-Implementar solução para gestão do PDSI.**	**- Revisar os procedimentos existentes para gestão e governança do PDSI.**	