PROCESSO DE GESTÃO DE RISCOS DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

REFERÊNCIAS

Decreto nº 12.572, de 4 de agosto de 2025, que institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da administração pública federal;

Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD;

Instrução Normativa GSI/PR 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, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;

Instrução Normativa GSI/PR nº 9, de 8 de janeiro de 2026, que altera a Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, e dispõe sobre a governança e a gestão da segurança da informação e cibernética no âmbito da administração pública federal;

Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação;

Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025;

Instrução Normativa nº 128, de 6 de novembro de 2018, instituiu a Política de Segurança da Informação da ANAC - PoSI;

Instrução Normativa nº 172, de 2 de agosto de 2021, que aprova a Política de Proteção de Dados Pessoais - PoPD no âmbito da Agência Nacional de Aviação Civil - ANAC;

Instrução Normativa nº 186, de 22 de fevereiro de 2023, institui a Política de Gestão de Integridade, de Riscos Corporativos e de Continuidade de Negócios da ANAC e o Comitê de Governança, Riscos e Controle;

Portaria nº 5.805, de 30 de agosto de 2021, que institui o Comitê de Segurança da Informação e Proteção de Dados Pessoais da ANAC;

Portaria nº 13.665, de 22 de janeiro de 2024, que designa o Encarregado pelo tratamento de Dados Pessoais;

Portaria nº 13.755, de 29 de janeiro de 2024, que designa o Gestor de Segurança da Informação da ANAC;

Portaria nº 9.457, de 6 de outubro de 2022, que dispõe sobre a gestão de inventário e mapeamento de ativos de informação da ANAC;

ISO/IEC 27001:2022 – Sistemas de gestão de segurança da informação;

ISO/IEC 27005:2022 – Diretrizes para a gestão de riscos de segurança da informação;

ISO/IEC 27701:2019 – Segurança da informação, privacidade e gestão da proteção de dados pessoais;

ISO 31000:2018 – Gestão de riscos;

Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações do Sistema de Administração de Recursos da Tecnologia da Informação do Poder Executivo Federal - MGR-SISP, versão 2.0;

Manual de Referência de Gestão de Riscos dos Processos Organizacionais da ANAC; e

Guia Orientativo para Elaboração de Relatório de Impacto à Proteção de Dados Pessoais - RIPD – Autoridade Nacional de Proteção de Dados - ANPD.

CAPÍTULO I

DO OBJETIVO

O presente manual tem o objetivo de estabelecer o processo de gestão de riscos de privacidade e de segurança da informação no âmbito da ANAC, definindo diretrizes e procedimentos para identificar, analisar, avaliar, tratar, monitorar e comunicar riscos associados a ativos de informação e ao tratamento de dados pessoais.

O processo aplica-se a todas as unidades organizacionais da ANAC e a seus colaboradores que tratem ou tenham acesso a ativos de informação ou dados pessoais sob responsabilidade da Agência.

São objetivos específicos:

I. proteger os ativos de informação da ANAC;
II. garantir a continuidade dos processos regulatórios e administrativos da Agência;
III. assegurar a conformidade com os requisitos legais, normativos e institucionais aplicáveis; e
IV. proteger os direitos e as liberdades fundamentais dos titulares de dados pessoais; e
V. contribuir para o cumprimento da Política Nacional de Segurança da Informação e da Lei Geral de Proteção de Dados Pessoais - LGPD.

CAPÍTULO II

DAS DEFINIÇÕES

Para os fins deste Processo, considera-se:

Ameaça: conjunto de fatores externos com o potencial de causar em dano para um sistema ou organização;

Agente responsável pela gestão de riscos de privacidade e segurança da informação: servidor efetivo do órgão responsável por elaborar o plano de gestão de riscos de privacidade e segurança da informação, o relatório de identificação, análise e avaliação dos riscos de privacidade e segurança da informação e o relatório de tratamento de riscos de privacidade e segurança da informação;

Ativo: tudo que tem valor para a organização, material ou não;

Ativos de informação - meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

Ativo crítico de informação: é todo aquele relacionado aos objetivos estratégicos da ANAC e que afeta a missão da Agência se for revelado, modificado, destruído ou mal-usado, ou seja, é o ativo requerido para executar as atividades-fim e de suporte da Instituição, bem como para desempenhar outras atividades essenciais para o alcance da sua missão;

Autoridade Competente: responsável por prover os recursos necessários à gestão de riscos; identificar responsáveis; iniciar as atividades de gestão de riscos; aprovar pontos importantes relativos à gestão de riscos tais como: objetivo, restrições e aprimoramentos da MGR-SISP. Essa função será exercida pela liderança do CSIP;

Controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas, estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;

CSIP: Comitê de Segurança da informação e de Proteção de Dados Pessoais;

Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável;

Dado Pessoal Sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados - ANPD. No escopo da gestão de riscos, é responsável por coordenar a gestão de riscos de privacidade, designar o agente responsável pela gestão de riscos de privacidade, aprovar o plano de gestão de riscos de privacidade e os relatórios de identificação, análise, avaliação e tratamento dos riscos de privacidade, bem como propor medidas preventivas à alta administração;

Gestor de riscos: é o agente responsável pela gestão de riscos de privacidade e/ou segurança da informação;

Gestor de segurança da informação - responsável pelas ações de segurança da informação no âmbito da ANAC. No escopo da gestão de riscos, é responsável por coordenar a gestão de riscos de segurança da informação, designar o agente responsável pela gestão de riscos de segurança da informação, aprovar o plano de gestão de riscos de segurança da informação e os relatórios de identificação, análise, avaliação e tratamento dos riscos de segurança da informação, bem como propor medidas preventivas à alta administração. ;

GRPSI: sigla para Gestão de Riscos de Privacidade e Segurança da Informação;

Impacto: resultado da ocorrência de determinado evento de risco;

Mapa de Risco: documento ou representação sistematizada que consolida os riscos identificados em um determinado escopo organizacional, indicando suas causas, probabilidades, impactos, níveis de criticidade e medidas de tratamento definidas;

Probabilidade: chance ou possibilidade de um evento de risco acontecer;

Responsável pela Unidade Organizacional: responsável por uma área da organização na qual a metodologia será implementada ou por uma área que deve prover informações para a gestão de riscos. Tem o papel de coordenar o fornecimento das informações necessárias à identificação e à estimativa de riscos e realizar melhorias necessárias quando as análises indicarem. Pode ser o chefe da UDVD ou pessoa por ele indicada;

Responsável por ativos: responsável por fornecer informações sobre os ativos que fazem parte da análise de riscos. Essas informações auxiliam a tomada de decisões sobre controles a serem implementados;

Risco: no sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade;

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Violação de segurança: situação que pode ocorrer quando uma vulnerabilidade de um ativo é explorada por uma ameaça;

Vulnerabilidade: fraqueza de um determinado ativo ou controle que pode ser explorado por uma ameaça.

CAPÍTULO III

DO ESCOPO

Este processo aplica-se aos ativos críticos de informação e privacidade da ANAC.

Os ativos críticos de informação da ANAC deverão ser formalmente definidos pela Superintendência de Tecnologia e Transformação Digital - STD, enquanto os ativos críticos de privacidade serão definidos pela Assessoria Técnica - Astec, devendo ambos ser submetidos à aprovação do Comitê de Segurança da Informação e de Proteção de Dados Pessoais - CSIP.

A monitoração e avaliação do processo ficará a cargo do gestor de segurança da informação e do encarregado pelo tratamento de dados pessoais, no âmbito de suas respectivas competências.

CAPÍTULO IV

DO PÚBLICO

Este processo se aplica:

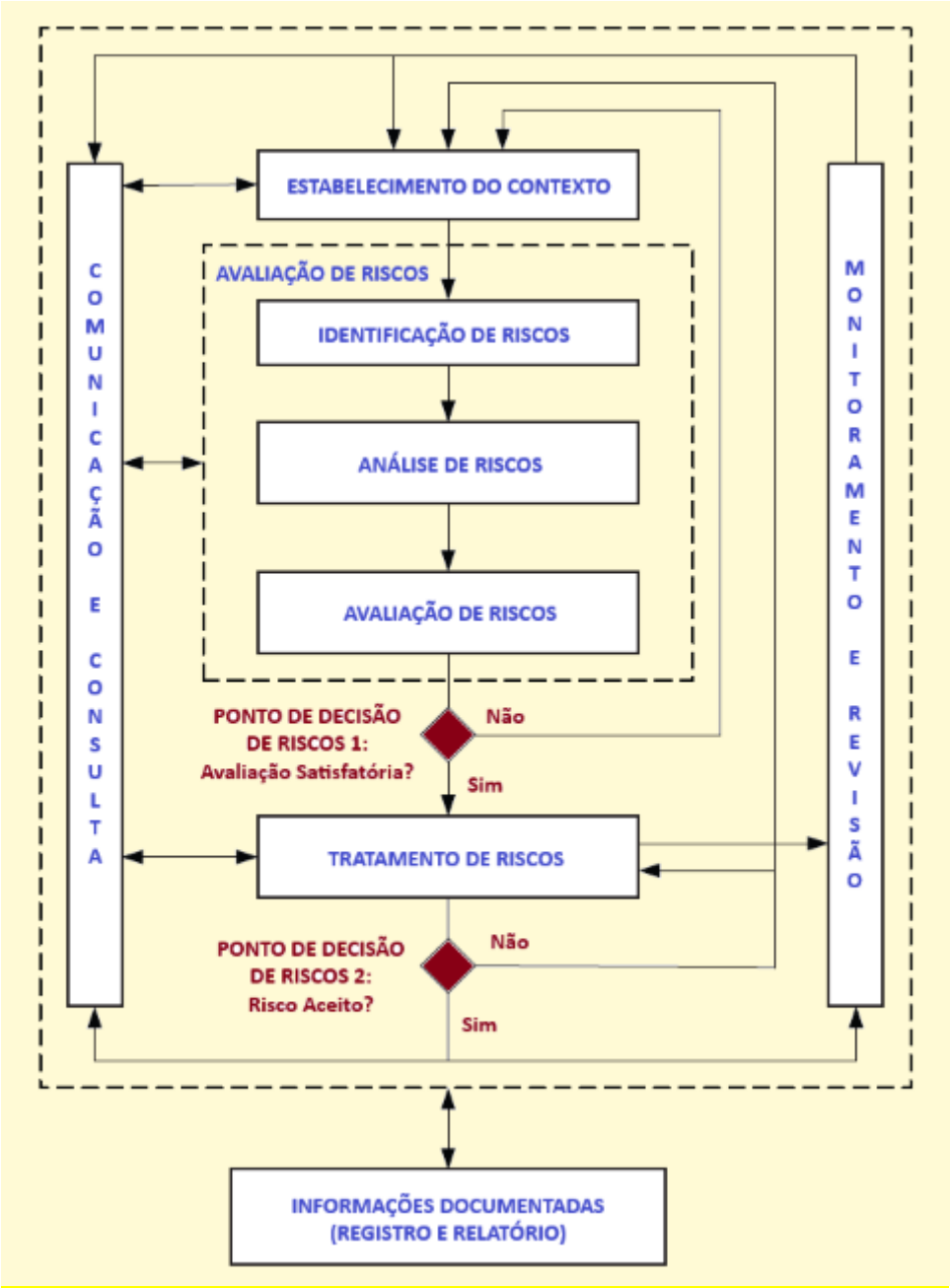
I - aos indivíduos responsáveis pela gestão ou que utilizem ativos de informação ou tratem dados pessoais no âmbito da ANAC; e

II - a provedores de serviços e entidades terceirizadas que tenham acesso a ativos de informação, redes, sistemas ou dados pessoais sob responsabilidade da ANAC .

CAPÍTULO V

DO PROCESSO DE GESTÃO DE RISCOS DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

O Processo segue o ciclo contínuo de Gestão de Riscos recomendado pela Norma ABNT NBR ISO/IEC 27005:2022.



Fonte: NBR ISO/IEC 27005:2023

Como resultado da execução da fase de avaliação de riscos e tratamento de riscos deverão constar os seguintes documentos, respectivamente:

- Relatório de identificação, análise e avaliação dos riscos (Anexo IV).
- Relatório de tratamento de riscos (Anexo V).

CAPÍTULO VI

DO ESTABELECIMENTO DO CONTEXTO

Compreende a proposição dos objetivos, escopo (estrutura funcional, processo, sistema, recurso ou determinado ativo) e limites da avaliação de riscos a ser realizada, observadas as Políticas de Segurança da Informação, de Proteção de Dados Pessoais e de Gestão de Integridade, de Riscos Corporativos e de Continuidade de Negócios da ANAC. As exclusões do escopo devem também ser definidas e justificadas.

Essa fase é composta pelas seguintes tarefas:

I. Definir gestor de riscos;
II. Definir objetivos, premissas, restrições e escopo do processo de GRPSI;
III. Validar objetivos, premissas, restrições e escopo do Processo de GRPSI;
IV. Definir Responsáveis Pelas Unidades da Organização;
V. Definir Responsáveis Por Ativos.

Definir gestor de riscos:

O gestor de segurança da informação e o encarregado pelo tratamento de dados pessoais deverão designar formalmente o gestor de riscos, também denominado agente responsável pela gestão de riscos de privacidade e segurança da informação, para a condução das próximas atividades do processo de GRPSI, no âmbito de suas respectivas competências.

Definir objetivos, premissas, restrições e escopo do processo de GRPSI

O gestor de riscos deve iniciar o processo de GRPSI e informar os objetivos genéricos (de alto nível) e os objetivos específicos, tais como os relacionados aos seguintes pontos: informações confidenciais, sistemas que requerem alta disponibilidade, sistemas e informações cruciais para a tomada de decisões etc.

Além disso, o gestor de riscos deve identificar e descrever os tipos de restrições que se apliquem, tais como questões técnicas, jurídicas, financeiras, de prazos etc.

O gestor de riscos deve identificar também as unidades dentro do escopo do processo de GRPSI e as que estão fora do escopo do processo. Devem ser identificados também o responsável por cada unidade identificada no escopo.

Validar objetivos, premissas, restrições e escopo do processo de GRPSI.

O gestor de segurança da informação e o encarregado pelo tratamento de dados pessoais deverão verificar, no âmbito de suas respectivas competências, se as informações definidas nas tarefas anteriores são estratégicas e se estão alinhadas às necessidades e às expectativas da organização.
Caso estejam de acordo, deverão registrar a aprovação do processo de GRPSI.

Definir Responsáveis Pelas Unidades da Organização

O Gestor de Riscos deve identificar os profissionais que assumirão os papéis de Responsável Pela Unidade da Organização.

Definir Responsáveis Por Ativos

Os Responsáveis Pelas Unidades da Organização devem identificar os profissionais que assumirão os papéis de Responsáveis Por Ativos em cada unidade e posteriormente notificar o gestor de riscos.

CAPÍTULO VII

DA IDENTIFICAÇÃO DE RISCOS

Esse processo trata da identificação e descrição de riscos no escopo do processo de GRPSI e das consequências adversas resultantes. Busca-se compreender possíveis ameaças e vulnerabilidades existentes e avaliar a extensão e a adequação dos controles utilizados.

Para fins de priorização, pode se utilizar os riscos identificados no Processo de Gestão de Riscos Corporativo para focar os esforços e recursos primeiro em setores mais críticos e, depois, nos sucessivamente menos críticos. Importante destacar que existem ameaças e vulnerabilidades que impactam a organização como um todo e, dessa forma, deve-se priorizar o tratamento dessas ameaças também.

Essa fase é composta pelas seguintes atividades:

I. Identificar ativos; e
II. Identificar ameaças, controles e vulnerabilidades.

Identificar ativos

Nesta atividade são identificados os ativos que estão no escopo do Processo de GRPSI, incluindo ativos de informação e ativos relacionados ao tratamento de dados pessoais.

De modo geral os tipos de ativos para a identificação e o registro são:

Ativos primários:

- Processos de negócio e suas atividades;
- Informações; e
- Dados pessoais tratados pela ANAC.

Ativos de suporte:

- **Hardware, por exemplo:**
    - Equipamentos de processamento fixos (microcomputadores, servidores etc.);
    - Equipamentos de processamento móveis (notebooks, celulares etc.);
    - Periféricos;
    - Mídias de dados (pen-drive, cd etc.);
    - Outras mídias não eletrônicas (documentos em papel).

- **Software, por exemplo:**
    - Sistemas operacionais;
    - Software de administração;
    - Pacotes de software;
    - Aplicações de negócio.

- **Redes, por exemplo:**
    - Mídias e apoio (equipamentos e protocolos, como Ethernet, protocolos e equipamento WiFi, Bluetooth, Firewall etc.);
    - Equipamentos intermediários (roteadores, hub, switch);
    - Interfaces de comunicação (adaptadores).

- **Pessoal, por exemplo:**
    - Tomadores de decisão (proprietários de ativos, responsáveis por unidades, representantes da Alta Administração.);
    - Usuários (pessoal que interage com os ativos, recursos humanos, terceirizados etc.);
    - Pessoal de operação e manutenção (administrador do sistema, administrador de banco de dados, help desk etc.);
    - Desenvolvedores (analistas, programadores etc.).

- **Locais/recursos, por exemplo:**
    - Ambiente externo (outras organizações, casas de pessoas etc.);
    - Zonas, locais (prédios, áreas de escritório, salas reservadas etc.);
    - Serviços essenciais (energia elétrica);
    - Comunicações (telefone);
    - Utilidades (nobreaks, ar-condicionado etc.).

- **Organização, por exemplo:**
    - autoridades (líderes, representantes da Alta Administração);
    - Estrutura da organização (gerenciamento de RH, financeiro...);
    - Projetos da organização (migração de sistemas, desenvolvimentos...);
    - Subcontratados (gerenciamento externo, consultores...).

A lista de tipos de Ativos de Suporte é abrangente é exemplificativa, deve-se assim avaliar quais subconjuntos desses tipos de ativos serão utilizados no processo.

Cada Responsável Pela Unidade da Organização, juntamente com o gestor de riscos, devem retomar as informações geradas nas atividades do Processo “Estabelecer Contexto” para definir como abordar a gestão de riscos em cada unidade no escopo do Processo de GRPSI. Deve ser decidido, para cada unidade, o nível de detalhamento a ser adotado na identificação de ativos.

Posteriormente, devem ser notificados os Responsáveis Pelas Unidades da Organização onde o processo será conduzido para que os ativos sejam identificados segundo a abordagem definida e nos prazos estabelecidos.

Os gestores de risco, como apoio dos responsáveis pelos ativos, devem identificar e registrar no Mapa de Riscos cada ativo que faz parte do escopo do Processo de GRPSI, incluindo aqueles que envolvam tratamento de dados pessoais.

Informações típicas que caracterizam os ativos são:

- natureza (primário ou suporte);
- tipo (hardware, software etc.);
- subtipo (notebook, pen-drive etc.);
- descrição; responsável pelo ativo;
- indicação da presença de dados pessoais, quando aplicável;
- responsável pela unidade que abriga o ativo;
- data de cadastro;
- localização física; e
- valor de reposição.

Esta tarefa é realizada em cada unidade da organização no escopo do Processo de GRPSI, em ordem priorizada por criticidade. O resultado da tarefa é o cadastro de cada ativo em cada unidade da organização que faz parte do escopo do Processo de GRPSI.

O gestor de riscos deve avaliar as informações sobre ativos no Mapa de Riscos.

Identificar ameaças, controles e vulnerabilidades

Para cada ativo identificado, devem ser analisadas e identificadas as ameaças, os controles e as vulnerabilidades associadas a cada ativo identificado, incluindo aquelas relacionadas ao tratamento de dados pessoais e à proteção da privacidade, quando aplicável.

O responsável por ativos deve, com o apoio e acompanhamento do responsável pela unidade da organização, para cada ativo identificado na atividade anterior, identificar, identificar, no Mapa de Riscos, as ameaças existentes (vide Anexo I – Lista de Ameaças), incluindo ameaças relacionadas à violação de dados pessoais, acesso não autorizado, uso indevido ou tratamento inadequado de dados pessoais, bem como descrever essas ameaças. Devem ser informados os controles aplicáveis (vide Anexo II – Lista de Controles) e a situação de implementação de cada controle (implementado ou não implementado).

A partir da análise dos controles, devem ser identificadas, no Mapa de Riscos, as vulnerabilidades (vide Anexo III – Lista de Vulnerabilidades) para as quais não há controles implementados e cuja exploração por uma ameaça pode incorrer em uma violação de segurança ou em incidente envolvendo dados pessoais.

O Responsável pela Unidade da Organização deve avaliar, no Mapa de Riscos, as informações das ameaças, controles e vulnerabilidades relacionadas aos ativos da unidade. Caso não estejam de acordo, o Responsável Pela Unidade da Organização deve realizar, juntamente com o Responsável Por Ativos, as alterações necessárias no Mapa de Riscos.

O gestor de riscos deve avaliar as informações no Mapa de Riscos e caso não esteja de acordo, deve notificar o Responsável Pela Unidade da Organização da necessidade de reexecutar uma ou mais das tarefas anteriores e informar o prazo para conclusão das tarefas, bem como as orientações para aprimoramento das informações.

CAPÍTULO VIII

DA ANÁLISE DE RISCOS

Esta etapa trata da estimação dos riscos identificados, incluindo aqueles relacionados à segurança da informação e à proteção de dados pessoais. A estimação visa compreender o impacto das consequências provocadas caso as ameaças aos ativos ocorram de fato, definindo quantitativamente o nível de impacto.

Trata também de ponderar sobre quais são as chances de que as ameaças se tornem realidade.

As seguintes atividades compõem essa etapa:

I. Avaliar Impactos;
II. Avaliar Probabilidades; e
III. Estimar Nível de Risco.

Avaliar Impactos – Segurança da Informação

A avaliação deve ser feita para cada ativo no escopo do processo e para cada ameaça ao ativo. O resultado da análise deve refletir a extensão do dano causado pela perda de atributos de segurança (confidencialidade, integridade e disponibilidade) associados ao ativo caso a ameaça se concretize (violação de segurança).

O responsável por ativos deve considerar as seguintes fontes de informação em sua análise:

- A lista de possíveis tipos de consequências;
- Informações históricas sobre incidentes;
- O conhecimento dos responsáveis pelo ativo e informações;
- Controles existentes: deve-se levar em conta os controles já estabelecidos para refletir o fato de que o impacto é menor se controles eficazes existem e maior caso contrário.

Cada atributo de segurança é contemplado separadamente, portanto, o responsável pela atividade realizará três análises distintas para cada ameaça e ativo.

As três análises para uma ameaça e ativo são consolidadas por meio de uma função:

I = F (IC, II, ID)

Sendo:

- I: Impacto.
- F: Função de consolidação de impacto.
- IC: Impacto relativo à Confidencialidade.
- II: Impacto relativo à Integridade.
- ID: Impacto relativo à Disponibilidade.

O valor do impacto resulta no maior valor entre IC, II, ID.

O resultado desta atividade é a estimativa de impacto para cada risco e a classificação desse impacto em uma determinada classe:

CONFIDENCIALIDADE	
Nível	**Descrição**
Inexistente (IN)	Informações expostas são públicas ou irrelevantes; não há risco à organização nem a terceiros.
Pequeno (P)	Vazamento de informações internas ou operacionais de baixo impacto; impacto reputacional ou operacional desprezível.
Moderado (M)	Acesso não autorizado a informações restritas, mas sem envolvimento de dados sensíveis ou críticos; risco controlável à imagem ou operação.
Grande (G)	Vazamento de informações confidenciais ou sensíveis (ex: dados pessoais ou estratégicos); impacto relevante à reputação, conformidade ou operação.
Extremo (E)	Comprometimento de informações altamente sensíveis, como dados protegidos por lei, propriedade intelectual crítica ou segredos comerciais; pode gerar sanções legais, perdas financeiras elevadas ou danos irreparáveis à reputação.

INTEGRIDADE	
Nível	**Descrição**
Inexistente (IN)	Alterações insignificantes em dados não críticos; sem impacto nas operações.
Pequeno (P)	Alterações em dados de apoio ou de baixa importância; possíveis erros menores que podem ser corrigidos facilmente.
Moderado (M)	Modificações em dados importantes que afetam processos internos, exigindo retrabalho ou validação adicional.
Grande (G)	Alterações ou corrupção de dados essenciais que afetam decisões, relatórios ou serviços críticos; pode causar falhas operacionais relevantes.
Extremo (E)	Comprometimento grave e generalizado da integridade de sistemas ou dados críticos; perda de confiança nos sistemas, impactos legais, operacionais e financeiros severos.

DISPONIBILIDADE	
Nível	**Descrição**
Inexistente (IN)	Nenhum serviço ou atividade é afetado.
Pequeno (P)	Poucos serviços ou atividades de menor importância são afetados; pode provocar atrasos desprezíveis.
Moderado (M)	Alguns serviços ou atividades são afetados, podendo causar atrasos significativos.
Grande (G)	Serviços essenciais são afetados, provocando atrasos graves e danos elevados.
Extremo (E)	Serviços essenciais são afetados severamente, gerando danos muito elevados e atrasos intoleráveis.

Avaliar Impactos – Privacidade

A avaliação do impacto no escopo de privacidade não considera os atributos de confidencialidade, integridade e disponibilidade. Ela se concentra na análise da gravidade dos potenciais efeitos sobre os direitos e as liberdades fundamentais dos titulares de dados pessoais, em conformidade com os princípios estabelecidos pela LGPD.

O processo de gestão de riscos de privacidade também contribui para demonstrar a adoção de medidas de governança e conformidade com a LGPD, em observância ao princípio da responsabilização e prestação de contas.

Nesse contexto, o impacto sobre a privacidade deve considerar as seguintes fontes de informação:

- informações históricas sobre incidentes envolvendo dados pessoais;
- controles existentes, considerando que a existência de controles eficazes pode reduzir o impacto potencial, enquanto sua ausência pode ampliá-lo;
- o grau de exposição ou acessibilidade das informações;
- a natureza dos dados pessoais tratados, com especial atenção aos dados pessoais sensíveis;
- o volume de titulares potencialmente afetados;
- o tratamento de dados de crianças e adolescentes;
- a extensão, a severidade e a reversibilidade dos prejuízos potenciais.

A avaliação do impacto em privacidade considera 4 (quatro) atributos: volume de titulares afetados, sensibilidade dos dados, impacto nos direitos e liberdades do titular e duração do impacto. O resultado para cada atributo é consolidado por meio de uma função:

$$I = Fp (VT, SD, DL, TI)$$

Sendo:

- I: Impacto.
- Fp: Função de consolidação de impacto de privacidade.
- VT: Impacto relativo ao volume de titulares afetados.
- SD: Impacto relativo à sensibilidade dos dados.
- DL: Impacto relativo aos direitos e liberdades dos titulares.
- TI: Impacto relativo à duração do impacto sobre os direitos e liberdades dos titulares.

O valor do impacto resulta no maior valor entre VT, SD, DL, TI.

O resultado desta atividade é a estimativa de impacto para cada risco e a classificação desse impacto em uma determinado classe:

Volume de titulares afetados

Nível	Descrição
Inexistente (IN)	Nenhum titular e afetado
Pequeno (P)	Até 10 titulares afetados
Moderado (M)	11 a 1.000 titulares afetados
Grande (G)	1.001 a 10.000 titulares afetados
Extremo (E)	Acima de 10.000 de titulares afetados

Sensibilidade dos dados	
Nível	**Descrição**
Inexistente (IN)	Não há tratamento de dados pessoais
Pequeno (P)	Tratamento de dados pessoais básicos ou públicos
Moderado (M)	Dados pessoais comuns que podem gerar algum impacto se exposto
Grande (G)	Dados pessoais sensíveis ou que podem gerar discriminação ou danos relevantes
Extremo (E)	Dados altamente sensíveis ou sigilosos (saúde, biometria, origem racial, dados de crianças etc.)

Impacto nos direitos e liberdades do titular	
Nível	**Descrição**
Inexistente (IN)	Nenhum impacto sobre os direitos do titular
Pequeno (P)	Impacto mínimo e facilmente reversível
Moderado (M)	Impacto moderado que pode gerar inconvenientes ao titular
Grande (G)	Impacto significativo nos direitos ou na privacidade do titular
Extremo (E)	Impacto severo, podendo gerar discriminação, danos financeiros ou morais graves

Duração do impacto	
Nível	**Descrição**
Inexistente (IN)	Nenhum impacto sobre os direitos do titular
Pequeno (P)	Impacto de curta duração e facilmente resolvido
Moderado (M)	Impacto temporário com algum esforço para resolução

Grande (G)	Impacto prolongado e difícil de reverter
Extremo (E)	Impacto permanente ou praticamente irreversível

A avaliação de impacto de privacidade busca estimar o grau de risco aos direitos e às liberdades fundamentais dos titulares de dados pessoais, subsidiando a adoção de medidas de mitigação e tratamento de riscos, em conformidade com a LGPD.

Quando identificado risco elevado aos direitos e liberdades dos titulares, poderá ser necessária a elaboração de Relatório de Impacto à Proteção de Dados Pessoais - RIPD, nos termos da LGPD e das orientações da Autoridade Nacional de Proteção de Dados - ANPD.

Avaliar Probabilidades

Os responsáveis por ativos definem, no Mapa de Riscos, as probabilidades dos riscos, ou seja, a probabilidade de que as ameaças se concretizem e provoquem danos os ativos ou incidentes relacionados ao tratamento de dados pessoais.

Esta avaliação pode ser baseada nos seguintes elementos:

- informações estatísticas gerais sobre a probabilidade de incidentes de segurança da informação ou incidentes envolvendo dados pessoais;
- informações da organização sobre histórico de ocorrência de incidentes de segurança (frequência, ou periodicidade de ocorrência);
- informações da organização sobre a frequência ou a periodicidade de ocorrência de uma ameaça específica e da exploração das vulnerabilidades associadas;
- para ações causadas propositalmente:
    - as fontes de ameaça;
    - características de capacidade da fonte em causar danos;
    - características de intenção e motivação de fonte em causar danos;
    - percepção exterior da atratividade e vulnerabilidade do ativo;
    - facilidade para converter a exploração da vulnerabilidade do ativo em uma recompensa;
- para ações causadas acidentalmente:
    - fatores geográficos propensos a gerar problemas;
    - fatores que podem favorecer erros humanos ou falhas de equipamentos;
- controles existentes: Importante notar que o nível de probabilidade de um risco se concretizar também é afetado pelo estado atual dos controles implementados na organização. Isto é, o responsável pela estimativa de probabilidades deve levar em conta os controles já estabelecidos para refletir o fato de que as probabilidades são menores se controles eficazes existem, e maiores caso contrário.

Para cada risco deve ser identificada a classe de probabilidade:

Descrição	**Frequência Estimada de Ocorrência**
Muito baixa	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.

Descrição	Frequência Estimada de Ocorrência
Baixa	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.
Média	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.
Alta	Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.
Muito Alta	Praticamente certa. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.

Deve-se também fornecer justificativas de classificação.

Estimar Nível de Risco

Os Responsáveis por Ativos, com o acompanhamento e apoio dos Responsáveis pelas Unidades, incluindo riscos relacionados à segurança da informação e ao tratamento de dados pessoais.

Esta atividade consolida as estimativas de impacto e as estimativas de probabilidade, em que, para uma dada ameaça a um ativo ou evento que possa afetar o tratamento de dados pessoais o nível de risco e a classe são calculados pela relação impacto x probabilidade:

A Figura a seguir apresenta a matriz de apetite ao risco, a mesma utilizada para os processos organizacionais da Agência, em termos de impacto e probabilidade.

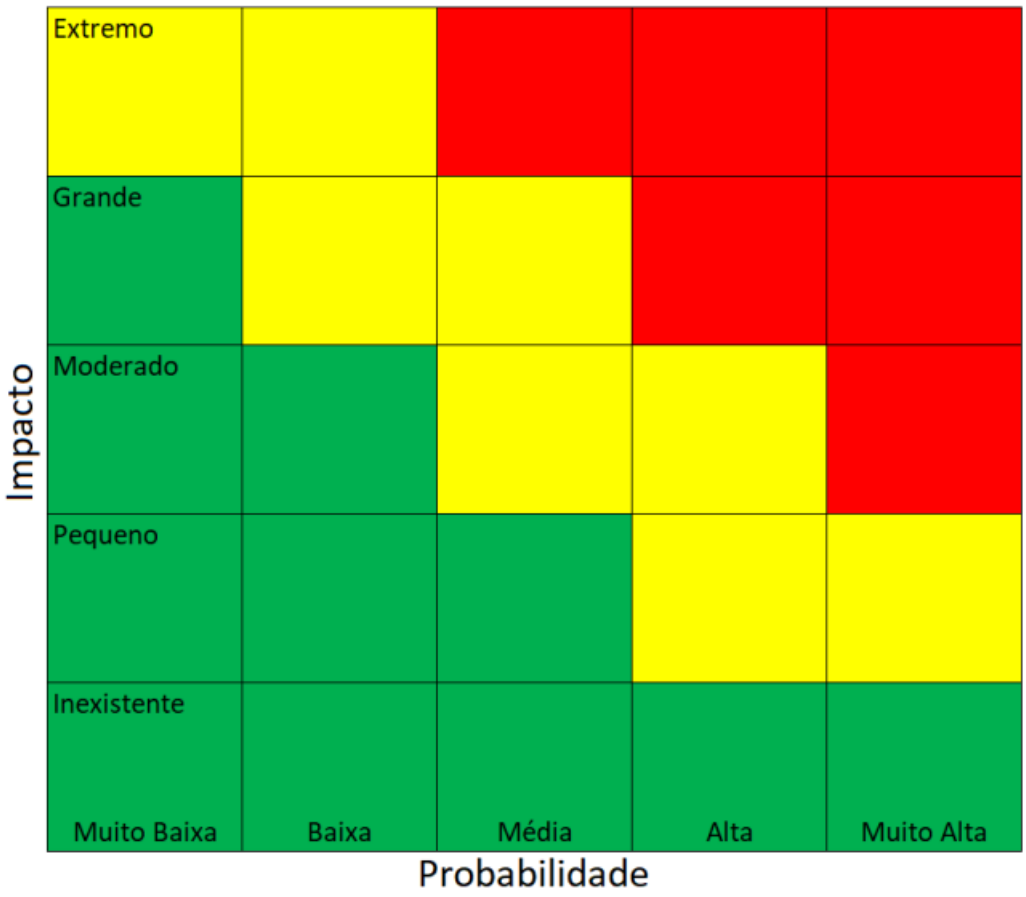


Figura 1-Relação impacto x probabilidade

A Tabela a seguir, apresenta as diretrizes de tratamento para cada evento de risco em razão da estimativa do nível de risco:

Nível de Risco	Ações de tratamento, comunicação e monitoramento
Alto	- Indica um risco além do apetite a risco da instituição. - Qualquer risco encontrado nessa área deve ter uma resposta, seja para eliminar o risco, ou diminuir seu impacto ou probabilidade. - O CSIP deverá ter conhecimento de todos os riscos enquadrados nesse nível. - Admite-se postergar o tratamento somente com autorização do Comitê.
Médio	- Indica um risco além do apetite a risco da instituição. - Qualquer risco encontrado nessa área deve ter uma resposta, seja para eliminar o risco, ou diminuir seu impacto ou probabilidade. - O CSIP deverá ter conhecimento de todos os riscos enquadrados nesse nível - Admite-se postergar o tratamento somente com autorização do titular máximo.
Baixo	- Indica um nível de risco aceitável para a instituição. - Não se faz necessário adotar medidas especiais para tratamento do risco.

Tabela 1: níveis de risco

O resultado desta atividade é um Mapa de Riscos, com cada risco identificando: ativo, ameaça ao ativo, estimativa de impacto, justificativa para a estimativa de impacto, estimativa de probabilidade e o nível de risco (alto, médio ou baixo).

CAPÍTULO IX

DA AVALIAÇÃO DE RISCOS

Neste ponto do processo de GRPSI, há uma visão mais clara de quais ameaças existem para os ativos e para o tratamento de dados pessoais, bem como do nível de proteção desses ativos por meio de controles.

Além disso, neste ponto já foi estimado o nível dos riscos resultantes de impactos e probabilidades apuradas.

O objetivo é identificar os riscos mais expressivos e estabelecer estratégias de resposta a esses riscos.

A etapa é definida pela seguinte atividade:

Classificar os Riscos

Nesta atividade, o gestor de riscos deve classificar os riscos de segurança da informação e de privacidade no Mapa de Riscos, criando uma lista ordenada dos riscos. Isso permite distinguir os riscos mais relevantes do processo como um todo, além de ser uma base para as decisões sobre quais riscos devem ser tratados prioritariamente.

Posteriormente, o gestor de riscos deve notificar os Responsáveis Pelas Unidades da Organização para que registre ciência da classificação de riscos e informe o prazo para realização da tarefa.

CAPÍTULO X

DO TRATAMENTO DE RISCOS

Nesta etapa do processo todas as análises realizadas e informações obtidas são utilizadas na tomada de decisão sobre como a organização agirá em relação aos riscos, incluindo riscos relacionados à segurança da informação e ao tratamento de dados pessoais.

O tratamento de riscos envolve a tomada de decisão sobre uma ou mais opções de tratamento. Estas opções são descritas a seguir.

- Mitigar os riscos. O nível de risco deve ser reduzido pela seleção e implementação de controles de modo que o risco residual possa ser reavaliado como sendo aceitável. Em geral, controles devem fornecer pelo menos um dos seguintes tipos de proteção:
    - Correção;
    - Eliminação;
    - Prevenção;
    - Minimização de impacto;
    - Dissuasão;
    - Detecção;
    - Recuperação;
    - Monitoramento; ou
    - Conscientização.

- Aceitar os riscos. Trata-se da decisão de reter o risco sem maiores ações. Se o nível dos riscos satisfaz o critério de aceitação, não existe necessidade de implementar controles adicionais e o risco pode ser retido, A decisão deve ser registrada formalmente no Mapa de Riscos e justificada.

- Transferir os riscos. Trata-se de transferir o risco para outra parte externa, que pode ser feita pela contratação de um seguro, que irá apoiar em relação às consequências do risco, ou por subcontratação de serviços.

- Evitar riscos. Quando riscos identificados são considerados muito altos, ou se os custos de implementação de outro tratamento de risco excedem os benefícios, a decisão deve ser feita para evitar o risco por completo, pela retirada de forma planejada de atividades existentes.

O tratamento de riscos segue algumas diretrizes:

1. Quando uma mitigação significativa de riscos pode ser obtida com custos relativamente baixos, esta opção deve ser implementada;
2. As consequências e a probabilidade dos riscos devem ser minimizadas tanto quanto possível, considerando níveis tratáveis de custo;
3. Deve-se considerar de forma especial eventos raros, cujas consequências tenham impacto muito grave;
4. As quatro opções para o tratamento de risco não são mutuamente exclusivas. Em alguns casos, a organização pode combinar mais de uma opção;
5. Alguns tratamentos de riscos podem atingir mais que um risco;
6. A escolha do tratamento de riscos deve levar em conta os resultados da estimativa de impacto, analisando de forma separada cada atributo de segurança (confidencialidade, integridade, disponibilidade) e, quando aplicável, os impactos relacionados à proteção de dados pessoais e aos direitos dos titulares. Deve ser priorizada a implantação de controles que tratam o atributo definido como mais crítico.

A etapa é dividida em três atividades:

I. Estimar Recursos Para o Tratamento dos Riscos
II. Definir Resposta aos Riscos
III. Implementar Resposta aos Riscos

Estimar Recursos Para o Tratamento dos Riscos

Deve ser feita uma estimativa do custo, esforço e de prazo para implementar os controles identificado nas situações “Não implementado”.

O responsável pela unidade da organização deve, com apoio dos responsáveis por ativos e do próprio gestor de riscos, estimar, no Mapa de Riscos, os custos de implementação dos controles para tratar cada risco, o quanto de esforço é necessário para implementar cada controle definido anteriormente, bem como identificar se existe alguma restrição que impacte na escolha do tratamento do risco.

Em especial, deve ser avaliada a disponibilidade de recursos humanos para realizar os tratamentos de riscos analisados.

Definir Resposta aos Riscos

O gestor de riscos deve analisar cada risco no Mapa de Riscos e identificar o nível do risco e o tratamento recomendado para este nível. Uma opção de tratamento (reduzir os riscos; reter os riscos; transferir os riscos; ou evitar os riscos) deve ser selecionada e uma justificativa deve ser fornecida. A opção por reduzir os riscos é vista como a solução mais comum a ser adotada na maior parte das situações.

O gestor de riscos deve analisar o estado de implementação dos controles (não implementado; implementado; não se aplica), bem como as estimativas para a implementação dos controles (custo, esforço, tempo e restrições). Ele também deve definir, para cada risco, um ou mais controles a serem implementados no Mapa de Riscos, bem como sua respectiva periodicidade de monitoramento.

Implementar Resposta aos Riscos

O gestor de riscos deve, para cada risco a ser tratado, associar um Plano de Tratamento de Riscos - PTR que aborde o risco. Um PTR tipicamente aborda mais de um risco. Deve ser definido e

comunicado um responsável pela elaboração de cada PTR. Tipicamente, o responsável pelo PTR deve ser um Responsável Pela Unidade da Organização.

O Responsável Pela Unidade da Organização deve levantar informações sobre o risco a ser tratado, incluindo, quando aplicável, aspectos relacionados ao tratamento de dados pessoais e às medidas de proteção da privacidade, tais como ativos envolvidos, ameaças identificadas, opções de tratamento, controles a serem implementados, estimativas e restrições, e detalhar as ações a serem tomadas, com suas respectivas estimativas no Plano de Tratamento de Riscos.

O Responsável Pela Unidade da Organização deve também, no PTR, alocar e comunicar os responsáveis por executar cada tratamento, nesse caso os Responsáveis por Ativos.

Após a avaliação e validação pelo gestor de riscos e pela autoridade competente, os responsáveis por ativos designados devem executar as ações previstas no PTR.

CAPÍTULO XI

DA COMUNICAÇÃO DOS RISCOS

A etapa de Comunicação consiste em um processo contínuo e iterativo para fornecer, compartilhar ou obter informações e promover o diálogo com as partes interessadas no processo de GRPSI.

Tem por objetivo comunicar o desenvolvimento das atividades e os resultados alcançados em todas as fases da gestão de riscos.

Este processo deve ser iniciado em paralelo com o Processo – Estabelecer Contexto, desenvolvendo-se simultaneamente com os demais processos durante todo o processo de gestão de riscos.

O CSIP deverá ser informado dos riscos classificados como de nível alto e poderá deliberar sobre medidas estratégicas relacionadas à segurança da informação e à proteção de dados pessoais.

O gestor de segurança da informação e o encarregado pelo tratamento de dados pessoais, após a aprovação dos relatórios de identificação, análise e avaliação dos riscos de segurança da informação e de privacidade, no âmbito de suas respectivas competências, deverão encaminhá-los conjuntamente à alta administração.

CAPÍTULO XII

DO MONITORAMENTO DOS RISCOS

Essa etapa tem por objetivo monitorar os resultados do Processo de GRPSI. Novas ameaças, novas vulnerabilidades e novos ativos podem alterar ou ampliar os riscos anteriormente avaliados, tornando necessário o monitoramento.

Também faz parte desse processo o acompanhamento do tratamento dos riscos, para assegurar que as medidas de resposta aos riscos planejadas sejam adequadamente implementadas.

Este processo desenvolve-se simultaneamente com os demais processos e as atividades são executadas durante todo o processo de gestão de riscos.

Compõem este processo as seguintes atividades:

I. Monitorar a Gestão de Riscos de Privacidade e Segurança da Informação
Monitorar o Tratamento de Riscos

Monitorar a Gestão de Riscos de Privacidade e Segurança da Informação

Os responsáveis por ativos, os responsáveis pelas unidades da organização, o gestor de riscos e a autoridade competente devem verificar, a qualquer momento do processo de GRPSI, se existem procedimentos ou novas informações que possam impactar ou alterar os resultados da Análise de Riscos de modo geral, tais como:

- novos ativos, substituídos ou descartados;
- restrições ou escopo que foram modificados;
- alterações na valoração dos ativos;
- novas ameaças e vulnerabilidades
- incidentes de segurança ou incidentes envolvendo dados pessoais que possam ocorrer após a análise de riscos; e
- alterações relevantes nas atividades de tratamento de dados pessoais, tais como novas finalidades, novos compartilhamentos ou mudanças no volume de dados tratados.

O gestor de riscos deve notificar os responsáveis pela realização de processos, atividades ou tarefas, fornecendo o prazo e as informações necessárias para que se procedam as atualizações

Monitorar o Tratamento de Riscos

Cada responsável pela unidade da organização responsável por um plano de tratamento de riscos deve avaliar periodicamente a execução do tratamento e registrar o progresso da implementação (em percentual realizado).

Ao final da implementação do PTR, o responsável deve avaliar a correção dos controles estabelecidos por meio de verificações e testes e deve fornecer uma descrição sobre as ações realizadas. Além disso, o responsável deve anexar uma evidência da correta implementação dos controles previstos no PTR e comunicar ao gestor de riscos o final da implementação do PTR.

O gestor de riscos deve obter as informações constantes de cada PTR, para verificar o status de cada atividade, do ponto de vista do cumprimento dos prazos, dos testes e da efetividade dos controles implementados.

Ao ser comunicado do final da implementação de um PTR, o gestor de riscos deve avaliar as evidências fornecidas e atualizar o estado de implementação dos controles tratados nos Planos de Tratamento de Riscos.

Aprovado o tratamento, gestor de riscos deve comunicar o gestor de segurança da informação e o encarregado pelo tratamento de dados pessoais dos resultados do tratamento de riscos, para decidir se o tratamento de riscos realizado é suficiente ou se outras ações são necessárias.

Neste ponto de decisão, atividades de processos anteriores podem ser reexecutadas se o julgamento indicar a necessidade de realizar outras ações para tratar os riscos.

Nesses casos, o gestor de riscos deve ser informado da necessidade de revisar decisões e devem ser fornecidas descrições das questões identificadas pela organização.

O gestor de riscos deve obter as informações sobre os riscos de modo geral, ou seja, todos os riscos que compõem o Mapa de Riscos precisam ser monitorados. Isso inclui, no caso de riscos aceitos (retidos), avaliar periodicamente se há alterações relevantes que justifiquem a definição de outro tratamento.

CAPÍTULO XIII

DAS DISPOSIÇÕES FINAIS

Este processo deverá ser revisado e atualizado a cada 4 (quatro) anos ou sempre que ocorrerem eventos ou fatos relevantes que exijam sua imediata alteração.

O relatório de identificação, análise e avaliação dos riscos de privacidade e 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 e ao encarregado pelo tratamento de dados pessoais, no âmbito de suas respectivas competências, para aprovação.

Os casos omissos serão resolvidos pelo gestor de segurança da informação e pelo encarregado pelo tratamento de dados pessoais, no âmbito de suas competências, podendo o tema ser submetido ao CSIP quando necessário.

ANEXO I – LISTA DE AMEAÇAS

- Abuso de autorização
- Acesso não autorizado a instalações físicas
- Acesso não autorizado a sistemas de TI
- Ataques de negação de serviço (DoS/DDoS)
- Ataques com mensagens especialmente preparadas
- Catástrofes naturais (incêndio, inundação, etc.)
- Engenharia social
- Erros humanos
- Espionagem
- Espionagem industrial
- Falhas de comunicação
- Falhas de dispositivos ou sistemas
- Falta de pessoal qualificado
- Falta de recursos
- Fraude e roubo
- Furto de identidade
- Interceptação de comunicações
- Interrupção de processos de negócio
- Mau funcionamento de dispositivos ou sistemas
- Malware e código malicioso
- Manipulação de hardware e software
- Manipulação de informações
- Perda de dados
- Perda de integridade de informações sensíveis
- Planejamento deficiente ou falta de ajuste
- Ransomware
- Repúdio de ações
- Sabotagem
- Uso indevido de informações pessoais
- Coleta excessiva ou desnecessária de dados pessoais
- Compartilhamento indevido ou não autorizado de dados pessoais
- Tratamento de dados pessoais em desacordo com a finalidade informada
- Retenção de dados pessoais por período superior ao necessário
- Reidentificação de dados pseudonimizados ou anonimizados
- Uso incorreto ou administração inadequada de dispositivos e sistemas
- Vazamento ou divulgação de informações confidenciais
- Vulnerabilidades ou erros de software

ANEXO II – LISTA DE CONTROLES

Para auxiliar na identificação de possíveis controles, devem ser utilizados catálogos de controles existentes associados às ameaças, como os fornecidos em IT-Grundschutz-Compendium (https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html) ou ISO/IEC 27002, bem como referenciais de proteção de dados pessoais e privacidade, como a ISO/IEC 27701 e as boas práticas previstas na LGPD.

ANEXO III – LISTA DE VULNERABILIDADES

Vulnerabilidade	Descrição
Falta de políticas de segurança documentadas	Ausência de diretrizes formais para gestão de acessos, classificação de dados ou resposta a incidentes ou tratamento e proteção de dados pessoais.
Governança inadequada	Falta de definição clara de papéis e responsabilidades na gestão de segurança da informação e proteção de dados pessoais.
Não conformidade com regulamentações	Descumprimento de leis setoriais (ex: LGPD) ou normas técnicas.
Procedimentos não padronizados	Rotinas inconsistentes para backup, atualizações ou controle de mudanças.
Falhas na continuidade de negócios	Ausência de planos de recuperação de desastres ou testes de contingência.
Gestão deficiente de fornecedores	Falta de cláusulas contratuais de segurança com terceiros.
Falta de treinamento em segurança e privacidade	Colaboradores desconhecem políticas de senhas ou identificação de phishing.
Privilégios excessivos	Acessos não alinhados ao princípio do menor privilégio (ex: administradores desnecessários).
Falhas no ciclo de vida de colaboradores	Ausência de processos de offboarding para revogação de acessos.
Configurações inseguras	Serviços desnecessários ativos, senhas padrão ou criptografia não habilitada.
Falhas de software	Bugs críticos em sistemas operacionais ou aplicações não corrigidas por updates.

Vulnerabilidade	Descrição
Proteção de rede insuficiente	Ausência de segmentação de rede, firewall mal configurado ou monitoramento passivo.
Controles de acesso deficientes	Biometria não implementada, registros de acesso não auditados ou áreas críticas desprotegidas.
Ausência de resiliência ambiental	Falta de sistemas anti-incêndio, UPS ou controle de umidade em datacenters.
Classificação inadequada	Dados sensíveis ou dados pessoais sem identificação e proteção diferenciada.
Falhas na criptografia	Chaves de encriptação mal gerenciadas ou algoritmos obsoletos.
Vazamento de informação	Armazenamento de dados confidenciais ou dados pessoais em mídias não criptografadas ou dispositivos móveis não seguros.
Falhas em serviços terceirizados	Interrupção de provedores de cloud, internet ou energia sem planos de contingência.
Riscos na cadeia de suprimentos	Componentes de hardware/software comprometidos antes da aquisição.
Tratamento de dados pessoais sem base legal	Realização de tratamento de dados pessoais sem fundamento jurídico válido previsto na LGPD.
Falha em considerar os direitos do titular dos dados pessoais	Ausência de mecanismos para garantir direitos como acesso, correção, exclusão, portabilidade e oposição ao tratamento, quando aplicável
Compartilhamento de dados pessoais sem base legal ou sem transparência ao titular	Transferência de dados pessoais a terceiros sem respaldo jurídico ou sem informar adequadamente o titular
Retenção prolongada de dados pessoais sem necessidade	Manutenção de dados pessoais por período superior ao necessário para a finalidade declarada

Vulnerabilidade	Descrição
Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular	Possibilidade de identificar ou correlacionar dados ao titular de forma inadequada, gerando exposição ou discriminação
Reidentificação de dados pseudoanonimizados	Capacidade de reconectar dados tratados como pseudoanonimizados à identidade do titular, comprometendo a privacidade

ANEXO IV – RELATÓRIO DE IDENTIFICAÇÃO, ANÁLISE E AVALIAÇÃO DE RISCOS DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Ativos		**Ameaças**		**Riscos Ordenados e Classificados**	**Controles**		**Tratamento de Riscos**	
ID	**Descrição**	**Tipo**	**Descrição**	**Classe Risco (Alto, Médio, Baixo)**	**Descrição**	**Situação/Justificativa**	**Opção de tratamento**	**Plano de Tratamento (PTR)**
A01	Descrição A01	Tipo Ameaça 1	Descrição Ameaça 1	CL Rsc 1	Descrição Controle 1	Situação/Justificativa Controle 1	Op 1	PTR x
					Descrição Controle 2	Situação/Justificativa Controle 2	Op 2	PTR x
					...	...	...	...
		Tipo Ameaça 2	Descrição Ameaça 2	CL Rsc 2	Descrição Controle 1	Situação/Justificativa Controle 1	Op 1	PTR x
					Descrição Controle 2	Situação/Justificativa Controle 2	Op 2	PTR x
					...	...	...	...
		...	...	...	...	...	...	...
...	...	...	...	...	...	...	...	...

ANEXO V – RELATÓRIO DE TRATAMENTO DE RISCOS

PTR – PLANO DE TRATAMENTO DE RISCOS					
Identificador:			**Unidade:**		
RESPONSÁVEIS					
Responsável pela execução do PTR			**Responsável pela definição do PTR**		
Nome:	**Telefone:**	**E-mails:**	**Nome:**	**Telefone:**	**E-mails:**

RESPONSÁVEIS							
Ativo	**Ameaça**	**Controle a ser implantado**	**Estimativa/Restrições**				**Evidência (situação)**
			Cst	**Esf**	**Prz**	**Rst**	
...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...

DATAS		
Data de Início:	**Data Prevista para a Finalização:**	**Data de Finalização:**