APROVA Instrução Normativa CGGDIESP-6/PGDI referente ao Anexo II, 3 – Tabela de Providências Complementares e Responsáveis – Gerenciamento de Risco: **Orientação Técnica - Gestão de Riscos de Segurança da Informação**, da Deliberação Normativa CGGDIESP-1, de 30/12/2021.

ORIENTAÇÃO TÉCNICA

Gestão de Riscos de Segurança da Informação

1. Objetivos

Esta orientação técnica tem os seguintes objetivos:

- Recomendar procedimento para elaboração de um Plano de Gestão de Riscos de Segurança da Informação, providência requerida pela Política de Governança de Dados e Informações (PGDI), no âmbito da Administração Pública estadual, instituída pela Deliberação Normativa CGGDIESP-1, de 30 de dezembro de 2021.

- Conscientizar sobre a importância da gestão de riscos para a redução de ocorrências de eventos adversos e impactos nos objetivos dos órgãos e entidades.

- Esclarecer definições inerentes à elaboração de um Plano de Gestão de Riscos.

2. Sumário

1. Objetivos
2. Sumário
3. Abrangência
4. Principais documentos relacionados e referenciais bibliográficos
5. Glossário
6. Contexto
7. Descrição das orientações técnicas (diretrizes, regras e/ou procedimentos)
7.1. Definir o objetivo e os benefícios esperados para a análise e a gestão de riscos do órgão ou entidade
7.2. Estabelecer o escopo para a Gestão de Riscos da Segurança da Informação
7.2.1. Documento com a relação dos serviços finalísticos
7.2.2. Inventário de dados
7.2.3. Inventário de sistemas e tecnologias
7.3. Identificar os eventos/ameaças e áreas de exposição
7.3.1. Situação desejada
7.3.2. Vulnerabilidades ou deficiências
7.3.3. Classificação das vulnerabilidades
7.3.4. Ameaças ou eventos
7.3.5. Riscos
7.4. Avaliar as probabilidades de ocorrência

7.5. Avaliar o potencial de impacto
7.6. Gradação do potencial de impacto
7.6.1. Gradação do potencial de impacto em um serviço
7.6.2. Gradação do potencial de impacto em dados e informações
7.6.3. Relatório de Impacto à Proteção de Dados Pessoais (RIPD)
7.7. Determinar o nível de risco (probabilidade x impacto)
7.8. Identificar alternativas para ações de mitigação e/ou contingência
7.8.1. Ações de mitigação
7.8.2. Ações de contingência
7.9. Avaliar e decidir quais ações serão adotadas e implantadas
7.9.1. Aplicabilidade
7.9.2. Aprovação das ações de mitigação e/ou contingência
7.9.3. Plano de implementação
7.9.4. Tolerância e aceitação de risco
7.10. Monitorar os riscos e fazer reavaliações periódicas
7.11. Conclusão

3. Abrangência

Órgãos e entidades da Administração Pública estadual.

4. Principais documentos relacionados e referenciais bibliográficos

- ADVISERA. 27001 Academy. *Step-by-step explanation of ISO 27001/ISO 27005 Risk Management*. Disponível em: https://info.advisera.com/27001academy/free-download/step-by-step-explanation-of-iso-27001-risk-management?_gl=1*5zqmqn*_ga*MTY3MzgyOTk5MS4xNjQ2OTQwMzk2*_ga_4P5GYSBRB2*MTY0Njk0MDM5NS4xLjEuMTY0Njk0MDQyNi4yOQ. Acesso em: 13 mar. 2022.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 31000:2018: Gestão de Riscos – Princípios e diretrizes. Rio de Janeiro, 2018.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 31010: Gestão de riscos – Técnicas para o processo de avaliação de riscos. Rio de Janeiro, 2012.
- BRASIL. Tribunal de Contas da União. *10 passos para a boa gestão de riscos*. Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo (Semec), 2018.
- BRASIL. Tribunal de Contas da União. *Manual de gestão de riscos do TCU*. Brasília: Secretaria de Planejamento, Governança e Gestão (Seplan), 2020.
- BRASIL. Tribunal de Contas da União. *Resolução TCU nº 1.148, de 2 de março de 1984*. Dispõe sobre a Política de Gestão de Riscos do Tribunal de Contas da União.
- BRASIL. *Resolução TCU nº 287, de 12 de abril de 2017*. Dispõe sobre a política de gestão de riscos do Tribunal de Contas da União e altera as Resoluções TCU 266, de 30 de dezembro de 2014, que define a estrutura, as competências e a distribuição das funções de confiança das unidades da Secretaria do Tribunal de Contas da União; a 261, de 11 de junho de 2014,

que dispõe sobre a Política de Segurança Institucional (PSI/TCU) e o Sistema de Gestão de Segurança Institucional do Tribunal de Contas da União (SGSIN/TCU) e a 247, de 7 de dezembro de 2011, que dispõe sobre a Política de Governança de Tecnologia da Informação do Tribunal de Contas da União. Disponível em: http://portal.tcu.gov.br/biblioteca-digital/politica-de-gestao-de-riscos-do-tcu.htm. Acesso em: 11 mar. 2022.

- BRASIL. *Guia de Avaliação de Riscos de Segurança e Privacidade* – LGPD. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_avaliacao_riscos.pdf/view. Acesso em: 20 jul. 2022.
- Decreto Estadual nº 64.790, de 13 de fevereiro de 2020, que institui a Central de Dados do Estado de São Paulo – CDESP, a Plataforma Única de Acesso – PUA e o Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo, e dá providências correlatas.
- Decreto Estadual nº 65.347, de 9 de dezembro de 2020, que dispõe sobre a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), no âmbito do Estado de São Paulo.
- Decreto Federal nº 9.203, de 22 de novembro de 2017, que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional.
- Lei Federal nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD).
- Política de Governança de Dados e Informações (PGDI), considerando, em seu Anexo II, a trigésima providência, Gestão de Riscos da Segurança da Informação.
- Orientação Técnica do CGGDIESP que instrui sobre "procedimentos para o uso compartilhado de dados pessoais pela Administração Pública estadual, incluindo compartilhamento internacional", conforme décima terceira providência requerida pela PPDP, em seu Anexo III.
- Guia Orientativo do CGGDIESP que instrui o "preenchimento do documento com a relação dos serviços finalísticos prestados ao cidadão, contendo informações sobre as respectivas finalidades, atribuição das bases legais e quais dados pessoais são tratados", conforme primeira providência requerida pela PPDP, em seu Anexo III.

Guia Orientativo do CGGDIESP que instrui o "preenchimento do modelo padrão do Relatório de Impacto à Proteção de Dados Pessoais (RIPD)" e o "Modelo para Elaboração da Política de Privacidade e Tratamento de Dados Pessoais", conforme sétima providência requerida pela PPDP, em seu Anexo III.

- Fluxo Operacional do CGGDIESP sobre os "Procedimentos para identificação e comunicação de incidentes ao Encarregado de Dados Pessoais", conforme décima nona providência requerida pela PPDP, em seu Anexo III.
- Orientação Técnica do CGGDIESP que instrui sobre como fazer o "inventário de dados objeto de tratamento nos serviços prestados ao cidadão ou serviços finalísticos", conforme quarta providência requerida pela PGDI, em seu Anexo II.
- Orientação Técnica do COETIC que instrui sobre "inventário de *hardware* e de *software*", conforme décima terceira providência requerida pela PGDI, em seu Anexo II.

- Modelo, Orientação Técnica e Fluxo Procedimental do CGGDIESP para o "Plano Geral de Resposta à Incidentes de Segurança da Informação", conforme vigésima nona providência requerida pela PGDI, em seu Anexo II.
- Manual Técnico Procedimental a ser realizado pelos órgãos e entidades para o "Procedimento de identificação e avaliação dos riscos", conforme trigésima primeira providência requerida pela PGDI, em seu Anexo II.

5. Glossário

Termos e siglas	Definição
Ação de contingência	Ação empregada para reduzir ou eliminar o impacto nos negócios que a ocorrência de um evento ou incidente trará à organização e, se possível, determinar o quanto de benefícios ou redução de impactos adversos essa ação preventiva promoverá.
Ação de mitigação	Ação empregada para reduzir ou eliminar a probabilidade de ocorrência de um evento ou incidente e, se possível, determinar o quanto de benefícios ou redução das chances de ocorrência essa ação preventiva promoverá.
Ameaça	Conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.
CGGDIESP	Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo. Órgão colegiado de caráter consultivo, normativo e deliberativo, responsável pela gestão da CDESP e por auxiliar o controlador no desempenho das atividades indicadas no artigo 3º do Decreto Estadual nº 65.347/2020.
***Backup* ou Cópia de Segurança**	Conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo a guarda, proteção, recuperação e fidelidade ao original. Também pode se referir à mídia em que a cópia é armazenada.
Exploração	Evento adverso malicioso e proposital que aproveita (explora) alguma deficiência, exposição ou vulnerabilidade da infraestrutura, do equipamento ou do sistema para a invasão ou perpetração de ação não autorizada (ex.: tentativa de quebra de senha fraca; invasão ao sistema por uma porta de acesso não protegida no código do SW).
Gestão de incidentes	Processo que atua na realização de ações sobre qualquer evento adverso relacionado à segurança cibernética dos sistemas ou da infraestrutura de computação, e cuida do tratamento das ocorrências não autorizadas ou suspeitas que possam trazer dano ou destruição de dados e informações.
Gestão de riscos	Processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.
Impacto	É o efeito (positivo ou negativo) que um evento, ou uma série de eventos, que se manifesta em um ou em vários locais, trará a organização.
Incidente de Segurança da Informação	Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando à perda individual ou conjunta da confidencialidade, integridade e disponibilidade.
LGPD	Lei Geral de Proteção de Dados – Lei nº 13.709/2018. Promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo, essa Lei rege o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, englobando amplo conjunto de operações que podem ocorrer em meios manuais ou digitais.
PGDI	Política de Governança de Dados e Informações. Instituída pela Deliberação Normativa CGGDIESP-1, de 30 de dezembro de 2021, publicada no DOE de 31 de dezembro de 2021, que estabelece parâmetros para as boas práticas em segurança da informação, para a privacidade e proteção de dados pessoais e para a gestão de dados e informações, de observância obrigatória pelos Órgãos e Entidades da Administração Pública estadual.
Política	Documento que estabelece as diretrizes a serem aplicadas em uma organização tendo em vista os objetivos definidos para ela.

Termos e siglas	Definição
PPDP	Política de Proteção de Dados Pessoais. Instituída pela Deliberação Normativa CGGDIESP-2, de 30 de dezembro de 2021, publicada no DOE de 31 de dezembro de 2021, e corresponde à compilação de normas e regras de boas práticas de governança e proteção para tratamento de Dados Pessoais, de observância obrigatória pelos Órgãos e Entidades da Administração Pública estadual.
Probabilidade	Refere-se as chances de um evento ou incidente ocorrer, ou ainda, com que frequência o evento ou incidente poderá acontecer.
Risco	Possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos, sendo mensurado em termos de impacto e de probabilidade.
RoPA	*Record of Processing Activities* (Registro das Atividades de Tratamento de Dados Pessoais).
SSCTI	Subsecretaria de Serviços ao Cidadão, Tecnologia e Inovação da Secretaria de Governo do Estado de São Paulo.
Superfícies de contato	Ponto no sistema ou na infraestrutura que pode ser acessado por um agente externo à estrutura. Na superfície de contato se darão as tentativas de violação de controles e invasão do sistema e, portanto, ela corresponde aos locais onde a investigação por exposições ou vulnerabilidades deve ser prioridade.
***User ID* ou UID**	Identificador único (*unique identifier*) em sistemas de computadores.
Vulnerabilidade	Qualquer limitação técnica ou estrutural na proteção do ambiente produtivo que possa ser explorada ou o conjunto de fatores externos ou internos que possam causar ou potencializar um incidente indesejado capaz de resultar em impactos para uma organização e que devem ser avaliados e mitigados por ações de segurança da informação.

6. Contexto

Segundo o Decreto federal nº 9.203/2017, art. 2º, inciso IV, a gestão de riscos é um processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla atividades como identificar, avaliar e gerenciar potenciais eventos que possam afetar o órgão ou entidade, e é destinado a fornecer segurança razoável quanto à realização de seus objetivos.

O conceito fundamental subjacente à política de governança e à gestão de riscos na Administração Pública é o de valor público: produtos e resultados gerados, preservados ou entregues pelas atividades de um órgão ou entidade que representem respostas efetivas e úteis às necessidades ou às demandas de interesse público e modifiquem aspectos do conjunto da sociedade ou de alguns grupos específicos reconhecidos como destinatários legítimos de bens e serviços públicos, segundo o Decreto federal nº 9.203/2017, art. 2º, inciso II.

Como as atividades de qualquer instituição envolvem riscos que, se não gerenciados adequadamente, poderão se materializar e comprometer sua capacidade de gerar, preservar ou entregar valor, a alta administração das organizações públicas deve estabelecer, manter, monitorar e aprimorar um processo cíclico e intrínseco ao planejamento estratégico, para gestão de riscos e controles internos, composto por atividades contínuas, desenhadas, estruturadas e implementadas para identificar exposições, detectar ameaças, estimar impactos, classificar riscos, avaliar alternativas de mitigação e contingência e promover ações de prevenção ou responder a eventos ou ameaças que possam impactar a implementação da estratégia e a consecução dos objetivos do órgão ou entidade, no cumprimento da sua missão institucional, segundo Decreto federal nº

9.203/2017, art. 17. De maneira similar, a PGDI, em seu artigo 36, determina que os órgãos e entidades devem estabelecer procedimento de identificação e avaliação dos riscos relacionados à segurança da informação e adotar as melhores práticas para o seu gerenciamento, estabelecendo medidas mínimas aptas a mitigar a ocorrência dos riscos identificados.

A gestão de riscos, quando corretamente implementada e aplicada de forma sistemática, estruturada e oportuna, pode tanto reduzir a probabilidade de ocorrência de um evento adverso quanto o seu impacto nos objetivos do órgão e entidade, fornecendo informações preciosas que darão suporte às decisões de alocação e ao uso apropriado dos recursos, tonando-se assim um processo essencial para a boa governança, pois contribui para a otimização do desempenho organizacional e para reduzir as incertezas que envolvem a definição da estratégia e o cumprimento dos objetivos das instituições públicas, aumentando a eficiência e a eficácia na geração, proteção e entrega de valor público e, por conseguinte, o alcance de resultados em benefício da sociedade. Ela exige uma estrutura de governança corporativa responsável por manter esse sistema cíclico vivo e em funcionamento.

Segundo o Instituto Nacional de Padrões e Tecnologia (NIST), órgão do Governo dos Estados Unidos, a primeira etapa da estruturação da capacidade de gerenciamento de risco é categorizar todas as informações de órgãos e entidades do setor público. E isto é elementar, pois sem a consciência da existência e a visibilidade clara da localização de todas as informações críticas e confidenciais que suportam a atividade-fim da instituição, bem como de todos os processos e sistemas que fazem o seu tratamento, é impossível detectar exposições, identificar vulnerabilidades e propor ações de prevenção e mitigação que criem, habilitem e fortaleçam um Programa de Proteção de Dados abrangente e eficaz.

Assim, mapeamento, classificação e categorização devem abranger o levantamento de todos os processos de tratamento de dados, todos os dados tratados por esses processos, todos os sistemas de tecnologia da informação que alojam ou habilitam a execução desses processos e toda a infraestrutura física, de *hardware* e de *software* que suportam os sistemas, com o detalhamento de seus componentes, sua arquitetura de integração e a configuração empregada em cada um desses componentes.

Esta orientação técnica, e a sétima providência da PPDP sobre "preenchimento do Modelo padrão do Relatório de Impacto à Proteção de Dados Pessoais (RIPD)", encontram-se no contexto de melhores práticas para gestão de riscos de segurança da informação e são fundamentais para o processo de adequação de órgãos e entidades à LGPD no que tange análises de riscos técnicos, regulatórios, residuais, riscos aos direitos fundamentais e às liberdades civis dos titulares de dados pessoais, entre outros, a fim de realizar ações para mitigar, eliminar ou aceitar os riscos. Por isso, é importante observar as orientações técnicas que envolvem mapeamentos ou inventários, bem como outros levantamentos realizados pelos órgãos e entidades pois, com base neles, será possível analisar as vulnerabilidades, ameaças e os riscos aos quais se encontram expostos.

Um dos resultados a serem alcançados com a gestão de riscos de segurança da informação é a confecção prévia do Plano Geral de Resposta a Incidentes de Segurança da Informação, conforme previsto na orientação técnica e fluxo que atende a vigésima nona providência da PGDI ("Plano Geral de Resposta à Incidentes de Segurança da Informação"). Caso haja suspeita ou ocorrência de incidente, seguir o fluxo operacional descrito na décima nona providência da PPDP, "Procedimentos para identificação e comunicação de incidentes ao Encarregado de Dados Pessoais".

Relação de temas abordados

- Gestão de riscos.
- Escopo.
- RoPA.
- Inventário de dados.
- Inventários de *hardware* e *software*.
- Análise de riscos.

7. Descrição das orientações técnicas (diretrizes, regras e/ou procedimentos)

Para elaborar um Plano de Gestão de Riscos de Segurança da Informação é necessário:

- definir o objetivo e os benefícios esperados para a análise e a gestão de riscos do órgão ou entidade;
- estabelecer o escopo para a gestão de riscos;
- identificar os eventos/ameaças e áreas de exposição;
- avaliar as probabilidades de ocorrência;
- avaliar o potencial de impacto;
- determinar o nível de risco (probabilidade × impacto);
- identificar alternativas para ações de mitigação e/ou contingência;
- avaliar e decidir quais ações serão adotadas e implantadas;
- monitorar os riscos e fazer reavaliações periódicas.

Com esses passos, demonstra-se uma atitude responsável e proativa para gestão de riscos.

A seguir, estão detalhados os itens para a elaboração de um Plano de Gestão de Riscos.

Nota: é a partir dele que órgãos e entidades poderão elaborar o manual técnico procedimental com a documentação das práticas adotadas para o gerenciamento de riscos, que corresponde à trigésima primeira providência da PGDI ("Procedimento de identificação e avaliação dos riscos").

7.1. Definir o objetivo e os benefícios esperados para a análise e a gestão de riscos do órgão ou entidade

Existem duas maneiras de operar e lidar com riscos: ser surpreendido por eventos que podem impactar adversamente o alcance dos objetivos do órgão ou entidade e somente então reagir a

esses eventos, o que caracteriza a cultura reativa de "apagar incêndios", ou antecipar-se a eles, adotando medidas conscientes que mantenham ou reduzam a probabilidade ou o impacto dos eventos nos serviços prestados. Apenas a segunda maneira pode ser considerada gestão de riscos.

Assim, é preciso tomar uma atitude responsável e proativa para a gestão de riscos e definir o objetivo e os benefícios esperados para a análise e a gestão de riscos do órgão ou entidade, seguindo estas etapas:

- Levar o assunto da implantação da gestão de riscos para a análise da alta administração. Ela e as instâncias de governança têm, coletivamente, a responsabilidade e o dever de prestar contas sobre o estabelecimento dos objetivos do órgão ou entidade, a definição de estratégias para alcançá-los e o estabelecimento de estruturas e processos para melhor gerenciar os riscos durante a realização dos objetivos:
    - Obter a aprovação da alta administração para implantar a gestão de riscos e o seu compromisso de apoio para tornar disponíveis os recursos necessários para que ela se torne de fato um elemento relevante do sistema de gestão do órgão ou entidade.
    - Designar uma equipe de gestão de riscos, com as definições de abrangência de atuação, papéis e responsabilidades dos seus participantes, qual será a frequência dos trabalhos de análise, como serão documentadas as análises e as conclusões, qual será a forma de deliberação das ações necessárias e como será feita a verificação de implementação das ações aprovadas. Se permitido pelos dirigentes, para melhorar o trabalho, formalize a participação da equipe em um Comitê de Gestão de Riscos.
- Estabelecer uma Política de Gestão de Riscos composta por objetivo, princípios e diretrizes que orientem a maneira de lidar com riscos no órgão ou entidade, como monitorá-los e como auditá-los:
    - Declarar o objetivo e os benefícios esperados com a gestão de riscos.
    - Compreender o contexto de risco, o ambiente externo e interno no qual o objeto de gestão de riscos se encontra inserido:
        - Relembrar os eventos significativos ocorridos nos últimos anos e que prejudicaram as atividades, os resultados ou a reputação do órgão ou entidade e as oportunidades valiosas que foram perdidas pelo fato de a instituição não ter se preparado para aproveitá-las.
        - Debater os prós e contras de continuar a deixar o órgão ou entidade exposto a esses e a outros riscos que ainda não se materializaram.
    - Identificar os parâmetros e critérios a serem considerados no Processo de Gestão de Riscos.

- Envolver sempre nas discussões e análises os proprietários dos processos e sistemas, para que estejam conscientes das condições atuais de exposição ou vulnerabilidade e possam participar ativamente na avaliação das alternativas e elaboração dos planos de ação que promoverão melhorias na infraestrutura e proteção de dados e sistemas.
- Avaliar também o envolvimento de outras áreas da organização, no sentido de ampliar a visão sobre os riscos e respectivos impactos no modelo de negócio ou serviço finalístico.
- Considerar que gestores são diretamente responsáveis por apoiar a cultura de gestão de riscos e por gerenciar riscos dentro de suas esferas de responsabilidade, conforme os limites de exposição a risco aceitáveis pelo órgão ou entidade (primeira linha de defesa).
- Considerar também levar para avaliação da alta administração a atribuição de responsabilidades a unidades ou funções para coordenar as atividades de gestão de riscos, fornecer suporte técnico aos gestores e monitorar riscos mais relevantes (segunda linha de defesa).
- Estabelecer a forma como serão tratados conflitos de interesse e como o desempenho da gestão de riscos será medido e reportado, validar com o dirigente e implementar.

- Manter a equipe de gestão sempre treinada e atualizada com relação à gestão de riscos:

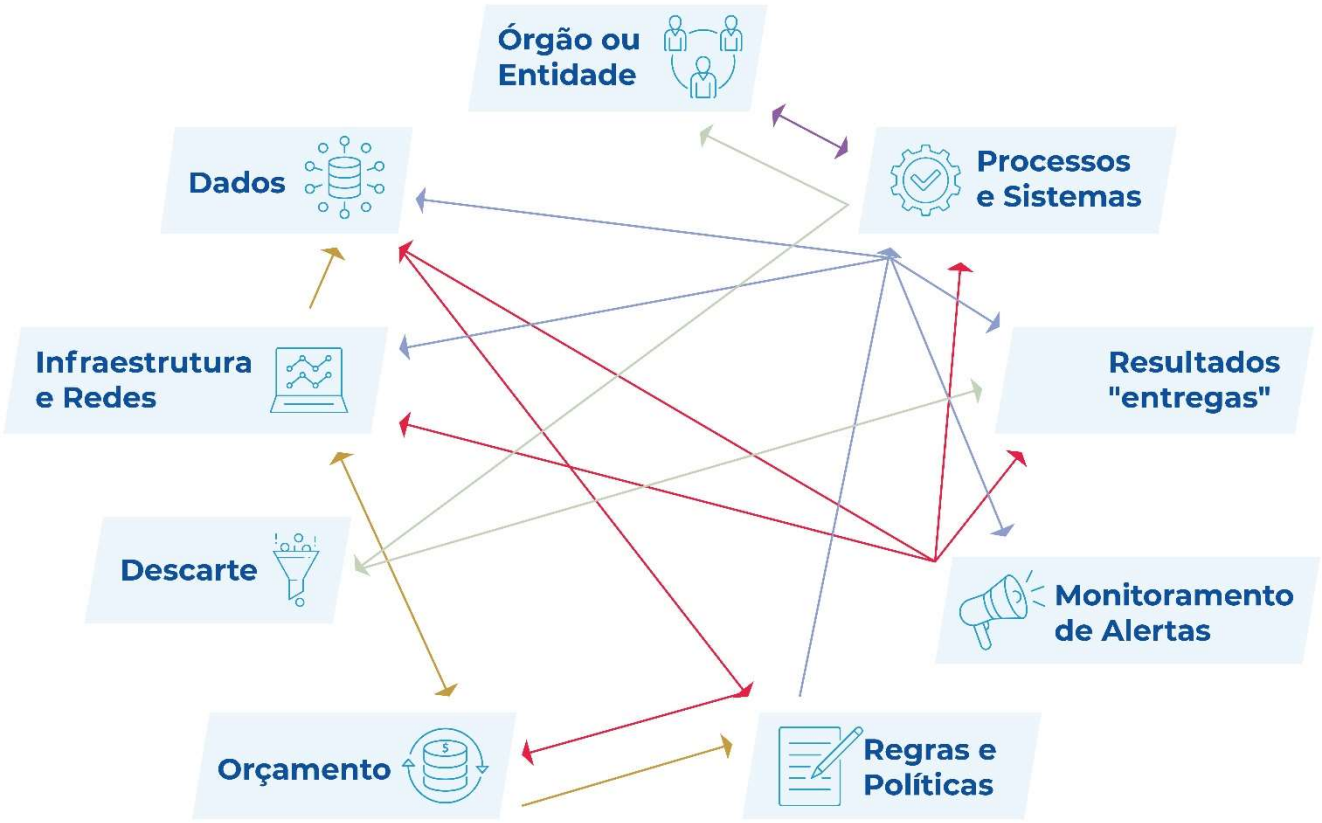
  - Debater sobre as responsabilidades e as expectativas da alta administração quanto a essa missão.
  - Compreender bem os conceitos, os princípios, as boas práticas, as técnicas e os benefícios da gestão de riscos. Com um bom entendimento desses aspectos e alinhadas as expectativas, o órgão ou entidade pode dar passos mais conscientes e seguros na implantação da gestão de riscos.

7.2. Estabelecer o escopo para a Gestão de Riscos da Segurança da Informação

Nesta etapa, é preciso estabelecer o escopo e fazer um levantamento detalhado dos serviços finalísticos do ponto de vista da segurança da informação, dos dados tratados por esses processos e os sistemas (infraestrutura, equipamentos e *software*) que os instrumentalizam:

- um processo;
- uma lista de ativos;
- uma localidade (exemplo: um *data center*);
- um *website*;
- um sistema ou aplicativo etc.

É importantíssimo conhecer, neste momento, as relações e interdependências entre os processos, sistemas, equipamentos e a infraestrutura para que seja possível fazer uma análise conjuntural consistente com a identificação clara de quais são os processos e dados críticos aos serviços finalísticos, quais são as suas vulnerabilidades e as ameaças que podem se materializar e impactar o bom andamento dos processos e objetivos do órgão ou entidade.



Fonte: Elaboração própria.

Para atingir esse levantamento dos processos, dados e sistemas para estabelecimento do escopo, a instituição pode seguir as orientações constantes no guia orientativo "Documento com a relação dos serviços finalísticos prestados ao cidadão, contendo informações sobre as respectivas finalidades, atribuição das bases legais e quais dados pessoais são tratados", conforme primeira providência da PPDP; na orientação técnica "Inventário de dados objeto de tratamento nos serviços prestados ao cidadão ou serviços finalísticos", conforme quarta providência da PGDI, e na orientação técnica "Inventário de *hardware* e de *software*", indicada na décima terceira providência da PGDI, ou usar outros métodos de diagnóstico e descoberta.

7.2.1. Documento com a relação dos serviços finalísticos

Verificar o "Documento com a relação dos serviços finalísticos prestados ao cidadão, contendo informações sobre as respectivas finalidades, atribuição das bases legais e quais dados pessoais são tratados" e o "Modelo Inventário Serviços Finalísticos – RoPA", a ser elaborado a partir do guia orientativo referente à primeira providência da PPDP, onde constam:

- a identificação do processo do serviço público finalístico, incluindo o nome atribuído ao processo, sua base legal (legitimidade) e quem é o responsável (ou dono do processo);
- quais são os dados manipulados pelo processo, incluindo como são capturados e como são armazenados;
- qual é o fluxo do processo, indicando como é feito o tratamento dos dados, os resultados esperados e as relações e interdependências com outros processos;
- a classificação do processo – crítico, dados pessoais ou dados pessoais sensíveis etc.

7.2.2. Inventário de dados

Verificar o "Inventário de dados objeto de tratamento nos serviços prestados ao cidadão ou serviços finalísticos" a ser elaborado a partir da orientação técnica referente à quarta providência da PGDI, onde constam:

- identificação do dado/campo;
- nome do banco de dados;
- local onde o banco de dados está hospedado (endereço do servidor);
- SGBD – Sistema Gerenciador de Banco de Dados;
- regras de validação ou fórmulas;
- sistemas que utilizam o banco de dados;
- ID do RoPA relacionado ao inventário de dados;
- *link* para acesso ao Diagrama de MER (modelo entidade relacionamento);
- *link* para acesso aos *logs*;
- em quais processos o banco de dados é usado.

7.2.3. Inventário de sistemas e tecnologias

Verificar o "Inventário de *hardware* e de *software*", a ser elaborado a partir da orientação técnica referente à décima terceira providência da PGDI, que deve contemplar os seguintes itens:

- Sistema de negócios (que implementa o processo ou serviço finalístico), incluindo o nome do sistema, quem é o responsável ou proprietário (*system owner*), se foi desenvolvido internamente ou se é comercial, qual é a versão atual, quais são as configurações técnicas e de controle e quais são as relações e interdependências com outros sistemas.
- Base de dados, incluindo o nome da base de dados, quem é o responsável ou proprietário (*data base owner*), se foi desenvolvida internamente ou se é comercial, qual é a versão atual, quais são os dados que compõem essa base de dados, a quais sistemas ela atende, qual é a arquitetura e quais são as configurações técnicas e de controle, se a base de dados possui política de *backup* estabelecida etc.
- *Hardware* (HW), elencando quantos e quais são os equipamentos de TIC existentes na área ou que rodam ou armazenam o sistema em análise e detalhando a categoria do HW, o

fabricante, a localização, quem é o responsável ou proprietário, quais são as configurações técnicas e de controle etc.

- *Software* (SW), elencando quantos e quais são os *softwares* que apoiam o sistema em análise e detalhando a categoria do SW, o fabricante, a versão e atualização, quem é o responsável ou proprietário, a quantidade em uso e a forma de licenciamento, quais são as configurações técnicas e de controle etc.

7.3. Identificar os eventos/ameaças e áreas de exposição

Definido o escopo da análise de risco e selecionados os processos, dados e sistemas, é hora de fazer um levantamento detalhado das superfícies de contato deles, áreas de exposição, deficiências ou vulnerabilidades, e identificar os eventos ou as ameaças que podem interromper as condições normais de produção dos processos, a operação dos sistemas ou até afetar as condições de proteção e preservação dos dados envolvidos.

7.3.1. Situação desejada

Observar quais são as condições normais (ou desejadas) de produção ou processamento de cada um dos processos e sistemas.

7.3.2. Vulnerabilidades ou deficiências

Identificar quais são as vulnerabilidades ou deficiências existentes em sua concepção, arquitetura, construção/desenvolvimento, implementação, operação ou proteção que possam ser exploradas impedindo a continuidade da produção, conforme as expectativas da situação desejada descrita no item anterior.

Alguns exemplos de vulnerabilidades ou deficiências:

- inexistência de *backup*;
- ponto único de falha (como único servidor, único disco de armazenamento ou único provedor de rede de telecomunicações);
- falta de controle de acesso para área crítica;
- falta de processo de autenticação individual;
- *firewall* não implementado para algum setor da rede;
- sistema sem antivírus atualizado e/ou sem aplicação das mais recentes correções de código disponibilizadas pelo fabricante/desenvolvedor (*patches* de segurança);
- falta de documentação de procedimentos operacionais;
- prática de gestão de mudança deficiente;
- inexistência de política de testes de vulnerabilidades ou inexistência de um plano para contingência de desastres;
- *data centers* ou locais de trabalho sem contingência ou com único caminho de acesso físico.

7.3.3. Classificação das vulnerabilidades

Fazer a classificação das vulnerabilidades identificadas para auxiliar na determinação da probabilidade de que sejam exploradas.

Exemplo de gradação de vulnerabilidade:

Vulnerabilidade	Descrição dos critérios de Vulnerabilidade ou Categoria de Exploração
Baixa	A vulnerabilidade pode ser explorada por um usuário com nível de conhecimento avançado para contornar os controles de acesso de forma intencional ou não intencional (são necessários níveis de conhecimento de especialista ou desenvolvimento de produtos para utilizar a interface de nível de comando com o sistema operacional ou ambiente) ou; O infrator pode obter o acesso não autorizado à informação utilizando *user id* de usuário geral ou exercer um ataque de negação de serviço (DOS).
Média	A vulnerabilidade pode ser explorada por um usuário com nível de conhecimento intermediário para burlar os controles de acesso (explorar a vulnerabilidade requer o conhecimento da interface de nível de comando com o sistema operacional ou ambiente).
Alta	O infrator pode burlar os controles de acesso do sistema, ou obter acesso a um *user id* que possua autoridade de administração de sistema, ou de segurança, utilizando um *user id* de usuário geral existente (que facilitará a sua identificação ou a de um cúmplice).
Muito alta	A vulnerabilidade pode ser explorada por um usuário com nível de conhecimento básico ou; O infrator pode burlar os controles de acesso do sistema ou obter acesso a um *user id* que possua autoridade de administração de sistema, ou de segurança, sem necessitar de um *user id* de usuário geral (permanecer incógnito).

7.3.4. Ameaças ou eventos

Nesta etapa, identificar o que pode atrapalhar o alcance do objetivo ou os resultados do órgão ou da entidade. Para isso, listar as ameaças ou eventos que possam ocorrer e causar impactos indesejados à condução de seus objetivos. As ameaças incluem alguns eventos que podem ser controlados previamente pelos órgãos e entidades e outros que não estão sob sua gestão. Ameaças sob alçada de órgãos ou entidades devem ser mitigadas, já as que estão além da alçada de órgãos ou entidades devem ser contornadas ou contingenciadas.

Alguns exemplos de ameaças ou eventos:

- furto de equipamentos ou mídias;
- acesso e/ou divulgação não autorizada de dados;
- invasão de sistemas mal desenhados ou pouco seguros;
- espionagem, escuta não autorizada;
- fraude em documentos e aprovações;
- greves de colaboradores;
- paralisação no transporte de carga ou de colaboradores;
- pandemias e outras emergências epidemiológicas;

- incêndios;
- tempestades, furacões, inundações, deslizamentos de terra e outras catástrofes naturais;
- erros operacionais ou infração intencional dos operadores;
- erros advindos da má qualidade do planejamento ou da execução de uma mudança estrutural;
- informação insuficiente sobre a finalidade do tratamento de dados e pagamento de multas por descumprimento legal das obrigações da LGPD.

7.3.5. Riscos

Na gestão de riscos, deve-se considerar as seguintes maneiras práticas de se gerenciar os riscos:

- Eliminar: o objetivo da eliminação é excluir completamente determinada ameaça. Por conta disso, até os objetivos do trabalho podem sofrer alterações drásticas.
- Mitigar: implementação de novos controles ou melhoria dos existentes para trazer o risco a um valor aceitável. Esses controles podem influenciar a probabilidade de ocorrência ou o impacto que o risco tem na atividade.
- Aceitar: o risco está em um nível aceitável ou por razões justificadas escolhe-se assumi-lo.

Definido o escopo (objeto da análise), identificadas as vulnerabilidades, exposições e ameaças, procurar destacar a quais riscos o objeto da análise estará sujeito. Depois, fazer uma lista desses riscos.

Nota: Importante avaliar também os riscos voltados à LGPD identificados no diagnóstico realizado pela Secretaria de Governo por meio da SSCTI, caso o órgão e entidade tenha respondido ao questionário. Isso permitirá verificar se os riscos ainda permanecem ou se já foram aceitos, mitigados ou eliminados por alguma medida técnica ou administrativa. Ressalta-se que podem ocorrer avaliações futuras, nas quais novos riscos poderão ser identificados e classificados.

Alguns exemplos de como riscos podem ser determinados:

Escopo/ Ativo	Ameaça/ Evento	Exposição/ Vulnerabilidade	Risco
Documentos em papel	Incêndio	Documentos não armazenados em ambiente antifogo	Potencial perda de disponibilidade das informações
		Não existem *backups* dos documentos	Potencial perda de disponibilidade das informações
	Acesso não autorizado	Documentos não estão trancados em um compartimento seguro	Potencial perda da confidencialidade das informações
Documentos digitais (ou digitalizados)	Falha no disco de armazenamento	Não existem *backups* dos documentos	Potencial perda de disponibilidade das informações

Escopo/ Ativo	Ameaça/ Evento	Exposição/ Vulnerabilidade	Risco
	Ataque de vírus ou código malicioso	Programa antivírus inexistente ou desatualizado	Potencial perda de disponibilidade (deleção ou criptografia), confidencialidade (vazamento ou publicação indevida) e integridade (adulteração) das informações
	Acesso não autorizado	Controle de acesso mal definido (acessos indiscriminados permitidos)	Potencial perda de disponibilidade (deleção ou criptografia), confidencialidade (vazamento ou publicação indevida) e integridade (adulteração) das informações
		Controle de acesso mal implementado (regras de limitação de acessos não foram seguidas)	Potencial perda de disponibilidade (deleção ou criptografia), confidencialidade (vazamento ou publicação indevida) e integridade (adulteração) das informações
Sistema	Administrador indisponível (em período de férias)	Não há um substituto credenciado e autorizado	Potencial perda de disponibilidade do sistema
	Erros frequentes	Falta de qualificação para exercer as funções de administração e suporte técnico	Potencial perda de disponibilidade do sistema e integridade das informações
	Ataque de vírus ou código malicioso	Programa antivírus inexistente ou desatualizado	Potencial perda de disponibilidade (interrupção do processamento) dos sistemas
	Acesso não autorizado	Controle de acesso mal implementado (regras de limitação de privilégios não foram seguidas)	Potencial perda de disponibilidade (interrupção do processamento e/ou bloqueio de novos acessos) e integridade (adulteração de parâmetros de controle ou outorga de privilégios para outros usuários) nos sistemas

7.4. Avaliar as probabilidades de ocorrência

Atribuir uma probabilidade de manifestação (ocorrência) de um evento ou exploração de uma ameaça conhecida:

Probabilidade de ocorrência		Descrição dos critérios de probabilidade de ocorrência
Numérica	**Descritiva**	
1% a 10%	Raro	Não é provável que aconteça
11% a 30%	Pouco provável	Pouco provável que ocorra ou baixa frequência de ocorrência (uma vez dentro de um ano)
31% a 50%	Provável	Provável que ocorra ou frequência média de ocorrência (talvez mais de uma vez dentro de um ano)
51% a 75%	Muito provável	Muito provável que ocorra ou com alta frequência de ocorrência (mais de uma vez mensalmente)

Probabilidade de ocorrência		Descrição dos critérios de probabilidade de ocorrência
Numérica	**Descritiva**	
76% a 100%	Praticamente certo	Praticamente certo que ocorra ou com altíssima frequência de ocorrência (mais de uma vez semanalmente ou diariamente)

7.5. Avaliar o potencial de impacto

Avaliar o potencial de impacto e as consequências que cada um dos eventos ou ameaças trará aos processos e sistemas em caso de ocorrência.

Exemplos de impactos aos quais os órgãos e entidades estão sujeitos:

- paralisação de serviços essenciais;
- exposição de imagem na imprensa;
- perda de confiança da sociedade e dos cidadãos;
- exposição da privacidade de cidadãos;
- perdas financeiras;
- perda ou roubo de dados corporativos ou pessoais;
- multas e sanções administrativas.

Algumas perguntas que poderão ajudar na determinação do potencial de impacto:

- Quais serviços finalísticos serão interrompidos em caso de falha ou interrupção no processo?
- Quem será impactado em caso de falha ou interrupção no processo?
- Qual será o impacto para o Estado em caso de falha ou interrupção no processo?
- Qual será o impacto para o cidadão em caso de falha ou interrupção no processo?
- Qual será o impacto para o cidadão, titular de dados pessoais afetados, em caso de vazamento de dados pessoais e dados pessoais sensíveis?
- Quais são as medidas e ações de mitigação que foram empregadas preventivamente na tentativa de reduzir ou eliminar a probabilidade de ocorrência das falhas ou interrupção no processo?
- Quais são as medidas e ações de contingência que devem ser empregadas corretivamente na tentativa de reduzir ou eliminar o impacto nos negócios em caso de ocorrência das falhas ou interrupção no processo?
    - As duas últimas perguntas assumem que já houve a avaliação e o tratamento (ou tentativa de tratamento) preventivo do risco em um momento anterior. Essa é uma condição regular já que a gestão de riscos é um processo cíclico e permanente e, mesmo riscos aparentemente já tratados, podem se materializar e apresentar impactos diferentes àqueles originalmente estimados.

7.6. Gradação do potencial de impacto

Os impactos podem variar desde vazamento até destruição de dados e informações, interrupção permanente ou temporária de um serviço finalístico ou ainda perda de ativos (roubo ou destruição). Assim, a escala de gradação dos impactos também varia de acordo com o tipo de ocorrência.

7.6.1. Gradação do potencial de impacto em um serviço

Avaliar os impactos que a ocorrência pode gerar na prestação de serviços pela instituição, como a perda de confiabilidade do cidadão, ações judiciais, danos à imagem da instituição em âmbito nacional e internacional, prejuízo à entidade em contratos com fornecedores e clientes, e paralização total ou parcial nas atividades desenvolvidas pelo órgão e entidade.

Impacto	Exemplos de descrição dos critérios de impacto nos serviços
Muito baixo	Não afeta a capacidade do órgão ou entidade de fornecer todos os serviços a todos os usuários.
	Os impactos possuem consequências pouco significativas.
Baixo	Efeito mínimo; o órgão ou entidade ainda pode fornecer todos os serviços essenciais para todos os usuários, mas perdeu eficiência.
	Os impactos possuem consequências reversíveis em curto e médio prazo e com custos pouco significativos.
Moderado	O órgão ou entidade perdeu a capacidade de fornecer um serviço crítico para um subconjunto de usuários do sistema.
	Os impactos possuem consequências reversíveis em curto e médio prazo e com custos baixos.
Alto	O órgão ou entidade perdeu a capacidade de fornecer um serviço crítico para um conjunto significativo de usuários do sistema.
	Os impactos possuem consequências reversíveis em médio ou longo prazo ou com custos altos.
Muito alto	O órgão ou entidade não é mais capaz de fornecer alguns serviços essenciais para nenhum usuário.
	Os impactos possuem consequências irreversíveis ou com custos inviáveis.

7.6.2. Gradação do potencial de impacto em dados e informações

Ocorrências podem também afetar a confidencialidade, integridade, autenticidade e disponibilidade dos dados e informações de órgãos e entidades, assim é necessário mensurar os impactos que o evento poderá gerar, tanto para a própria instituição como para outros entes parceiros ou mesmo aos titulares dos dados pessoais afetados.

Impacto	Exemplos de descrição dos critérios de impacto nos dados e informações
Baixo	Nenhuma informação relevante foi exposta, alterada, excluída ou de alguma maneira comprometida.
	O tempo de recuperação é previsível com os recursos existentes.
Moderado	Violação proprietária: informações proprietárias não classificadas, como informações de infraestrutura crítica protegida, foram acessadas ou expostas.

Impacto	Exemplos de descrição dos critérios de impacto nos dados e informações
	O tempo de recuperação é previsível com recursos adicionais.
Alto	Perda de integridade: algumas informações confidenciais ou proprietárias foram alteradas ou excluídas.
	O tempo de recuperação é imprevisível; recursos adicionais e ajuda externa são necessários.
Muito alto	Violação de privacidade: informações confidenciais de identificação pessoal (DP) de contribuintes, funcionários, beneficiários, cidadãos etc. foram acessadas ou expostas.
	A recuperação do incidente não é possível (por exemplo, dados confidenciais e/ou pessoais foram expostos e postados publicamente).

7.6.3. Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

Para os casos específicos nos quais há risco de impacto relevante aos titulares dos dados pessoais e dados pessoais sensíveis sob custódia do Estado, é importante que o órgão ou entidade adote ou crie métodos de avaliação de impacto, com base na LGPD, nos normativos e nas orientações do CGGDIESP, do Encarregado de Dados responsável pelo seu órgão ou entidade, e também nos normativos e orientações da Autoridade Nacional de Proteção de Dados (ANPD), para que possam identificar e estimar quais são os impactos esperados, ou já verificados, e quais ações foram tomadas preventivamente na tentativa de reduzir ou eliminar a probabilidade de ocorrência de perda ou vazamento de dados pessoais e dados pessoais sensíveis, bem como qual é a priorização que será dada ao tratamento dessas ocorrências caso sejam constatadas.

Além da análise de riscos nas operações (processos) de tratamento de dados pessoais voltados à segurança da informação, bem como de adequação à LGPD (riscos regulatórios), é fundamental realizar a análise dos altos riscos que podem gerar danos às liberdades civis e aos direitos fundamentais dos seus titulares, parte integrante no Processo de Gestão de Riscos.

Nota: o "Modelo para elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD)", com as devidas orientações de preenchimento no Guia Orientativo "Preenchimento do modelo padrão do Relatório de Impacto à Proteção de Dados Pessoais (RIPD)" está disponível na sétima providência da PPDP, e, como especificado lá, os encarregados de órgãos e entidades, com apoio de outras áreas e equipes técnicas, devem elaborar e publicar os RIPD.

7.7. Determinar o nível de risco (probabilidade x impacto)

A avaliação de riscos norteia a definição das medidas e dos mecanismos de mitigação e de contingência aos riscos. A prioridade de ação correspondente ao seu tratamento deverá ser definida por meio da análise da probabilidade da manifestação, ou ocorrência de uma ameaça ou evento, *versus* o potencial de impacto no caso de sua ocorrência.

A matriz a seguir, obtida a partir do cruzamento da probabilidade de ocorrência de um evento com o potencial impacto que ele trará ao órgão ou entidade, sugerirá quais riscos são mais críticos ou relevantes e devem ter prioridade de tratamento:

Matriz de nível de riscos						
Probabilidade		**Impacto**				
Numérica	Descritiva	Muito baixo	Baixo	Moderado	Alto	Muito alto
1% a 10%	Raro	Muito baixo	Baixo	Baixo	Moderado	Moderado
11% a 30%	Pouco provável	Baixo	Baixo	Moderado	Moderado	Alto
31% a 50%	Provável	Baixo	Moderado	Moderado	Alto	Alto
51% a 75%	Muito provável	Moderado	Moderado	Alto	Muito alto	Crítico
76% a 100%	Praticamente certo	Moderado	Alto	Alto	Crítico	Crítico

Não existe uma escala padrão absoluta para matrizes de avaliação de nível de risco. O gestor deve considerar o nível de análise adequado à sua realidade e que vai agregar valor à sua tomada de decisão.

7.8. Identificar alternativas para ações de mitigação e/ou contingência

Identificar, para cada um dos riscos avaliados, quais são as tecnologias, os procedimentos e os controles (ações ou mecanismos de mitigação e/ou contingência) que poderão ser empregados para seu tratamento.

7.8.1. Ações de mitigação

As ações de mitigação são aquelas empregadas na tentativa de reduzir ou eliminar a probabilidade de ocorrência de um evento adverso ou incidente (prevenção) ou ainda contornar ou eliminar os seus impactos após sua ocorrência (correção), e, se possível, determinando os benefícios ou a redução das chances de ocorrência que essa ação promoverá (ex.: adoção de redundância de servidores ou redes de comunicação; adoção de criptografia na transmissão de dados). Em geral, as ações de mitigação possuem um caráter mais amplo, ou até duradouro, e podem ser replicadas e adotadas em outras áreas do órgão ou entidade para o mesmo tipo de exposição e para tipos similares de objetos.

As ações de mitigação talvez não eliminem a probabilidade de quebra de um sistema único, por exemplo, ou impeçam a interceptação dos dados durante uma transmissão via internet, mas elas contornam de tal maneira a situação, que seus efeitos (impactos) são minimizados ou mesmo eliminados. Por exemplo, um servidor de contingência entra imediatamente em operação mantendo as condições de produção inalteradas ou mínimas e suficientes, por um período, quando o servidor principal sofre interrupção. Outro exemplo ocorre quando os dados interceptados em tráfego de rede encontram-se criptografados e, portanto, não podem ser corretamente acessados pelo interceptador e não trazem impactos aos seus titulares ou ao Estado.

7.8.2. Ações de contingência

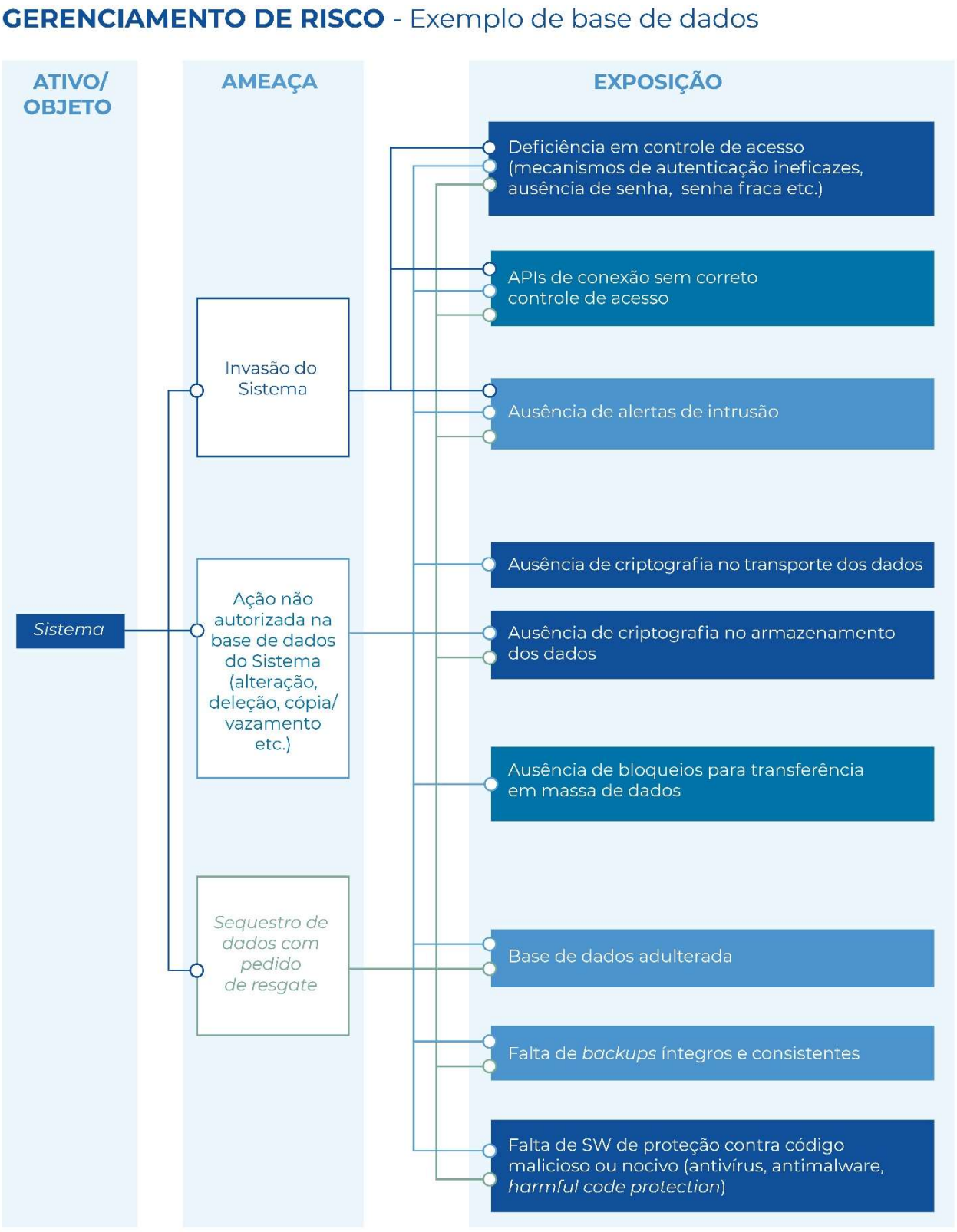
As ações de contingência são aquelas empregadas na tentativa de reduzir ou compensar o impacto nos processos e serviços finalísticos (atividades-fim da Administração Pública estadual) que a ocorrência de um evento adverso ou incidente trará ao órgão e entidade, e, se possível, determinando os benefícios ou a redução de impactos adversos que essa ação preventiva de contingência promoverá. Exemplos clássicos de uma ação de contingência são: a contratação de seguro contra acidentes; a ativação de um ambiente em situação de contingência paliativa, ou, ainda, o restabelecimento do sistema com a restauração dos *backups*, mas já tendo sofrido os impactos da interrupção da produção regular.

Outros exemplos

A figura a seguir está associando algumas das ameaças a que um *laptop* (objeto da análise) está sujeito, quais são as deficiências em procedimentos e/ou controles que podem facilitar que as ameaças se beneficiem dessas exposições e se materializem (ocorram) e quais seriam algumas ações contingenciais e de mitigação preventiva que poderiam ser adotadas para minimizar suas chances (probabilidade) de ocorrência ou redução dos impactos verificados após a ocorrência.

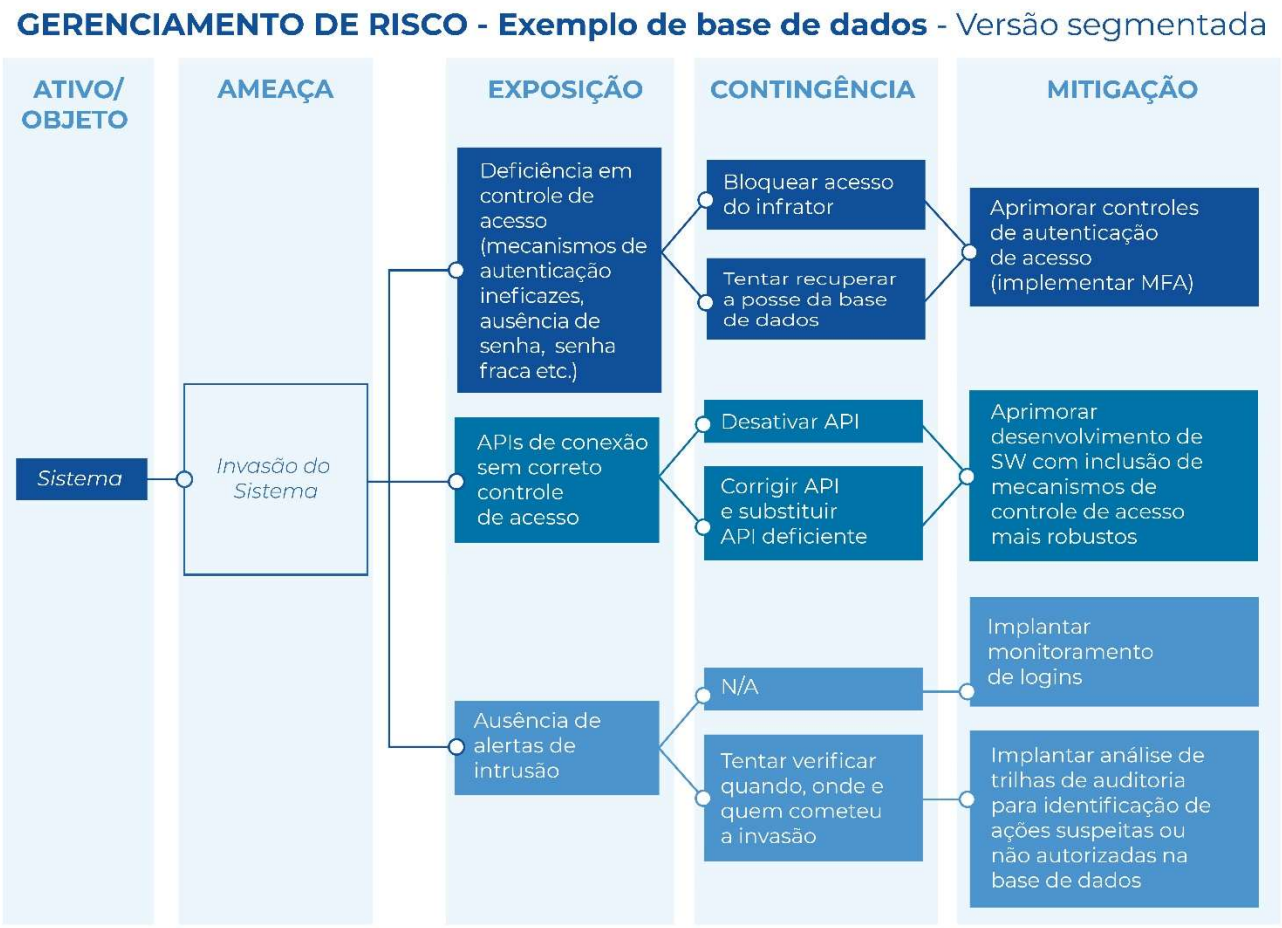
Fonte: Elaboração própria.

Já a figura a seguir mostra as ameaças que um sistema pode sofrer, bem como de que forma elas podem se concretizar:



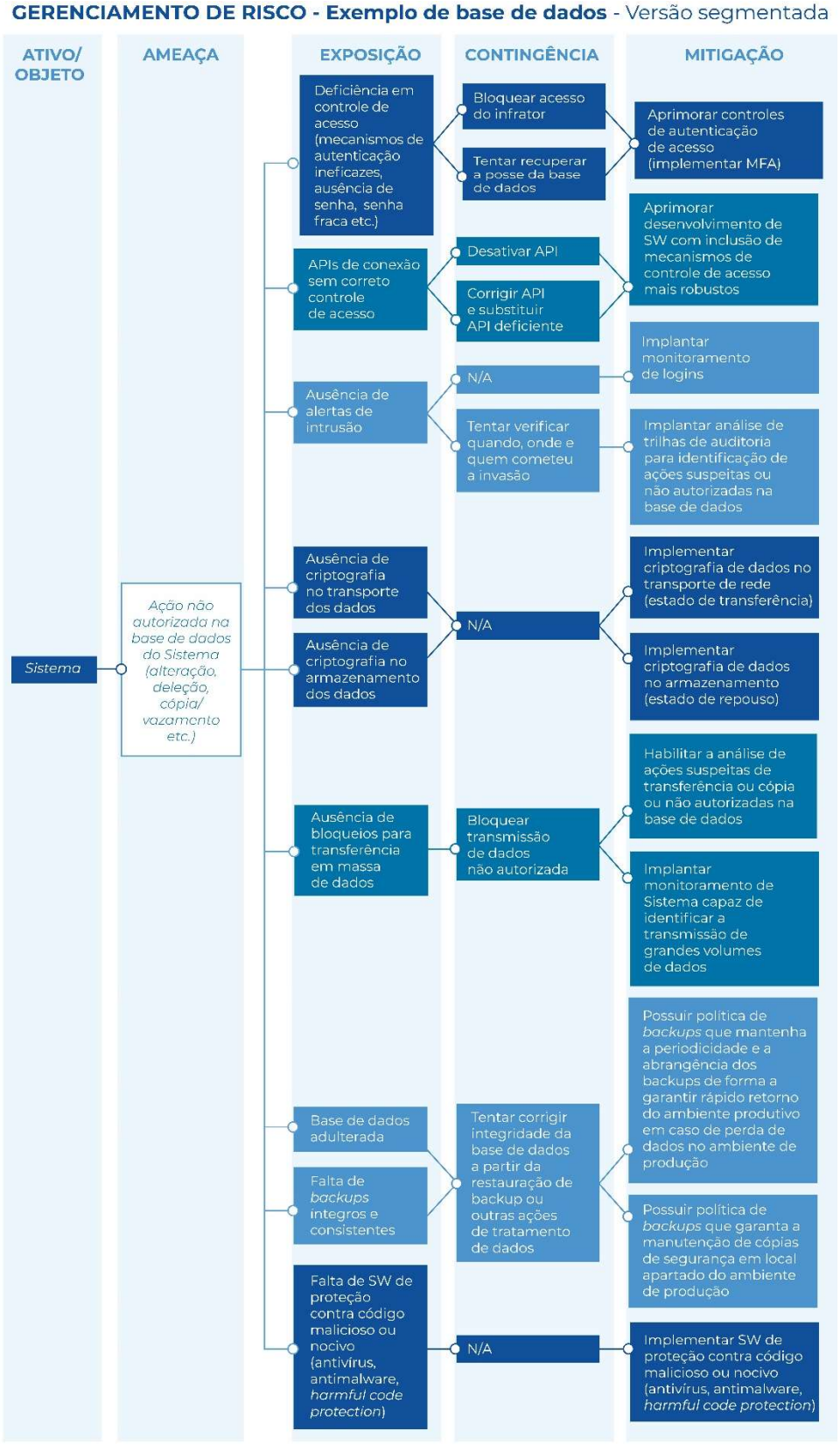
Fonte: Elaboração própria.

A seguir, é possível verificar como mitigar e contingenciar a ameaça "Invasão do Sistema":



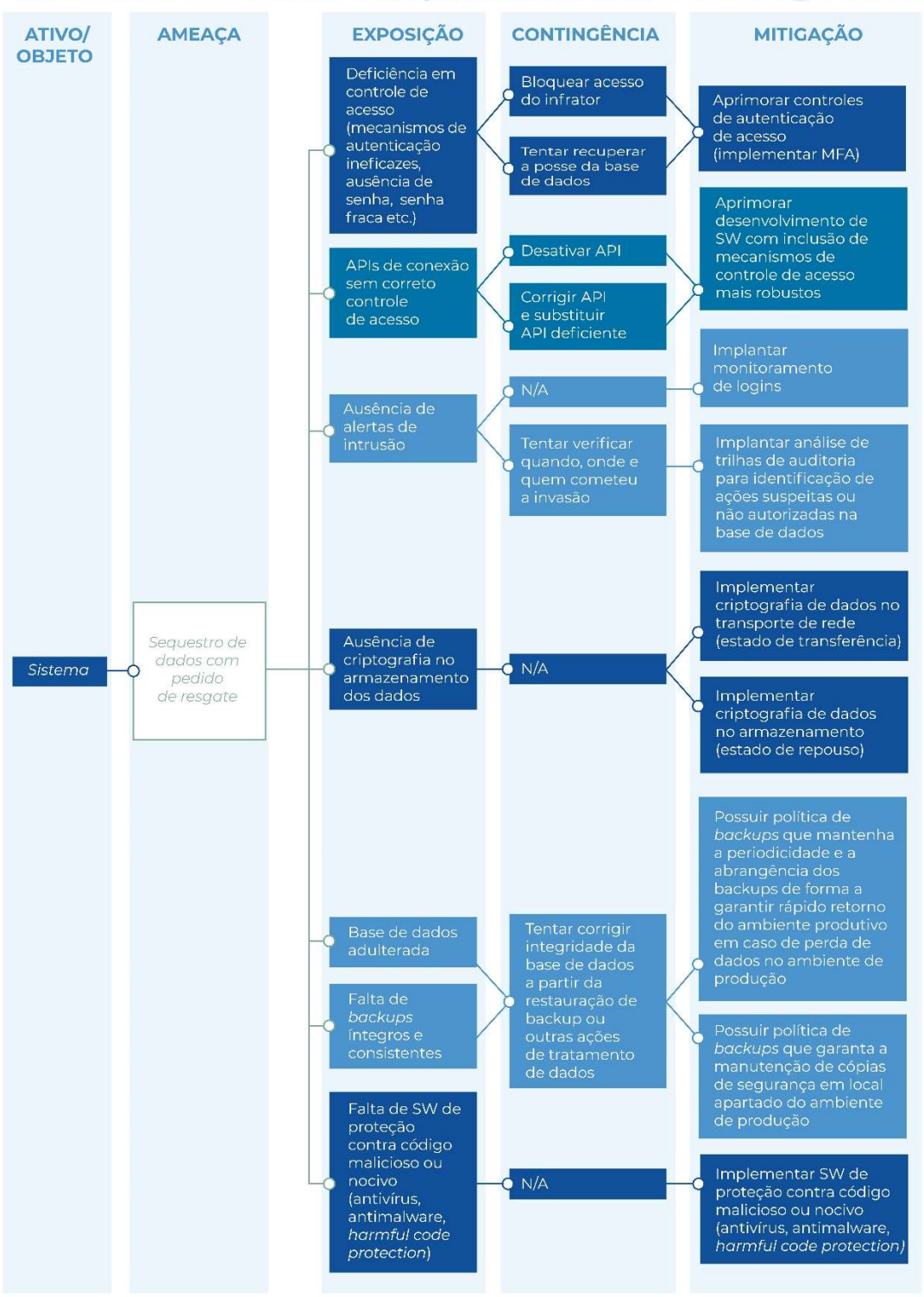
Fonte: Elaboração própria.

A seguir, é possível verificar como mitigar e contingenciar a ameaça "Ação não autorizada na base de dados do Sistema (alteração, deleção, cópia/vazamento etc.)":



Fonte: Elaboração própria.

A seguir é possível verificar como mitigar e contingenciar a ameaça "Sequestro de dados com pedido de resgate":



Fonte: Elaboração própria.

7.9. Avaliar e decidir quais ações serão adotadas e implantadas

O tratamento de riscos envolve a seleção de uma ou mais alternativas para modificar a criticidade dos riscos (probabilidade × impacto) e a elaboração de planos de implementação de ações que implicarão a mitigação e/ou contingência desses riscos. Selecionar a opção mais adequada envolve equilibrar, de um lado, os custos e esforços do tratamento do risco e, de outro, os benefícios decorrentes da ação.

Ações esperadas: avaliar a aplicabilidade para cada uma das medidas ou controles identificados, decidir quais medidas/controles serão adotadas e implantadas, planejar as atividades de aplicação das medidas/controles aprovados e documentar os riscos residuais.

7.9.1. Aplicabilidade

Para as alternativas em análise, pelo menos as que possuem maior relevância ou chance de adoção, descrever:

- qual é o risco que ela mitiga e/ou contingencia;
- quais são a eficácia e a eficiência esperadas;
- como ela poderá ser implementada;
- qual é a viabilidade técnica e financeira;
- qual é a relação de custo-benefício dessa adoção *versus* a opção arriscada de não se tomar ação nenhuma.

A decisão sobre quais das ações possíveis (medidas ou controles) serão de fato implantadas depende dessa avaliação de aplicabilidade e comparação do nível do risco em análise com o limite de exposição a riscos do órgão ou entidade (tolerância a risco), a fim de determinar se o risco é aceitável.

A efetividade da gestão de riscos é consequência direta da capacidade da organização para selecionar e implementar as alternativas adequadas para os riscos considerados mais significativos.

7.9.2. Aprovação das ações de mitigação e/ou contingência

Formalizar a aprovação das ações de mitigação e/ou contingência preventivas, para o fortalecimento da resiliência da infraestrutura e do ambiente produtivo, com os proprietários dos sistemas e da infraestrutura atingida por tais ações e com a alta administração.

- Documentar as orientações que serão encaminhadas para o Processo de Continuidade e Recuperação de Negócio para os casos de recuperação de desastres, incluindo:
    - os componentes da infraestrutura ou sistemas que estão envolvidos, bem como os responsáveis por eles;

- os prazos máximos de tolerância de ambiente improdutivo;
- as expectativas quanto à produtividade mínima desejada para ambientes operando em condição de contingência e os recursos mínimos necessários para essa condição;
- as ações de mitigação e/ou contingência preventivas sugeridas para o fortalecimento da resiliência da infraestrutura e do ambiente produtivo, para que possam ser analisadas quanto a sua correta implementação e/ou eficácia;
- notificações para as pessoas ou os grupos em caso de ocorrência de um desastre;
- como formar e mobilizar equipes de contenção, correção e restauração do ambiente produtivo;
- ações de mitigação e/ou contingência corretivas sugeridas;
- prazos de emissão de relatórios de *status* de tratamento do desastre.

- Documentar as orientações que serão encaminhadas para o Processo de Gestão de Mudanças, incluindo:

  - os componentes da infraestrutura ou os sistemas que serão objeto da mudança, bem como os responsáveis por eles;
  - a justificativa da mudança;
  - as ações de mitigação e/ou contingência preventivas que devem ser aplicadas;
  - o responsável pela realização das ações;
  - o prazo requerido para a realização da mudança.

Documentar também e estabelecer os procedimentos operacionais e/ou técnicos que serão encaminhados para o time de Gestão de Incidentes de Segurança da Informação para aplicação das ações de mitigação e/ou contingência de caráter corretivo nos casos futuros em que for constatada a exploração das vulnerabilidades previamente identificadas nesse Processo de Gestão de Riscos:

- notificações para as pessoas ou os grupos em caso de ocorrência de incidentes de segurança da informação.
- como formar e mobilizar equipes de contenção, correção e restauro.
- as ações de mitigação e/ou contingência corretivas sugeridas para que as equipes de contenção, combate, correção e regularização possam adotá-las de forma ágil quando de suas ocorrências.
- os prazos de emissão de relatórios de *status* de tratamento da ocorrência.
- as orientações para a criação de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) específico ao incidente em trabalho, conforme o modelo padrão do RIPD, e orientações de preenchimento, para os casos confirmados de exposição de dados pessoais e/ou dados pessoais sensíveis, encaminhamento do RIPD ao Encarregado de Dados da organização para revisão e posterior encaminhamento à ANPD (Autoridade Nacional de Proteção de Dados), pelo Encarregado de Dados, com prévia autorização do CGGDIESP.

7.9.3. Plano de implementação

Estabelecer um plano para implementação das ações de mitigação e/ou contingência preventivas:

- Revisar a priorização das ações para o tratamento do risco, orientando-se pela matriz desenvolvida no passo 8.6.
- Encaminhar as ações para as áreas responsáveis para sua respectiva análise e detalhamento técnico.
- Formalizar o plano de implementação dentro do Processo de Gestão de Mudanças.
- Registrar o plano de implementação no sistema de monitoramento, como um plano de ação de adequação à LGPD, para controle e monitoramento da equipe técnica do CGGDIESP.
- Monitorar a implantação das medidas aprovadas.

7.9.4. Tolerância e aceitação de risco

Infelizmente, nem todas as vulnerabilidades e exposições identificadas podem ser mitigadas ou contingenciadas preventivamente, por conta dos seguintes fatores:

- falta de uma ação de mitigação ou contingência conhecida e disponível no momento da análise;
- inviabilidade técnica que impeça a sua adoção naquele momento;
- inviabilidade financeira nos casos em que os custos projetados para a adequação da infraestrutura e/ou dos sistemas é superior aos impactos intangíveis e financeiros estimados.

Esses fatores influenciarão e calibrarão a chamada "**tolerância ao risco**" do órgão e entidade. E quando esses fatores analisados conduzirem a instituição a determinar que não haverá o emprego preventivo de alguma ação de mitigação ou contingência, a boa prática recomenda que seja feita uma documentação formal de "Aceitação de risco de exposição explorável de vulnerabilidade conhecida".

Essa boa prática possibilita que a análise da decisão seja revista e amplamente discutida, pela alta administração, pelos gestores de risco e proprietários dos sistemas envolvidos, e favorece o compartilhamento de responsabilidade pela decisão consciente e institucional de não se tomar ação nenhuma. Popularmente, a opção de se correr um risco calculado.

7.10. Monitorar os riscos e fazer reavaliações periódicas

Monitorar os riscos residuais e refazer as avaliações periodicamente a fim de detectar novas ameaças e exposições para seu tratamento preventivo:

- **Análise da eficácia e eficiência das ações implantadas:** haverá casos em que as ações originalmente avaliadas não atingirão a plenitude dos objetivos de segurança e proteção desejados:

- Assim, é importante que o órgão ou entidade analise a eficácia e eficiência das medidas/controles implantados, por meio de testes ou simulações, calcule o risco residual e, para os casos em que o risco residual for superior ao risco tolerado, refaça as análises em busca de novas medidas/controles de mitigação e/ou contingência para aprimoramento das proteções e redução de riscos.

- **Verificação periódica:** a equipe de gestão de riscos deve enviar ao time de gestão da segurança da informação as orientações quanto aos controles de monitoramento a serem empregados na verificação periódica das vulnerabilidades conhecidas que permanecem não totalmente mitigadas para confirmação de que seu nível de risco não evoluiu e que permanecem não merecedoras de tratamento por parte do gestor.
- **Monitoramento contínuo e reavaliações:** deverá promover um monitoramento contínuo em busca de:
  - novas vulnerabilidades;
  - novas alternativas de mitigação ou contingência, incluindo novas tecnologias para emprego futuro;
  - novos procedimentos operacionais que possam ser adotados;
  - atualizações do plano de ação de adequação à LGPD registrado no sistema de monitoramento para controle da equipe do corpo técnico do CGGDIESP.
- **Melhoria contínua:** buscar fazer revisões periódicas também nos regramentos e na estrutura que regem a Política de Gestão de Riscos do órgão ou entidade para seu contínuo aperfeiçoamento.

7.11. Conclusão

Embora seja impossível identificar todas as vulnerabilidades ou exposições da infraestrutura e dos sistemas que nela operam, e ainda que seja pouco provável que 100% das vulnerabilidades encontradas sejam completamente sanadas, deixar de gerenciar os riscos e ameaças que podem interferir na execução da estratégia e na consecução dos objetivos da instituição no cumprimento da sua missão não é uma opção.

A gestão de riscos deve ser implementada e aplicada de forma abrangente, sistemática, estruturada e cíclica, na busca incessante pela detecção antecipada de exposições inerentes à tecnologia e para a aplicação de ações e mecanismos de proteção e controle para o constante fortalecimento da resiliência da infraestrutura, proteção dos dados e preservação do ambiente produtivo.

Os resultados obtidos no Processo de Gestão de Riscos alimentarão outros processos institucionais, administrativos e operacionais, em especial o Processo de Gestão de Mudanças, o Processo de Continuidade de Negócio e Recuperação de Desastres e o Processo de Gestão de Incidentes de Segurança da Informação, e colaborarão de forma decisiva para a boa governança.

A partir do Plano de Gestão de Riscos estabelecido, o órgão ou entidade deve estruturar um manual técnico procedimental com a documentação das práticas adotadas. O manual deve descrever como o plano da instituição será executado, ou seja, o passo a passo dos procedimentos – assim, atenderá a providência trigésima primeira constante na PGDI ("Procedimento de identificação e avaliação dos riscos").