SÃO PAULO
GOVERNO DO ESTADO

CONTROLADORIA GERAL DO ESTADO

METODOLOGIA DE GESTÃO DE RISCOS

SÃO PAULO • JULHO DE 2023

CONTROLADORIA GERAL DO ESTADO DE SÃO PAULO - CGE

Av. Rangel Pestana, 300 - 18º andar - Sé - CEP: 01017-911
controladoria_geral@sp.gov.br

WAGNER DE CAMPOS ROSÁRIO
Controlador Geral do Estado

ROBERTO CÉSAR DE OLIVEIRA VIEGAS
Controlador Geral do Estado Executivo

DANIEL DA SILVA LIMA
Chefe de Gabinete

FABIANA RIBEIRO NOGUEIRA
Coordenadora de Controle Estratégico e Promoção de Integridade

KARINA KURODA
Diretora do Departamento de Gestão de Riscos e Controle Estratégico

AUTORIA E REVISÃO
Cristina Kuniyoshi
Gustavo Henrique Meireles Urbina
Susana Maria Mazete Gunji

Sumário

METODOLOGIA DE GESTÃO DE RISCOS

1. INTRODUÇÃO

Criada por meio da Lei Complementar nº 1.361/2021 e organizada pelo Decreto nº 66.850/2022, a Controladoria Geral do Estado de São Paulo (CGE-SP) tem por finalidade a adoção de providências necessárias à defesa do patrimônio público, ao controle interno, à auditoria pública, à correição, à prevenção e ao combate à corrupção, às atividades de ouvidoria, à promoção da ética no serviço público e ao incremento da transparência da gestão no âmbito da Administração Pública direta e indireta do Estado, exercendo a função de órgão central do Sistema Estadual de Controle Interno.

Em sua estrutura a CGE conta com a Coordenadoria de Controle Estratégico e Promoção de Integridade que, por meio do Departamento de Gestão de Riscos e Controle Estratégico, é responsável por estabelecer, fomentar, avaliar e aperfeiçoar práticas, políticas e processo de gestão de riscos, bem como propor modelos e ferramentas para a estruturação e implementação de gestão de riscos no âmbito da Controladoria e demais órgãos e entidades da Administração Pública estadual.

Esta metodologia de Gestão de Riscos apresenta os objetivos, princípios, responsabilidades e detalha cada uma das etapas da metodologia desenvolvida pela CGE. O propósito é servir como guia e dar suporte à concepção, implementação, monitoramento e melhoria contínua da gestão de riscos nos órgãos e entidades da Administração Pública direta e indireta do Estado.

Ela foi idealizada de forma a ser aplicável a todos os tipos, contextos e tamanhos de organizações. Incorpora as etapas necessárias para a operacionalização das atividades de gestão de riscos, por meio de uma abordagem sistemática, estruturada e abrangente, que se integra aos demais processos organizacionais.

A base teórico-conceitual desta metodologia foi pautada nos modelos amplamente utilizados internacionalmente e em normativos e referências nacionais de gestão de riscos, como: COSO-ERM (Committee of Sponsoring Organizations - Enterprise Risk Management); ABNT NBR ISO 31.000:2018 Gestão de Riscos - Princípios e Diretrizes; ABNT NBR ISO/IEC 31010:2021 Gestão de Riscos - Técnicas para o processo de avaliação de riscos; o Modelo das Três Linhas do IIA (The Institute of Internal Auditors); Metodologia de Gestão de Riscos da Controladoria Geral da União 2018 e 2020.

A adoção de metodologias diversas é uma opção de cada órgão e entidade, de forma personalizada à sua necessidade e contexto, sem prejuízo das competências da Coordenadoria de Controle Estratégico e Promoção de Integridade, da CGE, definidas no art. 2º, da Resolução CGE 9-2022.

2. CONTEXTUALIZAÇÃO HISTÓRICA

A preocupação com a gestão de riscos no setor público é relativamente recente no Brasil. A Emenda Constitucional nº 19/1998, conhecida como a Reforma Administrativa, introduziu o conceito de eficiência no rol dos princípios da Administração Pública, previstos no art. 37 da Constituição Federal de 1988. A partir desse momento, não se exigia apenas que o Estado atuasse sob o manto da legalidade, mas também com eficiência, a fim de alcançar os melhores resultados na prestação de serviços e atendimento aos interesses públicos.

Atributos como racionalização, produtividade, economicidade e celeridade foram adotados pela Administração Pública na busca pela melhor utilização dos recursos. A qualidade da gestão governamental se tornou fundamental, sobretudo em um ambiente dinâmico, de incertezas e recursos limitados.

Nesse contexto, surge a necessidade de monitoramento dos eventos capazes de interferir no alcance dos objetivos almejados e na entrega máxima de valor público.

3. OBJETIVOS

A Metodologia é uma ferramenta capaz de auxiliar os gestores públicos no processo de tomada de decisão, a fim de assegurar a devida aplicação dos recursos públicos e, consequentemente, a efetividade das políticas públicas.

Seus objetivos são:

I – Aumentar a probabilidade de atingimento dos objetivos organizacionais, por meio da identificação de potenciais eventos que possam afetar sua consecução;

II – Alinhar a atuação gerencial ao apetite a riscos do órgão;

III – Melhorar o controle interno da gestão;

IV – Aperfeiçoar os mecanismos de governança e prestação de contas, contribuindo para o uso eficiente, eficaz e efetivo de recursos;

V – Disseminar a cultura de gestão de riscos e controles internos;

VI – Estabelecer uma base confiável para o planejamento e a tomada de decisão.

4. PRINCÍPIOS

Em conformidade com a Política de Gestão de Riscos da CGE, e de acordo com a norma ABNT NBR ISO 31.000: 2018, constituem princípios da gestão de riscos:

I – Agregar valor e proteger o ambiente interno: o propósito da gestão de riscos é a criação e proteção de valor. Ela aumenta o grau de segurança na consecução dos objetivos, melhorando o desempenho.

II – Ser parte integrante dos processos organizacionais: a gestão de riscos é parte integrante de todas as atividades organizacionais, podendo ser aplicada a toda e qualquer ação que tenha um objetivo, produto ou entrega definidos.

III – Ter uma abordagem sistemática, estruturada e abrangente: processo sistemático, estruturado e abrangente para a gestão de riscos contribui para a eficiência das atividades organizacionais, o alcance de resultados consistentes e comparáveis.

IV – Ser personalizada e proporcional ao contexto externo e interno da organização: a estrutura e o processo de gestão de riscos são flexíveis, consideram a relação custo/benefício dos controles e a realidade operacional das unidades, adaptando-se e atendendo às suas necessidades.

V – Ser inclusiva e transparente, com envolvimento de todas as partes interessadas: o envolvimento apropriado e oportuno das partes interessadas possibilita que seus conhecimentos, pontos de vista e percepções sejam considerados.

VI - Ser dinâmica e capaz de responder a mudanças: riscos podem emergir, mudar ou desaparecer à medida que os contextos externo e interno de uma organização mudam. A gestão de riscos antecipa, detecta, reconhece e responde a essas mudanças e eventos de uma maneira apropriada e oportuna.

VII – Usar a melhor informação disponível: a gestão de riscos se baseia em informações históricas e atuais, expectativas futuras, pareceres de especialistas, entre outros. Explicitamente leva em consideração quaisquer limitações e incertezas associadas a essas informações e expectativas. Convém que a informação seja oportuna, confiável, clara e disponível para as partes interessadas pertinentes.

VIII – Considerar fatores humanos e culturais: o comportamento humano e a cultura influenciam significativamente a gestão de riscos, que deverá reconhecer as capacidades, percepções e intenções de pessoas externas e internas que podem facilitar ou dificultar o alcance dos objetivos.

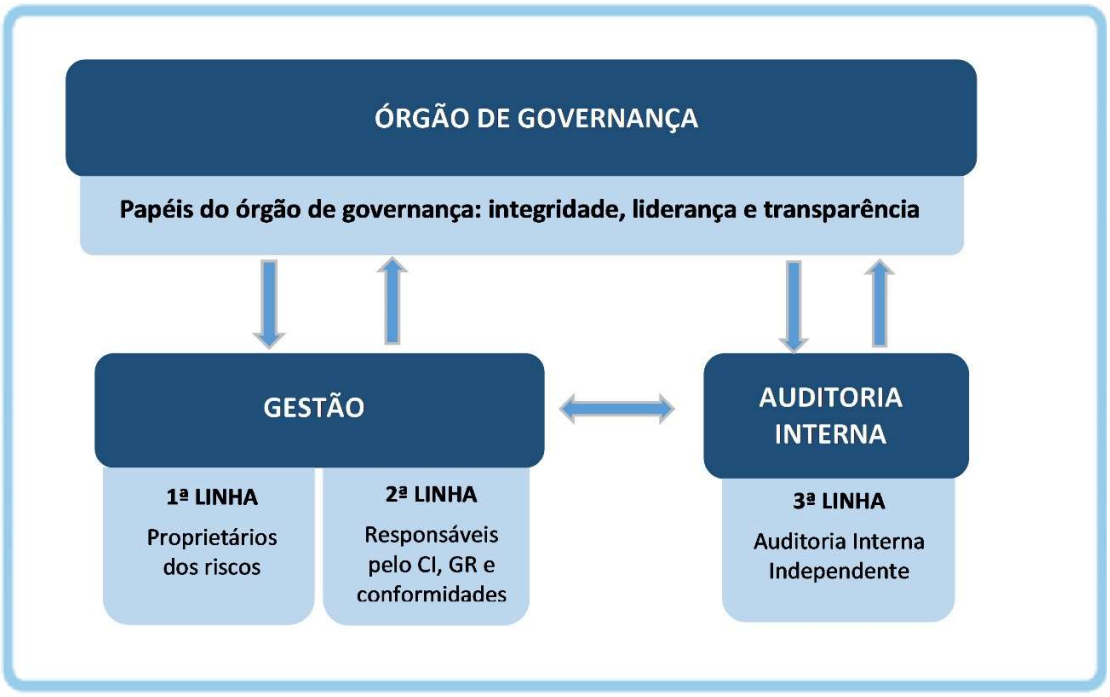
IX – Fomentar a melhoria contínua, por meio do aprendizado e experiências: tornar a gestão de riscos um processo contínuo, aumenta a capacidade da organização em identificar e tratar as incertezas. Assim, a gestão de riscos é melhorada continuamente por meio do aprendizado e experiências.

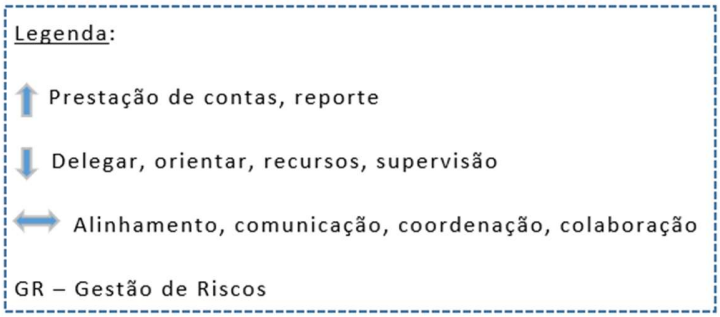
5. RESPONSABILIDADES

Por ser um modelo que pode ser adaptado e aplicado em todas as organizações e contextos, as responsabilidades em gestão de riscos da CGE se organizam consoante o Modelo de Três Linhas, do IIA - *The Institute of Internal Auditors.* É uma forma simples e eficaz de melhorar a comunicação da gestão de riscos e controle, por meio do esclarecimento dos papéis e responsabilidades essenciais.

Nessa estrutura em que todos têm alguma responsabilidade, atuam como elementos centrais: os gestores proprietários dos riscos, os especialistas em controles internos, gestão de riscos e conformidade, os auditores internos e os órgãos de governança. O modelo envolve pessoas e setores diversos, formando uma estrutura clara, com transparência na comunicação e na distribuição de funções.

Figura 1: Modelo de Três Linhas aplicado à Gestão de Riscos na CGE





Fonte: Modelo das três linhas do IIA 2020 (adaptado)

O Modelo adotado pela CGE compreende as seguintes responsabilidades:

I – Primeira Linha: composta pelos proprietários dos riscos, são os gestores em seus respectivos âmbitos e escopos de atuação, os responsáveis pelos processos de trabalho, projetos, atividades e ações desenvolvidos nos níveis estratégicos, táticos ou operacionais;

II – Segunda Linha: composta pelos responsáveis pelo controle interno, gestão de riscos e conformidade da organização, que têm como objetivo apoiar os gestores proprietários dos riscos para que cumpram com suas responsabilidades de Primeira Linha, fornecendo conhecimento e ferramentas adequados;

III – Terceira Linha: composta pela auditoria interna, que tem o papel de fazer uma avaliação objetiva e independente dos controles e da gestão de riscos.

Compete aos gestores proprietários dos riscos, como Primeira Linha:

I – Escolher os processos, projetos, atividades e ações que terão seus riscos gerenciados e tratados, observada a Política de Gestão de Riscos;

II – Definir os níveis de risco aceitáveis e elaborar os planos de ação para o tratamento dos riscos, considerando a declaração de apetite a riscos do órgão;

III – Realizar o acompanhamento da evolução dos níveis de risco e da efetividade dos planos de ação;

Compete aos responsáveis pelo controle interno, gestão de riscos e conformidade da organização, como Segunda Linha:

I – Apoiar a Primeira Linha na implantação, monitoramento e melhoria dos controles internos estabelecidos na gestão de riscos;

II – Monitorar os riscos que impactam o alcance dos objetivos estratégicos;

III – Avaliar a adequação, a suficiência e a eficácia do processo de gestão de riscos, revisando a política e a metodologia de gestão de riscos sempre que necessário;

IV – Assessorar os órgãos de governança nos temas técnicos acerca da gestão de riscos.

Compete à auditoria interna, como Terceira Linha:

I – Avaliar as atividades da Primeira e Segunda Linhas no que tange à eficácia dos controles internos e da gestão de riscos, assessorando-os quanto às melhores práticas;

II – Verificar a conformidade das atividades executadas com a Política de Gestão de Riscos;

III – Avaliar o desempenho da gestão de riscos, com o objetivo de promover a melhoria contínua do

processo, de forma a auxiliar a organização a alcançar seus objetivos estratégicos.

Compete ao órgão de governança:

I – Definir os limites de apetite a risco no nível institucional e a periodicidade de suas revisões;

II – Aprovar as revisões da política e metodologia de gestão de riscos;

III – Aprovar os planos de ação e as respectivas medidas de controle a serem implementadas;

IV – Zelar pelo alinhamento da gestão de riscos aos padrões de conduta e integridade, assim como ao planejamento estratégico da organização.

6. PROCESSO DE GESTÃO DE RISCOS

O processo de gestão de riscos envolve a aplicação sistemática de políticas, procedimentos e práticas que contemplam as atividades de identificação, análise, avaliação, tratamento e monitoramento de potenciais eventos que possam afetar os atingimentos dos objetivos da organização.

Figura 2: Processo de gestão de riscos da CGE

Fonte: Elaboração própria

O processo de gestão de riscos compreende as seguintes etapas:

I - Entendimento do Contexto: conhecer os objetivos organizacionais e os processos a eles relacionados, assim como definir os contextos internos e externos a serem levados em consideração ao gerenciar os riscos;

II - Identificação e Análise de Riscos: levantar os possíveis riscos associados aos objetivos organizacionais e processos, bem como suas causas e consequências;

III - Avaliação de Riscos: estimar os níveis dos riscos identificados, avaliando sua severidade com base em critérios de impacto e probabilidade de ocorrência, e definição do apetite a riscos;

IV - Tratamento de Riscos: eleger quais riscos terão suas respostas priorizadas e definir as respostas aos riscos, de forma a adequar seus níveis ao apetite estabelecido, além da escolha das medidas de controle associadas a essas respostas;

V - Comunicação e Monitoramento: acompanhar o desempenho, verificar adequação e suficiência dos controles internos, mantendo um fluxo contínuo de compartilhamento de informações entre as partes interessadas.

A seguir serão detalhadas as etapas da metodologia, visando orientar, de forma prática, como executar cada uma das atividades.

Ao final deste documento, nos anexos, estão reunidos todos os modelos de planilhas e formulários utilizados na metodologia. Os arquivos eletrônicos podem ser baixados em link específico na página eletrônica da Controladoria Geral do Estado de São Paulo.

6.1 Entendimento do Contexto

Esta etapa consiste na compreensão e análise do objeto da gestão de riscos, levando em consideração o contexto interno e externo da organização.

Como o processo de gestão de riscos pode ser aplicado em diferentes níveis (estratégico, operacional, programa, projeto ou outras atividades), é importante identificar claramente o escopo e os objetivos a serem considerados, assim como o alinhamento aos objetivos organizacionais.

Compreender o contexto é importante porque:

- Fatores organizacionais podem ser uma fonte de risco;
- É preciso ter clareza acerca do resultado ou objetivo em que se pretende chegar.

Os produtos gerados nessa etapa são:

- Planejamento Estratégico e Definição do Escopo (Quadro 1);
- Matriz SWOT (Quadro 2).

6.1.1 Planejamento estratégico

- Missão: refere-se à declaração da razão da existência do órgão;
- Visão: representa o destino desejado, o que ele pretende tornar-se a longo prazo;
- Valores: representam aquilo que o órgão acredita, defende e valoriza.

6.1.2 Definição do escopo

A definição do escopo consiste em levantar informações visando a compreensão do objeto da gestão de riscos. Quanto mais completa a compreensão, melhor o desenvolvimento do trabalho, desta forma, sugere-se registrar as informações descritas abaixo:

- Título: como o objeto-alvo da gestão de riscos pode ter naturezas diversas como um programa, processo, atividade ou projeto, é importante identificá-lo através de um título, por exemplo: Gestão de Riscos no processo de Contratação de Serviços.
- Objetivos: o entendimento do objeto da gestão de riscos envolve apontar quais os objetivos diretos são alcançados por ele, assim como os objetivos estratégicos atendidos. Para a identificação dos objetivos, pode-se buscar responder à questão “Quais são os propósitos do objeto alvo?”.

- Partes Interessadas: outro fator importante que se deve levar em consideração são as partes interessadas, que são intervenientes do objeto selecionado, os indivíduos ou grupos de indivíduos que afetam o objeto-alvo e são afetados por ele. Deve-se mapear os relacionamentos, percepções, valores, necessidades e expectativas das partes interessadas, internas e externas à organização. O envolvimento apropriado e oportuno das partes interessadas possibilita que seus conhecimentos, pontos de vista e percepções sejam considerados, resultando em melhor conscientização e gestão de riscos fundamentada.
- Normativos, Unidade Responsável e início do trabalho: por fim, listam-se os normativos que regulam o objeto-alvo, identificam-se sistemas de informação envolvidos, registra-se a Unidade Responsável pela Gestão de Riscos e o início do trabalho.

Fundamental ressaltar que a lista sugerida não é exaustiva, podendo ser estendida de acordo com a necessidade constatada pelo gestor do risco ou equipe responsável.

O Quadro a seguir ilustra um registro hipotético do contexto de gestão de riscos:

Quadro 1: Contexto de Gestão de Risco

PLANEJAMENTO ESTRATÉGICO	
ÓRGÃO/AUTARQUIA/FUNDAÇÃO	Secretaria Municipal de Finanças da Prefeitura de XY
MISSÃO	Prover e gerenciar os recursos financeiros com responsabilidade social e equilíbrio fiscal, buscando o desenvolvimento do município
VISÃO	Tornar-se referência em gestão pública, promovendo o desenvolvimento sustentável, social e econômico
VALORES	Ser ético, competente, comprometido, transparente e confiável

DEFINIÇÃO DO ESCOPO	
TÍTULO	Gestão de Riscos na Segurança da Informação e Comunicação
OBJETIVO(S) DIRETO(S)	Garantir a confidencialidade, integridade, disponibilidade e autenticidade dos dados e informações registrados pela organização
OBJETIVO(S) ESTRATÉGICO(S) ASSOCIADO(S)	Implantar, revisar, atualizar e supervisionar a execução da política de segurança da informação
PARTES INTERESSADAS	Sociedade Secretaria Servidores e terceirizados Gestores
LEIS E REGULAMENTOS RELACIONADOS	Lei 13.729, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados); Lei 12.965, de 23 de abril de 2014 (Marco Civil da Internet); Lei 12.527, de 18 de novembro de 2011 (Lei de acesso à Informação)
SISTEMAS	Sistema A,B Correio eletrônico Demais recursos de Tecnologia Informação e Comunicação
UNIDADE RESPONSÁVEL	Área de Tecnologia da Informação e Comunicação
DATA DE INÍCIO	13/03/2023

Fonte: Elaboração própria

6.1.3 Matriz SWOT

A matriz SWOT (do Inglês Strengths, Weaknesses, Opportunities and Threats) é uma ferramenta que ajuda na análise dos elementos do contexto interno e externo à organização, identificando forças, fraquezas, oportunidades e ameaças que podem afetar diretamente o objeto de gestão de riscos e, consequentemente, o atingimento dos resultados almejados.

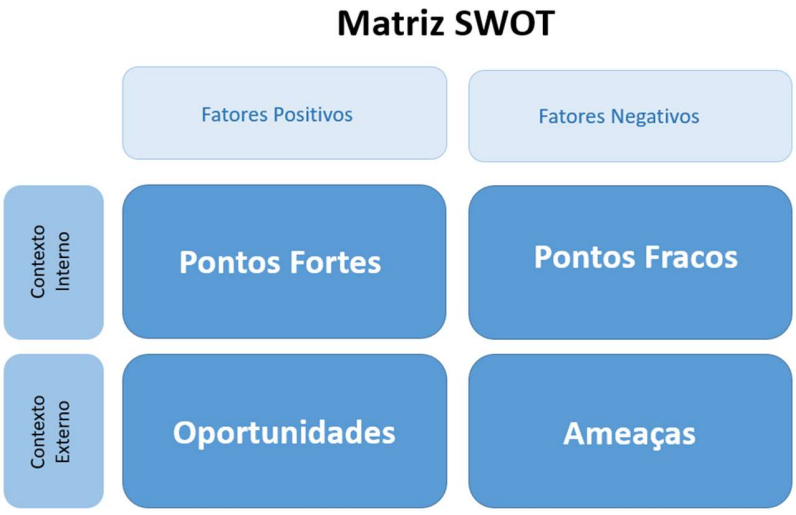
A análise do ambiente interno se concentra nas forças e fraquezas da organização, abrangendo os fatores sobre os quais ela tem controle ou pode intervir, como: visão, missão, valores, objetivos estratégicos, estrutura organizacional, governança, pessoas, sistemas, políticas, processos, cultura organizacional, entre outros.

Já a análise do ambiente externo identifica as oportunidade e ameaças, sendo representadas por um contexto favorável ou desfavorável sobre os quais a organização não tem poder de decisão ou influência. Reúne elementos como: fatores sociais, culturais, políticos, jurídicos, regulatórios, financeiros, tecnológicos, econômicos e ambientais.

Assim, observando as forças e oportunidades da matriz, tem-se os fatores positivos a serem aproveitados. Por outro lado, as fraquezas e ameaças identificadas, trazem os fatores negativos a serem observados e evitados.

A Figura 3 apresenta a forma gráfica de estruturação da Matriz SWOT e o Quadro 2 traz uma forma de registro dos elementos da análise de cenários.

Figura 3: Matriz SWOT



Fonte: Elaboração própria

Quadro 2: MATRIZ SWOT (Exemplo: Departamento de TIC)

ANÁLISE SWOT	
FORÇAS	**FRAQUEZAS**
Quadro próprio de especialistas em TIC qualificados	Falta de capacitação dos servidores/terceirizados em temas de segurança da informação
Ferramentas de proteção da informação instaladas em equipamentos e rede	Falta de capacitação dos servidores/terceirizados em legislação referente à segurança da informação e proteção de dados
Acesso restrito aos sistemas	Obsolescência de parte da infraestrutura de TIC
OPORTUNIDADES	**AMEAÇAS**
Preparar a organização para assimilar mudanças decorrentes do crescente uso da tecnologia no ambiente corporativo	Ataque hacker
Adequação à legislação e às boas práticas da segurança da informação e proteção de dados	Restrição orçamentária

Fonte: Elaboração própria

6.2 Identificação e Análise de Riscos

O objetivo desta etapa é identificar o maior número de eventos que possam atrapalhar o alcance dos resultados ou objetivos esperados, bem como suas causas e consequências.

Identificar e analisar os riscos é importante porque:

- Mapeia os eventos que podem interferir no alcance dos objetivos;
- Identifica as causas que podem desencadear os eventos de risco, assim como suas consequências;
- Torna a organização mais consciente e capaz de atuar diante dos potenciais eventos de risco.

O produto gerado nessa etapa é:

- Planilha de Apoio - Identificação e Análise de Riscos (Quadro 3).

A identificação dos riscos deve seguir os seguintes passos:

- Identificar com clareza os objetivos;
- Listar os eventos que possam vir a ter impacto negativo ou positivo no alcance dos objetivos;
- Descrever as possíveis causas de cada evento;
- Descrever como cada risco impacta o objetivo a ele associado.

A identificação de riscos reúne as atividades de reconhecer e registrar os eventos que possam ajudar ou impedir que uma organização alcance seus objetivos. Eventos são incidentes ou ocorrências originadas a partir de fontes internas ou externas, que afetam a organização, provocando impacto positivo, negativo ou ambos.

O propósito da identificação de riscos é mapear e agir preventivamente às situações que, se ocorrerem, poderão afetar o alcance dos resultados almejados. A finalidade é gerar uma lista abrangente de riscos baseada nestes eventos que possam aumentar, reduzir, inviabilizar, acelerar ou atrasar a realização dos objetivos.

A identificação dos riscos deve ser realizada em oficinas de trabalho ou, dependendo do objeto, pelo próprio gestor do risco. Podem ser utilizadas técnicas ou ferramentas que permitam a coleta do maior número

de riscos, como entrevistas, visitas técnicas, pesquisas, *Brainstorming*, Diagrama de *Ishikawa*, Método *Bow Tie*, entre outros. A norma ABNT NBR ISO 31.010: 2012 traz várias dessas técnicas, com uma tabela comparativa de aplicabilidade de cada uma das técnicas para cada tipo de análise de risco.

Conforme consta na metodologia da Controladoria Geral da União, os riscos podem ser identificados a partir de perguntas, como:

- Quais eventos podem EVITAR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem ATRASAR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem PREJUDICAR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem IMPEDIR o atingimento de um ou mais objetivos do processo organizacional?

Um evento pode ter múltiplas causas e consequências e pode afetar múltiplos objetivos. A análise de riscos pode ser realizada com vários graus de detalhamento e complexidade, dependendo do propósito da análise, da disponibilidade e confiabilidade da informação, e dos recursos disponíveis. Uma forma simples de diferenciar os componentes causa, risco e consequência, é raciocinar como demonstrado na Figura 4:

Figura 4: Componentes do Evento de Risco

Fonte: Metodologia de Gestão de Riscos – CGE-MG (adaptado)

- Causas: motivos que podem promover a ocorrência do risco;
- Consequências: resultados do risco que afetam os objetivos.

6.2.1 Categorias de risco

Utilizam-se categorias para agrupar os riscos classificando-os por temas, o que pode direcionar as responsabilidades após definido o tratamento necessário para sua mitigação:

- Operacional: eventos que podem comprometer as atividades, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas. Ex.: possibilidade de o espaço para armazenamento de dados pelas organizações do Estado não suportar o aumento das informações processadas diariamente;
- Legal/conformidade: eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades. Ex.: legislação que limita a capacidade de atuação do órgão ou que altere suas atribuições;
- Financeiro/orçamentário: eventos que podem comprometer a capacidade do órgão de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam

comprometer a própria execução orçamentária. Ex.: exigência de redução de custos nos órgãos/entidades do Estado, atraso no cronograma de licitações;

- Integridade: eventos relacionados a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta que podem comprometer os valores e padrões, assim como a realização dos objetivos. Ex.: recebimento de propina por servidor público;
- Político: por serem instituições públicas, as organizações do Estado sofrem uma considerável influência dos acontecimentos no ambiente político. Ex.: emenda parlamentar impactando a distribuição do orçamento do Estado;
- Pessoal/recursos humanos: refere-se ao impacto na estratégia causado por questões relacionadas a servidores cedidos, aos terceirizados, aos contratados, etc. Ex.: greve;
- Tecnologia da Informação: eventos relacionados a vazamento de informações sigilosas, invasões, fraudes digitais, perda de dados, falta de disponibilidade de sistemas, vulnerabilidades causadas por falta de conhecimento dos usuários, entre outros. Ex.: invasão hacker nos sistemas das organizações públicas;
- Estratégico: são aqueles que, uma vez materializados em eventos, afetam de maneira decisiva a consecução de um ou mais objetivos estratégicos da organização. São conjuntos de ações e diretrizes que mobilizam os recursos de uma organização visando ao ganho de competitividade em longo prazo. Ex.: mudanças das prioridades nas políticas públicas em razão de mudanças de Governo;

O Quadro 3 traz as informações que devem ser consolidadas na primeira parte da Planilha de Apoio - Identificação e Análise de Riscos, detalhando os objetivos impactados, os eventos de risco, as causas e as consequências possíveis, assim como a categorização dos eventos de risco.

Quadro 3: Planilha de Apoio - Identificação e Análise de Riscos

IDENTIFICAÇÃO E ANÁLISE DE RISCOS >>>					
ID	Objetivo	Evento de Risco (o que pode dar errado/favorecer a organização?)	Causas (o que pode causar esse evento?)	Consequências (quais os impactos para o objetivo?)	Categoria
1	Garantir a confidencialidade, integridade, disponibilidade e autenticidade dos dados e informações registrados pela organização.	Vazamento de dados e informações sigilosas	1) Falta de campanhas de conscientização 2) Falta de treinamento do usuário em segurança dos Sistemas de TIC 3) Não observância da LGPD por descuido ou desconhecimento	1) Desgaste da imagem institucional 2) Ações judiciais movidas pelo indivíduo ou organização exposta	Tecnologia da Informação

Fonte: Metodologia de Gestão de Riscos - Controladoria Geral do Distrito Federal (adaptado)

6.3 Avaliação de Riscos

Segundo o COSO-ERM, a avaliação de riscos permite que uma organização considere até que ponto eventos podem impactar a realização dos objetivos. Fatores externos e internos influenciam os eventos que poderão ocorrer, e essa incerteza de eventos é avaliada a partir de duas perspectivas – probabilidade e impacto.

A avaliação de riscos é importante porque:

- Avalia os riscos com base na probabilidade de sua ocorrência e impacto que poderiam causar nos resultados, permitindo que a organização considere os níveis de riscos;
- Verifica a existência de controles internos e sua eficiência em mitigar os riscos;
- Fornece a base para decisões sobre se o risco necessita ser tratado e como;
- Considera e trata de forma cuidadosa fatores como cenários, incertezas, complexidade e conectividade, assim como divergência de opiniões, vieses, percepções e julgamentos.

Os produtos gerados nessa etapa são:

- Planilha de Apoio - Avaliação de Riscos (Quadro 8);
- Matriz de Risco (Quadro 7).

A avaliação de riscos envolve os seguintes passos:

- Avaliar a probabilidade de ocorrência do evento de risco;
- Avaliar a magnitude do impacto que a ocorrência do evento de risco causará aos objetivos, dados os controles já existentes;
- Calcular o nível de risco, com base na Matriz de Risco;
- Identificar os controles já existentes e listar ações de controle complementares.

6.3.1 Avaliação de probabilidade

A probabilidade está diretamente relacionada à causa, sendo a chance de o evento de risco ocorrer dentro do prazo previsto para se alcançar o objetivo/resultado. Por exemplo, se o objeto da gestão de riscos é um projeto, estima-se a probabilidade da ocorrência do risco durante o prazo previsto para entrega do seu produto.

De acordo com a norma ABNT NBR ISO 31.010: 2012, para a avaliação de probabilidade três abordagens são comumente empregadas, podendo ser utilizadas individual ou conjuntamente:

a) a utilização de dados históricos para identificar eventos ou situações que ocorreram no passado e, assim, capazes de acontecerem no futuro. Entretanto, deve-se ter cautela, visto que os fatores que influenciam os eventos podem modificar-se com o passar do tempo. Dados gerados externamente também podem ser úteis como um ponto de controle ou para aprimorar a análise, como por exemplo a comparação com referências de mercado (benchmarking);
b) quando os dados históricos forem indisponíveis ou inadequados, é necessário deduzir a probabilidade utilizando técnicas preditivas, tais como análise de árvore de falhas e análise de árvore de eventos, quando dados numéricos secundários são combinados para produzir uma estimativa da probabilidade do evento principal. A ISO 31.010: 2012 traz, várias dessas técnicas, com uma tabela comparativa de aplicabilidade de cada uma das técnicas para cada tipo de análise de risco;
c) a opinião de especialistas pode ser utilizada em um processo sistemático e estruturado para estimar a probabilidade. Convém que os julgamentos dos especialistas recorram a todas as informações pertinentes disponíveis, incluindo informações históricas, específicas do sistema, específicas da organização, experimentais, de projeto etc. Existem diversos métodos formais para auxiliar o julgamento dos especialistas, como a abordagem Delphi, comparações emparelhadas, classificação de categorias e julgamentos de probabilidade absoluta.

6.3.2 Avaliação de impacto

Os eventos podem gerar impacto negativo, positivo ou ambos. Os que geram impacto negativo representam riscos que podem impedir a criação de valor ou mesmo destruir o valor existente. Os de impacto positivo podem contrabalançar os de impacto negativo ou representar oportunidades, que podem influenciar favoravelmente a realização dos objetivos, apoiando a criação ou a preservação de valor.

A avaliação do grau de impacto está diretamente relacionada à consequência do evento, podendo:

- relacionar as consequências do risco aos objetivos originais;
- considerar tanto as consequências imediatas quanto aquelas que podem surgir após decorrido um certo tempo, se isso for compatível com o escopo da avaliação;
- considerar as consequências secundárias, tais como aquelas que impactam os sistemas, atividades, equipamentos ou organizações, associados.

A metodologia de avaliação de riscos de uma organização inclui uma combinação de técnicas quantitativas e qualitativas. As técnicas quantitativas emprestam maior precisão e são utilizadas em atividades mais complexas e sofisticadas, requerem mais esforço e rigor, utilizando modelos matemáticos. Dependem sobremaneira da qualidade dos dados e das premissas adotadas, sendo mais relevantes para exposições que apresentem um histórico conhecido, uma frequência de sua variabilidade e permitam uma previsão confiável. A ISO 31.010: 2012 traz, várias dessas técnicas, com uma tabela comparativa de aplicabilidade de cada uma das técnicas para cada tipo de análise de risco.

Em geral, a Administração emprega técnicas qualitativas de avaliação se os riscos não se prestam à quantificação, se não há dados confiáveis em quantidade suficiente para a realização das avaliações quantitativas, ou, ainda, se a relação custo-benefício para obtenção e análise de dados não for viável.

Para indicar a probabilidade de que um evento ocorra em termos qualitativos, podem ser utilizadas escalas descritivas ou numéricas, como muito provável, possível e improvável. Da mesma forma, para indicar o impacto em termos qualitativos, termos como alto, médio e baixo. Caso os responsáveis pela gestão de riscos entendam pertinente, outros graus de severidade podem ser utilizados.

Para obter consenso sobre a probabilidade e o impacto de eventos de risco pelo uso de técnicas qualitativas de avaliação, as organizações poderão utilizar a mesma abordagem que usam na identificação dos eventos, como entrevistas e seminários ou oficinas de trabalho com a participação de pessoas que conheçam bem o objeto de gestão de riscos.

De acordo com a norma ABNT NBR ISO 31.000: 2018, a avaliação de riscos pode ser influenciada por divergência de opiniões, vieses, percepções do risco, julgamentos, qualidade da informação utilizada, quaisquer limitações das técnicas e como elas são executadas. Convém que estas influências sejam consideradas, documentadas e comunicadas aos tomadores de decisão.

Os Quadros 4 e 5 trazem as escalas de probabilidade e impacto utilizadas pela CGE. As escalas podem variar de acordo com o objeto de gestão e com o grau de precisão na definição dos níveis de probabilidade e impacto. Recomenda-se evitar o uso de matrizes simétricas, ou com pesos iguais para as variáveis, pois a dimensão impacto é mais importante que a dimensão probabilidade: um evento de impacto muito alto e de probabilidade de ocorrência muito baixa deve ser considerado uma grande preocupação pelo gestor. Por outro lado, um evento de impacto muito baixo, mesmo com alta probabilidade de ocorrência, não deve ser motivo de preocupação, afinal o impacto é mínimo. Assim, esse maior peso para a dimensão impacto é levado em consideração na classificação do Nível de Risco.

Quadro 4: Escala de Probabilidade

Escala de Probabilidade		
Probabilidade	**Descrição da Probabilidade**	**Peso**
Muito baixa	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	1
Baixa	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as cinrcusntâncias pouco indicam essa possibilidade.	2
Média	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam possibilidade moderada.	3
Alta	Provável. De forma até esperada, o evento poderá ocorrer pois as circunstâncias indicam fortemente essa possibilidade.	4
Muito alta	Praticamente certa. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	5

Fonte: Metodologia de Gestão de Riscos – Controladoria Geral da União (adaptado)

Quadro 5: Escala de Impacto

Escala de Impacto		
Impacto	**Descrição do Impacto**	**Peso**
Muito baixo	Nenhum ou mínimo impacto nos objetivos.	1
Baixo	Pequeno impacto nos objetivos.	3
Médio	Moderado impacto nos objetivos, porém recuperável.	5
Alto	Significativo impacto nos objetivos, de difícil reversão.	7
Muito alto	Catastrófico impacto nos objetivos, de forma irreversível.	10

Fonte: Metodologia de Gestão de Riscos –Controladoria Geral da União (adaptado)

6.3.3 Nível de risco

A multiplicação entre os valores de probabilidade e impacto irá definir o nível de risco, ou seja:

Nível de Risco = Probabilidade x Impacto

A partir do resultado do cálculo, o risco pode ser classificado dentro das seguintes faixas:

Quadro 6: Nível de Risco

Classificação do Risco	
Nível de Risco	**Faixa**
Risco Baixo	01 - 04
Risco Médio	05 - 09
Risco Alto	10 - 25
Risco Extremo	26 - 50

Fonte: Metodologia de Gestão de Riscos - Controladoria Geral da União (adaptado)

O Quadro 7 traz a Matriz de Risco, com os possíveis resultados da combinação das escalas de probabilidade e impacto, resultando em um valor que indica o nível de risco.

Quadro 7: Matriz de Risco

MATRIZ DE RISCO		PROBABILIDADE				
		MUITO BAIXA 1	BAIXA 2	MÉDIA 3	ALTA 4	MUITO ALTA 5
IMPACTO	MUITO ALTO 10	10	20	30	40	50
	ALTO 7	7	14	21	28	35
	MÉDIO 5	5	10	15	20	25
	BAIXO 3	3	6	9	12	15
	MUITO BAIXO 1	1	2	3	4	5

Fonte: Metodologia de Gestão de Riscos - Controladoria Geral da União (adaptado)

Segundo o modelo COSO-ERM, os riscos são avaliados com base em suas características inerentes e residuais.

- **Risco inerente** é o risco que uma organização terá de enfrentar na falta de medidas que a administração possa adotar para alterar a probabilidade ou o impacto dos eventos. No entanto, na prática, é muito difícil imaginar o cenário de risco inerente, pois é irreal pensar na completa inexistência de medidas de controle.
- **Risco residual** é aquele que ainda permanece após a resposta da administração. Em geral, a avaliação de impacto dos eventos parte de um cenário real, em que já existem medidas de controle. Por isso, quando se faz a avaliação de risco (estimativa de probabilidade e impacto), refere-se ao risco residual.

As avaliações de probabilidade, impacto e nível de risco devem ser inseridas na segunda parte da Planilha de Apoio - Avaliação de Riscos, conforme o Quadro 8.

Quadro 8: Planilha de Apoio - Avaliação de Riscos

AVALIAÇÃO DE RISCOS >>>							
Probabilidade		Impacto		Nível de Risco		Controles Identificados (existentes)	Controles Necessários (ações de controle)
Média	3	Alto	7	21	Alto	1) Política de uso dos sistemas de TIC 2) Política de proteção de dados	1) Campanha de comunicação em Segurança da Informação 2) Capacitação em temas de Segurança da Informação e Comunicação 3) Assinatura Termo de Responsabilidade no uso dos Sistemas de TIC

Fonte: Metodologia de Gestão de Riscos - Controladoria Geral do Distrito Federal (adaptado)

Por fim, são identificados os controles já existentes, relacionados a cada um dos eventos de risco, assim como são listadas as ações de controle complementares, que serão úteis para o acompanhamento dos impactos.

Da mesma forma que na identificação de eventos e avaliação de riscos, recomenda-se a realização de oficinas de trabalho com a participação de pessoas que conheçam bem o objeto de gestão de riscos, pois elas devem ser as mais habilitadas para mapeamento desses controles.

6.4 Tratamento de Riscos

O tratamento de riscos é importante porque reduz para um nível aceitável os riscos priorizados, equilibrando os benefícios relacionados ao alcance dos objetivos e os custos de sua implementação. Envolve a comparação dos resultados da avaliação de riscos com os critérios de risco estabelecidos, para determinar onde é necessária ação adicional. Assim, registra e fundamenta a tomada de decisões acerca do tratamento a ser dado a cada risco identificado.

O produto gerado nessa etapa é:

- Planilha de Apoio - Plano de Tratamento de Riscos (Quadro 10);
- Plano de Ação;
- Relatório Gerencial.

O tratamento de riscos envolve os seguintes passos:

- eleger quais riscos terão suas respostas priorizadas;
- escolher as medidas de tratamento a serem implementadas;
- definir e detalhar as respostas aos riscos, de forma a adequar seus níveis ao apetite estabelecido.

6.4.1 Apetite a risco

Apetite a risco é o nível de risco que a organização está disposta a aceitar, ou sua tolerância ao risco. Deve ser aprovado por uma instância de supervisão da alta administração, um órgão de governança.

6.4.2 Priorização de riscos

Uma vez definido o apetite a risco, os riscos cujos níveis estejam dentro da faixa de tolerância podem ser aceitos, e uma possível priorização para tratamento deve ser justificada. Os riscos que estejam acima da faixa de tolerância deverão ser tratados e monitorados, e uma possível falta de tratamento deve ser justificada.

Assim, com base nos níveis de riscos residuais calculados na etapa de avaliação de riscos e, definido o apetite a risco, estabelece-se a priorização da organização para tratamento.

6.4.3 Opções de tratamento aos riscos

Priorizados os riscos, o próximo passo é definir quais opções de tratamento serão adotadas. Cada risco deve ser relacionado a uma ou mais opções de tratamento, que incluem: mitigar, compartilhar, evitar ou aceitar os riscos, conforme aponta o Quadro 9.

Ao analisar a própria resposta, o gestor avalia o efeito sobre a probabilidade de ocorrência e o impacto do risco, assim como os custos e benefícios, selecionando, dessa forma, uma resposta que mantenha os riscos residuais dentro das tolerâncias a risco desejadas.

Quadro 9: Opções de tratamento aos riscos

Opções de Tratamento de Riscos	
Opções	**Descrição**
Mitigar	Um risco normalmente é mitigado quando é classificado como "Alto" ou "Extremo". A implementação de controles, neste caso, apresenta um custo/benefício adequado. Mitigar o risco significa implementar controles que possam diminuir as causas ou as consequências dos riscos, identificadas na etapa de Identificação e Análise de Riscos.
Compartilhar	Um risco normalmente é compartilhado quando é classificado como "Alto" ou "Extremo", mas a implementação de controles não apresenta um custo/benefício adequado. Pode-se compartilhar o risco por meio de terceirização ou apólice de seguro, por exemplo.
Evitar	Um risco normalmente é evitado quando é classificado como "Alto" ou "Extremo", e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco. Evitar o risco significa encerrar o processo organizacional. Nesse caso, essa opção deve ser aprovada pelo Comitê de Governança Interna.
Aceitar	Um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco. Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco.

Fonte: Metodologia de Gestão de Riscos - Controladoria Geral da União (adaptado)

6.4.4 Definição das medidas de tratamento

A escolha das medidas de resposta ao risco pode ser realizada em oficinas de trabalho com a participação de pessoas que conheçam bem o objeto de gestão de riscos. Recomenda-se a utilização de técnicas que permitam a identificação da maior quantidade de medidas de resposta ao risco, tais como *brainstorming*, *brainwriting*,

entrevistas, visitas técnicas, pesquisas etc.

São dicas que ajudam a identificação de medidas de resposta ao risco:

- Responder às seguintes perguntas-chave:
  - Que medidas poderiam ser adotadas para reduzir a probabilidade de ocorrência do risco?
  - Que medidas poderiam ser adotadas para reduzir o impacto do risco no objetivo?
  - É possível adotar medidas para transferir o risco?
- Considerar as fontes e causas dos riscos. A princípio, as medidas devem atacar as causas do risco, de modo a reduzir a probabilidade de ocorrência. Porém, também podem consistir em planos de contingência que amenizem os impactos, caso o risco se concretize, ou uma combinação das duas abordagens;
- Na decisão quanto à implantação das medidas de resposta ao risco, considerar a quantidade e o nível dos riscos mitigados por cada medida, bem como o grau de redução do nível do risco gerado pela medida;
- Considerar a viabilidade da implantação das medidas (custo-benefício, viabilidade técnica, tempestividade, efeitos colaterais do tratamento etc.).

Após decidir sobre as respostas, o gestor precisa desenvolver um plano de tratamento e assegurar-se de que a resposta ao risco seja conduzida. Ressaltando que sempre existirá algum nível de risco residual, não somente porque os recursos são limitados, mas também em decorrência da incerteza e das limitações inerentes a todas as atividades.

O Plano de Tratamento de Riscos é a terceira parte da Planilha de Apoio e detalha como serão operacionalizadas as medidas de tratamento, conforme demostrado pelo Quadro 10:

Quadro 10: Planilha de Apoio - Plano de Tratamento de Riscos

PLANO DE TRATAMENTO DE RISCOS >>>					
Prioridade	**Opções de Tratamento**	**Responsável**	**Ações**	**Status / Observação**	**Prazo**
1	**Mitigar**	Áreas de TIC e Educação Continuada	1) Elaboração de um calendário de ações em segurança da informação e comunicação 2) Prover capacitação em temas de segurança da informação e comunicação 3) Elaboração do Termo de Responsabilidade de TI	Em andamento	2º semestre de 2023

Fonte: Metodologia de Gestão de Riscos - Controladoria Geral do Distrito Federal (adaptado)

É importante que, na elaboração do plano de tratamento, avalie-se também a necessidade de melhorar ou extinguir controles ineficientes. Somente depois dessa avaliação, e se ainda identificada a necessidade de redução do nível do risco, podem ser propostos novos controles, observados sempre critérios de eficiência e eficácia da sua implementação.

Importante destacar que cabe aos gestores proprietários dos riscos, primeira linha, elaborar os planos de ação para o tratamento dos riscos, considerando a declaração de apetite a riscos do órgão.

6.5 Comunicação e Monitoramento

De acordo com a ISO 3100:2018, durante todas as etapas do processo de gerenciamento de riscos, é importante haver comunicação com as partes interessadas, a fim de assegurar que a informação pertinente seja coletada, consolidada, sintetizada e compartilhada.

Também é necessário monitorar e adaptar continuamente a estrutura de gestão de riscos para abordar mudanças nos contextos externos e internos, incluindo alterações nos critérios de risco e no próprio risco, que podem requerer revisão dos tratamentos adotados, assim como identificação de riscos emergentes. Ao fazer isso, a organização pode acompanhar e melhorar continuamente a adequação, suficiência e eficácia da estrutura de gestão de riscos.

A comunicação e o monitoramento são importantes porque:

- a comunicação busca promover a conscientização e o entendimento do risco;
- assegura que todos os envolvidos estejam cientes de seus papéis e responsabilidades;
- o monitoramento permite identificar fragilidades e possibilidades de melhorias no processo de gestão de riscos.

Os produtos gerados nessa etapa são:

- Plano de Comunicação (Quadro 11);
- Plano de Monitoramento (Quadro 12);
- Plano de Ação.

A comunicação e o monitoramento envolvem os seguintes passos:

- identificar os canais de comunicação da organização, para elaboração de um Plano de Comunicação;
- definir indicadores de desempenho para apresentação de resultados e acompanhamento do processo de gestão de riscos.

A comunicação tem como objetivo familiarizar os servidores com os conceitos de gestão de riscos. Ao compartilhar as informações e criar as condições para a participação das diferentes áreas de especialização em cada etapa do processo, considera pontos de vista diferentes na definição de critérios e avaliação de riscos. Todas essas ações contribuem para a construção de um senso de inclusão e propriedade entre os afetados pelo risco.

Além disso, assegura que todos os envolvidos estejam cientes de seus papéis e responsabilidades. Dessa forma, promove a conscientização e o entendimento do risco, a base sobre a qual decisões são tomadas, as razões pelas quais ações específicas são requeridas e seus resultados.

Dentre os principais benefícios da elaboração e implantação de um plano de comunicação formal, estão o fornecimento de informações com maior qualidade para a supervisão dos riscos e a tomada de decisão.

Os tipos de veículos de comunicação a serem utilizados depende da disponibilidade de cada organização, sendo os mais comuns: e-mail, intranet, mural, reuniões, oficinas de trabalho e capacitações, folhetos e cartazes, utilização de multiplicadores, redes sociais, comunicação por meio de sistemas, entre outros.

É fundamental mapear os canais de comunicação existentes na organização, assim como o público e partes interessadas, para a elaboração de um Plano de Comunicação, o qual deverá detalhar as ações, a mensagem, o objetivo, o público-alvo, o meio de comunicação, a frequência, o custo, o responsável pelo conteúdo e aprovação.

Quadro 11: Plano de Comunicação

PLANO DE COMUNICAÇÃO >>>							
Ação	Mensagem/ objetivo	Público-alvo	Midia	Frequência	Custo	Responsável	Aprovação
1) Promover capacitações sobre o uso consciente e seguro dos recursos de TIC	Conscientização de todos os usuários de recursos de TIC quanto a temas de segurança da informação	1) Servidores 2) Terceirizados	1) Intranet 2) E-mail Corporativo 3) Mural	Anual	Interno	Área de TIC	Área de educação continuada
2) Pop up na intranet com dicas de uso do e-mail	Ação educativa sobre o uso seguro do e-mail corporativo e pessoal	1) Servidores 2) Terceirizados	1) Intranet	Mensal	Interno	Área de TIC	Área de TIC

Fonte: Metodologia de Gestão de Riscos - CGE-SP

A gestão de riscos é dinâmica, dado que as respostas aos riscos, que se mostravam eficazes no início do processo, podem se tornar obsoletas, as atividades de controle podem não trazer os benefícios esperados ou podem perder a eficácia, assim como o contexto e os objetivos podem mudar.

Diante desse cenário, é fundamental estabelecer uma rotina de monitoramento contínuo capaz de verificar o desempenho e a efetividade das medidas mitigadoras implementadas. Para tanto, recomenda-se a definição de um Plano de Monitoramento composto por indicadores-chave de desempenho.

Os indicadores são métricas elaboradas para acompanhar a evolução dos eventos de risco e estabelecer pontos de alerta para sua ocorrência e monitoramento das consequências. O Quadro 12 apresenta um exemplo fictício de um Plano de Monitoramento com indicadores-chave de desempenho, fórmulas de cálculo, metas, periodicidade e possíveis planos de ação, caso a performance exija medidas corretivas.

Quadro 12: Plano de Monitoramento

PLANO DE MONITORAMENTO >>>							
Indicador	Fórmula	Interpretação	Responsável	Meta 2022	Resultado 2021	Periodicidade	Plano de Ação
Número de servidores e terceirizados capacitados em temas de segurança da informação	Número de servidores e terceirizados capacitados/Total de servidores e terceirizadosx100	Quanto maior o percentual, melhor	Área de educação continuada	100%	60%	Anual	Identificar servidores/terceirizados ainda não capacitados; Comunicar seus superiores hierárquicos para inclusão do servidor no próximo ciclo de
Infrações ao Termo de Responsabilidade de TIC	Quantidade de infrações ao Termo de Responsabilidade	Quanto maior o percentual, pior	Área de TIC	Zero	Zero	Trimestral	Nada a fazer

Fonte: Elaboração própria

O monitoramento tem como objetivo assegurar que a construção, implementação e resultados do processo de gestão de riscos se concretizem conforme o esperado. Também permite identificar fragilidades e possibilidades de melhoria. Ele é feito de forma descentralizada pelos proprietários dos riscos, que são os gestores em seus respectivos âmbitos e escopos de atuação (Primeira Linha, do Modelo de Três Linhas).

Os indicadores-chaves de desempenho que não alcançarem as metas previstas deverão ser revisados, cabendo aos gestores proprietários dos riscos a elaboração de um plano de ação com proposta de medidas visando a melhoria das métricas.

Como produto final de um ciclo de monitoramento e avaliação de indicadores, é possível que surjam sugestões de melhorias, revisões ou mudanças em qualquer das fases do processo ou da metodologia de gestão de riscos.

Compete à Terceira Linha, composta pelo controle interno, fazer uma avaliação objetiva e independente dos controles e da gestão de riscos. Complementarmente, é responsabilidade da Segunda Linha avaliar a adequação, a suficiência e a eficácia do processo de gestão de riscos, revisando a política e a metodologia de gestão de riscos sempre que necessário.

Considerações Finais

A metodologia é composta pelas etapas: entendimento do contexto, identificação e análise de riscos, avaliação de riscos, tratamento de riscos, comunicação e monitoramento. Cada etapa visa atingir os objetivos específicos do processo de gestão de riscos e controles internos da gestão.

Conforme citado anteriormente, a metodologia de gestão de riscos adotada pela CGE pode ser adaptada e aplicada em todas as organizações e contextos.

GLOSSÁRIO

Para fins deste documento, consideram-se os seguintes conceitos:

- **Accountability ou prestação de contas:** conjunto de procedimentos adotados pelas organizações públicas e pelos indivíduos que as integram que evidenciam sua responsabilidade por decisões tomadas e ações implementadas, incluindo a salvaguarda de recursos públicos, a imparcialidade e o desempenho das organizações;
- **Apetite a risco:** nível de risco que a organização está disposta a aceitar;
- **Contexto do processo de gestão de riscos:** compreensão dos ambientes externo e interno no qual a organização opera, e deve refletir o ambiente específico da atividade ao qual o objeto de gestão de riscos é aplicado;
- **Controle interno:** conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada, destinados a enfrentar os riscos e fornecer segurança razoável de que os objetivos organizacionais serão alcançados;
- **Eventos:** são incidentes ou ocorrências originadas a partir de fontes internas ou externas, que afetam a organização, provocando impacto positivo, negativo ou ambos;
- **Gestão de riscos:** aplicação sistemática de políticas, procedimentos e práticas que contemplam as atividades de identificação, análise, avaliação, tratamento e monitoramento de potenciais eventos que possam afetar a organização, cujo objetivo e fornecer segurança razoável quanto à realização dos objetivos da organização;
- **Governança pública:** conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade;
- **Medida de controle:** medida aplicada pela organização para tratar os riscos, aumentando a probabilidade de que os objetivos e as metas organizacionais estabelecidos sejam alcançados;
- **Meta:** alvo ou propósito com que se define um objetivo a ser alcançado;
- **Objetivo organizacional**: situação que se deseja alcançar de forma a se evidenciar êxito no cumprimento da missão e no atingimento da visão de futuro da organização;
- **Processo:** conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar produto, resultado ou serviço predefinido;
- **Proprietário do risco:** pessoa ou entidade com a responsabilidade e a autoridade para gerenciar o risco;
- **Risco:** possibilidade de ocorrência de um evento que tenha impacto no atingimento dos objetivos organizacionais.
- **Risco inerente:** risco a que uma organização está exposta sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto;
- **Risco residual:** risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco.

ANEXOS

Seguem abaixo todos os modelos de planilhas e formulários apresentados na metodologia. Os arquivos eletrônicos podem ser baixados em link específico na página eletrônica da Controladoria Geral do Estado de São Paulo.

Quadro 1: Contexto de Gestão de Risco

PLANEJAMENTO ESTRATÉGICO	
ÓRGÃO/AUTARQUIA/FUNDAÇÃO	
MISSÃO	
VISÃO	
VALORES	
DEFINIÇÃO DO ESCOPO	
TÍTULO	
OBJETIVO(S) DIRETO(S)	
OBJETIVO(S) ESTRATÉGICO(S) ASSOCIADO(S)	
PARTES INTERESSADAS	
LEIS E REGULAMENTOS RELACIONADOS	
SISTEMAS	
UNIDADE RESPONSÁVEL	
DATA DE INÍCIO	

Fonte: Metodologia de Gestão de Riscos - CGE-SP

Quadro 2: Matriz SWOT

MATRIZ SWOT	
FORÇAS	**FRAQUEZAS**
OPORTUNIDADES	**AMEAÇAS**

Fonte: Metodologia de Gestão de Riscos - CGE-SP

Quadro 3: Planilha de Apoio - Identificação e Análise de Riscos*

IDENTIFICAÇÃO E ANÁLISE DE RISCOS >>>					
ID	Objetivo	Evento de Risco (o que pode dar errado/favorecer a organização?)	Causas (o que pode causar esse evento?)	Consequências (quais os impactos para o objetivo?)	Categoria

Fonte: Metodologia de Gestão de Riscos - Controladoria Geral do Distrito Federal (adaptado)

Quadro 8: Planilha de Apoio - Avaliação de Riscos*

AVALIAÇÃO DE RISCOS >>>							
Probabilidade		Impacto		Nível de Risco		Controles Identificados (existentes)	Controles Necessários (ações de controle)

Fonte: Metodologia de Gestão de Riscos - Controladoria Geral do Distrito Federal (adaptado)

Quadro 10: Planilha de Apoio - Plano de Tratamento de Riscos*

PLANO DE TRATAMENTO DE RISCOS >>>					
Prioridade	Opções de Tratamento	Plano de Ação	Prazo	Responsável	Status/ Observação
1	Mitigar				
2	Compartilhar				
3	Evitar				
3	Aceitar				

Fonte: Metodologia de Gestão de Riscos - Controladoria Geral do Distrito Federal (adaptado)

Quadro 11: Plano de Comunicação

PLANO DE COMUNICAÇÃO >>>							
Atividades	Mensagem/ objetivo	Público-alvo	Mídia	Frequência	Custo	Responsável	Aprovação

Fonte: Metodologia de Gestão de Riscos - Controladoria Geral do Distrito Federal (adaptado)

Quadro 12: Plano de Monitoramento

PLANO DE MONITORAMENTO >>>							
Indicador	Fórmula	Interpretação	Responsável	Meta para 2022	Resultado em 2021	Periodicidade	Plano de Ação

Fonte: Metodologia de Gestão de Riscos - Controladoria Geral do Distrito Federal (adaptado)

REFERÊNCIAS BIBLIOGRÁFICAS

→ ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **NBR ISO 31000: Gestão de Riscos –Diretrizes**. Rio de Janeiro, 2018.

→ _____. **NBR ISO/IEC 31010: Gestão de Riscos - Técnicas para o Processo de Avaliação de Riscos**. Rio de Janeiro, 2012.

→ BRASIL. Controladoria Geral da União. **Metodologia de Gestão de Riscos**. Brasília, DF, 2018

→ _____. **Metodologia de Gestão de Riscos**. Brasília, DF, 2020.

→ BRASIL. Tribunal de Contas da União. **Referencial Básico de Gestão de Riscos**, DF, 2018.

→ COSO. Committee of Sponsoring Organizations of the Treadway Commission. **Enterprise Risk Management - ERM** (Gerenciamento de Riscos Corporativos. 2017.

→ Distrito Federal. Controladoria Geral do Distrito Federal. **Capacitação em Gestão de Riscos e Integridade**, 2022.

→ IIA. The Institute of Internal Auditors. **Modelo das 3 três linhas do IIA 2020 – Uma atualização das três linhas de defesa**.

→ INTOSAI (International Organization of Supreme Audit Institutions) - **Guias GOV 9100** (2004) e **GOV 9130** (2007).

→ Minas Gerais. Controladoria Geral do Estado de Minas Gerais. **Guia Metodológico de Gestão de Riscos de Processos**, 2021.

→ REINO UNIDO (UK). HM Treasury. Management of Risk - **Principles and Concepts - The Orange Book.** HM Treasury do HM Government, 2004.