GUIA METODOLÓGICO DE GESTÃO INTEGRADA DE RISCOS

CONTROLADORIA-GERAL DO ESTADO

MINAS GERAIS

GOVERNO DIFERENTE. ESTADO EFICIENTE.

GOVERNO DO ESTADO DE MINAS GERAIS
CONTROLADORIA-GERAL DO ESTADO

GUIA METODOLÓGICO DE GESTÃO INTEGRADA DE RISCOS

BELO HORIZONTE
ABRIL
2024

Nosso *propósito*

Ser integridade e eficiência por uma **sociedade** melhor.

Nossa *missão*

Aprimorar a gestão pública mineira, por meio da auditoria interna, da correição, da prevenção e combate à corrupção, promovendo eficiência, integridade, transparência e participação social.

Nossa *visão*

Ser excelência como órgão de controle interno, que contribui para uma administração pública íntegra, transparente e eficaz.

Nossos *valores*

- Integridade
- Comprometimento
- Integração e cooperação
- Independência técnica
- Humanização
- Foco no interesse público

CONTROLADORIA-GERAL DO ESTADO DE MINAS GERAIS

Cidade Administrativa Presidente Tancredo Neves
Rodovia Papa João Paulo II, 4.000 – Prédio Gerais, 12º andar
Bairro Serra Verde – Belo Horizonte/MG – CEP: 31630-901

CONTROLADOR-GERAL DO ESTADO
Rodrigo Fontenelle de Araújo Miranda

CONTROLADORA-GERAL DO ESTADO ADJUNTA
Luciana Cássia Nogueira

CHEFE DE GABINETE
Thomaz Anderson Barbosa da Silva

AUDITORIA-GERAL
Igor Martins da Costa

EQUIPE TÉCNICA RESPONSÁVEL
Anna Carolina de Oliveira Azevedo
Armando Noé Carvalho de Moura Junior
Márcio Vinícius de Araújo Silva
Olívia Bernardes Almeida
Omar Abreu Bacha
Rodrigo Flávio Ferreira dos Passos

COLABORAÇÃO
Cynthia Martins Vieira

EDITORAÇÃO
Assessoria de Comunicação Social

REVISÃO FINAL
Cynthia Martins Vieira

Como citar este material:

CONTROLADORIA-GERAL DO ESTADO DE MINAS GERAIS. **Guia Metodológico de Gestão Integrada de Riscos.** Belo Horizonte: CGE-MG, 2024. Disponível em: link de acesso. Acesso em: dd/mm/aaaa.

SUMÁRIO

1. INTRODUÇÃO

A gestão de riscos consiste em um “conjunto de atividades coordenadas para identificar, analisar, avaliar, tratar e monitorar riscos. É o processo que visa conferir razoável segurança quanto ao alcance dos objetivos” (TCU, 2018, *apud* VIEIRA e BARRETO, 2019, p. 100).

Consoante o *HM Treasury* do Governo do Reino Unido, no documento denominado *The Orange Book*, *apud* Miranda (2017):

> (...) risco é a incerteza do resultado e um bom gerenciamento de riscos permite que uma organização aumente sua confiança em alcançar os resultados desejados, restrinja de forma eficaz ameaças a níveis aceitáveis e tome decisões informadas sobre oportunidades de exploração (*HM TREASURY*, 2004, *apud* MIRANDA, 2017, p. 36).

Nesse sentido, a gestão de riscos refere-se a um processo contínuo que se estende por todos os níveis e processos organizacionais. Vieira e Barreto (2019), em referência ao TCU, afirmam que:

> Quando a gestão de riscos é corretamente implementada, de forma sistemática, estruturada e oportuna, gera benefícios que impactam diretamente cidadãos e outras partes interessadas da organização ao viabilizar o adequado suporte às decisões de alocação e uso apropriado dos recursos públicos, o aumento do grau de eficiência e eficácia no processo de criação, proteção e entrega de valor público, otimizando a conformidade e o desempenho, elevando os resultados entregues à sociedade (TCU, 2017a, p. 10, *apud* VIEIRA e BARRETO, 2019, p. 97).

Diante do exposto, o presente Guia tem como finalidade oferecer orientações técnicas específicas e objetivas acerca da gestão de riscos da Controladoria-Geral do Estado, conforme previsto nos seguintes instrumentos:

- ✓ Declaração de Apetite a Riscos, cuja revisão foi aprovada pela Resolução CGE nº 16, de 12 de dezembro de 2023;
- ✓ Política de Gestão de Riscos, cuja revisão foi aprovada pela Resolução CGE nº 17, de 12 de dezembro de 2023; e
- ✓ Instrução Normativa CGE/GAB nº 01, de 30 de novembro de 2021, que estabelece as orientações técnicas da atividade de Auditoria Interna Governamental do Poder Executivo Estadual.

As orientações técnicas previstas neste Guia, embora vinculadas diretamente à gestão de riscos no âmbito da CGE, podem ser tomadas como referências pelos demais órgãos e entidades do Poder Executivo Estadual na estruturação das suas políticas e dos seus procedimentos para gerenciamento dos riscos organizacionais.

Como resultado do trabalho, espera-se contribuir para o incremento do nível de maturidade da gestão de riscos da Controladoria-Geral do Estado (CGE), bem como para a implementação da gestão de riscos no Poder Executivo Estadual, por meio do aperfeiçoamento dos controles internos, minimização dos riscos a níveis aceitáveis e tomada de decisão fundamentada e tempestiva.

Por fim, o Guia está estruturado em onze itens, os quais tratam da introdução, dos princípios, diretrizes e objetivos da gestão de riscos da CGE, sua governança e seu funcionamento, o processo de gestão de riscos propriamente dito. Esses tópicos apresentam conteúdos centrais de uma política de gestão de riscos, que, no caso da Controladoria-Geral do Estado, está formalizada por meio da /Resolução CGE nº 17/2023. O Guia contempla, ainda, um glossário com a definição dos principais termos utilizados e referências bibliográficas.

2. PRINCÍPIOS DA GESTÃO DE RISCOS

A gestão de riscos deve estar alinhada ao propósito e à missão da organização, a qual deve estabelecer os princípios aplicáveis ao seu contexto e ambiente de atuação.

Na CGE, a gestão de riscos contém dez princípios, discriminados a seguir:

I - Fortalecer o alinhamento institucional e a atuação colaborativa das unidades do órgão;

II - Contribuir para a efetividade das disposições do Planejamento Estratégico e do Programa de Integridade;

III - Agregar valor à gestão e aperfeiçoar os controles internos do órgão;

IV - Subsidiar a tomada de decisões da alta gestão da CGE e dos Comitês integrantes da sua estrutura de governança;

V - Considerar a relação custo/benefício dos controles e a realidade operacional das unidades;

VI - Ser objetiva, transparente e contínua;

VII - Ser alinhada aos padrões de integridade e apetite a riscos do órgão;

VIII - Fomentar a inovação, a visão de futuro e a atuação integrada das unidades;

IX - Estimular a padronização técnica de atividades;

X - Integrar as ações e os processos do órgão, promovendo a sua melhoria contínua.

3. DIRETRIZES PARA A GESTÃO DE RISCOS

As diretrizes para o estabelecimento de uma gestão de riscos buscam definir as orientações aos órgãos e entidades no processo de identificação, análise, avaliação, tratamento, monitoramento e comunicação dos riscos, associados às suas operações e objetivos. Elas visam promover uma cultura de gestão de riscos que ajude a proteger e a criar valor para as partes interessadas.

No caso da CGE, as diretrizes para a gestão de riscos incluem:

I - Apoio inequívoco e comprometimento da alta administração;

II - Suporte da estrutura de governança do órgão;

III - Implementação gradual e integração metodológica;

IV - Atuação articulada das instâncias de gestão de riscos;

V - Definição de alçadas e agentes responsáveis;

VI - Melhoria contínua e acompanhamento dos níveis de maturidade do órgão;

VII - Análise do contexto interno e externo, com a identificação precisa dos critérios de fato e de direito aplicáveis ao processo de gestão de riscos;

VIII - Identificação das causas e consequências dos eventos de riscos, bem como seu impacto e probabilidade;

IX - Análise dos níveis de risco;

X - Avaliação do objeto conforme critérios técnicos previamente estabelecidos, com o escopo de aferir se determinado risco é aceitável;

XI - Elaboração de planos de ação para tratamento dos riscos;

XII - Monitoramento, comunicação e revisão periódicos.

4. OBJETIVOS DA GESTÃO DE RISCOS

Segundo previsto na Resolução CGE nº 17/2023, a gestão de riscos integra a estratégia gerencial da CGE e deve contribuir para o alcance de seu propósito, de sua missão e de seus objetivos organizacionais. Nesse sentido, todas as unidades e níveis hierárquicos, assim como seus processos de trabalho devem observar as disposições da Política de Gestão de Riscos, que tem como objetivos:

I - Identificar os eventos de risco de processos da CGE, viabilizando a atuação assertiva dos responsáveis pelo seu tratamento;

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

III - Adequar os controles internos ao tratamento dos riscos;

IV - Resguardar a integridade dos processos;

V - Incrementar a eficiência da gestão;

VI - Identificar oportunidades e ameaças;

VII - Aperfeiçoar os mecanismos de governança e *accountability*;

VIII - Fundamentar tecnicamente a tomada de decisões da gestão;

IX - Promover a modernização e conferir maior eficácia aos controles internos do órgão.

5. INSTÂNCIAS E RESPONSABILIDADES DA GESTÃO DE RISCOS

A norma ISO 31000/2018 ressalta a importância da Alta Administração assegurar a atribuição das instâncias e responsabilidades vinculadas à gestão de risco a todos as autoridades pertinentes, com a comunicação e divulgação em todos os níveis da organização.

A gestão de riscos da CGE apresenta as seguintes instâncias:

I - Comitê Estratégico de Governança (CEG);

II - Comitê de Governança, Integridade, Riscos e Controles (CGIRC);

III - Assessoria Estratégica e de Gestão de Riscos (AEGRI);

IV - Unidades da estrutura orgânica da CGE;

V - Gestores de Riscos das unidades da CGE.

São competências do Comitê Estratégico de Governança (CEG):

I - Aprovar a política de gestão de riscos da CGE e suas revisões;

II - Estabelecer estratégias para a implementação da gestão de riscos na CGE;

III - Determinar as tipologias de riscos que serão objeto de atuação da CGE;

IV - Aprovar a declaração de apetite a riscos da CGE e suas revisões periódicas;

V - Aprovar a metodologia de gestão de riscos e suas revisões;

VI – Realizar, em nível estratégico, o monitoramento da evolução dos riscos dos processos, bem como da efetividade dos planos de ação;

VII – Aprovar os portfólios de riscos e os Planos de Ação para gestão de riscos;

VIII - Avaliar o desempenho da gestão de riscos da CGE, com o escopo de promover o seu aperfeiçoamento;

IX - Promover ações de aderência à cultura do gerenciamento de riscos, em articulação com a Assessoria Estratégica e de Gestão de Riscos (AEGRI) e Comitê de Governança, Integridade, Riscos e Controles (CGIRC);

X - Zelar pelo alinhamento da gestão de riscos aos escopos do Planejamento Estratégico e do Programa de Integridade;

XI - Realizar a supervisão das demais instâncias de gestão de riscos da CGE;

XII - Disponibilizar, no que couber, recursos tecnológicos, financeiros e humanos para a efetividade da política de gestão de riscos.

Ressalta-se, no entanto, que o Controlador-Geral poderá, justificadamente, adotar, modificar ou recusar os entendimentos emitidos pelo CEG.

Já ao Comitê de Governança, Integridade, Riscos e Controles (CGIRC) compete desenvolver ações para o Programa de Integridade da CGE com o escopo de mitigar riscos à integridade. Adicionalmente, o comitê será responsável por disseminar a cultura de gestão de riscos no órgão. Destaca-se que o Programa de Integridade da CGE observará metodologia da Subcontroladoria de Transparência, Integridade e Controle Social para a identificação de riscos à integridade, desenvolvida especificamente para subsidiar a elaboração de Programas de Integridade. A Assessoria Estratégica e de Gestão de Riscos (AEGRI), por seu turno, tem como competências no processo de gestão de riscos da CGE:

I - Propor metodologia de gestão de riscos da CGE e suas revisões, em conjunto com a Auditoria-Geral;

II - Propor as funcionalidades necessárias para o sistema eletrônico de gerenciamento de riscos, em conjunto com a Auditoria-Geral;

III - Realizar o monitoramento da evolução dos processos e acompanhar a implementação dos planos de ação;

IV - Consolidar os resultados das unidades da CGE em relatórios gerenciais e encaminhá-los ao Presidente do CEG;

V - Realizar capacitações em gestão de riscos para o corpo funcional da CGE;

VI - Elaborar Plano de Comunicação de Gestão de Riscos, em articulação com a Assessoria de Comunicação Social;

VII - Monitorar o desempenho da gestão de riscos, com o escopo de promover o seu aperfeiçoamento;

VIII - Propor ao CEG indicadores de desempenho para gestão de riscos e modificações na declaração de apetite a riscos;

IX - Requisitar aos gestores de risco e às unidades da estrutura orgânica da CGE as informações necessárias para a realização de relatórios gerenciais, para as atividades de monitoramento, consolidação de informações e demais atividades relativas à gestão de riscos.

De outro modo, considera-se como proprietários dos riscos os dirigentes das unidades da estrutura orgânica da CGE nas quais os processos são desenvolvidos. Suas competências são:

I - Escolher os processos que terão os seus riscos gerenciados e tratados, considerando as prioridades da unidade e os efeitos negativos que os riscos possam causar;

II - Definir os níveis de risco aceitáveis, considerando a declaração de apetite a riscos do órgão;

III - Decidir quais riscos devem ter o seu tratamento priorizado;

IV - Elaborar planos de ação para tratamento dos riscos, em conjunto com os gestores de risco da unidade e avaliar os resultados obtidos;

V - Encaminhar à Assessoria Estratégica e de Gestão de Riscos a indicação de pelo menos 02 (dois) gestores de risco para a respectiva unidade.

Os gestores de riscos, por sua vez, devem orientar e realizar as etapas de levantamento, análise, avaliação, revisão, implementação e comunicação dos planos de ação para tratamento dos riscos dos processos das respectivas unidades administrativas as quais se vinculam. Suas indicações serão aprovadas por ato normativo do dirigente máximo da CGE ou a quem ele delegar e suas competências consistem em:

I – Levantar os riscos dos processos da respectiva unidade, realizando a sua análise, avaliação e revisão;

II - Elaborar os planos de ação para o tratamento dos riscos, observada a metodologia da CGE;

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

IV - Comunicar à Assessoria Estratégica e de Gestão de Riscos as mudanças significativas em seus processos;

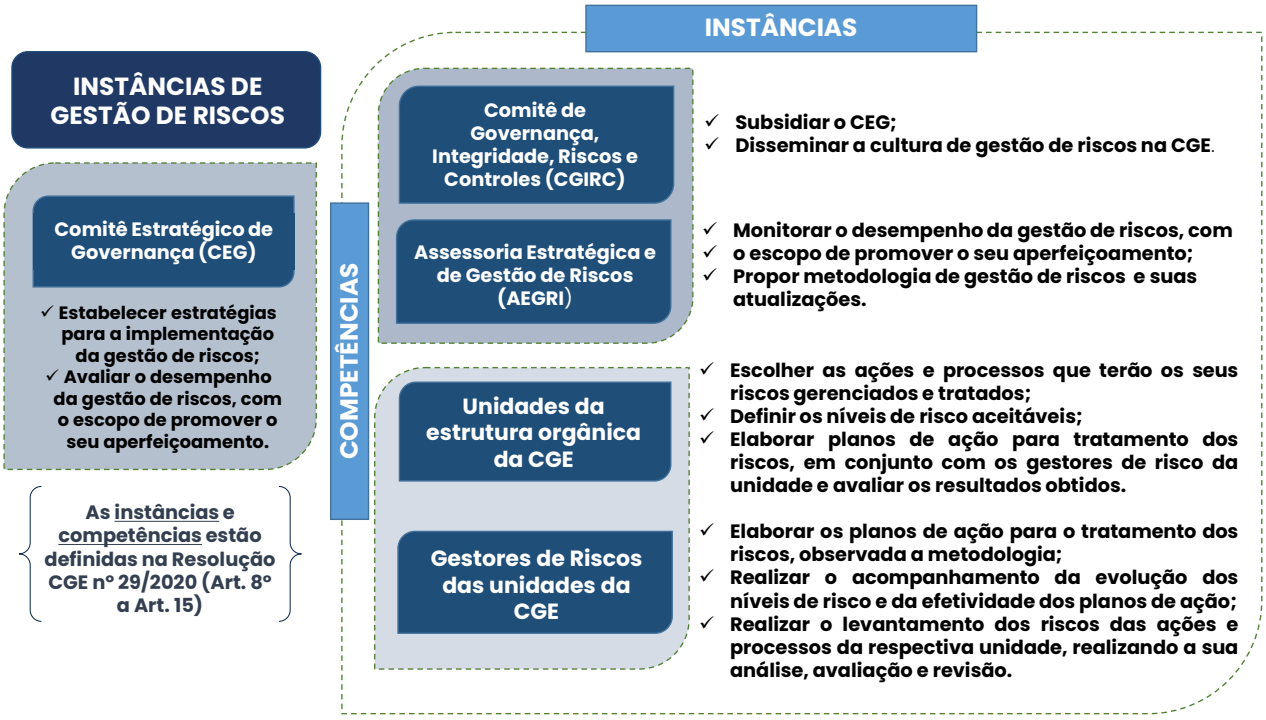
V - Responder as requisições da Assessoria Estratégica e de Gestão de Riscos;

VI - Disponibilizar as informações relativas à gestão de riscos dos processos sob sua responsabilidade aos comitês da estrutura de governança da CGE.

Adicionalmente, todo o corpo funcional da CGE é responsável por realizar o monitoramento da evolução dos níveis de risco e da efetividade dos planos de ação referentes aos processos nos quais estiverem envolvidos ou que tiverem conhecimento. Nesse sentido, os agentes públicos devem reportar ao gestor de risco de sua respectiva unidade administrativa qualquer fragilidade ou necessidade de aperfeiçoamento identificadas nos processos ou controles adotados.

Por fim, salienta-se que o Comitê Estratégico de Governança (CEG), Comitê de Governança, Integridade, Riscos e Controles (CGIRC), Assessoria Estratégica e de Gestão de Riscos (AEGRI), os proprietários dos riscos e os gestores de risco manterão fluxo regular de informações entre si. A seguir, evidencia-se a representação gráfica das instâncias de gestão de riscos da CGE e suas principais competências:

Figura 1 - Instâncias de gestão de riscos da CGE e suas principais competências



Fonte: Elaboração própria.

6. PROCEDIMENTOS OPERACIONAIS DA GESTÃO DE RISCOS

De acordo com o estabelecido na Resolução CGE nº 17/2023, os procedimentos operacionais, atribuições complementares e fluxos concernentes à gestão de riscos da CGE serão estabelecidos em metodologia proposta pela Assessoria Estratégica e de Gestão de Riscos (AEGRI) e aprovada pelo Comitê Estratégico de Governança (CEG).

A metodologia compreenderá, no mínimo, as seguintes fases:

I - Conhecer o ambiente interno e externo e os objetivos organizacionais: essa fase é caracterizada pela identificação dos fundamentos e dos objetivos relativos ao processo, bem como pela definição dos contextos interno e externo que serão considerados na gestão de riscos;

II - Definir o apetite a riscos: a definição do apetite a riscos será realizada pelo Comitê Estratégico de Governança (CEG), constituindo premissa de observância cogente às instâncias responsáveis pela gestão de riscos;

III - Identificar e analisar os riscos: fase em que são levantados os riscos relativos aos processos do órgão, bem como suas causas e consequências;

IV - Avaliar os Riscos: fase em que são determinados os níveis dos riscos levantados. A severidade dos riscos será aferida a partir de critérios de impacto e probabilidade;

V - Tratar os Riscos: fase em que são definidas as respostas aos riscos, com a elaboração de Planos de Ação com o escopo de manter a aderência dos níveis de risco aos ditames da Declaração de Apetite a Riscos do órgão;

VI - Comunicar e Monitorar os Riscos: deve ocorrer em todas as fases do processo, caracterizada pelo intercâmbio de informações entre as instâncias de gestão de riscos, viabilizando a melhoria contínua e evolução da maturidade do órgão.

Salienta-se que os processos da CGE poderão ser agrupados em macroprocessos para fins de aplicação da metodologia para gestão de riscos.

7. PROCESSO DE GESTÃO DE RISCOS

O processo de gestão de riscos é aplicável a ampla gama das atividades da organização em todos os níveis, incluindo estratégias, decisões, operações, processos, funções, projetos, produtos, serviços e ativos, e é suportado pela cultura e pela estrutura (ambiente) de gestão de riscos da organização (TCU, 2017).

Nesse contexto, são fases do ciclo de gestão de riscos da CGE:

Figura 2 - Ciclo de Gestão de Riscos

Fonte: Elaboração própria.

7.1. Conhecer o Ambiente e os Objetivos Organizacionais

Para a gestão dos riscos de macroprocessos/processos, é desejável que o primeiro passo consista em seu mapeamento. Deste modo, identifica-se o fluxo de todas as atividades realizadas e os pontos de decisão existentes no macroprocesso/processo em análise. Conhecer o fluxo do macroprocesso/processo permite obter uma visão sistêmica de seus objetivos, evidenciar gargalos e fragilidades, conhecer as relações existentes entre os diversos setores envolvidos no fluxo, reduzir falhas, melhorar a comunicação e a integração entre os diversos processos da organização, além de permitir a propositura de melhorias para sua otimização.

O conhecimento do macroprocesso/processo é indispensável para a evidenciação dos riscos que podem impactar seu desempenho e, até mesmo, o da organização. Dessa forma, independentemente da realização de mapeamento macroprocesso/processo, deve-se conhecer o ambiente e seus objetivos, de maneira a se obter uma visão sistêmica deste. Caso já exista um mapeamento, deve-se validá-lo a fim de garantir que os riscos sejam identificados com base em seu fluxo real e atual.

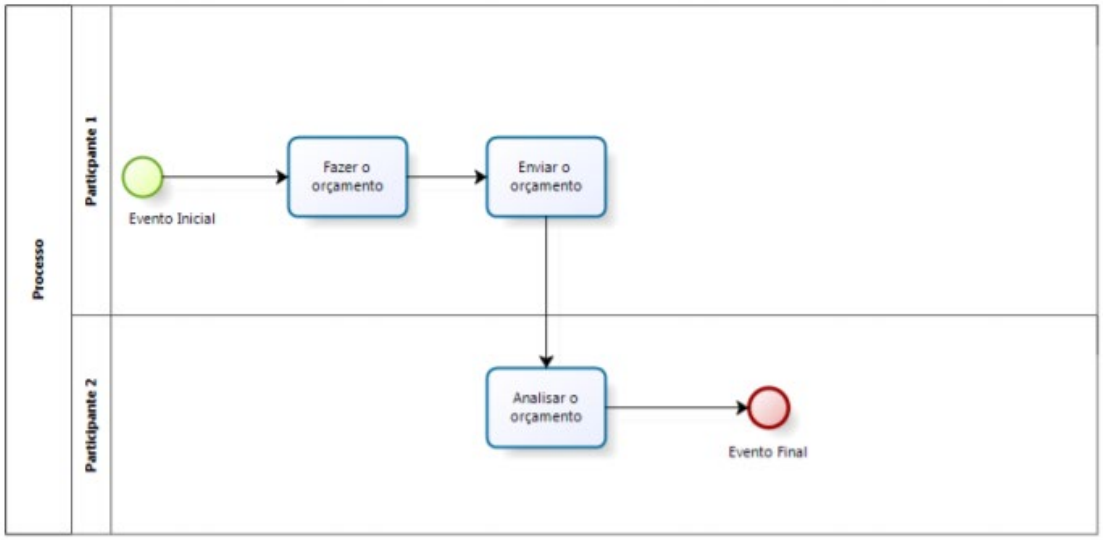
A Controladoria-Geral do Estado sugere a elaboração do mapeamento dos macroprocessos/processos por meio da utilização das técnicas: 5W2H (*Who, Where, Why, What, When, How much and How*), em português, Quem, O Que, Quando, Quanto, Por quê, Onde e Como; bem como "*Business Process Modeling Notation* – BPMN", ou seja, Notação para Mapeamento de Processos de Trabalho.

A técnica 5W2H é uma dentre as recomendadas pela literatura para a realização das etapas de análise e melhoria de processos (Madureira, Ferreira e Souza, 2006). O BPMN, por sua vez e conforme literatura, é a metodologia mais completa e mais utilizada atualmente, segundo Silva (2014, p. 33) *apud* Capote (2011).

O BPMN consiste em "(...) uma notação gráfica, padronizada internacionalmente, de modelagem de processos desenvolvida pela *Business Process Management Initiative* (BPMI), no *Object Management Group* (OMG)."

(SECRETARIA DE ESTADO DE PLANEJAMENTO E GESTÃO, 2013, p. 41), conforme figura a seguir. Para tanto, utiliza-se o *software* denominado "*Bizagi Process Modeler*".

Figura 3 – Modelagem BPNM



Fonte: UFMG. Guia Simplificado de Boas Práticas em Modelagem de Processos com BPMN. Disponível em: https://www.ufmg.br/dti/wp-content/uploads/2019/01/POP-0001-ANEXO-A-Guia-simplificado-de-boas-praticas-em-modelagem.pdf.

Além disso, pode ser aplicada a técnica denominada Matriz RECI[1].

Posteriormente, as ações devem ser validados pelos gestores, a fim de ratificar as informações prestadas. Nesse contexto, a partir da realização do mapeamento dos macroprocessos/processos, caso existente, é possível identificar os seguintes itens:

[1] A análise RECI trata-se de uma ferramenta que auxilia a identificar quem é responsável pelas atividades desenvolvidas, quem as executa, quem é consultado e quem é informado (TCU, 2001).

- ✓ Unidades administrativas em que o macroprocesso/processo é realizado;
- ✓ Nome e responsável pelo macroprocesso/processo;
- ✓ Objetivo estratégico o qual o macroprocesso/processo está vinculado;
- ✓ Atividades críticas do macroprocesso/processo;
- ✓ Sequência de atividades executadas no macroprocesso/processo;
- ✓ Responsáveis pela execução das atividades;
- ✓ Prazos e datas de realização das atividades;
- ✓ Local de realização das atividades;
- ✓ Justificativa para a realização das atividades;
- ✓ Procedimento realizado para a execução das atividades.

Releva dizer que a análise do fluxo processual permite evidenciar, caso existam, falhas na execução do macroprocesso/processo e oportunidades de melhoria no fluxo, a exemplo de: atrasos no processamento das atividades; indisponibilidade de documentos necessários à continuidade do fluxo; ociosidade ou deficiência de recursos humanos; retrabalho; falhas de comunicação; multiplicidade de instâncias de aprovação; falhas e erros; sobreposição de tarefas; e tempo de execução incompatível com a complexidade da atividade.

7.2. Definir o Apetite a Riscos

Apetite a riscos é a quantidade de risco que a organização deseja assumir para conseguir atingir seus objetivos (Brasiliano, 2018). Assim, o tipo e a quantidade de riscos que em conjunto a instituição está preparada para buscar, assumir ou reter correspondem à sua atitude perante o risco, refletem toda sua filosofia e influenciam sua cultura e estilo gerencial (COSO, 2007b, p. 20; ABNT, 2009, p. 2 *apud* Vieira e Barreto, 2019).

O apetite a riscos relaciona-se diretamente à estratégia organizacional, dirige o alinhamento entre pessoas e processos internos e orienta a alocação de recursos. Nesse contexto, o alinhamento do nível aceitável de variação em relação às metas previstas para o cumprimento dos objetivos de uma organização define a tolerância à riscos, ou seja, o desvio do nível do apetite a riscos (Brasiliano, 2023). Segundo este autor, a tolerância a risco refere-se a um alerta para evitar que a organização coloque em perigo a continuidade de seus negócios.

Em resumo, o apetite a riscos está mais relacionado à estratégia e à determinação do nível ideal de exposição ao risco para alcançar objetivos, enquanto a tolerância a riscos está mais relacionada à capacidade operacional de suportar e gerenciar os riscos dentro de limites predefinidos. Ambos os conceitos são cruciais para uma gestão eficaz de riscos em uma organização, pois ajudam a equilibrar a busca por oportunidades com a capacidade de lidar com as incertezas e ameaças.

Vieira e Barreto (2019, p. 141) afirmam que “É importante que o apetite a riscos seja estabelecido no início do processo de gerenciamento de riscos para que regras de avaliação possam ser claramente definidas”. Sendo assim, nesse momento, a organização deve elaborar sua Declaração de Apetite a Riscos, a qual deve ser aprovada por uma instância de supervisão da Alta Gestão, a exemplo de Comitês de Governança Participativa.

Releva dizer que o apetite a riscos é dinâmico, podendo ser modificado de acordo com o contexto e situação percebida em um dado momento. Nesse sentido, é possível que uma determinada organização adapte suas estratégias de gerenciamento de risco de acordo com as características e necessidades específicas de cada processo.

A diferenciação do apetite ao risco permite que a organização concentre seus recursos e esforços de gerenciamento de riscos nas áreas consideradas mais críticas ou estratégicas. Isso garante que os recursos sejam alocados de forma eficiente, priorizando a proteção dos aspectos mais importantes para o alcance dos objetivos organizacionais. Na Controladoria-Geral, o apetite a riscos foi aprovado pelo Comitê Estratégico de Governança e consiste em ato contínuo,

atualmente oficializado pela Resolução CGE nº 16/2023, de 12 de dezembro de 2023:

Figura 4 – Declaração de Apetite a Riscos da CGE

Fonte: Elaboração própria.

Consoante a referida Resolução, a Declaração de Apetite a Riscos é um importante instrumento que sintetiza a cultura de risco e direciona o planejamento estratégico da Controladoria-Geral, norteando os demais planos e permitindo que a Alta Administração otimize a alocação de recursos orçamentários, humanos e tecnológicos, dentre outros.

São elementos da Declaração da CGE: propósito da organização; tipos e níveis de risco dispostos a admitir na realização das atividades e objetivos organizacionais; período de revisão do apetite; unidades administrativas responsáveis por sua revisão e monitoramento; indicadores de monitoramento por tipo de risco; ações mitigadoras por tipo de risco; nível de maturidade em riscos da organização; nível de apetite a riscos e tolerância a riscos por tipo de risco.

A declaração apresenta os seguintes indicadores de monitoramento por tipo de risco definido:

- ✓ Risco Estratégico: Aprovação/Revisão bienal do Planejamento Estratégico e Monitoramento da execução do Planejamento Estratégico;
- ✓ Risco Operacional: Proteção a *ciberataque* e Proteção de dados pessoais;
- ✓ Risco Orçamentário: Monitoramento da despesa;
- ✓ Risco Reputacional: CGE na mídia;
- ✓ Risco de Integridade: Aplicação de penalidades, Monitoramento do Plano de Integridade e Revisão do Plano de Integridade ou elaboração de novo Programa de Integridade;
- ✓ Risco de Conformidade: Conformidade legal.

Salienta-se que tanto o Apetite a Riscos como a Tolerância a Riscos são acompanhados pelo Comitê Estratégico de Governança e monitorados permanentemente pela Alta Administração e pela Assessoria Estratégica e de Gestão de Riscos.

A Controladoria-Geral é conservadora em seu apetite a riscos e, portanto, tem um baixo apetite em todas as categorias de riscos consideradas.

7.3. Identificar os Riscos na Execução

Nessa etapa, devem ser identificados os eventos em potencial que, caso ocorram, afetarão o desenvolvimento do macroprocesso/processo, a entrega dos produtos e o atingimento dos objetivos. De acordo com a ISO 31000/2018, na identificação dos riscos é recomendado que a organização:

> Identifique as fontes de riscos, áreas de impacto, eventos (incluindo mudanças nas circunstâncias) e suas causas e consequências potenciais. A finalidade desta etapa é gerar uma lista abrangente de riscos baseada nestes eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos (ISO 31000/2018, p. 12).

A norma ISO 31010/12 apresenta diversas técnicas de identificação de riscos. A escolha da técnica ou do conjunto de técnicas apropriados depende do grau de maturidade em gestão de riscos da organização, da filosofia de gestão, do porte, do volume de recursos envolvidos e da natureza dos objetivos (Souza e Santos, 2019). Dentre as ferramentas e técnicas disponíveis, pode-se citar: *Brainstorming*, Matriz SWOT, Diagrama de *Ishikawa* e Método *Bow Tie*, conforme figuras a seguir:

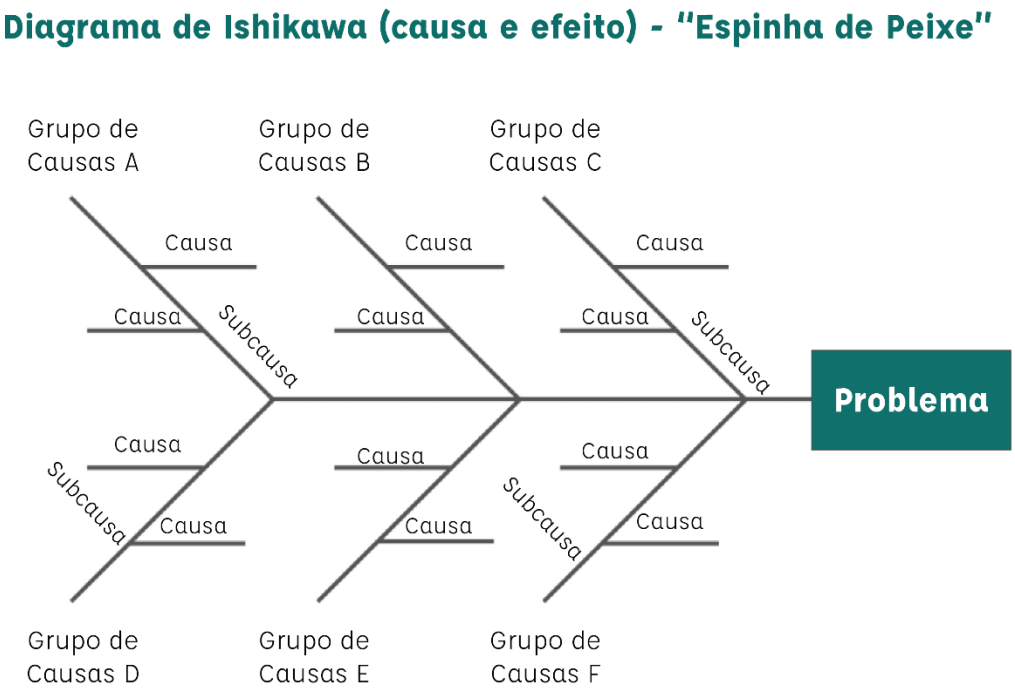
Figura 5 - Brainstorming

Fonte: Freepik.

Figura 6 - Matriz SWOT

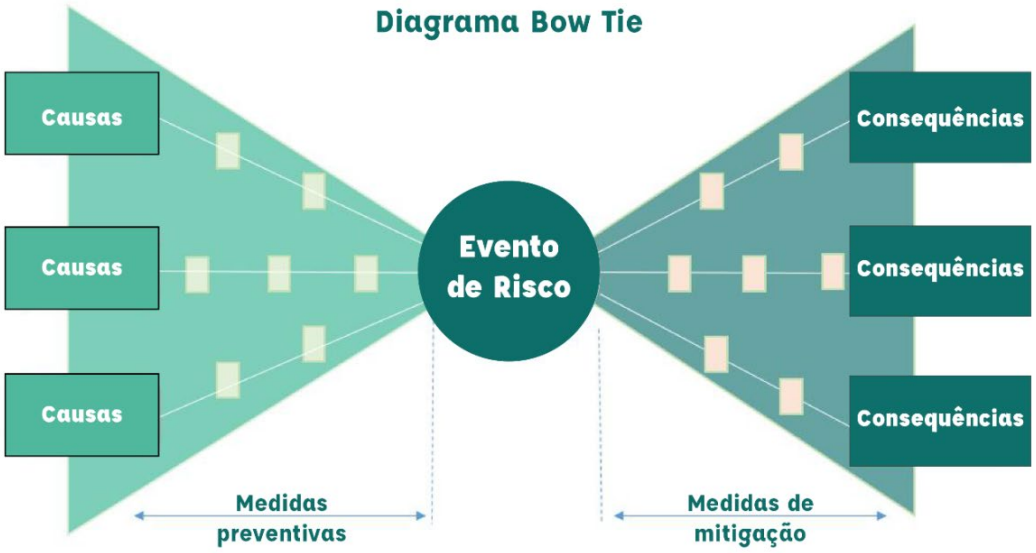
Fonte: Elaboração própria.

Figura 7 – Diagrama de *Ishikawa*



Fonte: Elaboração própria.

Figura 8 - Método *Bow Tie*



Fonte: Ministério do Planejamento, Desenvolvimento e Gestão. *Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão*, p. 28, 2017. Figura adaptada

Na Controladoria-Geral do Estado, comumente são realizadas reuniões de *brainstorming* com os gestores, juntamente com aplicação da Matriz SWOT, a fim de identificar as fragilidades do macroprocesso/processo e avaliar o cenário. Este é avaliado sobretudo quanto às fraquezas e ameaças, conectando posteriormente as fragilidades identificadas às causas dos eventos de riscos levantados.

Releva dizer que entre os aspectos considerados para a compreensão do ambiente interno, sobressaem-se os organizacionais (políticas, estrutura, estratégias, rede de comunicação, regras etc.), de pessoal (treinamentos, sistemas de incentivo, de avaliação de desempenho etc.) e de produção (eficiência dos processos operacionais e uso de tecnologia, entre outros).

O conhecimento do ambiente externo, por sua vez, envolve a percepção de fatores econômicos, sociais, políticos, legais, tecnológicos, climáticos etc. (macro ambiente), bem como forças exercidas pelos clientes, pelos fornecedores e demais atores envolvidos.

Outro aspecto importante refere-se à incerteza, que constitui o primeiro requisito do risco. Assim, para que um acontecimento seja considerado um risco, deve ser possível e de ocorrência indeterminada. Se um evento for impossível, deixa de ser um risco (exemplo: volta ao mundo em um segundo). Por outro lado, se um determinado evento for possível e plenamente previsível, isto é, de ocorrência certa, deixará de ser considerado um risco (exemplo: o sol nasce pelas manhãs).

Ademais, não há que se falar em risco se sua ocorrência for irrelevante, ou seja, se não houver efeito sobre determinada atividade ou procedimento, por inexistir ameaça ao alcance de um objetivo. Logo, a ocorrência de uma avalanche nos Alpes não traz implicações para a produção de soja no Brasil, por ser irrelevante e não constituir risco ao empreendimento.

Diante do exposto, verifica-se que o risco consiste no “(...) efeito que a incerteza tem sobre os objetivos da organização. É a possibilidade de ocorrência de eventos que afetem a realização ou alcance dos objetivos, combinada com o impacto dessa ocorrência sobre os resultados pretendidos” (TCU *apud* VIEIRA e BARRETO, 2019, p.98). Nesse sentido, se refere a um evento ou uma

condição incerta que, se ocorrer, terá um efeito negativo na execução do macroprocesso/processo.

Destaca-se que na Controladoria-Geral do Estado são realizados encontros periódicos com os proprietários dos riscos e com os gestores de riscos para auxiliá-los na identificação dos riscos relevantes (núcleo ou eventos de riscos), assim como dos controles adotados em cada atividade do macroprocesso/processo.

Os controles são um conjunto de políticas, normas “(...) e procedimentos que ocorrem em toda a organização para autorizar, verificar, reconciliar e revisar o desempenho”. Referem-se a “(...) qualquer processo, política, dispositivo, prática ou ação e medida adotada pela gestão” (...) com a finalidade de alcançar os objetivos organizacionais e proporcionar confiança no que diz respeito à eficácia e eficiência dos recursos, através da minimização dos riscos relevantes (VIEIRA e BARRETO, 2019, p.143).

Do ponto de vista da gestão de riscos, podemos classificá-los em controles preventivos e controles contingenciais. O controle preventivo é um conjunto de medidas e procedimentos adotados antecipadamente para evitar a ocorrência de falhas, erros ou fraudes nos processos governamentais. O objetivo principal do controle preventivo é identificar e mitigar os riscos antes que eles se concretizem, minimizando possíveis impactos negativos.

O controle contingencial refere-se às medidas e ações planejadas para lidar com eventos de riscos ocorridos e que podem impactar negativamente nos objetivos de uma organização. O objetivo do controle contingencial é estabelecer planos de contingência eficazes para responder rapidamente a situações imprevistas e minimizar danos ou impactos negativos.

Em resumo, a combinação de controles preventivos e contingenciais é fundamental para uma abordagem abrangente de gestão de riscos em organizações governamentais. Enquanto os controles preventivos buscam evitar problemas antes que ocorram, os controles contingenciais estão prontos para responder eficientemente caso ocorram eventos adversos. Essa abordagem ajuda a garantir a resiliência e a eficiência dos processos governamentais.

Cabe destacar que o objetivo da avaliação dos controles é servir como subsidio para a etapa de avaliação dos riscos, isto é, na prática seu resultado ajuda a definir o peso da probabilidade e impacto daquele risco.

A avaliação dos controles utilizada na CGE consta a seguir:

Tabela 1 – Avaliação dos Controles

Descrição	Classificação
Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco	Forte
Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente	Satisfatório
Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas	Mediano
Controles têm abordagens *ad hoc* (provisórias/pontuais), tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas	Fraco
Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais	Inexistente

Fonte: Elaboração própria.

Nessa etapa, os gestores passam a detalhar os eventos de riscos no trinômio (causa/evento/consequência), conforme figura a seguir. Assim, para

cada causa ou consequência diferentes apresentadas para o evento, tem-se a formação do trinômio do risco.

Figura 9 - Trinômio de Risco

Fonte: Elaboração própria.

A causa consiste na fonte do risco ou vulnerabilidade existente na organização que dá origem a um evento. Em outras palavras, é um fato ou circunstância que influencia de forma direta ou intrínseca a ocorrência do evento, o porquê do risco.

Por outro lado, nos termos da norma ABNT NBR ISO 31000:2018, evento é a ocorrência ou mudança em um conjunto específico de circunstâncias. O evento pode consistir em uma ou mais ocorrências e ter diversas causas. Ademais, é possível relacionar-se a algo que não irá acontecer, entretanto, não deve ser simplesmente o não alcance do objetivo da atividade.

A consequência, por sua vez, diz respeito ao efeito que o evento de risco terá sobre o alcance dos objetivos organizacionais. Salienta-se que deve ser mais próxima possível da atividade correspondente.

Portanto, cada evento, combinado com determinada causa e consequência específica, traduz-se em um risco individual. O risco identificado denomina-se risco residual, que “(...) é aquele que ainda permanece após a resposta da administração. É o risco remanescente após a implementação de atividades de controle que visam reduzir sua probabilidade e/ou impacto” (BRASILIANO, 2018, p. 160).

7.4. Analisar os Riscos

De acordo com Vieira e Barreto (2019, p. 132), a análise de riscos consiste em:

> (...) processo que permite compreender a natureza e determinar o nível de risco, de modo a subsidiar a sua avaliação e eventual tratamento. A análise de riscos é uma função da probabilidade de ocorrência e do impacto das consequências. Ou seja, o nível do risco é expresso pela combinação da probabilidade de ocorrência do evento e das consequências resultantes no caso de materialização do evento, o impacto nos objetivos. O resultado final desse processo será o de atribuir a cada risco identificado uma classificação, tanto para a probabilidade quanto para o impacto do evento, cuja combinação determinará o nível do risco. A função risco é fundamentalmente um produto das variáveis probabilidade e impacto.

O TCU (2018), por sua vez, afirma que a análise de riscos "Compreende o reconhecimento e a descrição dos riscos relacionados aos objetivos/resultados de um objeto de gestão de riscos, envolvendo a identificação de possíveis fontes de riscos." (TCU, 2018, p. 22)

Nesse contexto, probabilidade é o peso selecionado de acordo com a frequência estimada de ocorrência do risco. O impacto consiste no peso selecionado de acordo com a ocorrência identificada. Já o valor do risco é uma função tanto da probabilidade quanto da medida do impacto a ele vinculado. A metodologia proposta pela CGE para aferição do risco consiste na seguinte equação:

Equação 1 - Determinação do risco

$$R = P \times I$$

Em que:

R= risco

P= Probabilidade

I = Impacto

Para o valor a ser registrado como probabilidade, deve-se atribuir o peso conforme a frequência esperada para o evento de risco (Tabela 2). Assim, a probabilidade do risco acontecer corresponde à probabilidade do evento ocorrer.

Tabela 2 - Pesos da Probabilidade

Descrição	Peso
Evento praticamente certo (de 100 vezes, acontece mais de 90 vezes)	5
Evento provável (de 100 vezes, acontece mais de 75 e menos que 90 vezes)	4
Evento possível (de 100 vezes, acontece mais de 40 e menos que 75 vezes)	3
Evento remoto (de 100 vezes, acontece mais de 10 e menos que 40 vezes)	2
Evento raro (de 100 vezes, acontece de 1 a 10 vezes)	1

Fonte: Elaboração própria.

De outro modo, para mensurar o impacto, deve-se atribuir o peso segundo o grau de efeito que o evento apresenta nas ações de gestão da organização, de acordo com o propósito para o qual foram criadas. Para uma determinada instituição, o risco de imagem pode representar a maior preocupação do gestor, enquanto para outra o risco orçamentário seria o mais importante. Nesse sentido, o gestor deve definir a categoria predominante do risco, conforme tabela a seguir:

Tabela 3 - Categorias de Impacto

Categoria de Impacto	Definição
Estratégico	Decisões que podem afetar negativamente o alcance dos objetivos da organização
Integridade	Práticas de corrupção, desvios éticos e de conduta destoantes dos valores e padrões preconizados pela organização
Operacional	Perdas resultantes de falhas, deficiências ou inadequação de processos internos, estrutura, pessoas, sistemas, tecnologia, assim como de eventos externos
Imagem/ Reputação	Comprometimento da confiança da sociedade em relação à capacidade da organização em cumprir sua missão institucional e interferência direta na imagem da organização
Orçamentário/ Financeiro	Comprometimento dos recursos orçamentários e financeiros necessários à realização das atividades da organização
Comunicação	Eventos que podem impedir ou dificultar a disponibilidade de informações para a tomada de decisões e para o cumprimento das obrigações de prestação de contas às instâncias controladoras e à sociedade
Conformidade/ Legal	Não cumprimento de princípios constitucionais, legislações específicas ou regulamentações externas aplicáveis ao negócio, bem como de normas e procedimentos internos

Fonte: Elaboração própria.

A tabela seguinte ilustra os pesos de impacto:

Tabela 4 - Pesos de Impacto

Descrição	Peso
O impacto compromete acentuadamente os objetivos da contratação e as ações de gestão, afetando aspectos financeiros, o cumprimento de prazos, a imagem/reputação e/ou a integridade	10
O impacto compromete os objetivos da contratação e as ações de gestão, afetando aspectos financeiros, o cumprimento de prazos e/ou a imagem/reputação	7
O impacto pode comprometer os objetivos da contratação e as ações de gestão, afetando aspectos financeiros e/ou cumprimento de prazos	5
O impacto é pouco relevante ao alcance dos objetivos da contratação e às ações de gestão	3
O impacto é mínimo no alcance dos objetivos da contratação e nas ações de gestão	1

Fonte: Elaboração própria.

Para cada risco identificado, atribuem-se os pesos de probabilidade e impacto, obtendo-se o risco residual.

Determinado o valor do risco residual, propõe-se a utilização da matriz de riscos (tabela 5), para classificar qualitativamente o valor do risco através da definição dos níveis de risco (tabela 6). Estes, por sua vez, especificam a partir de quais valores os riscos são considerados pequenos, moderados, altos e críticos.

Tabela 5 - Matriz de Riscos (Valor do Risco)

Matriz de Riscos						
Impacto	Muito Alto	5	15	35	35	50
	Alto	4	12	20	28	40
	Médio	3	9	15	21	30
	Baixo	2	6	10	14	20
	Muito Baixo	1	3	5	7	10
		Rara	Remota	Possível	Provável	Praticamente certa
		Probabilidade				

Fonte: Elaboração própria.

Tabela 6 - Nível de Severidade Padrão (Classificação do Risco)

NIVEL	VALOR	SÍMBOLO
CRÍTICO	MAIOR OU IGUAL A 28	
ALTO	MAIOR OU IGUAL A 10 E MENOR QUE 28	
MODERADO	MAIOR OU IGUAL A 5 E MENOR QUE 10	
PEQUENO	MENOR QUE A 5	

Fonte: Elaboração própria.

Nesse aspecto, cabe ressalvar que esse nível de severidade padrão do risco pode ser influenciado pelo percentual de tolerância ou pelo apetite ao risco da organização.

Vale ressaltar que esta metodologia não utiliza o conceito de risco inerente, o qual consiste no risco natural, próprio de uma atividade ou do processo, sem considerar qualquer ação que a organização possa realizar para alterar a probabilidade de sua ocorrência ou o impacto que ele provoque (Ministério da Transparência e Controladoria Geral da União – CGU, 2018). Nesse sentido, Brasiliano (2018) afirma que o risco inerente desconsidera a execução de controles para mitigá-lo.

Ademais, é importante dizer que para classificar os riscos residuais, determina-se a probabilidade e o impacto para todos os riscos identificados, por meio de reuniões periódicas com os gestores dos macroprocessos/processos, para identificação dos pesos de frequência da probabilidade e ofensividade do impacto.

Por fim, a partir do apetite a riscos inicialmente definido, a organização determinará quais riscos poderão ser aceitos e quais necessariamente deverão ser minimizados, conforme seção seguinte. Ressalta-se, no entanto, a obrigatoriedade, em tese, de tratamento dos riscos residuais críticos e altos, a fim de modificar sua classificação, tendo em vista o impacto destes no atingimento dos objetivos dos macroprocessos/processos/atividades.

7.5. Tratar os Riscos

O tratamento de riscos envolve a seleção de uma ou mais opções para modificar o nível do risco (a probabilidade ou o impacto) e a elaboração de planos de tratamento que, uma vez implementados, implicarão a introdução de novos controles ou a modificação dos existentes (TCU, 2017).

Formas de tratar riscos, não mutuamente exclusivas ou adequadas em todas as circunstâncias, incluem evitar, reduzir, transferir e aceitar o risco. Selecionar a opção mais adequada envolve equilibrar, de um lado, os custos e esforços de implementação e, de outro, os benefícios decorrentes. Deve-se

considerar a possibilidade de que novos riscos sejam introduzidos pelo tratamento e a existência de riscos cujo tratamento não seja economicamente justificável (INTOSAI *apud* TCU, 2017).

Nesse contexto, para o tratamento dos riscos, o gestor deve identificar e selecionar as respostas a riscos que os reduzam a patamares aceitáveis, de acordo com o seu apetite a riscos (tabelas 7 e 8). Os resultados de desempenho do tratamento, eficácia e eficiência dos controles aplicados, devem refletir na severidade minimizada dos riscos.

Tabela 7 - Nível de Risco x Apetite a Riscos

		Nível de Risco			
		Pequeno	Moderado	Alto	Crítico
Apetite a Riscos	Baixo	Aceitar	A critério	Tratar	Tratar
	Médio	Aceitar	Aceitar	Tratar	Tratar
	Alto	Aceitar	Aceitar	A critério	Tratar

Fonte: Elaboração própria.

Tabela 8 - Apetite a Riscos - Legenda

Apetite a Riscos – Legenda	
Baixo (Conservador)	A organização aceita a possibilidade de ocorrência de eventos de riscos baixos
Médio (Moderado)	A organização aceita a possibilidade de ocorrência de eventos de riscos baixo e moderados

Apetite a Riscos – Legenda	
Alto (Arrojado)	A organização aceita a possibilidade de ocorrência de eventos de riscos baixo, moderado e altos

Fonte: Elaboração própria.

As respostas a riscos dizem respeito aos controles internos (procedimentos e normas estabelecidas pelos órgãos/entidades) ajustados ou criados pelos gestores em um plano de ação com a função de cumprir com os objetivos organizacionais e proporcionar confiança no que diz respeito à eficácia e eficiência dos recursos, através da redução dos riscos relevantes. Os resultados do desempenho do tratamento, eficácia e eficiência dos controles aplicados, devem refletir na severidade minimizada dos riscos.

De modo geral, considera-se que os eventos de riscos situados nos quadrantes definidos como risco alto e risco crítico são indicativos de necessidade de controles mais rígidos, devido aos impactos que podem provocar no atingimento dos objetivos dos macroprocessos/processos, enquanto os riscos situados nos quadrantes de risco pequeno e moderado seriam um indicativo de controles mais moderados. Ressalta-se, também, que em alguns casos não haveria necessidade de implementar controles e/ou até retirar controles. Entretanto, o tipo de resposta poderá ser alterado, mediante justificativas apresentadas pelo gestor e aprovadas pelas instâncias de supervisão da Alta Gestão.

A seguir, apresentam-se os tipos de tratamento de riscos e os níveis de risco por apetite a riscos:

Figura 10 - Tipos de Tratamento de Riscos

EVITAR	Optar por não executar um processo ou atividade. Única forma de se eliminar totalmente o risco. Exemplo: gestão de projetos, quando a relação custo/benefício projetada está em perigo

ACEITAR	Assumir a possibilidade de ocorrência de um risco conscientemente. Aproveitar uma oportunidade. Exemplo: não é necessária nenhuma ação
MITIGAR/REDUZIR	Reduzir a probabilidade ou a consequência de um risco, em direção ao apetite a riscos da organização. Exemplos: monitoramento de cenários, a fim de se antecipar a eventuais mudanças no panorama político; elaboração de planos de contingência, com o objetivo de preparar a organização caso determinado cenário previsto se concretize
TRANSFERIR	Reduzir a probabilidade ou a consequência de um risco, transferindo ou compartilhando com outra organização. Exemplos: terceirização de atividades e contratação de seguros

Fonte: Ministério do Planejamento, Desenvolvimento e Gestão (2017) e Miranda (2017) adaptado CGE-MG.

O tratamento dos riscos, portanto, pressupõe a elaboração de um Plano de Ação, o qual estabelece o que será feito, qual controle será implementado ou aperfeiçoado, o cronograma de implementação, os custos e os responsáveis pelo acompanhamento.

7.6. Monitorar os Riscos

De acordo com a ISO 31000/18, o monitoramento é parte integrante e essencial da gestão de riscos, cuja finalidade é:

a) detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco e no próprio risco, que podem requerer revisão dos tratamentos atualmente adotados e suas prioridades, e levar à identificação de riscos emergentes;

b) obter informações adicionais para melhorar a política, a estrutura e o processo de gestão de riscos;

c) analisar eventos - incluindo os “quase incidentes”, mudanças, tendências, sucessos e fracassos e aprender com eles; e

d) garantir que os controles sejam eficazes e eficientes no desenho e na operação.

O monitoramento dos riscos de macroprocesos/processos fornece a informação atualizada e objetiva identificar fragilidades e possibilidades de melhorias, como aprimorar o fluxo do macroproceso/processo, bem como verificar o desempenho e eficiência do plano de ação, operacionalizado por meio dos controles implementados.

Salienta-se que os riscos mudam ao longo do tempo e devem ser monitorados para que a organização possa realizar os ajustes necessários. Ademais, é importante dizer que o monitoramento integra todo o processo de gerenciamento de riscos.

Na Controladoria-Geral, conforme dito anteriormente, compete à Assessoria Estratégica e de Gestão de Riscos realizar o monitoramento da evolução dos riscos e acompanhar a implementação dos planos de ação.

O Plano de Ação estabelece o que será feito (*What*), qual controle será implementado ou aperfeiçoado (*How*), a área responsável pela implementação (*Where*), o responsável pelo acompanhamento (*Who*), o custo (*How much*) e o cronograma de implementação (*When*).

O método 5W2H, muito utilizado na gestão de projetos, consiste em responder questões fundamentais: What (o que será feito), Why (por que será feito), Where (onde será feito), When (quando será feito), Who (quem fará), How (como será feito) e How much (quanto custará). A utilização das palavras em inglês no parêntese se dá devido à origem do método, que surgiu nos Estados Unidos. Além disso, manter as palavras em inglês ajuda na padronização e facilita a compreensão em ambientes internacionais ou multinacionais, onde o inglês é frequentemente utilizado como língua franca. Essa prática contribui para garantir uma comunicação clara e eficaz em contextos globalizados, onde a uniformidade na linguagem é essencial para o entendimento e execução das atividades planejadas.

7.7. Comunicar os Riscos

Durante todas as etapas ou atividades do processo de gestão de riscos deve haver uma efetiva comunicação informativa e consultiva entre a organização e as partes interessadas, internas e externas, para:

a) auxiliar a estabelecer o contexto apropriadamente e assegurar que as visões e percepções das partes interessadas, incluindo necessidades, suposições, conceitos e preocupações sejam identificadas, registradas e levadas em consideração;

b) auxiliar a assegurar que os riscos sejam identificados e analisados adequadamente, reunindo áreas diferentes de especialização;

c) garantir que todos os envolvidos estejam cientes de seus papéis e responsabilidades, e avalizem e apoiem o tratamento dos riscos. (TCU, 2017)

Nesse contexto, a organização usa canais de comunicação para suportar o gerenciamento de riscos, promover sua cultura e desempenho em toda a instituição. A comunicação deverá ser oportuna e adequada e deve ser entendida como um canal que movimenta as informações em todas as direções – dos superiores aos subordinados, e vice-versa.

8. CONSIDERAÇÕES FINAIS

É fundamental ressaltar a importância da aplicação da gestão de riscos nas organizações como parte essencial de um planejamento estratégico eficaz. Ao atuar preventivamente na identificação, avaliação e tratamento dos riscos, as empresas conseguem minimizar impactos negativos, potencializar oportunidades e garantir a sustentabilidade de seus negócios a longo prazo.

Vale ressaltar que a implementação eficaz da gestão de riscos não se trata apenas de adotar ferramentas e técnicas, é, sobretudo, um processo de mudança de cultura organizacional.

Nesse contexto, a participação ativa e comprometida da Alta Gestão se torna fundamental para o sucesso da implementação da gestão de riscos. É por meio do envolvimento e apoio da liderança que se promove a integração dos princípios de gestão de riscos em todos os níveis da organização, criando uma cultura de segurança, transparência e responsabilidade.

A atuação proativa da Alta Gestão no fomento de boas práticas de gestão de riscos não apenas fortalece a resiliência da empresa, mas também demonstra o comprometimento com a excelência operacional e a criação de valor sustentável para a organização como um todo.

9. GLOSSÁRIO

➞ *Accountability*: Trata-se do 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;

➞ Análise RECI: Ferramenta que auxilia a identificar quem é responsável pelas atividades desenvolvidas, quem as executa, quem é consultado e quem é informado (TCU, 2001);

➞ Análise SWOT: Ferramenta utilizada para fazer análise de cenário (ou análise de ambiente). Divide-se em *Strengths* (forças), *Weaknesses* (fraquezas), *Opportunities* (oportunidades) e *Threats* (ameaças). O Ambiente interno da organização é integrado por suas Forças e Fraquezas e o Ambiente externo é composto pelas Oportunidades e Ameaças;

- Força: característica interna, controlável pela gestão, que representa uma facilidade para o alcance dos objetivos; refere-se às habilidades, capacidades e competências básicas da organização que atua em conjunto, colaborando para o alcance de suas metas e objetivos;

- Fraqueza: fator interno, controlável pela gestão, que oferece risco à execução dos processos. Corresponde a deficiências e características que devem ser superadas ou contornadas para que a organização possa alcançar o nível de desempenho desejado;
- Ameaça: Situação externa, não controlável pela gestão, que impõe dificuldade no cumprimento dos objetivos das unidades organizacionais e/ou instituição, e restringe o alcance das metas estabelecidas, comprometendo, assim, o crescimento organizacional;
- Oportunidade: possibilidade de que um evento afete positivamente o alcance de objetivos.

➞ Apetite a riscos: Refere-se aos tipos e níveis de riscos que o órgão se dispõe a admitir na realização das suas atividades e objetivos;

➞ Auditoria Interna Governamental (AIG): Uma atividade independente e objetiva de avaliação e de consultoria, desenhada para adicionar valor e melhorar as operações de uma organização, que deve buscar auxiliar as organizações públicas a realizarem seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de governança, de gerenciamento de riscos e de controles internos. Indivíduos que operam independentemente da gestão para oferecer avaliação e conhecimentos sobre a adequação e eficácia da governança e do gerenciamento de riscos (incluindo controle interno);

➞ Causa: Fonte do risco ou vulnerabilidade existente na organização que dá origem a um evento. É um fato ou circunstância que influencia de forma direta ou intrínseca a ocorrência do evento, o porquê do risco;

➞ Consequência: Efeito que o evento de risco terá sobre o alcance dos objetivos organizacionais;

➞ Controle: Qualquer ação tomada pela administração, conselho ou outras partes interessadas para gerenciar riscos e aumentar a probabilidade de que

os objetivos e metas estabelecidos serão alcançados. A administração planeja, organiza e dirige a execução de ações suficientes para prover razoável certeza de que os objetivos e metas serão alcançados. Incluem a forma de organização, as políticas, sistemas, procedimentos, instruções, normas, comissões, planos de contas, previsões, orçamentos, cronogramas, reportes, registros, listas de verificações, métodos, dispositivos e auditoria interna;

- Controle Preventivo: controle cujo objetivo é prevenir a materialização do evento de risco;

- Controle Contingencial: controle voltado para tratar as consequências do evento de risco, ou seja, reduzir ou mitigar os efeitos de sua materialização sobre os objetivos organizacionais;

- Controle adequado/eficaz: Está presente se a administração o tenha planejado e organizado (desenhado) de maneira que forneça uma razoável segurança de que os riscos da organização tenham sido gerenciados eficazmente e de que as metas e objetivos da organização serão atingidos eficiente e economicamente. O controle adequado ou eficaz pode ser compreendido como o controle planejado e organizado (desenhado) de maneira que forneça uma razoável segurança de que os riscos da organização tenham sido gerenciados eficazmente e de que as metas e objetivos da organização serão atingidos eficiente e economicamente e que esteja funcionando como desenhado;

- Controles internos da gestão: Conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de servidores dos órgãos e entidades do Poder Executivo Estadual, destinados a enfrentar os riscos e fornecer segurança razoável de que, na consecução da missão da entidade, os seguintes objetivos gerais serão alcançados: execução ordenada, ética, econômica, eficiente e eficaz das operações; cumprimento das obrigações de

accountability; cumprimento das leis e regulamentos aplicáveis; e salvaguarda dos recursos para evitar perdas, mau uso e danos;

- Declaração de Apetite a Riscos: Documento técnico aprovado pelo Comitê Estratégico de Governança (CEG) que define o posicionamento institucional da CGE acerca do seu apetite a riscos e traz orientações sobre aspectos centrais da gestão de riscos no órgão, abrangendo os tipos e níveis de risco que deverão ser identificados, indicadores de monitoramento e ações mitigadoras por tipo de risco, o nível de apetite e tolerância a riscos por tipo de risco e o nível de maturidade em riscos;

- Evento: Ocorrência ou mudança em um conjunto específico de circunstâncias (ABNT NBR ISO 31000:2018);

- Gestão de Riscos: Trata-se do processo para identificar, analisar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza quanto ao alcance dos objetivos da organização e incrementar o processo de tomada de decisão com base em informações gerenciais preventivas;

- Governança: 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. A governança de uma organização requer estruturas e processos apropriados que permitam a prestação de contas por parte de um corpo administrativo às partes interessadas quanto à supervisão organizacional através da integridade, liderança e transparência e ações (incluindo o gerenciamento de riscos) da gestão para atingir os objetivos da organização por meio da tomada de decisões baseada em riscos e da aplicação de recursos;

- Impacto: grau de efeito que o evento de risco apresenta nas ações de gestão da organização;

- Mapa de Riscos: documento que materializa a análise dos riscos que possam comprometer o sucesso da licitação e a boa execução contratual e que propõe controles capazes de mitigar as possibilidades ou os efeitos da sua ocorrência;

- Matriz de Riscos: instrumento que permite identificar eventos de risco supervenientes à contratação que possam impactar no seu equilíbrio econômico-financeiro, bem como definir as medidas necessárias para tratar os riscos e as responsabilidades entre as partes;

- Medida ou Ação de Controle: Mecanismo utilizado pelo órgão para tratar os riscos levantados, que pode incidir na causa ou na consequência;

- Plano de Ação: Conjunto de medidas ou ações de controle utilizados pela gestão para tratamento dos riscos;

- Probabilidade: frequência estimada de ocorrência do evento de risco;

- Processo: Conjunto de atividades executadas sistematicamente em uma lógica sequencial pelo órgão ou unidade para a transformação de entradas (*inputs* ou insumos) em saídas (*outputs*, produtos ou serviços);

- Risco: Trata-se da possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos, sendo medido em termos de impacto e de probabilidade;

- Risco Inerente: Risco a que um macroprocesso/processo está exposto sem considerar os controles internos que possam mitigar a sua probabilidade ou impacto;

- Risco Residual: Risco a que um macroprocesso/processo está exposto considerando os controles internos existentes;

- Tolerância a risco: Desvio do nível do apetite a riscos (BRASILIANO, 2023);

- Valor do risco: Função da probabilidade e da medida do impacto vinculados ao evento de risco.

10. REFERÊNCIAS

BRASILIANO, Antônio Celso Ribeiro. **Gestão de riscos cibernéticos [livro eletrônico]: foco nos negócios: joias da coroa.** 1. ed. São Paulo: Sicurezza, 2023.

BRASILIANO, Antônio Celso Ribeiro. **Inteligência em riscos [livro eletrônico]: gestão integrada em riscos corporativos.** 2. ed. rev. e ampl. São Paulo: Sicurezza, 2018.

CONTROLADORIA GERAL DO ESTADO – CGE. **Capacitação em auditoria baseada em riscos**, 2014. Apostila.

CONTROLADORIA GERAL DO ESTADO – CGE. **Guia de consultoria em gerenciamento de riscos de processos de trabalho.** 2019.

CONTROLADORIA-GERAL DO ESTADO DE MINAS GERAIS. **Planejamento Estratégico da CGE 2024-2027**. [2024].

Instrução Normativa CGE/GAB nº 01, de 30 de novembro de 2021. **Estabelece as orientações técnicas da atividade de Auditoria Interna Governamental do Poder Executivo Estadual**. 2021.

ISO 31000/2018. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Gestão de riscos — princípios e diretrizes**. Rio de Janeiro. 2018.

MADUREIRA, Espartaco; FERREIRA, André Ribeiro; e SOUZA, Maíra Gabriela S.. **Análise de melhoria de processos.** Brasília: Enap, 2006.

Manual de gestão de riscos do TCU. Secretaria de Planejamento, Governança e Gestão (Seplan). Brasília, 2018.

MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA GERAL DA UNIÃO – CGU. **Metodologia de gestão de riscos**. Brasília, abril de 2018.

MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO – MP. **Manual de gestão de integridade, riscos e controles internos da gestão**. Brasília, janeiro de 2017.

MIRANDA, Rodrigo F. A. **Implementando a gestão de riscos no setor público**. Belo Horizonte: Ed. Fórum, 2017.

Resolução CGE nº 16, de 12 de dezembro de 2023. **Aprova a revisão da Declaração de Apetite a Riscos da Controladoria-Geral do Estado.** 2023.

Resolução CGE nº 17, de 12 de dezembro de 2023. **Dispõe sobre a revisão da Política de Gestão de Riscos da Controladoria-Geral do Estado (CGE).** 2023.

Roteiro de auditoria de gestão de riscos. Secretaria de Métodos e Suporte ao Controle Externo. Brasília, 2017.

SECRETARIA DE ESTADO DE PLANEJAMENTO E GESTÃO. **Guia para melhoria de processos no Governo de Minas Gerais.** [2013].

SILVA, Jéssica Souza. **O mapeamento de processos organizacionais no setor público:** Estudo de caso do escritório de processos da Agência Nacional de Vigilância Sanitária – ANVISA. Brasília, 2014.

SOUZA, Keblerson Roberto; SANTOS, Franklin Brasil. **Como combater o desperdício no setor público: gestão de riscos na prática**. Belo Horizonte. Fórum, 2019.

TRIBUNAL DE CONTAS DA UNIÃO. **Técnicas de Auditoria: análise RECI**. Secretaria de Fiscalização e Avaliação de Programas de Governo. Brasília, 2001.

UNIVERSIDADE FEDERAL DE MINAS GERAIS. **Guia Simplificado de Boas Práticas em Modelagem de Processos com BPMN.** Diretoria de Tecnologia da Informação. Belo Horizonte, 2019.

VIEIRA, James Batista; BARRETO, Rodrigo Tavares de Souza. **Governança, gestão de riscos e integridade**. Brasília: Enap, 2019.

CONTROLADORIA-GERAL
DO ESTADO

MINAS
GERAIS

GOVERNO
DIFERENTE.
ESTADO
EFICIENTE.