Guia Metodológico de **Gestão de Riscos de Processos**

CONTROLADORIA-GERAL DO ESTADO

MINAS GERAIS

GOVERNO DIFERENTE. ESTADO EFICIENTE.

GOVERNO DO ESTADO DE MINAS GERAIS
CONTROLADORIA-GERAL DO ESTADO

GUIA METODOLÓGICO DE GESTÃO DE RISCOS DE PROCESSOS DA CGE

Março de 2021

Controlador-Geral do Estado

Rodrigo Fontenelle de Araújo Miranda

Corregedor-Geral

Vanderlei Daniel da Silva

Subcontroladora de Transparência e Integridade

Nicolle Ferreira Bleme

Auditora-Geral

Luciana Cássia Nogueira

Chefe da Assessoria Estratégica e de Gestão de Riscos

Omar Abreu Bacha

Elaboração

Armando Noé Carvalho de Moura Junior

Olívia Bernardes Almeida

Omar Abreu Bacha

Rodrigo Flávio Ferreira dos Passos

MISSÃO

Promover a integridade e aperfeiçoar os mecanismos de transparência da gestão pública, com participação social, da prevenção e do combate à corrupção, monitorando a qualidade dos gastos públicos, o equilíbrio fiscal e a efetividade das políticas públicas.

VISÃO

Ser referência nacional na área de controle e reconhecido pela sociedade como um órgão de excelência no fortalecimento da integridade pública.

VALORES

Foco no cidadão; Transparência; Valor e ética;

Integridade; Prestação de contas; Conformidade (*compliance*);

Cooperação interinstitucional; Responsabilidade ambiental e social.

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, aos agentes públicos da Controladoria-Geral do Estado, acerca da gestão de riscos de processos da instituição, conforme previsto nos seguintes instrumentos:

- ✓ Plano de Integridade, instituído pela Resolução CGE nº 31, de 14 de setembro de 2018, cuja ação 21 consiste em Implementar o Gerenciamento de Riscos;
- ✓ Declaração de Apetite a Riscos, aprovada pela Resolução CGE nº 19, de 28 de maio de 2020;
- ✓ Política de Gestão de Riscos, aprovada pela Resolução CGE nº 29, de 18 de agosto de 2020; e
- ✓ Instrução Normativa CGE/AUGE nº 04, de 18 de julho de 2020, que estabelece as orientações técnicas da atividade de Auditoria Interna Governamental do Poder Executivo Estadual.

Como resultado do trabalho, espera-se contribuir para a implementação da gestão de riscos de processos na Controladoria-Geral do Estado e, por consequência, para o aperfeiçoamento de seus 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, um glossário com a definição dos principais termos utilizados, bibliografia, referências bibliográficas e apêndices com modelos de formulários a serem preenchidos.

2. PRINCÍPIOS DA GESTÃO DE RISCOS

A gestão de riscos da CGE deve estar alinhada com sua missão e 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 Plano 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 e a visão de futuro;

XIX - Estimular a padronização técnica de atividades;

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

3. DIRETRIZES PARA A GESTÃO DE RISCOS

São diretrizes para a gestão de riscos da CGE:

I - Apoio inequívoco e comprometimento da alta administração;

II - Suporte da estrutura de governança do órgão;

III - Implementação gradual, com prioridade para os riscos estratégicos;

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, impacto e probabilidade da ocorrência de eventos de risco;

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 29, 18 de agosto de 2020, a gestão de riscos integra a estratégia gerencial da CGE e deve contribuir para a alcance de sua missão e de seus objetivos organizacionais. Nesse sentido, todas as unidades e níveis hierárquicos, assim como suas ações e processos devem observar as disposições da Política de Gestão de Riscos, que tem como objetivos:

I - Identificar os eventos de risco às ações e processos internos 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 das ações e 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 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 atualizações;

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

III - Definir a periodicidade do monitoramento dos riscos e da revisão do portfólio de riscos;

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

V - Aprovar a declaração de apetite a riscos da CGE e suas atualizações periódicas;

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

VII - Aprovar as funcionalidades necessárias para o sistema eletrônico de gerenciamento de riscos;

VIII - Aprovar a indicação de gestores de risco das unidades da CGE;

IX - Aprovar os Planos de Ação para gestão de riscos;

X - Realizar, em nível estratégico, o monitoramento da evolução dos riscos das ações e processos, bem como da efetividade dos planos de ação;

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

XII - 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);

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

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

XV - 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:

I - Subsidiar o CEG na definição dos gestores de risco das unidades;

II - Subsidiar o CEG no estabelecimento de estratégias para a implementação da gestão de riscos na CGE;

III - Propor ao CEG modificações na declaração de apetite a riscos;

IV - Realizar ações de capacitação em gestão de riscos, em articulação com a Assessoria Estratégica e de Gestão de Riscos (AEGRI);

V - Disseminar a cultura de gestão de riscos na CGE.

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 atualizações;

II - Propor as funcionalidades necessárias para o sistema eletrônico de gerenciamento de riscos;

III - Realizar o monitoramento da evolução dos riscos das ações e processos e da efetividade 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;

XIX - 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, os proprietários dos riscos consistem nos dirigentes das unidades da estrutura orgânica da CGE nas quais as ações ou processos são desenvolvidos. Suas competências são:

I - Escolher as ações e 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 ao CGIRC 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 das ações e processos das respectivas unidades administrativas as quais se vinculam. Suas indicações serão aprovadas por ato normativo do CEG e suas competências consistem em:

I - Realizar o levantamento dos riscos das ações e 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 suas ações e processos;

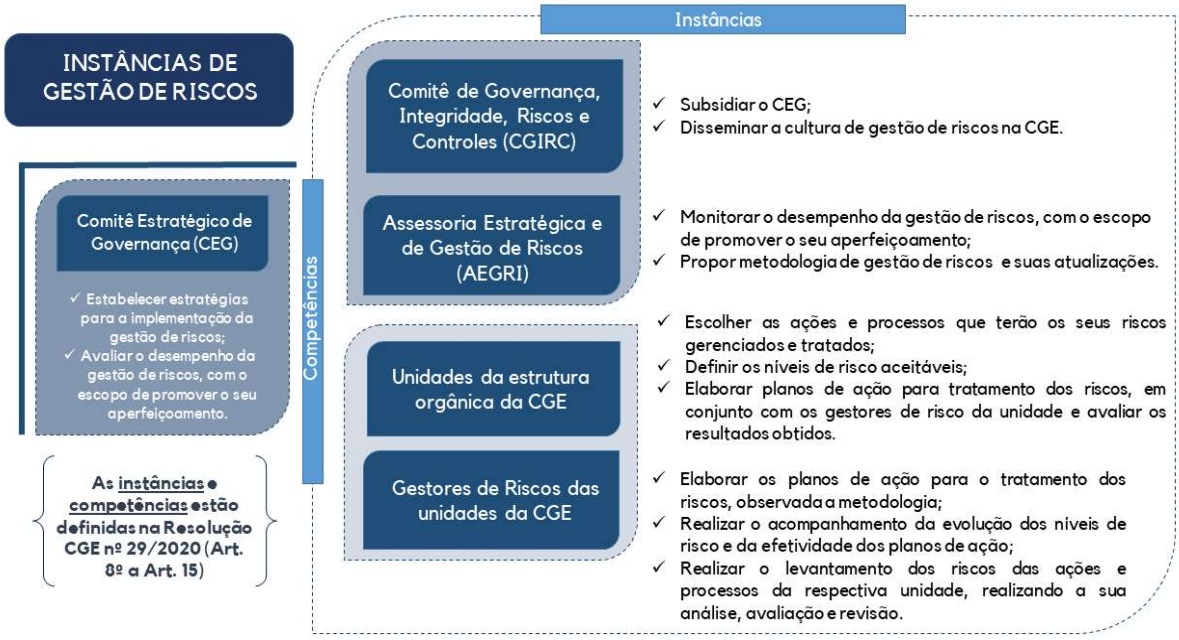
V - Responder as requisições da Assessoria Estratégica e de Gestão de Riscos;

VI - Disponibilizar as informações relativas à gestão de riscos das ações e 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 e ações 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 constatadas nas ações, 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: Controladoria-Geral do Estado de Minas Gerais - CGE-MG

6. PROCEDIMENTOS OPERACIONAIS DA GESTÃO DE RISCOS

De acordo com o estabelecido na Resolução CGE nº 29, 18 de agosto de 2020, 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 à ação ou 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 - Identificação e análise dos riscos: fase em que são levantados os riscos relativos às ações e processos do órgão, bem como suas causas e consequências;

IV - Avaliação dos 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 - Tratamento dos 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 - Comunicação e Monitoramento dos 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.

É importante pontuar que a Resolução permite a utilização de metodologias diversas para a gestão de riscos estratégicos e de processos da CGE. Nesse sentido, o Guia Metodológico de Gestão de Riscos Estratégicos, aprovado pela Resolução CGE nº 26, teve como objetivo acompanhar os riscos que poderiam prejudicar o alcance dos objetivos estratégicos dos órgãos e entidades do Estado de Minas Gerais:

Figura 2 – Guia Metodológico de Gestão de Riscos Estratégicos

Fonte: Controladoria-Geral do Estado de Minas Gerais - CGE-MG

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, e em consonância com o previsto na Resolução CGE nº 29, 18 de agosto de 2020 e na metodologia de Gestão de Riscos de Processos adotada pela Auditoria-Geral.

São fases do ciclo de gestão de riscos da CGE:

Figura 3 - Ciclo de Gestão de Riscos de Processos

Fonte: Controladoria-Geral do Estado de Minas Gerais - CGE-MG

7.1. Conhecer o Ambiente e os Objetivos Organizacionais

Para a gestão dos riscos de 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 processo em análise. Conhecer o fluxo do 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.

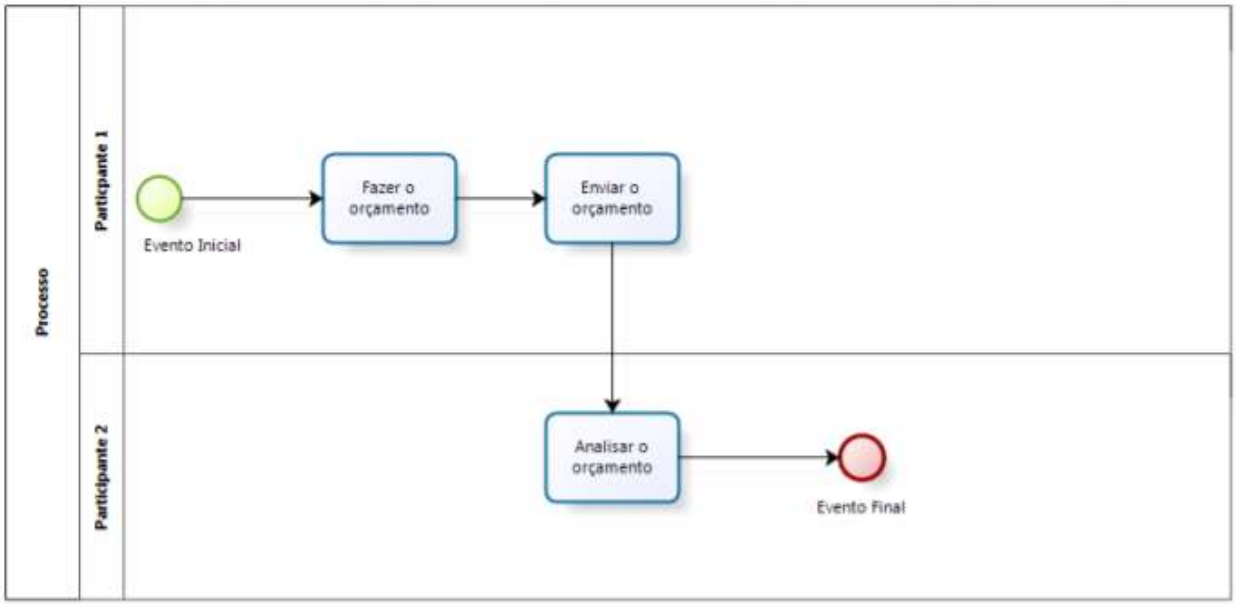
O conhecimento do processo é indispensável para a evidenciação dos riscos que podem impactar seu desempenho e, até mesmo, o da organização. Dessa forma, independentemente da realização do mapeamento do processo, deve-se conhecer o ambiente e seus objetivos, de maneira a se obter uma visão sistêmica deste. 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.

Na Controladoria-Geral do Estado, a AEGRI, em conjunto com as unidades do Órgão Central, irá elaborar o mapeamento dos processos que terão seus riscos gerenciados. Como metodologia serão utilizadas as 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, 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 4 – 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.

Adicionalmente, as atividades executadas em cada processo devem ser transcritas para as planilhas constantes dos Apêndices A e B, "Diagrama de Fluxo" e "Folha de Processo" (detalhes do processo), respectivamente, exceto as colunas riscos e controles. Além disso, pode ser aplicada a técnica denominada Matriz RECI[1].

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

- ✓ Unidades administrativas em que o processo é realizado;

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

- ✓ Nome e responsável pelo processo;
- ✓ Ação estratégica a qual o processo está vinculado;
- ✓ Atividades críticas do processo;
- ✓ Sequência de atividades executadas no 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 falhas na execução do 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 Risco

Apetite a risco é a quantidade de risco que a organização deseja assumir para conseguir atingir seus objetivos (Brasiliano, 2018). Vieira e Barreto (2019, p. 141) afirmam que "É importante que o apetite a risco 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 Risco, a qual deve ser aprovada por uma instância de supervisão da Alta Gestão, a exemplo de Comitês de Governança Participativa.

Importante ressaltar que o apetite a risco é dinâmico, podendo ser modificado de acordo com o contexto e situação percebida em um dado

momento. Na Controladoria-Geral, o apetite a risco foi aprovado pelo Comitê Estratégico de Governança e, consiste em ato contínuo, oficializado pela Resolução CGE nº 19/2020, de 29 de maio de 2020:

Figura 5 – Declaração de Apetite a Riscos da CGE

Fonte: Controladoria-Geral do Estado de Minas Gerais - CGE-MG

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: missão da organização; tipos e níveis de risco dispostos a assumir na realização das atividades e objetivos organizacionais; período de revisão do apetite; unidades administrativas responsáveis por sua aprovação, 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.

Considerando o nível de maturidade da instituição em riscos, a declaração apresenta os seguintes indicadores de monitoramento por tipo de risco definido:

- ✓ Risco Estratégico: Aprovação/Revisão anual do Planejamento Estratégico e Monitoramento da execução do Planejamento Estratégico;
- ✓ Risco Operacional: Proteção a *ciberataque* e Continuidade dos Negócios;
- ✓ Risco Orçamentário: Monitoramento da despesa;
- ✓ Risco Reputacional: CGE na mídia;
- ✓ Risco de Integridade: Aplicação de penalidades e Monitoramento do Plano de Integridade;
- ✓ Risco de Conformidade: Conformidade legal.

Salienta-se que tanto o Apetite a Riscos como a Tolerância a Riscos serão 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

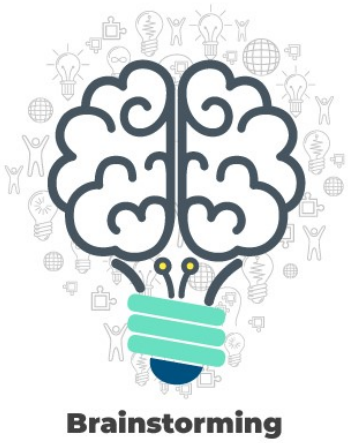
Nessa etapa, devem ser identificados os eventos em potencial que, caso ocorram, afetarão o desenvolvimento do processo, a entrega dos produtos e o atingimento dos objetivos. De acordo com a ISO 31000/2018, na identificação dos riscos é recomendado que a organização:

> 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 apropriadas 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 6 - Brainstorming

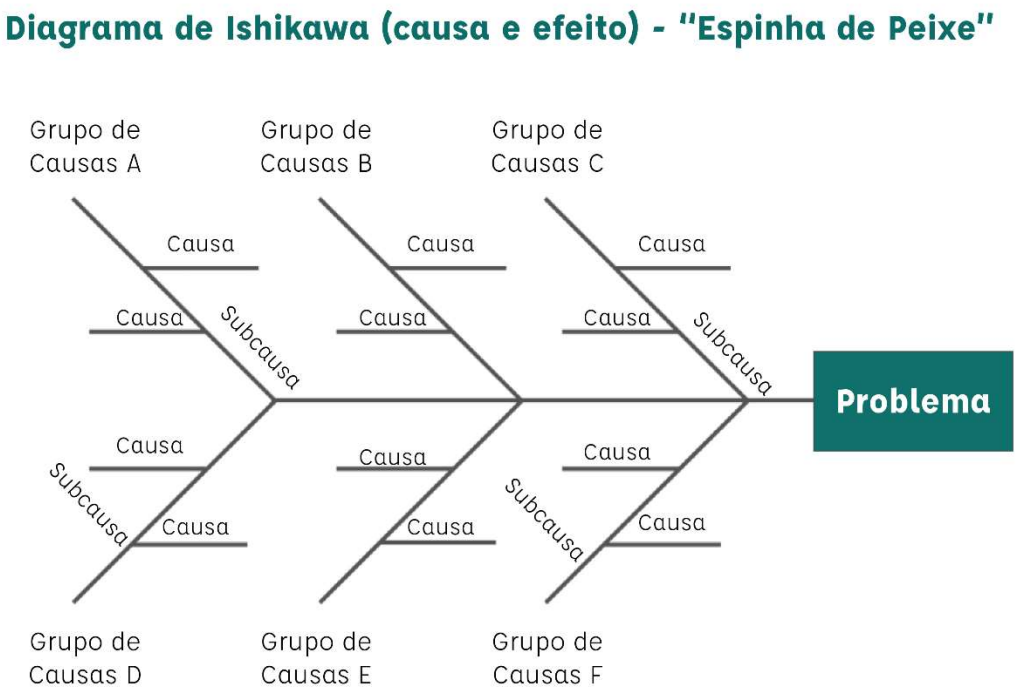


Fonte: Freepik

Figura 7 - Matriz SWOT

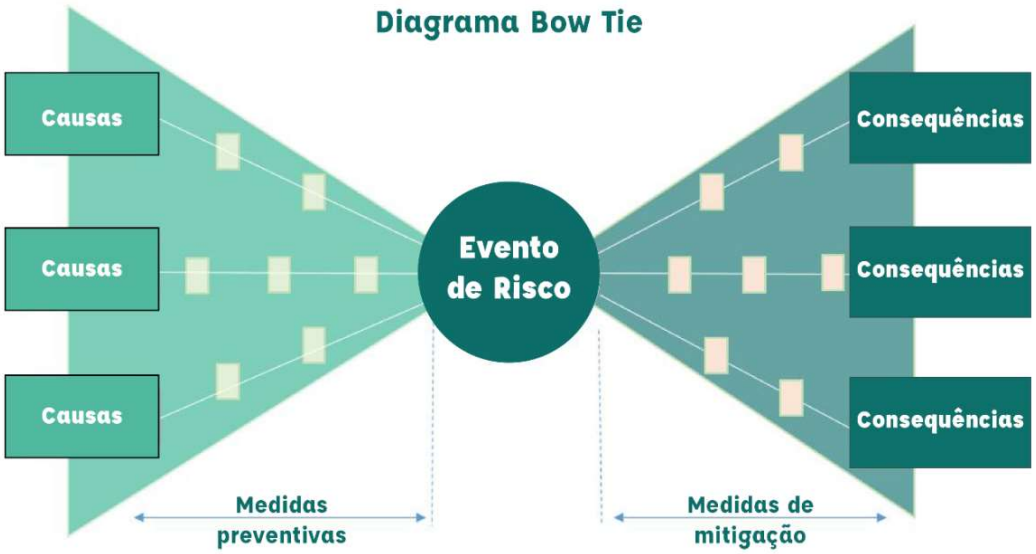
Fonte: Controladoria-Geral do Estado de Minas Gerais - CGE-MG

Figura 8 – Diagrama de *Ishikawa*



Fonte: Controladoria-Geral do Estado de Minas Gerais - CGE-MG

Figura 9 - 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, inicialmente, serão realizadas reuniões de *brainstorming* com os gestores, juntamente com aplicação da Matriz SWOT, a fim de identificar as fragilidades do processo e avaliar o cenário. Este será 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 processo.

Destaca-se que serão realizadas reuniões periódicas 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[2] adotados em cada atividade do processo. As informações serão narradas pelos gestores e os dados serão transcritos para a planilha “Folha de Processo”.

Posteriormente, com as atividades transcritas para a planilha “Análise de Risco” (Apêndice C), os gestores passarão a detalhar os eventos de riscos no trinômio (causa/evento/consequência), conforme figura a seguir. Deste modo, para cada causa ou consequência diferentes apresentadas para o evento, tem-se a formação do trinômio do risco. Salienta-se que cada trinômio deve ser transcrito em uma linha da planilha.

Figura 10 - Trinômio de Risco

Fonte: Controladoria-Geral do Estado de Minas Gerais - CGE-MG

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

[2] Os controles são um conjunto de políticas, normas “(...) e procedimentos que ocorrem em toda a organização para autorizar, verificar, reconciliar e revisar o desempenho. Os controles são 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).

possível relacionar-se a algo que não irá acontecer, entretanto, não deve ser simplesmente o não alcance do objetivo da atividade.

Vale ressaltar que os riscos relevantes constantes da “Folha de Processo” referem-se ao núcleo ou evento de riscos, ou simplesmente evento, o qual constará no trinômio causa/evento/consequência.

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 no:

> (...) 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 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 1). Assim, a probabilidade do risco acontecer corresponde à probabilidade do evento ocorrer.

Tabela 1 - Pesos da Probabilidade

Descrição	Frequência	Peso
Evento que ocorre quase sempre	>90%	5
Evento que ocorre na maioria das circunstâncias	> = 75%<= 90%	4
Evento que provavelmente ocorre	>= 40%< 75%	3
Evento que deve ocorrer em algum momento	>= 10% <40%	2
Evento pode ocorrer em circunstâncias excepcionais	< 10%	1

Fonte: Controladoria-Geral do Estado de Minas Gerais - CGE-MG

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 reputacional pode representar a maior preocupação do gestor, enquanto para outra o risco orçamentário é o mais importante.

Neste sentido, é possível que o gestor defina um número menor de categorias de impacto relevantes para o processo, contudo, deve haver, no mínimo, 4 (quatro) categorias. Como o impacto na organização apresenta diversas nuances, utilizam-se as seguintes categorias:

Tabela 2 - Categorias de Impacto

Categoria de Impacto	Definição
Operacional	Prejuízo à qualidade do produto entregue ou serviço prestado à população, procedente de falha ou deficiência na atividade operacional do órgão ou entidade
Reputacional	Prejuízo à imagem do órgão ou entidade (e, consequentemente, do próprio Governo) perante a sociedade (cidadãos, contribuintes, grupos beneficiados por políticas governamentais etc.) e outros órgãos ou entidades das três esferas de governo
Conformidade	Sanções em razão de descumprimento de dispositivos legais e indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela instituição
Integridade	Favorecimento ou facilidade de práticas de corrupção, fraudes, irregularidades, bem como desvios éticos e de conduta.
Patrimonial [1]	Perdas patrimoniais procedentes de apropriação indébita de informações (patentes, pesquisas, informações financeiras etc.) e de danos ou desvios de propriedade (recursos e bens patrimoniais)
Orçamentário	Eventos que podem comprometer a própria execução orçamentária ou a capacidade do órgão/entidade em receber recursos orçamentários necessários à realização de suas atividades

Fonte: Controladoria-Geral do Estado de Minas Gerais - CGE-MG

Nota: 1 - Caso existente

É importante dizer que cada categoria apresenta importância distinta ao se avaliar o impacto do risco na organização. Sendo assim, com a finalidade de reduzir a subjetividade na determinação de cada categoria, atribui-se peso específico em percentual, por meio da utilização do modelo *Analytic Hierarchy Process* (AHP)[3], versão MS Excel 2010 (extensão xlsx), no site: *https://bpmsg.com/ahp/ahp-calc.php*.

Após a definição de quantidade de categorias e de sua relevância no processo selecionado, deve-se realizar a comparação da importância dois-a-dois entre as categorias. No caso de serem iguais, deve-se registrar 1. Nos demais casos, deve-se registrar, de 2 a 9, o grau de importância de uma categoria em relação à outra. Posteriormente, deve-se calcular o percentual e ajustar a comparação até que o CR (*Consistency Ratio*) fique abaixo de 10%. Os percentuais de cada categoria de impacto demonstrados na tabela *Priorities* devem ser transcritos para a planilha "Análise de Riscos". Diante disso, os pesos podem ser atribuídos por cada consequência e categoria de impacto.

A tabela a seguir ilustra a descrição das categorias de impacto e seus respectivos pesos.

Tabela 3 - Pesos de Impacto por Categorias

Operacional	Reputacional	Conformidade	Orçamentário	Patrimonial	Integridade	Peso
Evento cuja consequência prejudica em mais de 90% a entrega do produto/serviço	Com destaque na mídia nacional, podendo atingir os objetivos estratégicos da organização	Determina interrupção das atividades	Altíssimo impacto estimado na execução da ação orçamentária correspondente (>=70%)	Perda patrimonial alta	Decisão administrativa de responsabilização[1] relativa a práticas de corrupção, fraudes, irregularidades e desvios éticos e de conduta	10
Evento cuja consequência prejudica em mais de 70% a	Com destaque na mídia nacional, provocando	Determina ações de caráter pecuniário	Grande impacto estimado na execução da ação orçamentária	Perda patrimonial relevante	Processo de responsabilização instaurado relativo a práticas	7

[3] O modelo AHP foi desenvolvido por Goepel, Klaus D., modelo BPMSG AHP Excel, disponível em *http://bpmsg.com*, cuja versão é de livre uso.

Operacional	Reputacional	Conformidade	Orçamentário	Patrimonial	Integridade	Peso
entrega do produto/serviço	exposição significativa		correspondente (>=50% e <70%)		de corrupção, fraudes, irregularidades e desvios éticos e de conduta	
Evento cuja consequência prejudica em mais de 30% a entrega do produto/serviço	Com destaque na mídia regional, provocando exposição significativa	Determina ações de caráter corretivo	Médio impacto estimado na execução da ação orçamentária correspondente (>=30% e <50%)	Perda patrimonial de representatividade média	Investigação instaurada relativa a práticas de corrupção, fraudes, irregularidades e desvios éticos e de conduta	5
Evento cuja consequência prejudica em até 30% a entrega do produto/serviço	Pode chegar à mídia, provocando a exposição por um curto período de tempo	Determina ações de caráter preventivo	Pouco impacto estimado na execução da ação orçamentária correspondente (>=10% e <30%)	Perda patrimonial pouco representativa	Notícias de práticas de corrupção, fraudes, irregularidades e desvios éticos e de conduta	3
Evento cujo impacto pode ser absorvido por meio de atividades formais	Impacto apenas interno	Pouco ou nenhum impacto	Impacto irrelevante estimado na execução da ação orçamentária correspondente (>10%)	Perda patrimonial irrelevante	Possibilidade de ocorrência de práticas de corrupção, fraudes, irregularidades e desvios éticos e de conduta	1

Fonte: Controladoria-Geral do Estado de Minas Gerais - CGE-MG

Nota: 1 – Entende-se por processo de responsabilização os procedimentos para aplicação de sanções administrativas à agentes públicos e pessoas jurídicas.

Para cada risco identificado, atribuem-se os pesos de probabilidade e impacto, obtendo-se o risco residual. Determinado seu valor, propõe-se a utilização da matriz de riscos (tabela 4), para classificar qualitativamente o valor do risco através da definição dos níveis de risco (tabela 5). Estes, por sua vez, especificam a partir de quais valores os riscos são considerados extremos, altos, médios ou baixos.

Tabela 4 - Matriz de Riscos (Valor do Risco)

PROBABILIDADE						
	Quase Certo - 5	5	15	25	35	50
	Muito Provável - 4	4	12	20	28	40
	Provável - 3	3	9	15	21	30
	Pouco Provável - 2	2	6	10	14	20
	Rara - 1	1	3	5	7	10
		Irrelevante - 1	Pequeno - 3	Moderado - 5	Alto - 7	Muito Alto - 10
	IMPACTO					

Fonte: Controladoria-Geral do Estado de Minas Gerais - CGE-MG

Tabela 5 - Nível de Severidade (Classificação do Risco)

NIVEL	VALOR	SÍMBOLO
EXTREMO	MAIOR OU IGUAL A 28	
ALTO	MAIOR OU IGUAL A 10 E MENOR QUE 28	
MÉDIO	MAIOR OU IGUAL A 5 E MENOR QUE 10	
BAIXO	MENOR QUE 5	

Fonte: Controladoria-Geral do Estado de Minas Gerais - CGE-MG

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 processos, para identificação dos pesos de frequência da probabilidade e ofensividade do impacto em cada categoria.

Da mesma maneira, ressalta-se que para mensurar o percentual das categorias de impacto, serão definidos em reuniões com os gestores responsáveis pelo processo, e por meio da ferramenta AHP – *Analytic Hierarchy Process*, percentuais de cada categoria de impacto e quais categorias de impacto serão utilizadas, ressaltando que conforme citado anteriormente, deve-se utilizar pelo menos quatro categorias.

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 7.5. Ressalta-se, no entanto, a obrigatoriedade de tratamento dos riscos residuais extremos e altos, a fim de modificar sua classificação, tendo em vista o impacto destes no atingimento dos objetivos da atividade.

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 minimizem a patamares aceitáveis do apetite e da tolerância a riscos. Os resultados do desempenho do tratamento, eficácia e eficiência dos controles aplicados, devem refletir na severidade minimizada dos riscos.

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 minimização dos riscos relevantes.

De modo geral, considera-se que os eventos de riscos situados nos quadrantes definidos como risco alto e risco extremo são indicativos de necessidade de controles mais rígidos, devido aos impactos que podem provocar no atingimento dos objetivos dos processos, enquanto os riscos situados nos quadrantes de risco baixo e médio 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 respectivos exemplos:

Figura 11 - Tipos de Tratamento de Riscos

EVITAR	Eliminar a fonte do risco. Exemplo: gestão de projetos, quando a relação custo/benefício projetada está em perigo.
ACEITAR	Não fazer nada. Nenhuma medida é adotada para afetar a probabilidade ou o grau de impacto do risco. Exemplo: não é necessária nenhuma ação.
REDUZIR	Controlar ou diversificar o risco. Adoção de medidas para reduzir a probabilidade ou impacto ou ambos. 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	Transferir o risco. Redução da probabilidade ou impacto dos riscos pela transferência de uma porção do risco. 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 e os responsáveis pelo acompanhamento. O modelo de Plano de Ação encontra-se no Apêndice D.

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 processos fornece a informação atualizada e objetiva identificar fragilidades e possibilidades de melhorias, como aprimorar o fluxo do 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 de processos.

Na Controladoria-Geral, conforme dito anteriormente, compete à Assessoria Estratégica e de Gestão de Riscos realizar o monitoramento da evolução dos riscos das ações e processos e da efetividade dos planos de ação, de acordo com modelo constante do Apêndice D.

O Plano de Ação estabelece o que será feito, qual controle será implementado ou aperfeiçoado, o cronograma de implementação, os responsáveis pelo acompanhamento, bem como os indicadores chave de risco e sua periodicidade de apuração.

Os indicadores chaves de risco são métricas elaboradas para acompanhar a evolução dos eventos de risco e estabelecer pontos de alerta para sua ocorrência e seu monitoramento. Como exemplos, podem-se citar: número de indisponibilidades de sistemas, tempo de recuperação de sistemas, quantidade de exceções à Política de Ética, % de descumprimento de determinado cronograma, etc. A periodicidade de sua apuração, por sua vez, se refere ao espaço temporal em que os indicadores serão medidos, tal como: mensal, bimestral, quadrimestral, semestral ou anual.

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 de processos, 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. 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;

- Apetite a risco: 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 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. O conceito de controles internos da gestão também pode ser compreendido como o processo conduzido pela direção e pelo corpo de servidores dos órgãos e entidades do Poder Executivo Estadual, desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados à execução ordenada, ética, econômica, eficiente e eficaz das operações; ao cumprimento das obrigações de *accountability*; e ao 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 risco, trazendo a missão da organização; tipos e níveis de risco dispostos a assumir na realização das atividades e objetivos organizacionais; período de revisão do apetite; unidades administrativas responsáveis por sua aprovação, 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;

- 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 aos

stakeholders 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;

- Indicadores chaves de risco: métricas elaboradas para acompanhar a evolução dos eventos de risco e estabelecer pontos de alerta para sua ocorrência e seu monitoramento. Como exemplos, podem-se citar: número de indisponibilidades de sistemas, tempo de recuperação de sistemas, quantidade de exceções à Política de Ética, % de descumprimento de determinado cronograma, etc.;

- Matriz de Risco: Ferramenta que classifica qualitativamente os pesos de impacto e probabilidade e determina o nível de risco. Identifica a criticidade de cada risco (BRASILIANO, 2018);

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

- Periodicidade de apuração dos indicadores chaves de risco: espaço temporal em que os indicadores serão medidos, tal como: mensal, bimestral, quadrimestral, semestral ou anual;

- 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: Série de atos adotados pelo órgão para o alcance de um resultado previamente estabelecido;

- 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 uma ação ou processo está exposto sem considerar os controles internos que possam mitigar a sua probabilidade ou impacto;

- Risco Residual: Risco a que uma ação ou processo está exposto considerando os controles internos existentes;

- Tolerância a risco: Desvio do nível do apetite a risco (BRASILIANO, 2018, p. 129);

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

9. BIBLIOGRAFIA

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

➞ _____. Resolução CGE nº 31, 14 de setembro de 2018. **Institui o Plano de Integridade da Controladoria-Geral do Estado**. 2018.

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

10. REFERÊNCIAS BIBLIOGRÁFICAS

➞ 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. **Guia de consultoria em gerenciamento de riscos de processos de trabalho.** 2019.

➞ _____. Instrução Normativa CGE/AUGE nº 04, de 18 de julho de 2020. **Estabelece as orientações técnicas da atividade de Auditoria Interna Governamental do Poder Executivo Estadual.** 2020.

➞ _____. Resolução CGE nº 19, de 28 de maio de 2020. **Aprova a Declaração de Apetite a Riscos da Controladoria-Geral do Estado.** 2020.

➞ _____. Resolução CGE nº 26, de 20 de julho de 2020. **Dispõe sobre a metodologia para a gestão de riscos estratégicos no âmbito da Controladoria-Geral do Estado.** 2020.

➞ _____. Resolução CGE nº 29, de 18 de agosto de 2020. **Dispõe sobre a Política de Gestão de Riscos da Controladoria-Geral do Estado (CGE).** 2020.

➞ 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.

- 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.
- 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.
- _____. **Roteiro de auditoria de gestão de riscos.** Secretaria de Métodos e Suporte ao Controle Externo. Brasília, 2017.
- _____. **Manual de gestão de riscos do TCU.** Secretaria de Planejamento, Governança e Gestão (Seplan). Brasília, 2018.
- 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.

APÊNDICES

APÊNDICE A - Diagrama de Fluxo

Processo:
Objetivos do Processo:

Atividades

Nº	**Descrição Sintética**
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

Fonte: Controladoria-Geral do Estado de Minas Gerais - CGE-MG.

Nota: A utilização de planilhas poderá ser substituída por sistema eletrônico.

APÊNDICE B - Folha de Processo

Número da Atividade	Descrição		Objetivo	Responsável	Setor	Documentos	Riscos (Identificados)	Controles (Situação Informada)	Observações
	Sintética	Detalhada							

Fonte: Controladoria-Geral do Estado de Minas Gerais - CGE-MG.

Nota: A utilização de planilhas poderá ser substituída por sistema eletrônico.

APÊNDICE C - Análise de Riscos

Número Atividade	Risco Identificação				Estimativa de Probabilidade e Impacto (por Categoria de Impacto)																		Risco Classificação			
					Risco Operacional			Risco Reputacional			Risco de Conformidade			Risco de Integridade			Risco Patrimonial [1]			Risco Orçamentário						
	Nº	Causa	Evento	Consequência	%			%			%			%			%			%			Valor	Nível	Símbolo	Observações da unidade
					P	I	Rc	P	I	Rc	P	I	Rc	P	I	Rc	P	I	Rc	P	I	Rc				

Fonte: Controladoria-Geral do Estado de Minas Gerais - CGE-MG.

Notas: 1 - Não é obrigatória a identificação da totalidade de categoria de riscos acima elencada. Contudo é necessária a identificação de pelo menos quatro categorias de risco;

2 - As categorias de risco variam de acordo com as disposições da Declaração de Apetite a Riscos publicada pelo órgão ou entidade;

3 - A utilização de planilhas poderá ser substituída por sistema eletrônico.

APÊNDICE D - Plano de Ação de Gerenciamento de Riscos de Processos

Nº	Atividade	Unidade Responsável	Controle Existente no Processo	Causa	Evento	Consequência	Valor do Risco	Classificação do Risco	Indicador Chave de Risco[1]	Periodicidade de Apuração do Indicador Chave de Risco[2]	Tipo de Tratamento a ser Realizado[3]	Justificativa caso não adote ação para os riscos	Descrição da Ação	Gestor Responsável	Data Início da implantação	Data Final da implantação	Status[4]	Observações[5]

Fonte: Controladoria-Geral do Estado de Minas Gerais - CGE-MG.

Notas: 1 - Conforme a seguir: 1 – evitar; 2 – aceitar; 3 – reduzir e 4 – transferir;
2 - Segundo os seguintes níveis: 1- a iniciar; 2 - em execução; 3 - concluída; e 4 – não concluída no exercício;
3 - Com o objetivo de inserir informações qualitativas sobre o gerenciamento, execução e resultados do Plano de Ação, caso necessário;
4 - A utilização de planilhas poderá ser substituída por sistema eletrônico.