DELIBERAÇÃO CONSAD Nº01/2021

Delibera e implementa o manual da Política de Gestão de Riscos da Empresa Mineira de Comunicação.

O CONSELHO DE ADMINISTRAÇÃO DA EMPRESA MINEIRA DE COMUNICAÇÃO, tendo em vista o disposto na Lei nº 22.294, de 20 de setembro de 2016, no uso de atribuições que lhe confere o art. 24, incisos XXXIII e XXXV, do Decreto nº 47.750, 12 de novembro de 2019, a Resolução CONSAD nº03/2020. e

CONSIDERANDO o constante dos autos do processo nº 3150.01.0000302/2021-92,

RESOLVE:

1. INTRODUÇÃO E OBJETIVO

1.1. Elaborada nos termos da legislação aplicável, em especial a Lei Federal nº13.303/2016, a presente Política tem por objetivo definir as diretrizes, conceitos e responsabilidades do processo interno de gerenciamento de riscos da Empresa, incluindo os procedimentos adequados para a identificação, categorização, avaliação, tratamento e monitoração dos riscos atrelados aos negócios, suas parceiras e suas permissionárias, adotando o baixo apetite ao risco, com perfil conservador.

2. APROVAÇÃO

2.1. A presente Política foi aprovada em reunião do Conselho de Administração da EMC realizada em 21 de dezembro de 2021, nos termos do Estatuto Social da Empresa no Decreto Estadual nº47.750/2019.

3. DIRETRIZES

3.1. A EMC deverá adotar cinco componentes de análise na composição da avaliação dos riscos de seus negócios, quais sejam:

I - ambiente de controle;

II - evitar ou eliminar o risco;

III - aceitar o risco;

IV - atividades de controle; e

V - atividades de monitoramento.

3.1.1. Ambiente de Controle significa o conjunto de normas, processos e estruturas organizacionais para todos os componentes da estrutura de gerenciamento de riscos. O ambiente de controle é composto pelo:

I - Estatuto Social da EMC, seu Código de Conduta, Ética e Integridade, políticas, regulamentos e regimentos internos aprovados pelo Conselho de Administração, bem como todas as leis, regulamentos, normas, decretos e outras disposições a que a EMC se submeta,

II - práticas adotadas por cada uma das áreas da EMC, visando manter seus negócios operando de forma eficiente, eficaz, ética e íntegra; e

III - órgãos de governança corporativa, a Diretoria, o Conselho de Administração e os empregados da EMC.

3.1.2. Evitar ou Eliminar o Risco significa a decisão de não se envolver com a atividade, processo ou serviço que gere determinado risco, ou agir de forma a descontinuar ou se retirar daquela atividade, processo ou serviço.

3.1.3. Aceitar o Risco significa as ações de retenção, redução, transferência ou exploração de determinado risco. Deve-se entender:

I - como retenção, a manutenção do risco no nível atual de impacto;

II - como redução, as ações para redução do nível de impacto do risco;

III - como transferência, a utilização de seguros ou de eventual terceirização da atividade de risco para uma empresa de maior especialização; e

IV - exploração como o acréscimo do grau de exposição da EMC ao risco, possibilitando outras vantagens competitivas.

3.1.4. Atividades de Controle significa o conjunto de atividades desenvolvidas no âmbito da EMC visando ao gerenciamento dos riscos, incluindo:

I - a revisão e aprovação das normas e procedimentos;

II - a revisão e/ou aprovação de atividades, processos e serviços;

III - a prévia avaliação legal ou regulatória de atividades, processos e serviços;

IV - o estabelecimento e aplicação de um programa de gestão de continuidade de negócios; e

V - o monitoramento de atividades, processos e serviços para controle dos riscos existentes.

3.1.5. Atividades de Monitoramento significa as atividades de mapeamento das diversas áreas da EMC, sendo responsável pela detecção de novos riscos e por determinar a efetividade dos controles implementados para os riscos conhecidos, devendo cobrir toda e qualquer operação da empresa. Através das atividades de mapeamento, os riscos são identificados, categorizados e avaliados, proporcionando um mecanismo facilitador para a tomada de decisão pela área competente.

3.1.6. Em atendimento ao inciso X, art. 42 da Lei 13.303, regulamentado pelo inciso IV, do art. 71 do Decreto nº 8.945, em âmbito federal, e pelo Decreto nº 47.154, em âmbito estadual, na preparação do processo licitatório e na contratação

de obras e serviços, devem ser indicados os riscos identificados na contratação e as responsabilidades das partes para cada situação indesejada, por meio de uma matriz de riscos.

3.1.7. O processo de gestão de risco e elaboração da matriz de risco deve seguir a metodologia apresentada anexa a esta Política como Anexo I, que segue as normativas da CGE/MG.

4. RISCOS

4.1. Caracterizar-se-ão como riscos, o potencial de eventos ou tendências continuadas que pode afetar negativamente a realização dos objetivos da empresa ou de suas atividades e processos, causando perdas financeiras, flutuações em receitas futuras, impacto em imagem, bem como todo e qualquer outro fator que tenha o potencial de afetar negativamente as atividades da empresa.

4.2. Os riscos podem ser externos e internos. Riscos externos são eventos associados ao ambiente macroeconômico, político, social, natural ou setorial em que a EMC opera, sendo imprevisíveis devido à falta de capacidade da empresa de intervir diretamente sobre estes eventos. Por outro lado, os riscos internos são eventos originados na própria estrutura da empresa, pelas suas atividades ou colaboradores.

4.3. Os riscos aplicáveis à EMC serão categorizados em:

a) Risco Estratégico;

b) Risco de Imagem;

c) Risco Regulatório/Legal;

d) Risco Operacional;

e) Risco Político;

f) Risco Tecnológico; e

g) Risco Ambiental.

4.3.1. Risco Estratégico significa a possibilidade de implementação de estratégias malsucedidas ou ineficazes, que não alcancem os resultados esperados e/ou aumentem a concorrência e/ou os demais riscos a que a empresa está suscetível.

4.3.2. Risco de Imagem significa aqueles eventos que trazem danos à reputação da EMC.

4.3.3. Risco Regulatório/Legal significa a possibilidade de que leis ou regulamentos, inclusive suas modificações ou não observância total ou parcial, possam trazer impactos estratégicos, de imagem e/ou financeiros para a EMC e suas parceiras, afiliadas e permissionárias, e/ou afetar significativamente a habilidade da empresa de administrar eficientemente os seus negócios.

4.3.4. Risco Operacional significa a possibilidade de ocorrência de perdas resultantes de falhas, deficiências ou inadequações de processos internos, pessoas ou de eventos externos.

4.3.5. Risco Político significa o risco oriundo de uma mudança no ambiente político na República Federativa do Brasil, no Estado de Minas Gerais ou na localidade em que a EMC e mantenha ou venha a manter operações.

4.3.6. Risco Tecnológico significa o risco de uma inoperância ou falha de sistemas, processos e equipamentos de tecnologia que processam e controlam todas as operações da EMC.

4.3.7. Risco Socioambiental significa o risco de perdas em consequência de efeitos negativos no meio-ambiente e na sociedade, decorrentes de impacto ambiental, impactos em povos e comunidades nativas e proteção da saúde humana, de propriedades culturais e da biodiversidade.

5. RESPONSABILIDADE

5.1. São responsáveis pela execução e acompanhamento da presente Política, o Conselho de Administração, a Auditoria Interna e a Diretoria da empresa.

5.2. Competirá ao Conselho de Administração:

I - estabelecer os limites de tolerância aos riscos que a EMC deverá observar no exercício de suas atividades;

II - monitorar e reavaliar periodicamente os riscos estratégicos e de imagem;

III - quando solicitado pela Diretoria ou pela Auditoria Interna, avaliar a situação da EMC em relação aos riscos categorizados no item 4.3; e

IV - reavaliar, junto a Auditoria Interna, a adequação da estratégia de gerenciamento de riscos da empresa.

5.3. Competirá à Diretoria da EMC:

I - formular os objetivos estratégicos para implementação dos negócios aprovados pelo Conselho de Administração, dentro dos limites de tolerância aos riscos aprovados pelo mesmo;

II - identificar e categorizar os riscos mencionados no item 4.3 acima, adotando medidas para o seu combate;

III - monitorar os riscos aos quais a Companhia está exposta;

IV - executar ações de resposta aos riscos até que o risco volte a se adequar aos níveis de tolerância estabelecidos pelo Conselho de Administração da EMC;

V - manter a adequada comunicação externa dos mecanismos de gerenciamento de riscos adotados pela EMC;

VI - consolidar o resultado do mapeamento dos riscos, avaliando sua eficácia;

VII - elaborar relatórios anuais para a Auditoria Interna sobre os resultados dos mapeamentos; e

VIII - sempre que solicitado, apresentar ao Conselho de Administração e a Auditoria Interna o mapa de riscos da EMC e realizar o acompanhamento da implementação das respostas ao risco apontado.

5.4. A Auditoria Interna vincula-se ao Conselho de Administração. São atribuições dessas áreas:

I - orientar e promover a aplicação das normas, diretrizes e procedimentos de integridade, risco e conformidade para EMC;

II - coordenar a gestão da conformidade e dos controles internos necessários, incluindo os aspectos de fraude e corrupção;

III - orientar e promover a aplicação das políticas de gestão de riscos de acordo com a legislação vigente; e

IV - exercer outras atribuições que lhe forem conferidas pelo Conselho de Administração.

5.5. Compete aos empregados e funcionários da Companhia:

I - executar as iniciativas da Diretoria para implementação dos objetivos estratégicos;

II - executar a atividades de controle;

III - apoiar a Diretoria na gestão de riscos, auxiliando na identificação, mapeamento e opinando em eventuais ações de resposta; e

IV - executar as ações de respostas aos riscos mapeados dentro dos prazos estabelecidos.

5.6. É assegurada ao titular da área da Auditoria Interna, no exercício de suas atribuições, a possibilidade de se reportar diretamente ao Conselho de Administração nas hipóteses do art. 9º, §4º da Lei n.º 13.303/2016.

ANEXO I

As disposições do anexo I estão discriminadas em arquivo de extensão PDF e encontram-se disponibilizadas no sítio eletrônico oficial da EMC no endereço: www.emc.mg.gov.br

Documento assinado eletronicamente por **Maristela Rangel Pinto**, **Chefe de Gabinete**, em 29/12/2021, às 17:02, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Documento assinado eletronicamente por **Mauro Araújo Câmara**, **Assessor(a)**, em 30/12/2021, às 10:53, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Documento assinado eletronicamente por **Lina Patricia Rocha Laredo**, **Empregada Pública**, em 30/12/2021, às 11:24, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Documento assinado eletronicamente por **Antonio Carlos Caldeira Ramos**, **Conselheiro**, em 30/12/2021, às 11:34, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **40240061** e o código CRC **4B11C73C**.

Guia Metodológico de

GESTÃO DE RISCOS ESTRATÉGICOS

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 ESTRATÉGICOS
Maio de 2020

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

Superintendente Central de Auditoria em Gestão de Riscos e de Programas

Armando Noé Carvalho de Moura Junior

Diretor Central de Auditoria de Gestão de Riscos

Ramon Diego de Carvalho

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

Ramon Diego de Carvalho

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 risco consiste no "(...) processo que trata dos riscos e oportunidades que afetam a criação, a destruição ou a preservação de valor nas organizações." (VIEIRA e BARRETO, 2019, p. 97). Nesse contexto, Brasiliano (2018), em referência ao COSO II - Comitê de Organizações Patrocinadoras da Comissão *Treadway*, 2004, afirma que:

> O gerenciamento de riscos corporativos é um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatíveis com o apetite a risco[1] da organização e possibilitar garantia razoável do cumprimento dos seus objetivos. (BRASILIANO, 2018, p. 52)

No que concerne aos órgãos e entidades governamentais, Vieira e Barreto (2019) apresentam seus benefícios:

> Uma gestão de riscos eficaz melhora as informações para o direcionamento estratégico e para a tomada de decisões de responsabilidade da governança, contribui para a otimização do desempenho na realização dos objetivos de políticas e serviços públicos. Dessa forma, contribui para o aumento da confiança dos cidadãos nas agências públicas, além de prevenir perdas e auxiliar na gestão de incidentes e no atendimento a requisitos legais e regulamentares. (TCU *apud* VIEIRA e BARRETO, 2019, p. 110)

Um dos principais modelos internacionais de referência em gestão de riscos aplicável às organizações públicas é o COSO 2017. De acordo com este modelo, o gerenciamento de riscos corporativos se baseia no desenvolvimento e manutenção de práticas alinhadas com as estratégias e objetivos das organizações, adaptadas, por sua vez, a ambientes de negócios cada vez mais complexos, globais e altamente dependentes de tecnologia.

Nesse sentido, o COSO 2017 ressalta a importância de se considerar o risco tanto no processo de definição das estratégias como na melhoria da performance das organizações. Além disso, enfatiza outros dois aspectos igualmente relevantes e que podem ter um

[1] O apetite a risco consiste no "(...) nível de riscos que a agência pública está disposta a aceitar para atingir os objetivos, criando e protegendo valor para as partes interessadas." (VIEIRA e BARRETO, 2019, p. 99)

grande efeito no valor da organização, quais sejam, a possibilidade de desalinhamento entre a estratégia e a missão, a visão e os valores fundamentais da organização, bem como as implicações da estratégia escolhida.

A figura a seguir ilustra o processo de gerenciamento de riscos corporativos proposto pelo modelo. Nela, verifica-se o destaque da escolha da estratégia. Uma vez definida, esta demanda um processo decisório estruturado que analisa os riscos e alinha os recursos com a missão e a visão da organização.

Figura 1 – Gerenciamento de Riscos Corporativos

Fonte: COSO Gerenciamento de Riscos Corporativos – Integrado com Estratégia e Performance - Sumário Executivo (COSO, 2017).

Nota: Tradução: Missão, Visão e Valores Fundamentais; Estratégia e Objetivos de Negócios; Desempenho Aprimorado.

Segundo Miranda (2017, p.36), o modelo explora a gestão da estratégia e dos riscos a partir de três perspectivas, quais sejam:

- ✓ **Possibilidade de os objetivos estratégicos e de negócios não se alinharem com a missão, a visão e os valores fundamentais da organização.**
- ✓ **As implicações da estratégica escolhida.**
- ✓ **Os riscos na execução da estratégia.**

Na mesma linha, Brasiliano (2018, p. 11) afirma que o COSO 2017 "(...) integra a gestão de riscos com a gestão do desempenho, explorando como que a identificação e avaliação de riscos podem impactar a implementação da estratégia e o alcance dos objetivos de negócios".

Deste modo, o modelo enfatiza a importância do gerenciamento de riscos corporativos no planejamento estratégico e sua incorporação em toda a organização. Assim, apresenta um conjunto de princípios que se organizam em cinco componentes que harmonizam distintos pontos de vista e estruturas operacionais e melhoram as estratégias e a tomada de decisões, conforme figura a seguir:

Figura 2 – Componentes do Gerenciamento de Riscos Corporativos

Fonte: COSO Gerenciamento de Riscos Corporativos – Integrado com Estratégia e Performance - Sumário Executivo (COSO, 2017).

Nota: Tradução: Missão, Visão e Valores Fundamentais; Desenvolvimento de Estratégia; Formulação de Objetivos de Negócio; Implementação e Performance; Valor Aprimorado.

1. **Governança e Cultura *(Governance and Culture*):** a governança estabelece o tom da organização, intensifica a importância e define responsabilidades de supervisão sobre o gerenciamento de riscos corporativos. A cultura consiste em valores éticos, comportamentos esperados e entendimento do risco em toda a organização;

2. **Estratégia e Definição de Objetivos *(Strategy and Objective-Setting*):** o gerenciamento de riscos corporativos, a estratégia e a definição de objetivos trabalham em conjunto no processo de planejamento estratégico. O apetite a risco é definido e alinhado com a estratégia; e os objetivos de negócios colocam em prática a estratégia, além de constituírem alicerce para a identificação, avaliação e resposta aos riscos;

3. **Performance:** é necessário identificar e avaliar os riscos que podem impactar a execução da estratégia e dos objetivos de negócios. Os riscos devem ser priorizados considerando o grau de severidade e o contexto do apetite a risco. Além disso, a organização define as respostas aos riscos e obtém uma visão consolidada do portfólio e do montante de riscos assumidos. Em seguida, os resultados são comunicados às principais partes interessadas envolvidas com a supervisão dos riscos;

4. **Análise e Revisão *(Review and Revision*):** a análise da performance permite refletir sobre o bom funcionamento dos componentes do gerenciamento de riscos corporativos, dentro do contexto de mudanças substanciais, além de ajustes necessários;

5. **Informação, Comunicação e Divulgação *(Information, Communication and Reporting*):** é necessário um processo contínuo de obtenção e compartilhamento de informações precisas, procedentes de fontes internas e externas, bem como das diversas camadas e processos de negócios da organização.

Diante do exposto, o presente Guia foi idealizado em função da necessidade de acompanhamento dos riscos que poderiam prejudicar o alcance dos objetivos estratégicos dos órgãos e entidades do Estado de Minas Gerais.

Neste sentido, é necessária uma avaliação destes riscos, por meio do levantamento de informações com os gestores responsáveis pelas ações estratégicas[2], alinhadas, por sua vez, aos Objetivos e Diretrizes Estratégicas do Estado, previstos no Plano Mineiro de Desenvolvimento integrado – PMDI, visando identificar eventuais fragilidades existentes na estratégia dos órgãos/entidades, em seus processos de trabalho e em sua estrutura de controles.

Como resultado do trabalho, espera-se contribuir para a efetividade do planejamento estratégico das organizações estaduais, por meio do aperfeiçoamento dos controles e minimização dos riscos a níveis aceitáveis.

[2] As ações estratégicas dizem respeito a como serão operacionalizados os objetivos estratégicos, isto é, quais principais ações ou iniciativas serão realizadas visando garantir o cumprimento dos objetivos estratégicos da instituição.

2. DESENVOLVIMENTO DA METODOLOGIA

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, a metodologia de Gestão de Riscos Estratégicos proposta no presente guia, apresenta o seguinte ciclo:

Figura 3 - Ciclo de Gestão de Riscos Estratégicos

2.1. Conhecer o Ambiente e os Objetivos Organizacionais

Esta etapa implica na articulação de objetivos, na definição de parâmetros internos e externos e no estabelecimento de escopo e critérios para o processo de gestão dos riscos. Isso envolve identificar os principais fatores do ambiente interno e externo, analisar as partes interessadas, fixar os objetivos e determinar os critérios de análise e avaliação dos riscos (apetite a risco, tolerância[3] etc.) (Vieira e Barreto, 2019).

[3]A tolerância a risco é o desvio do nível do apetite a risco (BRASILIANO, 2018, p. 129)

Caso o órgão/entidade estadual não possua planejamento estratégico elaborado e atualizado conforme a última versão do Plano Mineiro de Desenvolvimento Integrado (PMDI 2019-2030), recomenda-se que as Diretrizes Estratégicas do PMDI sejam alinhadas ou incorporadas ao planejamento estratégico dos órgãos e entidades como objetivos estratégicos e que as ações estratégicas consistam em um detalhamento desses objetivos estratégicos, em formato de ações. Portanto, as ações estratégicas devem necessariamente ser vinculadas aos objetivos estratégicos da organização, que, por sua vez, devem estar alinhados às Diretrizes Estratégicas do PMDI, a fim de garantir a compatibilidade entre os instrumentos de planejamento estratégico do Estado e de seus órgãos e entidades.

Para a gestão do risco estratégico, o foco encontra-se no acompanhamento de fatores que podem tornar vulnerável o alcance dos objetivos estratégicos. Na condução do levantamento destas informações, é necessário realizar reuniões periódicas de *Brainstorming* com os gestores responsáveis pelas ações estratégicas da organização, alinhadas aos Objetivos Estratégicos e às Diretrizes Estratégicas do Estado definidas no PMDI, em uma análise de cenário quanto as fraquezas e ameaças do ambiente que poderão impactar no atingimento destas ações estratégicas. Para a análise de cenário, pode ser utilizado o método SWOT[4]. As referidas técnicas apresentam os modelos a seguir.

Figura 4 - Brainstorming

[4] Análise SWOT é uma ferramenta utilizada para fazer análise de cenário (ou análise de ambiente), sendo usada como base para gestão e planejamento estratégico de uma corporação ou empresa.

Figura 5 - Método SWOT

Fonte: Rock Content: https://rockcontent.com/blog/como-fazer-uma-analise-swot/

2.2.Definir o Apetite a Risco

Apetite a risco é a quantidade de risco que a organização deseja assumir para conseguir atingir seus objetivos. O apetite a risco está diretamente relacionado à estratégia da organização e é levado em conta na ocasião de sua definição, visto que as estratégias expõem a organização a diferentes riscos. O gerenciamento destes ajuda a administração a selecionar uma estratégia capaz de alinhar a criação de valor com o apetite a risco (Brasiliano, 2018, p. 128).

No que concerne às organizações públicas, o COSO 2007 e a ABNT 2009 salientam que "O tipo e a quantidade de riscos que em conjunto a organização está preparada para buscar, reter ou assumir correspondem à atitude da agência pública perante o risco e reflete toda a filosofia da organização, influenciando sua cultura e estilo gerencial." (COSO e ABNT *apud* VIEIRA e BARRETO, 2019, p. 99).

Adicionalmente, Vieira e Barreto (2019) 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" (VIEIRA e BARRETO, 2019, p. 141). 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.

É recomendável que a declaração contenha, no mínimo, os seguintes elementos: 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.

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, o apetite a risco foi aprovado pelo Comitê Estratégico de Governança e, ato contínuo, oficializado pela Resolução CGE nº 19/2020.

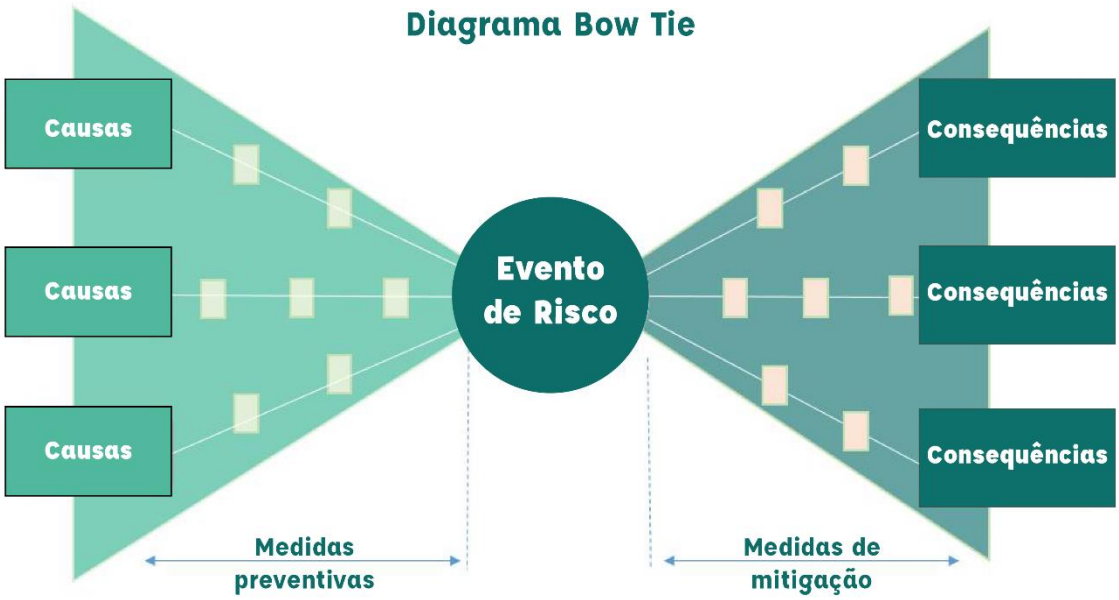
2.3. Identificar os Riscos na Execução

Nessa etapa, devem ser identificados os eventos em potencial que, caso ocorram, afetarão a organização e terão algum efeito adverso na capacidade de implementar adequadamente a estratégia. 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)

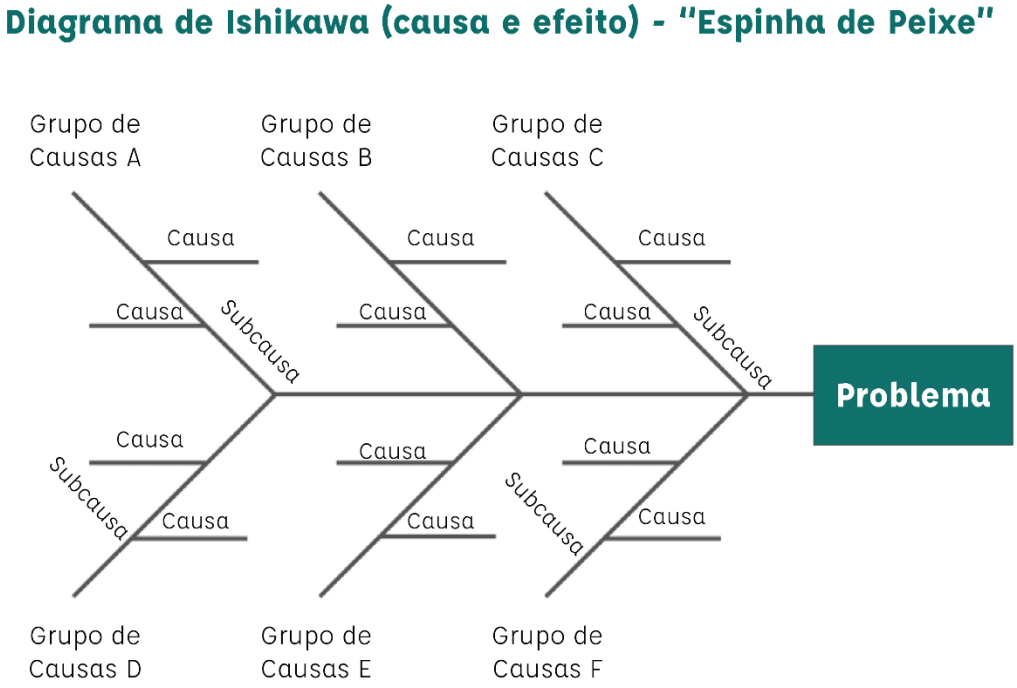
Para identificar os riscos, há uma boa variedade de ferramentas e técnicas disponíveis. Pode-se citar como exemplos de técnicas: *Brainstorming*, Diagrama de *Ishikawa*, Método *Bow Tie*, entre outros, conforme figuras a seguir. A norma ISO 31010/12 apresenta diversas técnicas de identificação de riscos.

Figura 6 - 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.

Figura 7 – Diagrama de *Ishikawa*



Fonte: Assessoria de Comunicação Social - CGE-MG

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). Nesta etapa de identificação dos riscos, é necessário relacionar cada risco com sua dimensão[5], assim como definir o indicador-chave[6] de risco. As dimensões do risco a serem utilizadas são:

Político: Principalmente por ser instituições públicas, as organizações do Estado sofrem uma considerável influência dos acontecimentos no ambiente político.

Ex.: Emenda parlamentar impactando a distribuição do orçamento do Estado.

Tecnológico: Dimensão relacionada ao desenvolvimento tecnológico, acesso às inovações e disponibilidade de ferramentas, materiais e internet.

Ex.: Possibilidade do espaço para armazenamento de dados pelas organizações do Estado não suportar o aumento das informações processadas diariamente.

Legal, Regulatório ou Procedimentos: Leis ou regulamentos externos podem impactar as organizações do Estado no alcance dos objetivos/ações estratégicos, bem como os procedimentos internos de trabalho.

Ex.: Regulamento exigindo a apresentação pelos órgãos/entidades do Estado, em 180 dias, de todos os terrenos pertencentes ao poder público.

Físico ou Logístico: Ambiente físico ou logístico refere-se ao provimento de recursos e espaços para a execução de todas as atividades da organização.

Ex.: Necessidade imediata de desocupação da sede da instituição do Estado para reparos na rede elétrica e hidráulica.

Econômico ou financeiro: Possibilidade da situação econômica e financeira do país impactar o alcance dos objetivos/ações estratégicos dos órgãos/entidades do Estado.

Ex.: Exigência de redução de custos nos órgãos/entidades do Estado.

[5] Dimensão de risco é uma categoria agrupada segundo a origem/natureza do risco.
[6] 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.

Força de Trabalho: Refere-se ao impacto na estratégia causado por questões relacionadas aos servidores, cedidos, terceirizados, contratados, etc.

Ex.: Greve dos terceirizados.

Partes Interessadas: Partes Interessadas são os demais intervenientes nos processos das organizações do Estado, tais como: cidadão, sociedade, fornecedores, demais órgãos, etc.

Ex.: Ausência de informações das estatais.

As informações levantadas devem ser consolidadas no Mapa de Riscos (tabela 01), que detalhará nesta etapa, entre outras informações, as ações estratégicas, os eventos de riscos estratégicos, as dimensões dos riscos, os controles associados existentes, as causas e as consequências possíveis, bem como os indicadores-chaves de riscos e sua periodicidade.

Tabela 1 - Mapa de Riscos

Diretriz Estratégica	Objetivo Estratégico	Ação Estratégica	Unidade Responsável	Causa	Evento de Risco	Consequência	Dimensão	Controle Existente	Probabilidade	Impacto	Valor do Risco	Classificação do Risco	Indicador Chave de Risco	Periodicidade de Apuração do Indicador Chave de Risco

Fonte: Kaplan & Mikes (2012) adaptado CGE-MG

Ressalta-se que a probabilidade, o impacto, o valor do risco e a classificação do risco serão inseridos na tabela quando da avaliação do risco, próxima etapa do ciclo de gestão, a ser tratado na seção seguinte.

Ademais, os principais conceitos presentes na tabela e ainda não esclarecidos constam a seguir:

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). Sendo assim, se refere a um evento ou uma condição incerta que, se ocorrer, terá um efeito negativo na execução da ação estratégica.

Causa, por sua vez, é a fonte do risco ou vulnerabilidade existente na organização que dá origem a um evento. Já a consequência diz respeito ao efeito que o evento de risco terá sobre o alcance das ações estratégicas planejadas.

Adicionalmente, 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)

A periodicidade de apuração dos indicadores chaves de risco, por sua vez, se refere ao espaço temporal em que os indicadores serão medidos, tal como: mensal, bimestral, quadrimestral, semestral ou anual.

2.4.Avaliar os Riscos

O COSO (2007) destaca a importância desta etapa de avaliação dos riscos:

> (...) a avaliação de riscos permite que uma organização considere até que ponto os eventos em potencial podem impactar a realização dos objetivos. Essa avaliação fundamenta-se em duas perspectivas, probabilidade e impacto, e geralmente utiliza uma combinação de métodos qualitativos e quantitativos. (COSO 2007 *apud* SOUZA e SANTOS, 2019, p.129)

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 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

Tabela 2 - Pesos da Probabilidade

PROBABILIDADE			
DESCRIÇÃO	**OCORRÊNCIA**	**FREQUENCIA**	**PESO**
Quase Certo	Evento que ocorre quase sempre	> = 90%	5
Muito Provável	Evento que ocorre na maioria das circunstâncias	>= 75%<= 90%	4
Provável	Evento que provavelmente ocorre	>= 40% <75%	3
Pouco Provável	Evento que deve ocorrer em algum momento	>= 10% <40%	2
Rara	Evento pode ocorrer em circunstâncias excepcionais	< 10%	1

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

Tabela 3 - Pesos do Impacto

IMPACTO		
DESCRIÇÃO	**OCORRÊNCIA**	**PESO**
Muito Alto	Prejudica totalmente o alcance dos objetivos estratégicos / ações estratégicas (entrega de produtos/serviços e cumprimentos de metas)	10
Alto	Prejudica em mais de 50% o alcance dos objetivos estratégicos / ações estratégicas (entrega de produtos/ serviços e cumprimentos de metas)	7
Moderado	Prejudica parcialmente o alcance dos objetivos estratégicos / ações estratégicas (entrega de produtos/serviços e cumprimento de metas)	5
Pequeno	Necessária ação gerencial para impedir que seja prejudicado o alcance dos objetivos estratégicos / ações estratégicas (entrega de produtos/serviços e cumprimento de metas)	3
Irrelevante	Não prejudica o alcance dos objetivos estratégicos / ações estratégicas	1

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

Determinado o valor de cada risco, propõe-se a utilização da matriz de riscos (tabela 04), para classificar qualitativamente o valor do risco através da definição dos níveis de risco (tabela 05), os quais 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 A 5	

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

Por fim, a partir do apetite a riscos inicialmente definido, a organização determinará quais riscos poderão ser aceitos e quais necessariamente deverão ser minimizados, na perspectiva metodológica que os extremos e altos deverão ser tratados, conforme seção a seguir.

2.5.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).

Para o tratamento dos riscos, o gestor deve identificar e selecionar as respostas a riscos que minimizem estes 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.

Figura 8 - 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

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, 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.

O tratamento pressupõe 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. Ao propor as ações de controle em resposta aos riscos, o gestor deve considerar o apetite a risco estabelecido, bem como os custos e os benefícios envolvidos.

A seguir, apresenta-se modelo de Plano de Ação:

Tabela 6 – Modelo de Plano de Ação

Riscos Mapeados												Plano de Ação							
Nº	Diretriz Estratégica	Objetivo Estratégico	Ação Estratégica	Unidade Responsável	Causa	Evento de Risco	Consequência	Controle Existente	Valor do Risco	Classificação do Risco	Indicador Chave de Risco	Periodicidade de Apuração do Indicador Chave de Risco	Tipo de Tratamento a ser Realizado	Justificativa Caso Não Adote Ação para os Riscos Extremos e Altos*	Descrição da Ação	Gestor Responsável	Data de Início da Implantação	Data Final da Implantação	Status[1]	Observações[2]

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

* Conforme apetite a riscos aprovado pela organização;

[1] Segundo os seguintes níveis: 1- a iniciar; 2 - em execução; e 3 - concluída;

[2] Com o objetivo de inserir informações qualitativas sobre o gerenciamento, execução e resultados do Plano de Ação, caso necessário.

2.6.Comunicar e Monitorar

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.

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

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 estratégicos fornece a informação atualizada e objetiva identificar fragilidades e possibilidades de melhorias, bem como verificar o desempenho e eficiência do Plano de Ação, operacionalizado por meio dos controles implementados. Lembrando que os riscos mudam ao longo do tempo e devem ser monitorados para que a organização possa realizar os ajustes necessários.

Após a aplicação do presente modelo de gestão de riscos estratégicos, para a apresentação dos resultados e acompanhamento do monitoramento, uma boa prática de transparência consiste no desenvolvimento de reportes, por meio de *Dashboards*[7].

Por fim, na perspectiva do monitoramento da evolução dos riscos estratégicos, a aferição dos indicadores chaves de risco de acordo com a periodicidade definida, permite a atualização dos cenários de relevância dos riscos.

[7] *Dashboards* são painéis que mostram métricas e indicadores importantes para alcançar objetivos e metas traçadas de forma visual, facilitando a compreensão das informações geradas.

3. BIBLIOGRAFIA

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

➞ PRICEWATERHOUSE COOPERS LLP. **COSO: gerenciamento de riscos corporativos** - Estrutura Integrada - 2007.

4. 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.

➞ COSO **Gerenciamento de riscos corporativos - estrutura integrada**: Sumário Executivo e Estrutura (versão em Português), vol.2.AICPA, 2007.

➞ COSO – **Gerenciamento de riscos corporativos – integrado com estratégia e performance** - Sumário Executivo - 2017.

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

➞ KAPLAN, Robert; MIKES, Anette. **Managing risks: a new framework**. Harvard Business Review. June, 2012.

➞ 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.

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

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