Cartilha de Implementação da Gestão de Riscos

1ª EDIÇÃO - 2024

CONTROLADORIA GERAL DO MUNICÍPIO

Prefeitura de Salvador

CGM

PREFEITURA MUNICIPAL DO SALVADOR

BRUNO SOARES REIS
Prefeito

MARIA RITA GOES GARRIDO
Controladora Geral do Município

LUÍS HENRIQUE GUIMARÃES BRANDÃO
Corregedor Geral

MARIA JÚLIA CASTRO WEGELIN
Coordenadora Central de Auditoria

MARCELO E SOUZA SILVA
Coordenador Central de Acompanhamento dos Núcleos de Controle Interno

ALLYSSON VIEIRA DA CONCEIÇÃO
Coordenador Central de Controle

CAMILA CARVALHO FONSECA
Coordenadora Central de Transparência, Normas e Informações Gerenciais

Elaboração:

SIMONE DOS SANTOS ANDRADE SILVA
Chefe do Núcleo de Auditoria De Gestão de Riscos, Integridade e Programa de Governo

SANDRO AUGUSTO MAGALHÃES RIBEIRO
Auditor Interno

https://cgm.salvador.ba.gov.br
instagram: @cgmsalvador

SUMÁRIO

1. Introdução

Diante dos desafios que se impõem à administração pública no Brasil, colocar em prática um processo de tomada de decisão baseada em riscos, tem como finalidade ampliar a capacidade institucional em lidar, de forma mais eficaz, com as incertezas e contribuir para o uso eficiente e efetivo dos recursos públicos, mediante a identificação, avaliação e tratamento dos riscos, que podem afetar o alcance dos objetivos e resultados almejados.

No caso específico da Prefeitura Municipal do Salvador (PMS), o Planejamento Estratégico 2021-2024, fruto de um processo de análise e reflexão acerca dos grandes objetivos a serem alcançados, em benefício dos cidadãos soteropolitanos, contemplou áreas temáticas distribuídas em sete eixos estratégicos, dentre os quais o da Capital da Eficiência, que visa aprimorar os instrumentos de gestão, incluindo a perspectiva baseada em gerenciamento de riscos.

Nesse contexto, a implementação da Gestão de Riscos na PMS, tem o potencial de melhorar a capacidade dos órgãos e entidades, da administração direta e indireta, em antecipar e responder a eventos incertos e indesejados, salvaguardando a implementação da estratégia e o alcance dos seus objetivos, no cumprimento da sua missão institucional.

A adoção de tal medida, capitaneada pela alta administração, configura importante indicador de maturidade gerencial e requisito necessário a uma boa governança.

Assim, certos da relevância do tema para a administração municipal, esta cartilha apresenta uma sequência de passos, exemplos de boas práticas e procedimentos mínimos necessários a serem observados pelos gestores para a implantação da Gestão de Riscos na sua instituição.

2. Objetivo da Cartilha

A presente cartilha tem por objetivo auxiliar os órgãos e entidades municipais quanto aos procedimentos necessários à Implementação da Estrutura e do Processo de Gestão de Riscos, a partir da apresentação de boas práticas a serem observadas.

Cabe ressaltar que as abordagens apresentadas nesse documento são orientativas, podendo sofrer adequações ao longo do processo de implementação da gestão de riscos na PMS, visando atender às necessidades de cada organização.

3. Público-Alvo

As orientações trazidas na presente cartilha destinam-se aos diversos atores municipais comprometidos com a implementação da gestão de riscos, com destaque para os dirigentes máximos, gestores, servidores, colaboradores, além de um importante protagonista denominado gestor do risco.

Dica para o gestor

Gestor do risco é a pessoa, papel ou unidade do órgão/entidade com autoridade e responsabilidade para gerenciar um risco.

Portal do Servidor (Gov)

4. Por que implementar a Gestão de Riscos?

As atividades de qualquer organização, independentemente do tipo e tamanho, envolvem riscos que, se não gerenciados adequadamente, podem se materializar e comprometer sua capacidade de gerar, preservar ou entregar valor.

Riscos
Eventos que podem ocorrer e afetar negativamente (ameaças) ou positivamente (oportunidades) o alcance dos objetivos de uma instituição ou unidade organizacional.

Nesse sentido é possível dizer que existem duas maneiras de lidar com os riscos:

1. ser surpreendido por eventos que podem impactar adversamente o alcance dos objetivos da organização e então reagir a eles, o que caracteriza a cultura de "apagar incêndios"; ou

2. antecipar-se a eles, adotando medidas conscientes que mantenham ou reduzam a probabilidade ou o impacto dos eventos nos objetivos.

Apenas a segunda maneira pode ser chamada de gestão de riscos, que também habilita a organização a aproveitar oportunidades.

Desse modo, entendendo a Gestão de Risco como elemento essencial para uma boa governança, ao priorizar a sua implementação a organização aumenta a probabilidade de alcance dos seus objetivos, melhora a identificação de oportunidades e ameaças, e estabelece uma base confiável para a tomada de decisão e para o planejamento governamental.

Dica para o gestor

A Gestão de Riscos efetivamente implantada possibilita ao gestor antecipar, identificar e lidar com situações de risco e a se preparar para enfrentá-los da melhor maneira possível.

5. Qual o contexto da Gestão de Riscos em Salvador?

A Gestão de Riscos em Salvador foi inaugurada pelo Decreto Municipal nº 37.837/2023 que aprovou a Política de Governança e determinou que a alta administração deverá estabelecer, manter, monitorar e aprimorar sistema de gestão de riscos e controles internos.

Abordando de forma mais específica e detalhada o tema, em 29/11/2023, foi publicado o Decreto nº 37.836/2023 estabelecendo as diretrizes gerais da Gestão de Riscos no âmbito do Poder Executivo Municipal.

Esse mesmo normativo tornou obrigatória a instituição de uma política de gestão de risco para cada órgão e entidade, cabendo-lhes adotar as medidas necessárias à implementação da Estrutura e do Processo de Gestão de Riscos no âmbito de suas unidades.

(...)

"Art. 15. A alta administração dos Órgãos e Entidades do Poder Executivo Municipal deverá estabelecer, manter, monitorar e aprimorar Sistema de Gestão de Riscos e Controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional."
(Decreto 37.837/2023).

ATENÇÃO!

A Nova Lei de Licitações e Contratos Administrativos Nº 14.133/2021, que passou a vigorar por completo a partir de 01.01.2024, estabeleceu no seu Art. 11, parágrafo único, a responsabilidade da alta administração, do órgão ou entidade, pela governança das contratações e a obrigação de implementar processos e estruturas, inclusive ***de gestão de riscos e controles internos.***

6. Entendendo a Gestão de Riscos

- **Gestão de Riscos ou Gerenciamento de Riscos?**

A Gestão de Riscos é uma atividade coordenada pela alta administração para dirigir e controlar uma organização no que se refere a riscos.

Já o Gerenciamento de Riscos, parte integrante da Gestão de Riscos, é compreendido como um processo dinâmico e permanente para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza quanto ao alcance dos objetivos da organização.

- **Qual a abrangência da Gestão de Riscos? Onde pode ser aplicada?**

A gestão de riscos abrange todos os tipos de organização e pode ser aplicada onde existe a chance de ocorrer um evento incerto.

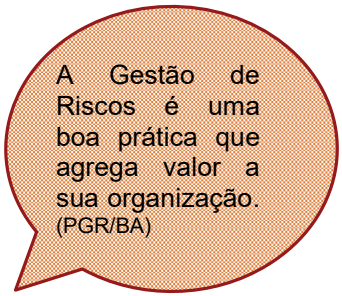
Segundo Manual de Gestão de Riscos do TCU (2020), pode ser aplicada a qualquer contexto organizacional que tenha um objetivo claro, ou do qual resulte um produto ou serviço definido e que esteja sujeito a incertezas.

Risco zero não existe, pois sempre há uma chance de ocorrer um evento incerto.

- **Qual o objeto da Gestão de Riscos?**

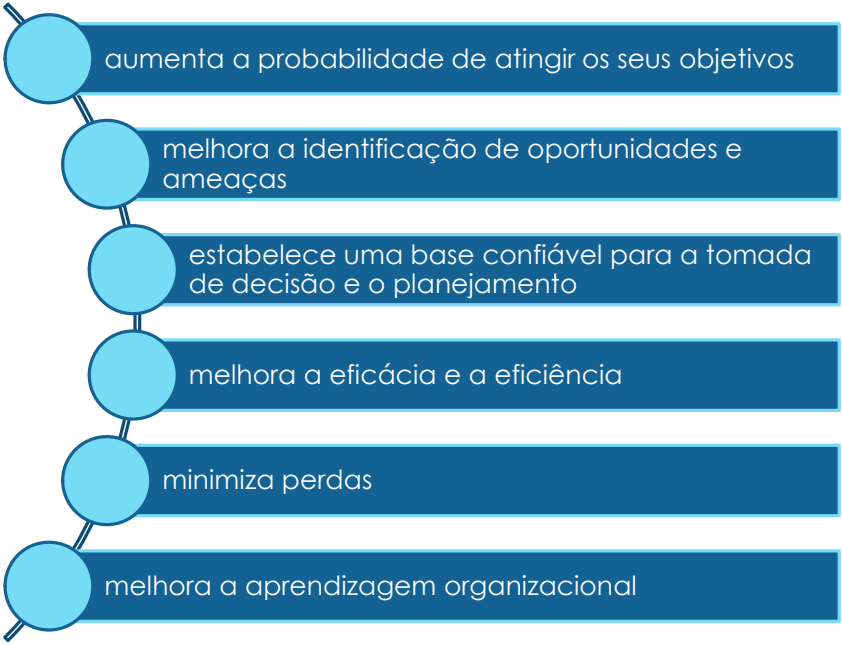
Podem ser objeto da gestão de riscos:

1. objetivos da organização;
2. resultados;
3. metas;
4. unidades organizacionais;
5. processos de trabalho;
6. atividades;
7. projetos;
8. informações/dados (segurança da informação);
9. integridade e ética;
10. iniciativas ou ações de plano institucional;
11. recursos que dão suporte à realização dos objetivos do órgão ou entidade.



- **Quais os Benefícios da Gestão de Riscos?**

A organização pública que incorpora a gestão de riscos à sua cultura e às suas atividades alcança os seguintes benefícios:



Tudo isso se traduz em melhores resultados na implementação de políticas públicas e na prestação de serviços de interesse da sociedade.

ATENÇÃO!

A gestão de riscos não resolve (milagrosamente) todos os problemas da organização, mas ajuda a prevenir e a mitigá-los.

- **Papéis e responsabilidades**

Na Prefeitura Municipal de Salvador, nos termos do Decreto nº 33.988/2021, que regulamenta o Sistema de Controle Interno Integrado do Poder Executivo Municipal, os papéis e as responsabilidades de cada um dos participantes envolvidos nas atividades de gestão de riscos e controle segue o Modelo das Três Linhas[1], do *The Institute of Internal Auditors* (IIA).

Esse modelo constitui-se em um guia para as organizações melhorarem a governança e o gerenciamento de riscos, a partir da definição de três linhas de responsabilidades dentro da estrutura de Governança.

A figura a seguir ajuda a esclarecer os papéis e responsabilidades de cada linha e a forma com que se dá a colaboração e a comunicação entre elas.

Figura 01: O Modelo das Três Linhas do The IIA

[1] Atualização da Declaração de Posicionamento do IIA: As Três Linhas De Defesa No Gerenciamento Eficaz de Riscos e Controles, ocorrida em 2020 pelo *The Institute of Internal Auditors* (IIA).

Aplicando o referido modelo do IIA aos órgãos e entidades da PMS, obtém-se a seguinte definição das linhas de atuação na Gestão de Risco:

- **Primeira linha:** composta por servidores, gestores e responsáveis que atuam no gerenciamento de riscos dos processos organizacionais;
- **Segunda linha**: atuam comitês internos de governança, diretorias, assessorias específicas, assessorias jurídicas, unidades setoriais de controle ou outras unidades equivalentes designadas, para tratar de riscos e controles internos;
- **Terceira linha**: atua a auditoria interna do órgão central de controle interno[2] que tem a responsabilidade de fornecer avaliação e consultoria independente e objetiva sobre os processos de gestão de riscos, controles internos e governança, que os gestores da primeira e segunda linhas são responsáveis.

▪ A relação entre governança e gestão

[2] A Controladoria Geral do Município do Salvador é o órgão central do Sistema de Controle Interno Integrado – SICOI.

O papel da governança é liderar a organização, observando os princípios da integridade, da transparência e da prestação de contas à sociedade, para o atingimento dos seus objetivos institucionais.

A responsabilidade da gestão é atingir os objetivos organizacionais, desempenhando os papéis da primeira e segunda linhas.

A interação entre governança e gestão pode ser melhor compreendida observando a figura a seguir:

Figura 02: Relação entre governança e gestão

Fonte: Referencial Básico de Governança do TCU (2ª Versão)

Dessa forma, enquanto a gestão é inerente e integrada aos processos organizacionais, sendo responsável pelo planejamento, execução, controle, ação, enfim, pelo manejo dos recursos e poderes colocados à disposição de órgãos e entidades para a consecução de seus objetivos, a governança provê direcionamento, monitora, supervisiona e avalia a atuação da gestão, com vistas ao atendimento das necessidades e expectativas dos cidadãos e demais partes interessadas. (TCU, 2014)

7. A Gestão de Riscos na PMS

A gestão de riscos na PMS foi formatada numa abordagem aplicável a todas as organizações da administração municipal e tem como referências principais:

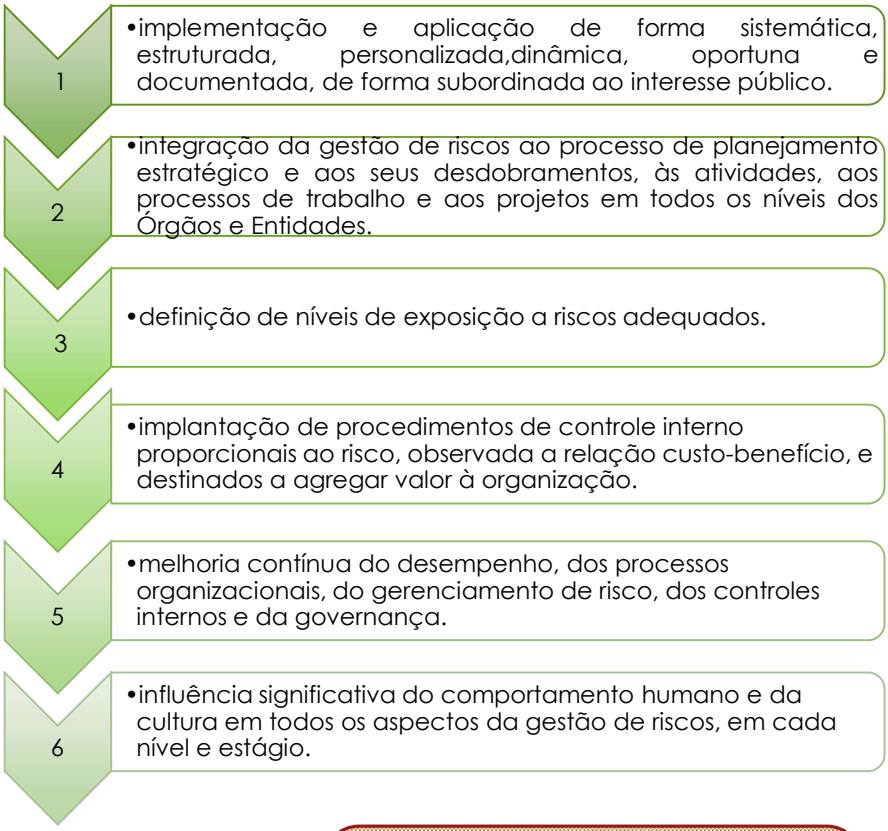
Nos termos da ISO 31000:2018, a implementação da Gestão de Riscos requer uma arquitetura que contemple os seguintes componentes estruturantes:

- Princípios;
- Estrutura;
- Processo.

A sinergia desse trinômio (princípios, estrutura e processo) é fundamental para que a gestão de riscos seja eficiente, eficaz e consistente. Muitas vezes, esses componentes podem existir total ou parcialmente na organização, necessitando de algum tipo de adaptação ou melhoramento.

Nesse sentido, foram estabelecidos no Decreto n° 37.836/2023, que regulamenta as diretrizes da Gestão de Riscos no âmbito do Poder Executivo, os princípios a serem observados para implantação da Gestão de Riscos no Município:

Figura 03: Princípios para implementação da Gestão de Riscos



Dica para o gestor

Esses princípios constituem os fundamentos essenciais para uma gestão de riscos eficaz.

Orientada por esses princípios, será apresentada uma sequência de passos a serem observados pelos gestores na Implementação das etapas de Estrutura e do Processo de Gestão de Riscos.

- **Estrutura de Gestão de Riscos:** Criação de um ambiente sistematizado de gestão de riscos, correspondendo ao conjunto de política, processo, definição de responsabilidades e outros elementos necessários para a promoção da integração da gestão de riscos às atividades e funções dos órgãos e entidades municipais.
- **Processo de Gestão de Riscos**: Implantação e manutenção do conjunto de atividades que se inicia com a análise do contexto e definição de escopo e se encerra com a elaboração do plano de tratamento de riscos, sendo a comunicação e o monitoramento, atividades relevantes para a integração de todas as etapas do Processo de Gestão de Riscos.

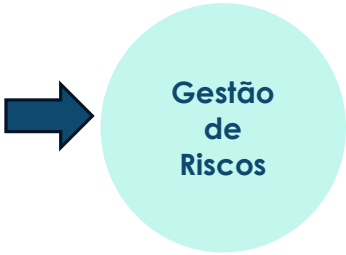
No apêndice dessa cartilha, a título de sugestão, foram anexados alguns modelos de documentos relacionados à implantação da Gestão de Riscos, que podem ser adaptados para a realidade de cada órgão e entidade municipal.

8. Estrutura da Gestão de Riscos

O propósito da estrutura da gestão de riscos é apoiar a organização na integração da gestão de riscos às atividades e funções significativas. A eficácia da gestão de riscos dependerá da sua integração na governança e em todas as atividades da organização, incluindo a tomada de decisão. (ISO 31000: 2018)

Dito isso, a Implementação da Estrutura de Gestão de Riscos de Salvador envolverá a criação de um ambiente sistematizado, personalizado de acordo com as necessidades de cada órgão ou entidade e composto por um conjunto de elementos, a exemplo de:

- **Política de gestão de riscos**
- **Processo de gestão de riscos**
- **Definição de responsabilidades**
- **Plano de comunicação**
- **Monitoramento e análise crítica**



A seguir, são apresentados 07 (sete) passos fundamentais a serem observados pela alta administração para a estruturação da gestão de riscos em sua organização:

Passo 1: Comprometimento da Alta Administração

Passo 2: Entendimento sobre a Gestão de Riscos

Passo 3: Definição de Responsabilidades

Passo 4: Elaboração da Política de Gestão de Riscos

Passo 5: Definição do Apetite a Riscos

Passo 6: Elaboração de um Plano de Comunicação

Passo 7: Monitoramento e Análise Crítica

Passo 1

Comprometimento da Alta Administração

A demonstração de apoio, liderança e comprometimento da alta administração é fundamental para o êxito da gestão de riscos. Esse passo se concretizará mediante a implementação dos componentes que alicerçam a estrutura e das ações que asseguram a alocação dos recursos necessários para gerenciar riscos.

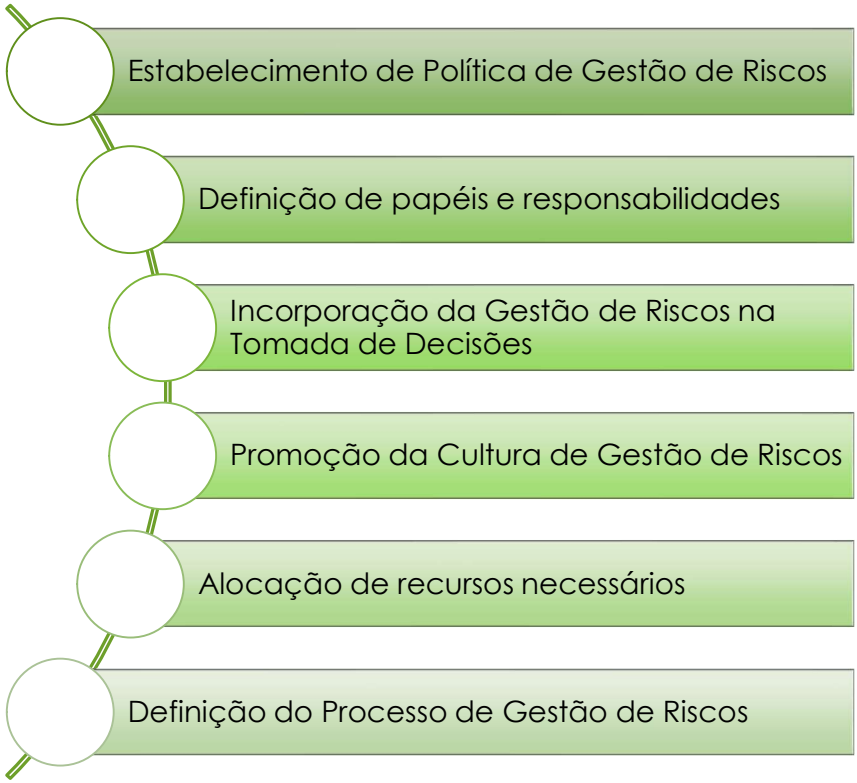
Nesse contexto, o Referencial Básico de Gestão de Riscos do TCU, ao tratar do papel de liderança da alta administração, destaca:

> (...)
>
> Espera-se que assumam um compromisso forte e sustentado com a gestão de riscos, promovendo-a e dando suporte, e exerçam supervisão para obter comprometimento com o tema em todos os níveis da organização, de modo que se possa ter uma expectativa razoável de que, no cumprimento da sua missão institucional, a organização entende e é capaz de gerenciar os riscos associados à sua estratégia para atingir os seus objetivos de gerar, preservar e entregar valor às partes interessadas, tendo o cidadão e a sociedade como destinatários principais. (TCU, 2018)

Ressalvadas as peculiaridades e os contextos específicos de cada órgão ou entidade da Administração Municipal, de maneira geral, o

apoio, liderança e comprometimento da alta administração na gestão de riscos ocorrerá da seguinte forma:

Figura 04: Forma de comprometimento da alta administração



- **Ações sugeridas**

1ª ação: Reunião da Alta Administração com o *staff* do órgão ou entidade (diretoria, gerência, coordenadoria, assessoria, chefia de setor etc.), a fim de:

- Relacionar eventos significativos que prejudicaram atividades, resultados ou a imagem do órgão ou entidade;
- Relacionar os efeitos (possíveis danos) enfrentados pelo órgão ou entidade decorrentes da inexistência de mapeamento e plano de tratamento dos eventos de risco materializados;
- Debater as vantagens e desvantagens de deixar o órgão ou entidade exposto(a) a esses e a outros eventos de risco que ainda não se materializaram;
- Declarar os objetivos e os benefícios esperados com a implementação da gestão de riscos.

2ª ação: Assinatura de um termo de compromisso pela alta administração, conforme Anexo I, aprovando a implantação da gestão de riscos;

3ª ação: Institua o Comitê Interno de Governança (CIG), conforme determina o Decreto Municipal 37.837/2023.

- **Responsáveis pelas ações**

Alta Administração e *staff* da organização.

Produtos esperados:

a) Identificação dos principais eventos de riscos e seus efeitos já enfrentados pelo órgão/entidade;

b) Declaração dos objetivos e os benefícios esperados com a implementação da gestão de riscos;

c) Assinatura do termo de compromisso de implantação da gestão de riscos.

d) Portaria instituindo Comitê Interno de Governança, com a nomeação dos seus integrantes, conforme Anexo II.

Passo 2

Entendimento sobre a Gestão de Riscos

A compreensão acerca dos conceitos, termos, diretrizes e boas práticas de gestão de riscos é fundamental para a disseminação de uma cultura de riscos pautada nas peculiaridades de cada organização e no equilíbrio necessário à sua implementação.

Nesse passo, relembrando o conceito das linhas de atuação do IIA (Tópico 6. Entendendo a Gestão de Riscos – Papéis e Responsabilidades), a sugestão é que o processo de compreensão e conhecimento acerca dos assuntos de gestão de riscos observe as seguintes fases:

1ª fase: Inicie com a alta administração e servidores que atuam na segunda linha de atuação, com a responsabilidade de estruturação da gestão de riscos no órgão ou entidade;

2ª fase: Em seguida, parta para a Primeira linha, denominada proprietária do risco, a ser capacitada de forma gradual, por unidade organizacional, na medida que a implementação da gestão de riscos avance na organização;

3ª fase: Estimule e promova a aprendizagem dos servidores e demais colaboradores do órgão ou entidade, sobre a gestão de riscos.

Dica para o gestor

A capacitação sobre gestão de riscos para servidores e colaboradores poderá ocorrer com a participação em cursos gratuitos promovidos por escolas de governo, a exemplo da ENAP.

- **Ações sugeridas**

1ª ação: Institua um grupo de trabalho ou atribua ao Comitê Interno de Governança (CIG) a tarefa de dar início à implementação da gestão de riscos do órgão ou entidade;

2ª ação: Participe de cursos e seminários sobre gestão de riscos, bem como estude os principais referenciais teóricos e boas práticas sobre o tema;

Principais normativos e manuais:
- ISO 31000:2018;
- Manual de Gestão de Riscos e Referencial de Gestão de Riscos do TCU;
- Metodologia de Gestão de Riscos da

3ª ação: Analise as informações da organização, tais como: regimento, organograma, planejamento estratégico e processos mapeados (se existentes);

4ª ação: Conheça a experiência de outras organizações que já avançaram em gestão de riscos, inteirando-se dos benefícios que estão sendo colhidos;

5ª ação: Elabore plano de ação para implementação da gestão de riscos no órgão ou entidade.

6ª ação: Fomente o conhecimento sobre gestão de riscos em reuniões e *workshops* internos.

- **Responsáveis pelas ações**

A alta administração pela definição dos papéis do CIG e este, com o apoio do gestor do risco, *staff e* servidores da organização para as demais ações.

Produtos esperados:

a) Grupo de trabalho ou atribuição ao Comitê Interno de Governança

b) Plano de ação para implementação da gestão de riscos;

c) Capacitação do corpo técnico realizada.

Passo 3

Definição de Responsabilidades

A definição de papéis e responsabilidades é essencial para o funcionamento regular e eficaz de uma organização. Se bem identificados melhoram a comunicação, reduzem conflitos, aumentam a eficiência e promovem o alinhamento com os objetivos almejados.

Desse modo, a definição clara dos papéis e responsabilidades de cada grupo de profissionais e de unidades da organização contribuem para uma gestão de riscos eficaz, propiciando aos colaboradores o entendimento acerca dos limites das suas atribuições e a sua participação na estrutura de gestão de riscos, permitindo que estejam informados, habilitados e autorizados a exercer seus papéis e responsabilidades no gerenciamento de riscos.

(10 passos para a Boa Gestão de Riscos. TCU, 2018).

> Responsabilidades claras devem ser definidas para que cada grupo de profissionais entenda os limites de suas responsabilidades e como seus cargos se encaixam na estrutura geral de gestão de riscos da organização (IIA, 2013).

- **Ações sugeridas**

1ª ação: Analise o contexto interno e externo da organização, a complexidade de suas operações, o sistema vigente de gestão de riscos, a estrutura de governança e os recursos disponíveis;

2ª ação: Defina um conjunto suficiente de papéis e responsabilidades para dar início à estruturação da gestão de riscos a partir do modelo das três linhas do IIA;

3ª ação: Identifique os gestores ou proprietários de riscos diretamente responsáveis por apoiar a cultura de gestão de riscos e por gerenciar riscos dentro de suas esferas de responsabilidade (primeira linha de atuação).

4ª ação: Atribua responsabilidades a unidades ou funções, como por exemplo aos Gestores, a identificação de eventos de risco;

5ª ação: Elabore matriz RACI de responsabilidades, conforme Anexo III. Esta ferramenta visa alinhar as equipes de trabalho dos órgãos e entidades quanto a compreensão dos seus papéis e responsabilidades.

A elaboração da Matriz RACI consiste em definir: **Responsável**, **Autoridade**, **Consultado** e **Informado**, para cada uma das etapas e atividades listadas.

- **Responsáveis pelas ações**

O CIG com o apoio do gestor do risco e *staff* da organização. Para a alta administração compete a aprovação da matriz de responsabilidades.

Produtos esperados:
a) Definição de papéis e responsabilidades;
b) Matriz RACI de responsabilidades aprovada.

Passo 4

Elaboração da Política de Gestão de Riscos

A política de gestão de riscos é um instrumento normativo que reúne a declaração das intenções e as diretrizes gerais de uma organização relacionadas à gestão de riscos.

De acordo com o Decreto Municipal nº 37.836/2023, a política de gestão de riscos dos órgãos e entidades municipais deverá especificar, como referencial básico:

I - princípios e objetivos organizacionais;

II - diretrizes:

a) **gestão de riscos integrada** ao planejamento estratégico, aos processos e às políticas da organização;

b) **monitoramento periódico** dos riscos, identificação, avaliação e tratamento;

c) **medição e avaliação do desempenho** da gestão de riscos;

d) forma de **integração** das instâncias dos Órgãos e Entidades responsáveis pela gestão de riscos;

e) **utilização de metodologia e ferramentas** para o apoio à gestão de riscos;

f) **desenvolvimento contínuo** dos agentes públicos em gestão de riscos; e

g) **melhoria permanente** da estrutura e do processo de gestão de riscos.

III - competências e responsabilidades para a efetivação da gestão de riscos no âmbito dos Órgãos e Entidades.

Também em consonância com a política de gestão de riscos os Órgãos e Entidades devem considerar, ao efetuarem o

mapeamento e avaliação dos riscos, no mínimo, as seguintes tipologias de riscos:

Quadro 01 – Tipologia dos Riscos	
TIPOLOGIA	**DEFINIÇÃO**
Estratégicos	Eventos que podem impactar na missão, nas metas ou nos objetivos estratégicos do órgão ou entidade.
Operacionais	Eventos que podem comprometer as atividades do órgão ou entidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas.
Legais	Eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade.
Financeiros/ Orçamentários	Eventos que podem comprometer a capacidade do órgão ou entidade de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações.
De integridade	Eventos relacionados a fraudes, irregularidades e/ou desvios éticos e de conduta que podem comprometer os valores e padrões preconizados pelo Poder Público municipal e a realização de seus objetivos.

Convém ressaltar que cada órgão ou entidade, em função das suas peculiaridades, pode ter riscos específicos, que devem ser considerados na sua política de gestão de riscos, a exemplo de riscos ambientais, tecnológicos, atuariais, de corrupção, de imagem, dentre outros.

- **Ações sugeridas**

1ª ação: Conheça as regulamentações sobre a gestão de riscos de outros órgãos/entidades, trocando informações que otimizem a construção da sua política;

2ª ação: Elabore a política de gestão de riscos, conforme Anexo IV, adequando-a às especificidades da sua organização;

3ª ação: Divulgue a política entre colaboradores, evidenciando a sua relevância para o sucesso da organização no alcance da sua missão institucional.

- **Responsáveis pelas ações**

O CIG com o apoio do *staff* da organização será responsável pela elaboração e divulgação da política. A alta administração instituirá a Política de Gestão de Riscos, mediante portaria.

Produtos esperados:

a) Política de Gestão de Riscos aprovada e publicada.

Passo 5

Definição do apetite a risco

Apetite a risco é o nível ou quantidade de risco que uma organização está disposta a aceitar para atingir os seus objetivos.

Trata-se de um conceito importante para as instituições, uma vez que o estabelecimento do apetite a riscos baliza todo o processo de gerenciamento de riscos da organização, possibilitando o enfrentamento dos riscos mais relevantes que podem comprometer os objetivos institucionais.

Dica para o gestor

O apetite a riscos bem definido pela Administração contribui para o alcance dos objetivos de forma mais segura e eficaz, minimizando a exposição a riscos, melhorando a tomada de decisão e tornando a gestão de riscos mais eficiente.

A definição do apetite a riscos delimita os riscos da organização que obrigatoriamente necessitarão de medidas de tratamento e aqueles que não será exigida obrigatoriedade de tratamento.

O apetite a riscos de cada órgão ou entidade municipal será definido, aprovado e formalizado pelo seu dirigente máximo, mediante um documento intitulado **Declaração de Apetite a Riscos**, estabelecendo os níveis de riscos que a Administração está disposta a aceitar para atingir seus objetivos, conforme quadro 02.

Informações para a Declaração de Apetite a Riscos

- missão da organização;
- tipologias e níveis de risco estabelecidos;
- unidades administrativas responsáveis por sua aprovação, revisão e monitoramento;
- nível de maturidade em riscos da organização;
- nível de apetite e tolerância a riscos; e
- período de revisão do apetite a riscos.

Quadro 02: Nível de Tolerância a Risco

APETITE A RISCO	DETALHAMENTO DA TOLERÂNCIA AO RISCO
Agressivo	Alta tolerância ao risco, a Administração está disposta a arriscar para alcançar os objetivos da organização, aceitando imprevisibilidade nas suas ações.
Moderado	Tolerância moderada ao risco, a Administração busca ampliar os resultados da organização sem arriscar muito. Seu objetivo é avaliar as oportunidades e os riscos de modo "equilibrado".
Conservador	Baixa tolerância ao risco, a Administração aceita pouca ou nenhuma volatilidade e imprevisibilidade nas suas ações. Um perfil conservador evita se expor a riscos para alcance dos objetivos da organização.

Vale destacar que no setor público, leis, regras, regulamentos, normas e mecanismos de regulação e controle estabelecem limites para atuação do gestor e restringem a flexibilidade para definição do apetite. Nesse sentido, o apetite a risco da gestão pública, em geral, tende ao **perfil conservador**.

Entretanto, algumas atividades públicas, em função de sua natureza, terão apetite a risco alto. Certas iniciativas exigem dose maior de risco do gestor público. É o caso de pesquisas e desenvolvimentos de novas tecnologias. A inovação comporta, em si, risco maior, pela incerteza do resultado.

Outrossim, no serviço público, a definição de um apetite a riscos diferente do conservador é uma decisão de elevada importância que, além de devidamente consubstanciada, deve ser tomada com muita cautela.

Nesse caso, além dos requisitos mencionados anteriormente, a Declaração de Apetite a Riscos deverá contemplar, os níveis de risco, critérios de aceitação do risco, respostas aos riscos e justificativa relativa à adoção do perfil de apetite a riscos diverso do conservador.

- **Ações sugeridas**

1ª ação: O órgão ou entidade realiza a avaliação do nível de maturidade em relação a gestão de riscos, conforme Anexo V;

2ª ação: O Comitê Interno de Governança (CIG) valida o nível de maturidade do órgão ou entidade em relação a gestão de riscos;

3ª ação: A Alta Administração elabora a proposta de apetite a risco do órgão ou entidade utilizando como parâmetros mínimos, o levantamento dos eventos significativos e respectivos efeitos que prejudicam as atividades, resultados ou a imagem do órgão ou entidade, bem como a avaliação do nível de maturidade;

4ª ação: O CIG analisa e valida a proposta de apetite a riscos, encaminhando a Declaração de Apetite a Riscos, conforme Anexo VI, para aprovação da alta administração;

5ª ação: O dirigente máximo do órgão ou entidade aprova e formaliza a Declaração de Apetite a Riscos.

- **Responsáveis pelas ações**

O *staff* do órgão ou entidade realiza a avaliação do nível de maturidade por unidade, o CIG valida e consolida as informações e a alta administração declara concordância (ou não) com a avaliação realizada.

Quanto a Declaração de Apetite a Riscos, a alta administração elabora proposta de declaração e após análise e validação do CIG, aprova e formaliza a mesma.

Produto esperado:

a) Avaliação do Nível de Maturidade em relação a Gestão de Riscos;

b) Declaração de Apetite a Riscos.

Passo 6

Elaboração de um plano de comunicação

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

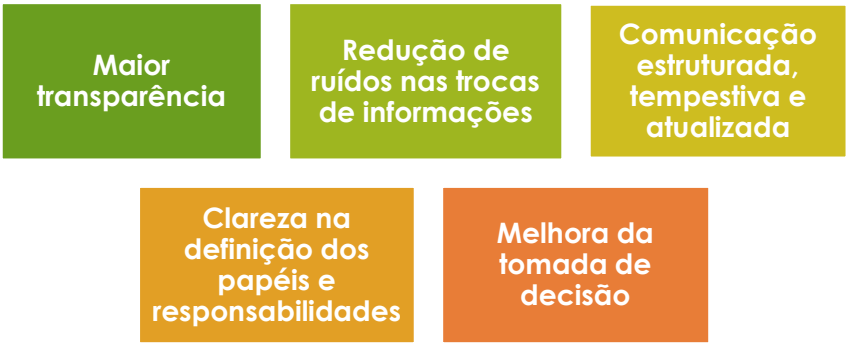
> a) auxiliar a estabelecer o contexto apropriadamente e assegurar que as visões e percepções das partes interessadas, incluindo necessidades, suposições, conceitos e preocupações sejam identificadas, registradas e levadas em consideração;
>
> b) auxiliar a assegurar que os riscos sejam identificados e analisados adequadamente, reunindo áreas diferentes de especialização; e
>
> c) garantir que todos os envolvidos estejam cientes de seus papéis e responsabilidades, e avalizem e apoiem o tratamento dos riscos. (TCU, 2018)

O propósito da comunicação e da consulta é auxiliar as partes interessadas na compreensão do risco, na base sobre a qual decisões são tomadas e nas razões pelas quais ações específicas são requeridas. (ISO 31000: 2018)

Nessa perspectiva, torna-se relevante a sistematização de um plano de comunicação por parte dos órgãos e entidades.

O Plano tem por objetivo estruturar as ações de comunicação para que os colaboradores de cada órgão/entidade entendam a importância do que está sendo comunicado, compreendam as mudanças operacionais e organizacionais de forma que possam acompanhar e apoiar o progresso da gestão de riscos.

Um plano de comunicação estruturado possibilita que as informações sobre riscos sejam transmitidas de forma eficaz e tempestiva aos colaboradores da organização, proporcionando:



A título de sugestão, apresenta-se a seguir alguns tópicos necessários a um Plano de Comunicação:

- Introdução;
- Objetivos do Plano de Comunicação;
- Produtos (O que precisa ser comunicado);
- Objetivo da comunicação (Qual é o propósito da comunicação);
- Canal de comunicação (Qual o meio pelo qual a comunicação é transmitida);
- Emissor Responsável (Quem é o responsável pela emissão da comunicação);
- Público-alvo (quem se deve comunicar);
- Frequência (Quando a comunicação deve ser emitida?).

Dica para o gestor

Informações sobre a gestão de riscos devem circular pela organização, à exceção daquelas consideradas sigilosas nos termos da lei. Órgãos de controle e cidadãos devem ser informados sobre as medidas adotadas para enfrentar os riscos e aproveitar as oportunidades mais significativas. (10 passos para a Boa Gestão de Riscos do TCU).

- **Ações sugeridas**

1ª ação: Elabore um Plano de Comunicação relativo à gestão de riscos, conforme Anexo VII, e promova a sua divulgação junto aos colaboradores;

2ª ação: Crie canais de comunicação que possibilitem ouvir as partes interessadas que compõem a organização;

3ª ação: Promova a disseminação da gestão de riscos da organização, comunicando sobre atividades e os resultados alcançados, em reuniões, intranet, e-mails etc.;

4ª ação: Fomente o conhecimento sobre a cultura de riscos, por meio de cursos e palestras, por exemplo, como forma de promover o engajamento, a conscientização e o entendimento dos colaboradores em relação a gestão de riscos.

- **Responsáveis pelas ações**

Comitê Interno de Governança podendo contar com o apoio do *staff* das unidades da organização.

Produtos esperados:

a) Plano de comunicação aprovado;

b) Ações/campanhas de comunicação sobre riscos.

Passo 7

Monitoramento e Análise crítica

O propósito do monitoramento e análise crítica é assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados do processo de gestão de riscos.

O monitoramento e análise crítica incluem planejamento, coleta e análise de informações, registro de resultados e fornecimento de retorno, devendo ocorrer simultaneamente, durante todo o processo de gestão de riscos e integrado a todas as instâncias envolvidas. (ISO 31000:2018)

O TCU ao ressaltar a importância do monitoramento e análise crítica na gestão de riscos no Referencial Básico de Gestão de Riscos destaca que esta etapa tem por finalidade:

> (a) detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco e no próprio risco, que podem requerer revisão dos tratamentos de riscos e suas prioridades, assim como identificar 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) assegurar que os controles sejam eficazes e eficientes no projeto e na operação (ABNT, 2009).

Esse passo visa garantir o funcionamento da gestão de riscos dentro dos padrões previamente estabelecidos, propiciando a sua melhoria contínua e quando necessário, a correção tempestiva e oportuna de quaisquer desvios ou problemas que surjam na organização.

Em Salvador, a responsabilidade pelas atividades de monitoramento e análise crítica atende a seguinte configuração:

Figura 05: Responsáveis pela atividade de monitoramento e análise crítica

- **Ações sugeridas**

1ª ação: Estabeleça medidas que propiciem o monitoramento da gestão de riscos, tais como: indicadores de desempenho e definição de responsabilidades e periodicidade pelo monitoramento da gestão de riscos da organização.

- **Responsável pela ação**

Os responsáveis e suas atribuições estão vinculados aos três níveis de gestão (estratégico, tático e operacional), conforme figura 05.

Produto esperado:

a) Informações estruturadas que propiciem o acompanhamento e o aperfeiçoamento/melhoria da gestão de riscos, por meio de relatórios periódicos que auxiliarão na tomada decisão e na priorização de ações para o Planejamento Estratégico.

9. Processo de Gestão de Riscos

A implementação do processo de gestão de riscos envolve a aplicação sistemática e prática de tudo que foi definido pela Administração na fase de estruturação, detalhada anteriormente no Tópico 8 da Cartilha.

São etapas do Processo de Gestão de Riscos:

I. Entendimento do escopo e do contexto;

II. Identificação de riscos;

III. Identificação e avaliação dos controles;

IV. Cálculo do nível do risco;

V. Definição de respostas aos riscos;

VI. Validação dos resultados;

VII. Comunicação e monitoramento.

As etapas do processo de gestão de riscos, embora estejam dispostas de forma sequencial, na prática elas são iterativas, ou seja, ocorrem repetidas vezes, o que permite que as experiências anteriores aperfeiçoem, continuadamente, as atuais.

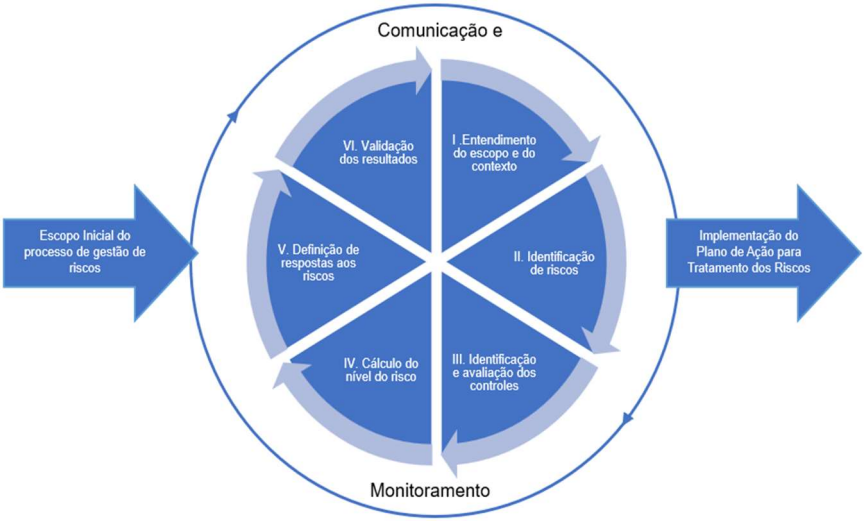
Para que a iteratividade proporcione evolução, melhoramento e refinamento sucessivo do processo de gestão de riscos, é importante que todas as etapas do processo sejam documentadas.

Dica para o gestor

Convém que o processo de gestão de riscos seja parte integrante da gestão e da tomada de decisão, e seja integrado na estrutura, operações e processos da organização. Pode ser aplicado nos níveis estratégico, operacional, de programas ou de projetos (ISO 31000:2018).

A figura a seguir, apresenta o ciclo da gestão de riscos a ser aplicada nos órgãos e entidades da PMS:

Figura 06: Ciclo da Gestão de Riscos



Fonte: Adaptação da figura 2, constante da Metodologia de Gestão de Riscos da CGU.

9.1. Etapas do Processo de Gestão de Riscos

9.1.1 Entendimento do escopo e do contexto

Esta etapa do processo de gestão de riscos se divide em entendimento do escopo e entendimento do contexto, conforme detalhamento a seguir:

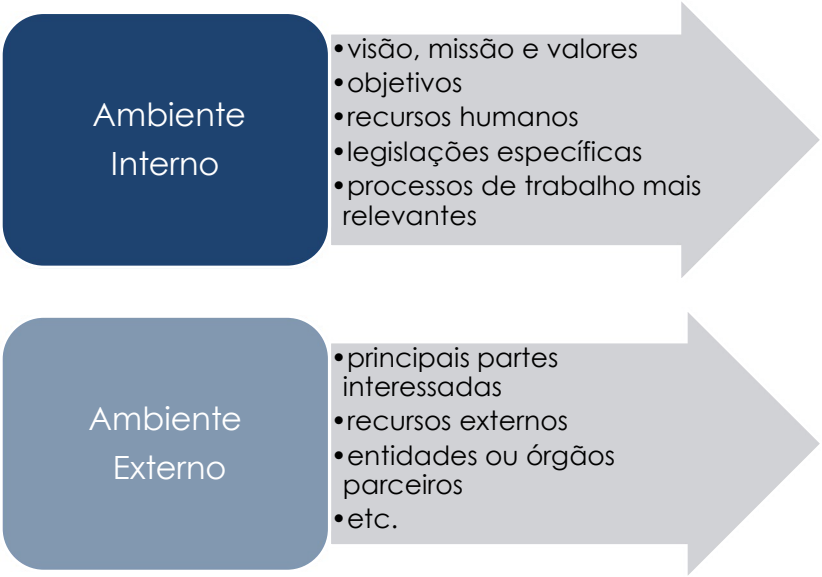
Entendimento do Contexto

O entendimento do contexto engloba a compreensão do propósito da organização, da sua estrutura, dos seus objetivos, o ambiente no qual o objeto de gestão de riscos está inserido e de outros aspectos relevantes, constituindo-se em etapa essencial do processo de gestão de risco.

As informações produzidas, a partir do entendimento do contexto interno e externo da organização nortearão as etapas seguintes do processo de gestão de riscos, em especial, a etapa de identificação dos riscos.

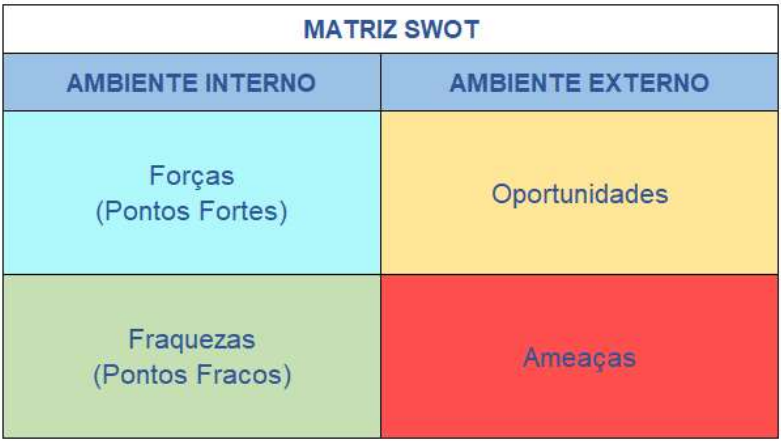
Para entendimento do contexto interno e externo em que o objeto da gestão de riscos se encontra inserido, sugere-se a coleta de informações, observando:

Figura 07: Informações ambiente interno e externo



A partir dessas informações é possível realizar a análise de forças e fraquezas do ambiente interno, bem como as oportunidades e ameaças do ambiente externo, através da Matriz SWOT (*Strengths, Weaknesses, Opportunities e Threats*).

Figura 08: Matriz SWOT



• Forças - são pontos positivos, de destaque ou de excelência, levando em consideração o ambiente interno.

• Fraquezas - são pontos negativos, de fragilidade, levando em consideração o ambiente interno.

• Oportunidades - são fatores impostos pelo ambiente externo e que podem trazer benefício ao processo.

• Ameaças - são fatores impostos pelo ambiente externo e que podem prejudicar o processo.

Entendimento do Escopo

Entendido o contexto em que a organização está inserida passa-se a estabelecer o escopo da gestão de riscos, incluindo os seus objetivos específicos e alinhamento aos objetivos organizacionais.

Como o processo de gestão de riscos pode ser aplicado em diferentes níveis (por exemplo, estratégico, operacional, programa, projeto ou outras atividades), é importante ser claro sobre o escopo em consideração, os objetivos pertinentes a serem considerados e o seu alinhamento aos objetivos organizacionais (ISO 31000:2018).

O escopo da gestão de riscos priorizado deve ser relevante para organização, relacionado à sua atividade finalística e estar alinhado aos objetivos previstos em seu planejamento estratégico.

Dica para o gestor

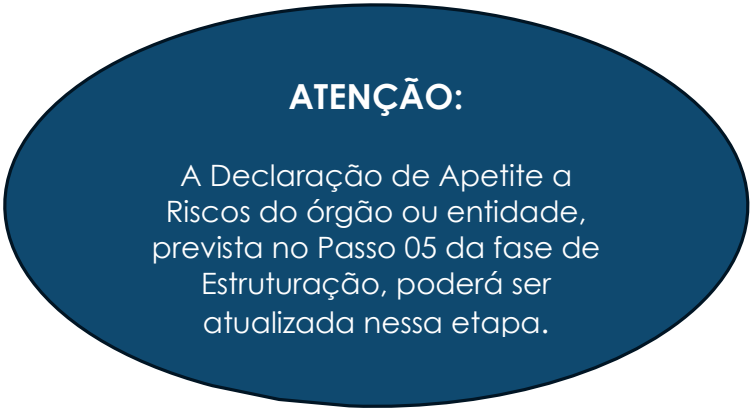
> O investimento na gestão de riscos deve ser maior nos processos que mais entregam ou devem entregar valor para as partes interessadas, bem como nas atividades de suporte que podem estar limitando a capacidade de entrega dos processos finalísticos. (Referencial Básico de Gestão de Riscos)

A priorização dos processos que serão objeto da gestão de riscos pode ocorrer por meio de discussões internas, baseada na experiência dos gestores da organização ou mediante a utilização de critérios objetivos que considerem:

- orçamento;
- recursos humanos;
- relevância para o cumprimento da missão institucional;
- recomendação dos órgãos de controle interno e externo; e
- complexidade da organização.

Visando apoiar os órgãos e entidades municipais na definição do escopo inicial do processo de gestão de riscos e considerando a obrigatoriedade de implementação da gestão de riscos estabelecida na Lei nº 14.133/2021, recomenda-se a priorização do macroprocesso das contratações públicas, incluído a gestão e fiscalização de contratos, que é uma das áreas mais sensíveis e estratégicas para a administração pública.

Tal recomendação não impede a definição de outros escopos considerados relevantes pela administração.



- **Ações sugeridas**

1ª ação: Elabore a Matriz SWOT contemplando informações do contexto interno e externo que podem influenciar o alcance dos objetivos da organização;

2ª ação: Relacione os processos que terão seus riscos gerenciados, bem como os respectivos responsáveis pelo gerenciamento de riscos e critérios utilizados para priorização de processos;

3ª ação: Identifique o objetivo de cada processo priorizado e delimite o seu alcance/resultado pretendido.

- **Responsáveis pelas ações**

O *staff* das unidades da organização com o apoio do corpo técnico e supervisão do Comitê Interno de Governança. A alta administração aprova a lista de processos que serão priorizados.

Produtos esperados:

a) Análise do escopo e entendimento do contexto da organização;

b) Lista dos processos priorizados que serão objeto da gestão de riscos.

9.1.2 Identificação de riscos

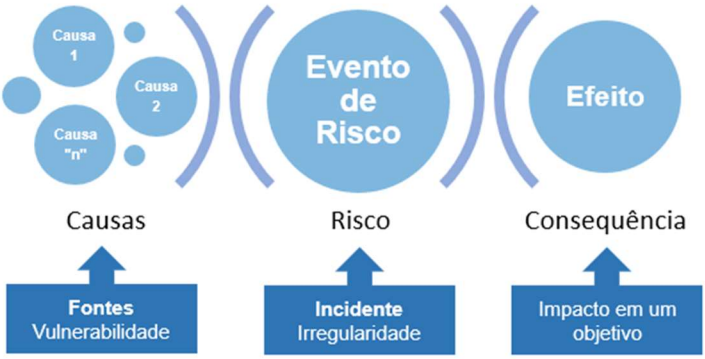
Essa etapa visa detectar, reconhecer e descrever eventos de riscos que podem interferir no alcance dos objetivos de uma organização, bem como as suas respectivas causas e consequências.

Os eventos são situações em potencial que podem causar impacto na consecução dos objetivos da organização, caso venham a ocorrer. Podem ser positivos ou negativos, sendo que os eventos negativos são denominados riscos, enquanto os positivos, oportunidades. (Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão do antigo Ministério do Planejamento, Desenvolvimento e Gestão - MP).

Nessa metodologia, inicialmente, trataremos apenas sobre eventos negativos.

O entendimento do escopo e do contexto realizado na Etapa I apresenta importantes insumos que auxiliarão a identificação de riscos.

Figura 09: Causas, Evento de Riscos e Consequências



Fonte: Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão - MP

Causas: condições que dão origem à possibilidade de um evento ocorrer, também chamadas de fatores de riscos e podem ter origem no ambiente interno e externo.

Risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos.

Consequência: o resultado de um evento de risco sobre os objetivos do processo.

Dica para o gestor

Para cada risco identificado deverão ser elencadas as possíveis causas e consequências.

Como identificar os eventos de riscos?

A identificação de riscos pode basear-se em:

- dados históricos;
- análises teóricas;
- opiniões de pessoas informadas e especialistas; e
- necessidades das partes interessadas.

A fase de identificação implica em relacionar o maior número de riscos que pode afetar os objetivos estratégicos e avaliá-los, extraindo aqueles que, pela sua importância, devem merecer a atenção da alta administração e, portanto, devem ser levados ao seu conhecimento.

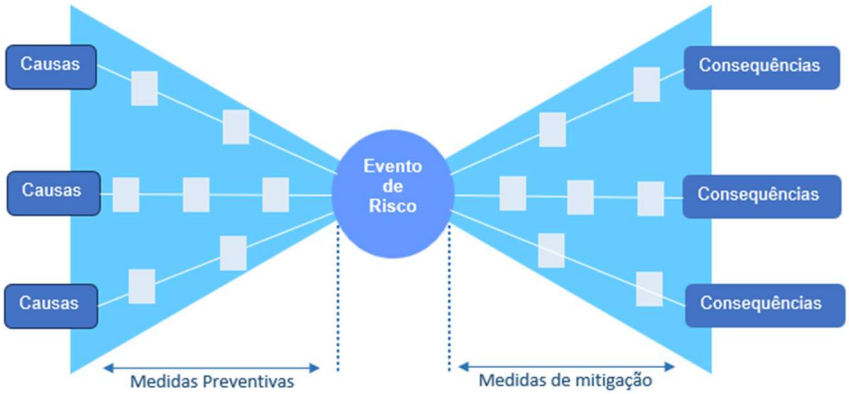
Importante que pessoas com conhecimento adequado sejam envolvidas na identificação de riscos e que a organização utilize ferramentas e técnicas de identificação de riscos que sejam adequadas aos seus objetivos, às suas capacidades e aos riscos enfrentados (ABNT, 2009).

Segundo o TCU[3], envolver a equipe também ajuda a criar a responsabilidade em relação ao processo de gestão de riscos e o comprometimento em relação ao tratamento dos riscos.

Existem diversas técnicas que podem ser utilizadas na identificação de riscos, a exemplo de: brainstorming, oficinas, fluxogramas e bow-tie.

A análise bow-tie, também conhecida como gravata borboleta, (Figura 10), possibilita que para cada evento de risco identificado sejam relacionadas as suas possíveis causas e consequências, bem como as formas de prevenir a ocorrência do risco e as formas de mitigar as consequências caso o risco se materialize.

Figura 10: Análise *Bow-tie*



Segundo o TCU[4] algumas dicas facilitam a identificação dos riscos:

- responder à seguinte pergunta-chave: o que pode atrapalhar o alcance do objetivo/resultado?

[3] Referencial Básico de Gestão de Riscos de Gestão. 2018.

[4] Manual de Gestão de Riscos do TCU. 2ª Edição. 2020

- considerar os fatores de sucesso para a consecução dos objetivos – qualquer evento que afete o fator de sucesso potencialmente afeta o objetivo/resultado;
- considerar as principais fontes de riscos: infraestrutura, pessoal, processos e tecnologia.

Também, elaborar a sintaxe do risco pode auxiliar a sua identificação:

Descrição	Informação necessária
Devido a _____	Causa, fonte
poderá (ão) acontecer _____	Evento de Risco
o que poderá levar a _____	Consequência, efeito
impactando _____	Dimensão de objetivo impactada

A seguir exemplo de aplicação da sintaxe do risco:

Descrição		Informação necessária
Devido a	falta de manutenção da rede elétrica do almoxarifado de medicamentos da Secretaria Municipal de Saúde	Causa, fonte
poderá (ão) acontecer	um incêndio	Evento de Risco
o que poderá levar a	perda total dos medicamentos em estoque	Consequência, efeito
impactando	a distribuição de medicamentos à população	Dimensão de objetivo impactada

Os riscos identificados serão classificados como estratégicos, operacionais, legais, financeiros/orçamentário e de integridade, conforme indicado no quadro 01.

- **Ações sugeridas**

1ª ação: Levante os dados sobre o desempenho da organização, em especial dos processos relevantes delimitados na Etapa 1 – Entendimento de escopo e de contexto;

2ª ação: Organize oficinas de trabalho para identificação dos riscos, com a participação do gestor do risco e de servidores que conheçam os processos em foco;

3ª ação: Obtenha uma lista de riscos em ordem de significância, contemplando no mínimo as seguintes informações: Unidade organizacional; Processo selecionado; Objetivo; Evento de Risco; Causas, Consequências; Tipologia do risco; Período da análise e responsável;

4ª ação: Apresente os riscos identificados à alta administração, que oportunamente decidirá quais serão priorizados.

Riscos-chave são aqueles que podem afetar significativamente o alcance dos objetivos e o cumprimento da missão institucional, a imagem e a segurança da organização e de pessoas. Em razão do impacto potencial que podem ter nos resultados da organização, os riscos-chave devem ser conhecidos pela alta administração. (10 passos para a Boa Gestão de Riscos).

- **Responsáveis pelas ações**

Gestor do risco, servidores e colaboradores que atuam diretamente no processo e *staff* das unidades da organização com a supervisão do Comitê Interno de Governança.

Produto esperado:

a) Lista de riscos identificados contemplando causas e consequências.

9.1.3 Identificação e avaliação dos controles existentes

Essa etapa consiste na identificação, verificação e avaliação dos controles internos preexistentes que objetivam mitigar os riscos identificados na Etapa II.

Os controles internos são classificados em:

- **Controles preventivos:** controles existentes e que atuam sobre as possíveis causas do risco, com o objetivo de prevenir a sua ocorrência;
- **Controles detectivos:** controles existentes que atuam na detecção da materialização de um risco ou de sua iminência; e
- **Controles contingenciais:** controles existentes executados após ocorrência do risco com o intuito de diminuir o impacto de suas consequências.

Uma vez realizada a identificação dos controles existentes, para cada um dos riscos identificados e priorizados, deve ser avaliada a eficácia e eficiência desses controles, bem como se devem ser modificados, mantidos ou eliminados. Nessa etapa, também pode ser identificada a necessidade de implementação de novos controles internos.

Nessa perspectiva, a avaliação da eficiência e eficácia dos controles associados aos riscos da organização, pode ocorrer mediante a análise de seus atributos e estabelecimento de um fator numérico que representa o nível de confiança desse controle.

No contexto da Prefeitura Municipal do Salvador, a análise será mensurada com base no Fator de Avaliação de Controle - FAC, conforme detalhado no quadro a seguir:

QUADRO 03 - ESCALA DE AVALIAÇÃO DE CONTROLES		
Nível de Confiança	**Atributos do controle**	**Fator de Avaliação de Controle (FAC)**
Inexistente	Controle não existe, mal desenhado ou mal implementado, ou seja, não funcional.	1
Fraco	Controle tende a ser aplicado caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	0,8
Mediano	Controle implementado mitiga alguns aspectos do risco, mas não contempla todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	0,6
Satisfatório	Controle implementado e sustentado por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitiga o risco satisfatoriamente.	0,4
Forte	Controle implementado pode ser considerado a "melhor prática", mitigando todos os aspectos relevantes do risco.	0,2

Fonte: Adaptação da Tabela 5.6 do Guia de Avaliação de Maturidade da Gestão de Riscos do TCU

- **Ações sugeridas**

1ª ação: Compare os controles existentes com os riscos identificados visando avaliar a sua aplicabilidade, a necessidade de aprimoramento/correção, bem como a relação custo x benefício.

2ª ação: Atribua um Fator de Avaliação de Controle (FAC) para os controles de cada risco identificado, nos termos do quadro 03 – Escala de Avaliação dos Controles.

- **Responsáveis pelas ações**

Gestor do risco, servidores e colaboradores que atuam diretamente no processo e *staff* das unidades da organização com a supervisão do Comitê Interno de Governança.

Produtos esperados:

a) Lista de controles preventivos, detectivos e contingenciais existentes, com indicação do Nível de Confiança e Fator de Avaliação de Controle (FAC);

b) Atualização da lista de riscos contemplando os controles existentes.

9.1.4 Cálculo do nível do risco

Nessa etapa serão calculados os níveis de risco dos eventos identificados a partir de critérios de probabilidade e impacto.

Para uma melhor compreensão dessa etapa entende-se como:

- **Probabilidade:** chance de um determinado evento acontecer;
- **Impacto:** efeito de um determinado evento sobre um objetivo.

O nível do risco é expresso pela combinação da probabilidade de ocorrência do evento e das consequências resultantes no caso de materialização do evento, ou seja, do impacto nos objetivos:

Os quadros 04 e 05 apresentam as escalas de probabilidade e impacto, respectivamente, que servirão de referência para o cálculo do nível de risco.

QUADRO 04 - ESCALA DE PROBABILIDADE		
Probabilidade	**Descrição da Probabilidade**	**Peso**
Praticamente certa	**Ocorrência quase garantida** no prazo associado ao objetivo do processo.	5
Provável	**Repete-se com elevada frequência** no prazo associado ao objetivo ou há muitos indícios que ocorrerá nesse horizonte.	4
Possível	**Repete-se com frequência razoável** no prazo associado ao objetivo ou há indícios que possa ocorrer nesse horizonte.	3
Rara	O histórico conhecido aponta para **baixa frequência de ocorrência** no prazo associado ao objetivo.	2
Improvável	**Acontece apenas em situações excepcionais**. Não há histórico conhecido do evento ou não há indícios que sinalizem sua ocorrência.	1

Fonte: Quadro criado a partir do Manual de Gestão de Riscos do TCU (2ª edição) e Metodologia de Gestão de Riscos da CGU.

QUADRO 05 - ESCALA DE IMPACTO		
Impacto	**Descrição do impacto nos objetivos/resultados relacionados ao alcance de metas, entrega de produtos/serviços e prazo**	**Peso**
Muito Alto	**Catastrófico** impacto, de **consequência irreversíve**l, decorrente de **paralisação** das operações ou atividades de processos, projetos ou programas da organização.	5
Alto	**Significativo** impacto, de **difícil reversão**, decorrente de **interrupção** das operações ou atividades de processos, projetos ou programas da organização.	4
Médio	**Moderado** impacto, de **possível reversão**, decorrente de **interrupção** das operações ou atividades de processos, projetos ou programas da organização.	3
Baixo	**Pequeno** impacto, **sem interrupção** das operações ou atividades de processos, projetos ou programas da organização, porém, com **redução da eficiência**.	2
Muito Baixo	**Mínimo** impacto, que **não afeta** as operações ou atividades de processos, projetos ou programas da organização.	1

Fonte: Quadro criado a partir da Metodologia de Gestão de Riscos da CGU.

O nível de riscos é calculado a partir da multiplicação dos valores de probabilidade e impacto e corresponde ao possível impacto nos objetivos do processo em foco.

$$NR = P \times I$$

Onde:
NR = Nível do risco
P = Probabilidade do risco
I = Impacto do risco

Nesse contexto, o cálculo do Nível de Risco compreende a análise dos riscos em dois cenários distintos, quais sejam:

1) Sem considerar os controles preexistentes implementados pela organização. Nesse cenário é mensurado o nível do risco inerente; e,

2) Considerando os controles existentes implementados pela organização. Nesse cenário obtém-se o nível do risco residual.

- Risco inerente: risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto;
- Risco residual: risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco (IN MP, CGU 01/2016).

O Nível de Risco obtido da multiplicação dos pesos das escalas de probabilidade e impacto, tanto no cenário de cálculo do Risco Inerente quanto no cenário de Risco Residual, será classificado de acordo com a escala indicativa dos níveis de gravidade dos riscos, apresentada a seguir:

QUADRO 06: ESCALA INDICATIVA DOS NÍVEIS DE RISCO			
RB (RISCO BAIXO)	RM (RISCO MÉDIO)	RA (RISCO ALTO)	RE (RISCO EXTREMO)
de 0 a 4	de 5 a 10	de 12 a 16	de 20 a 25

Visando um melhor entendimento acerca da análise do Nível de Risco Inerente e Residual apresenta-se a seguir, detalhamento dos cálculos relacionados aos cenários anteriormente citados:

- Primeiro cenário:

No primeiro cenário são considerados, exclusivamente, os riscos inerentes da organização, ou seja, os riscos brutos a que ela está sujeita sem considerar qualquer tipo de controle interno preexistente para mitigar riscos.

Nesse cenário, o cálculo realizado de acordo com a probabilidade e impacto, da ocorrência de cada evento de risco, sem considerar as ações de controle implementadas pela organização, definirá o Nível de Risco Inerente (NRI) do órgão/entidade, conforme fórmula a seguir:

$$NRI = P \times I$$

Onde:

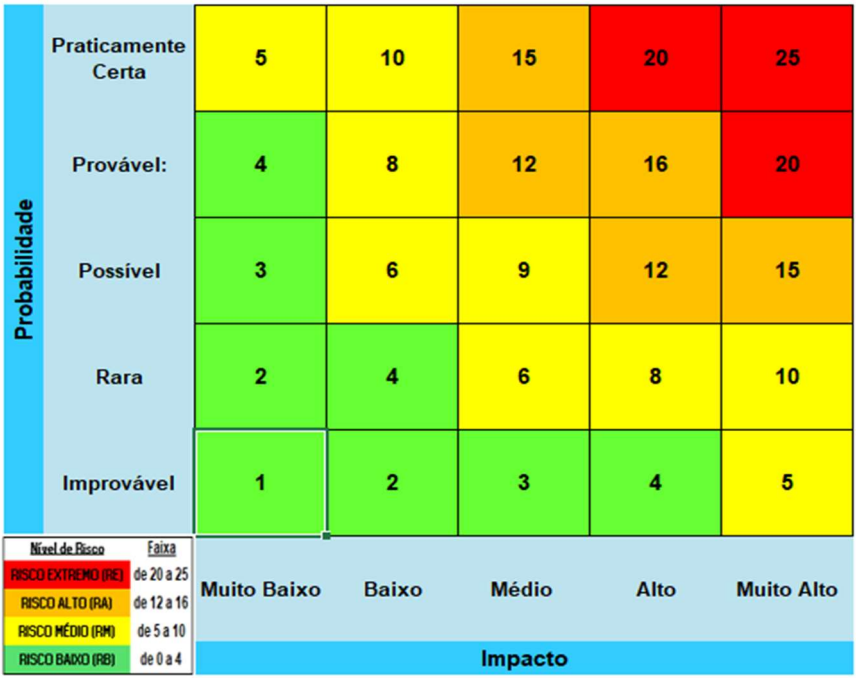
NRI = Nível do risco inerente

P = Probabilidade do risco (sem considerar controles internos existentes)

I = Impacto do risco (sem considerar controles internos existentes)

A matriz a seguir apresenta os possíveis resultados da combinação probabilidade *versus* impacto, no cenário de cálculo do NRI:

Figura 11: Matriz de Riscos Inerentes



A seguir apresenta-se, a título de exemplo, o cálculo do Nível de Risco Inerente (NRI) dos riscos identificados e a sua respectiva classificação na escala indicativa dos níveis de gravidade dos riscos (quadro 06):

QUADRO 07 – EXEMPLO DE CÁLCULO DO NÍVEL DE RISCO INERENTE			
Riscos identificados	**Probabilidade (P)**	**Impacto (I)**	**NRI = (P x I)**
Descrição do risco 1	Praticamente certa (5)	Muito Alto (5)	**25 (RE)**
Descrição do risco 2	Praticamente certa (5)	Médio (3)	**15 (RA)**
Descrição do risco 3	Possível (3)	Baixo (2)	**6 (RM)**
Descrição do risco "n"	Improvável (1)	Alto (4)	**4 (RB)**

Fonte: Adaptação da tabela 5.5 do Guia de Avaliação de Maturidade da Gestão de Riscos do TCU.

- Segundo cenário

No segundo cenário, a mensuração do nível do risco ocorre após a avaliação dos mecanismos de controles já implementados pela organização para reduzir a probabilidade e o impacto de sua ocorrência.

Esse cenário tem como resultado o nível de risco residual que corresponde ao nível de risco remanescente enfrentado pela organização, após a aplicação dos controles para reduzi-lo, e ocorre da seguinte forma:

- ✓ Inicialmente, deve-se revisar e atualizar (se necessário) a avaliação dos controles existentes, realizada na Etapa III do processo de gestão de riscos, por meio de uma lista dos controles vigentes, com indicação dos respectivos Fatores de Avaliação de Controle (FAC);
- ✓ Em seguida, deve-se incidir o FAC sobre o valor do Nível de Risco Inerente (NRI = P x I) para se obter o Nível de Risco Residual (NRR) da organização.

O Nível de Risco Residual (NRR) considera em sua mensuração todos os mecanismos de controle implementados pela organização sendo definido pela seguinte fórmula:

$$NRR = NRI \times FAC$$

Onde:

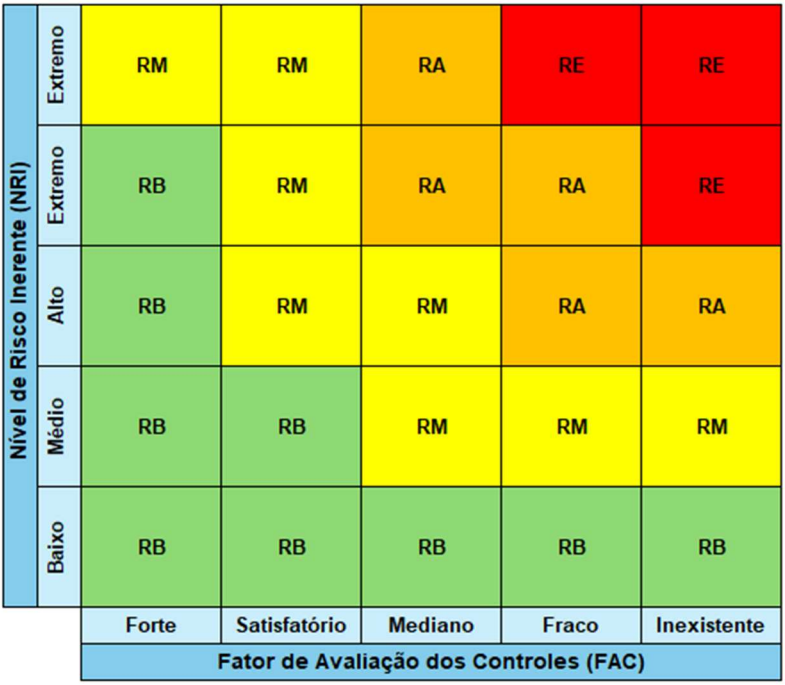
NRR = Nível do risco residual

NRI = Nível do risco inerente

FAC = Fator de Avaliação de Controle (FAC)

A matriz a seguir apresenta o resultado da combinação Nível de Risco Inerente *versus* FAC no cenário de cálculo do NRR:

Figura 12: Matriz de Riscos Residuais



Observações:

1. O eixo relativo ao Nível de Risco Inerente (NRI) da matriz anterior utiliza como referências os valores constantes da faixa dos níveis de gravidade dos riscos. Adicionalmente, vale ressalvar que para o NRI Extremo, em razão da sua criticidade no processo de gestão de riscos, serão utilizados os referenciais, mínimo (20) e máximo (25):

Nível de Risco	Faixa
RISCO EXTREMO (RE)	de 20 a 25
RISCO ALTO (RA)	de 12 a 16
RISCO MÉDIO (RM)	de 5 a 10
RISCO BAIXO (RB)	de 0 a 4

2. O eixo relativo ao Fator de Avaliação dos Controles adotou os seguintes valores para efeito de avaliação da eficiência e eficácia dos controles (Quadro 03):

FORTE	SATISFATORIO	MEDIANO	FRACO	INEXISTENTE
0,2	0,4	0,6	0,8	1

A seguir, em continuidade à exemplificação constante do quadro 07, apresenta-se o cálculo do Nível de Risco Residual (NRR) e a sua respectiva classificação na escala indicativa dos níveis de gravidade dos riscos (quadro 06):

QUADRO 08 – EXEMPLO DE CÁLCULO DO NÍVEL DE RISCO RESIDUAL						
Riscos	**Probabilidade (P)**	**Impacto (I)**	**NRI = (P x I)**	**Nível de Confiança do Controle**	**FAC**	**NRR = NRI x FAC**
Risco 1	Praticamente certa (5)	Muito Alto (5)	25 (RE)	Inexistente	1	**25 (RE)**
Risco 2	Praticamente certa (5)	Médio (3)	15 (RA)	Fraco	0,8	**12 (RA)**
Risco 3	Possível (3)	Baixo (2)	6 (RM)	Mediano	0,6	**3,6 (RB)**
risco "n"	Improvável (1)	Alto (4)	4 (RB)	Forte	0,2	**0,8 (RB)**

Fonte: Adaptação da tabela 5.7 do Guia de Avaliação de Maturidade da Gestão de Riscos do TCU.

A diferença entre o valor do risco inerente e o risco residual demonstrará a atual eficácia dos controles implementados na mitigação dos riscos identificados. (Metodologia de Gestão de Riscos da CGU).

Essa informação auxiliará a identificação e avaliação dos controles existentes (Etapa III), no que se refere a mensuração da eficiência

e eficácia dos controles na mitigação dos riscos, bem como na identificação de melhorias dos controles atuais.

A compreensão propiciada nesse tópico contribuirá para a tomada de decisão acerca dos riscos analisados, sobretudo no que diz respeito a:

- Necessidade de tratamento de determinado risco;
- Riscos priorizados para tratamento;
- Atividades que devem ser realizadas ou descontinuadas;
- Controles internos que devem ser implementados;
- Controles internos que devem ser modificados, mantidos ou eliminados.

Dica para o gestor

A decisão por alterar, manter, implementar ou eliminar controles internos devem necessariamente observar a relação custo-benefício.

- **Ações sugeridas**

1ª ação: Calcule o Nível de Risco Inerente e o Nível de Risco Residual do processo em foco;

2ª ação: Ordene a lista de riscos por nível de risco e submeta-a à alta administração para fins de priorização e medidas de tratamento dos riscos;

3ª ação: A alta administração decide quais os riscos que merecerão ações mitigadoras e a prioridade de tratamento.

- **Responsáveis pelas ações**

Gestor do risco, servidores e colaboradores que atuam diretamente no processo e *staff* das unidades da organização com a supervisão do Comitê Interno de Governança. A alta administração aprova inventário contemplando priorização dos riscos.

Produtos esperados:
a) Nível de Risco Inerente;
b) Nível de Risco Residual;
c) Matriz de Riscos;
d) Inventário de riscos ordenados por nível de risco.

9.1.5 Definição de respostas aos riscos

A etapa de definição de respostas aos riscos compreende o planejamento das ações necessárias à modificação do nível de cada risco identificado, de forma a adequá-lo ao apetite estabelecido para os processos organizacionais, além da escolha das medidas de controle associadas a essas respostas.

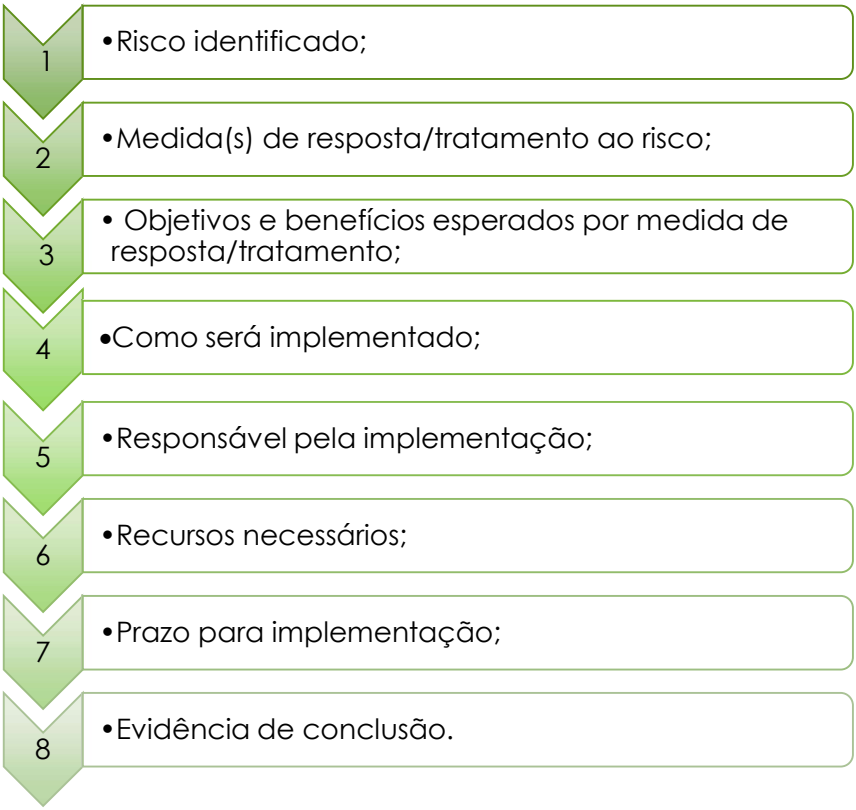
Essa etapa tem como objetivo definir medidas para mitigar as ameaças aos objetivos institucionais. Nesse prisma, as medidas de resposta ou tratamento de riscos estão relacionadas a cada risco identificado e ao seu respectivo nível do risco e incluem evitar, transferir, mitigar e aceitar o risco, conforme apresentado no quadro a seguir:

QUADRO 09 - OPÇÕES DE TRATAMENTO DO RISCO		
TRATAMENTO	**DESRIÇÃO**	**OBSERVAÇÃO**
Evitar	Evitar o risco significa descontinuar a atividade, interromper o processo de trabalho.	Um risco normalmente é evitado quando a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco com a organização. Geralmente esse risco é classificado como "Alto" ou "Extremo"
Transferir/ Compartilhar	Transferir o risco significa compartilhar o risco com terceiros, como no caso dos seguros.	Um risco normalmente é compartilhado quando é classificado como "Alto" ou "Extremo", mas a implementação de controles não apresenta um custo/benefício adequado.
Mitigar	Mitigar o risco significa implementar medidas para evitar que o risco se concretize e/ou medidas para atenuar o impacto e as consequências caso ocorra.	Um risco normalmente é mitigado quando é classificado como "Alto" ou "Extremo". A implementação de controles, neste caso, apresenta um custo/benefício adequado.
Aceitar	Aceitar o risco significa que não há necessidade de adotar quaisquer medidas mitigatórias.	No entanto deve-se avaliar se é o caso de monitorar ao longo do tempo. Um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco. Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco.

Fonte: "Quadro 8: Opções de tratamento do risco" da Metodologia de Gestão de Riscos da CGU e figura "Possibilidades de Tratamento dos Riscos", pág. 33 do Manual de Gestão de Riscos do TCU.

A implementação das medidas de resposta aos riscos ou tratamento de riscos ocorrerá por meio de um Plano de Ação, a ser definido pelo Gestor do Risco com apoio do Comitê Interno de Governança (CIG), que deve conter, pelo menos as seguintes informações:

Figura 13: Composição do plano de ação para tratamento dos riscos:



- **Ações sugeridas**

1ª ação: Elabore um Plano de Ação para Tratamento dos Riscos, incluindo a avaliação da relação custo-benefício de cada opção de resposta/tratamento dos riscos;

2ª ação: Valide as ações do plano junto às demais unidades organizacionais envolvidas;

3ª ação: Encaminhe o Plano de Ação para Tratamento dos Riscos para validação do CIG que posteriormente submeterá à aprovação do gestor máximo do órgão ou entidade.

- **Responsáveis pelas ações**

O Gestor do risco e o *staff* das unidades da organização elaboram o plano de tratamento, o CIG valida e a alta administração aprova.

Produto esperado:

a) Plano de Ação para Tratamento dos Riscos.

9.1.6 Validação dos resultados

Os resultados das etapas anteriores e o Plano de Ação para Tratamento dos Riscos devem ser aprovados pelo dirigente máximo do órgão ou entidade.

O Plano de Ação para Tratamento dos Riscos aprovado será encaminhado para a unidade responsável pelo processo organizacional para fins de implementação. Nesse caso, o plano de ação também se aplica a outras unidades que porventura participem desse processo.

- **Ações sugeridas**

1ª ação: Aprovação dos resultados das etapas anteriores, assim como o Plano de Ação para Tratamento dos Riscos;

2ª ação: Encaminhamento do Plano de Ação para Tratamento dos Riscos para implementação por parte da unidade organizacional.

- **Responsáveis pelas ações**

A alta administração aprova os resultados das etapas anteriores e o plano de tratamento dos riscos. O Gestor do risco e o *staff* das unidades da organização, com o apoio do CIG, implementa as medidas previstas nesse plano.

Produto esperado:

a) Plano de Ação para Tratamento dos Riscos aprovado.

9.1.7 Comunicação e Monitoramento

Essa etapa que compreende comunicação e monitoramento, ocorre simultaneamente às demais, ou seja, durante todo o processo de gerenciamento de riscos.

Ela é responsável pela integração de todas as instâncias envolvidas, bem como pelo monitoramento contínuo da própria Gestão de Riscos, com vistas à sua melhoria.

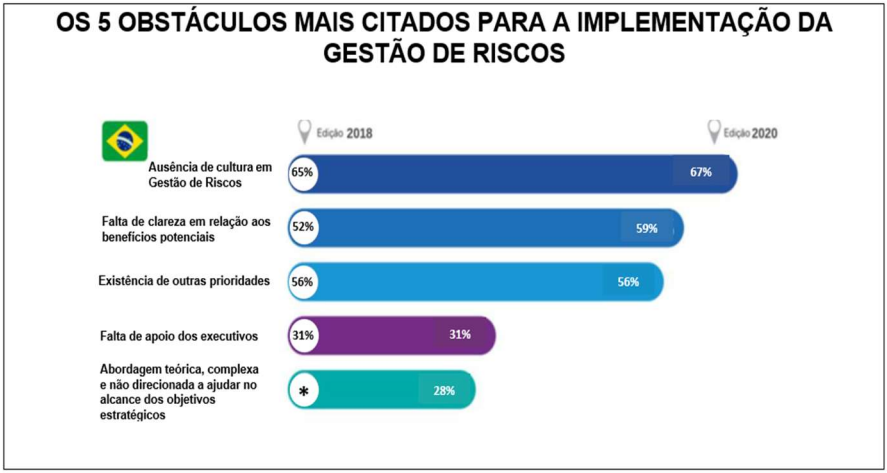
O êxito dessa etapa está diretamente ligado a existência de um plano de comunicação bem elaborado, possibilitando a transmissão eficaz e oportuna de informações sobre riscos aos colaboradores da organização.

Para informações mais detalhadas sobre essa etapa, verificar os passos 06 e 07 do Tópico 8 - Estrutura da Gestão de Riscos.

10. Desafios para implantação da Gestão de Riscos

De acordo com a “Pesquisa da Maturidade do Processo de Gestão de Riscos no Brasil” realizada pela empresa KPMG em 2020, os maiores obstáculos para a implantação da gestão de riscos nas empresas brasileiras são os constantes da figura a seguir:

Figura 14: Obstáculos para implementação da gestão de riscos



Fonte: KPMG (Figura extraída de *slide* do curso de Introdução à Gestão de Riscos promovido pela ENAP e CGU em 2023)

Nesse contexto, destacam-se como principais desafios enfrentados pelas empresas brasileiras:

a) Ausência de cultura em Gestão de Riscos

Grande parte das empresas brasileiras não dispõe de uma cultura consolidada de gestão de riscos. Isto significa que a cultura existente está focada na solução dos problemas (“apagar incêndios”), que porventura ocorram durante os processos organizacionais;

b) Falta de clareza em relação aos benefícios potenciais

A maioria das empresas não tem clareza sobre os benefícios da gestão de riscos, o que pode levar ao entendimento errôneo de que não é um investimento e sim, um custo adicional e desnecessário;

c) Existência de outras prioridades

Associado aos itens anteriores, boa parte das empresas priorizam o enfrentamento dos desafios operacionais que ocorrem no dia a dia da organização em detrimento da gestão de riscos.

As medidas exemplificadas a seguir, contribuem para a superação dos principais desafios enfrentados pelas organizações na implementação da gestão de riscos:

- Promoção da cultura de gestão de riscos visando a sua internalização no ambiente organizacional;
- Processo de tomada de toda e qualquer decisão da organização pautado com base na gestão de riscos;
- Divulgação dos possíveis benefícios da implementação da gestão de riscos para toda a organização, como forma de sensibilizar e angariar o apoio da alta administração e dos seus colaboradores;
- Disseminação das boas práticas, bem como dos resultados positivos, de outros órgãos que implementaram a gestão de riscos.

Dica para o gestor

A Controladoria Geral do Município é o órgão responsável pela orientação dos gestores na implementação da estrutura e do processo de Gestão de Riscos nos órgãos e entidades da PMS.

11. Conclusão

Essa cartilha apresenta informações básicas sobre a gestão de riscos, incluindo conceitos e orientações sobre os seus principais normativos. Traz também um arranjo para implementação e estruturação da gestão de riscos em cada órgão ou entidade municipal.

Na compreensão da gestão de riscos como um dos pilares da governança, os gestores têm à disposição um grande instrumento para auxiliar a administração municipal no planejamento, execução e controle de suas atividades. A sua implantação permitirá um salto na qualidade dos serviços e das entregas das políticas públicas à sociedade.

Por fim, num cenário de necessidade constante de aperfeiçoamento da gestão pública, seja pelos problemas históricos, seja pelas transformações sociais, econômicas e tecnológicas dos últimos anos, a gestão de riscos constitui-se em uma ferramenta poderosa, com grande potencial de auxiliar à Prefeitura Municipal de Salvador no cumprimento de sua missão institucional.

12. Anexos (Modelos)

- Anexo I - Termo de Compromisso;
- Anexo II - Portaria do Comitê Interno de Governança;
- Anexo III - Matriz RACI;
- Anexo IV - Portaria da Política de Gestão de Riscos;
- Anexo V - Avaliação de Maturidade da Gestão de Riscos;
- Anexo VI - Declaração de Apetite a Riscos;
- Anexo VII - Plano de Comunicação;
- Anexo VIII - Fluxogramas da Gestão de Riscos.

13. Referências

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

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT. NBR ISO 31000: Gestão de riscos: Princípios e diretrizes. Rio de Janeiro: ABNT, 2009.

BAHIA. Secretaria da Fazenda do Estado da Bahia. Auditoria Geral do Estado. Cartilha Programa de Gestão de Risco (PGR). Bahia: Auditoria Geral do Estado, 2022.

BAHIA. Secretaria da Fazenda do Estado da Bahia. Auditoria Geral do Estado. Guia de Aplicação Programa de Gestão de Riscos (PGR). Bahia: Auditoria Geral do Estado, 2023.

BELO HORIZONTE. Controladoria-Geral do Município. Gestão de Riscos. Belo Horizonte: Controladoria-Geral do Município, 2019.

BRASIL. Controladoria Geral da União. Metodologia de Gestão de Riscos. (Versão 2.0).

BRASIL. Decreto n.º 9.203, de 22 de novembro de 2017. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional.

BRASIL. Instituto Brasileiro de Geografia e Estatística. Metodologia de Gestão de Riscos do IBGE. Rio de Janeiro: IBGE, 2019.

BRASIL. Ministério da Agricultura, Pecuária e Abastecimento. Guia de Gestão de Risco. Brasília: MAPA, 2021.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. Metodologia de gestão de riscos. Brasília: Ministério da Ciência, Tecnologia e Inovações, 2022.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão – MP. Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão. Brasília: Ministério do Planejamento, Desenvolvimento e Gestão – MP, 2017.

BRASIL. Ministério do Planejamento, Orçamento e Gestão e a Controladoria Geral da União. Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal.

BRASIL. Presidência da República. Metodologia de Gestão de Riscos. Brasília: Presidência da República.

BRASIL. Superior Tribunal de Justiça. Gestão de Riscos. Brasília: STJ, 2016.

BRASIL. Tribunal de Contas da União. 10 Passos para a Boa Gestão de Riscos. Brasília: TCU, 2018.

BRASIL. Tribunal de Contas da União. Avaliação de Maturidade da Gestão de Riscos. Brasília: TCU, 2018.

BRASIL. Tribunal de Contas da União. Manual de Gestão de Riscos do TCU (2ª Edição). Brasília: TCU, 2020.

BRASIL. Tribunal de Contas da União. Referencial Básico de Gestão de Riscos. Brasília: TCU, 2018.

BRASIL. Tribunal de Contas da União. Referencial Básico de Governança Aplicável a Órgãos e Entidades da Administração Pública (2ª versão). Brasília: TCU, 2014.

BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios. Guia de Gestão de Riscos e Controles. Brasília: TJDFT, 2019.

CONTROLADORIA GERAL DA UNIÃO. Modelo Avaliação de Maturidade da Gestão de Riscos. Brasília: CGU, 2020. Disponível em: https://repositorio.cgu.gov.br/handle/1/44987.

CONTROLADORIA-GERAL DO ESTADO DE GOIÁS. Ação 17 - Modelo Maturidade Municípios. Goiás: CGE-GO. Disponível em: https://www.controladoria.go.gov.br/pcm/ assets/files/ material/trilha6/A%C3%A7%C3%A3o% 2017%20-20Modelo %20 Maturidade%20Munic% C3% ADpios.xlsx.

CONTROLADORIA-GERAL DO ESTADO DE GOIÁS. Modelo Termo de Compromisso Programa de Compliance Público -

PCP. Goiás: CGE-GO. Disponível em: https://www.controladoria.go.gov.br/files/Declaracoes/Anexo2_12988.pdf.

CURSO INTRODUÇÃO À GESTÃO DE RISCOS, 2023, Plataforma Virtual de Ensino à Distância. Anais do curso Introdução à Gestão de Riscos. EAD: Escola Nacional de Administração Pública - Enap, 2023.

GOIÁS. Controladoria-Geral do Estado de Goiás. Guia do Programa de Compliance Público Municipal. Goiás.

GOIÁS. Controladoria-Geral do Estado de Goiás. Plano de Comunicação do Programa de Compliance Público - Eixo Gestão de Riscos. Goiás: CGE-GO, 2023.

GOIÁS. Secretaria de Estado da Segurança Pública. Programa de Compliance Público da Secretaria de Estado da Segurança Pública – Eixo IV – Gestão de Riscos. Goiás.

MINAS GERAIS. Controladoria-Geral do Estado de Minas Gerais. Declaração de Apetite a Riscos da Controladoria-Geral do Estado. Minas Gerais: CGE-MG, 2020.

MINAS GERAIS. Controladoria-Geral do Estado de Minas Gerais. Guia Metodológico de Gestão de Riscos de Processos. Minas Gerais. CGE-MG, 2020.

MINAS GERAIS. Controladoria-Geral do Estado de Minas Gerais. Guia Metodológico de Gestão de Riscos de Processos. Minas Gerais. CGE-MG, 2021.

MINAS GERAIS. Controladoria-Geral do Estado de Minas Gerais. Guia Metodológico de Gestão de Riscos Estratégicos. Minas Gerais. CGE-MG, 2020.

PERNAMBUCO. Secretaria da Controladoria-Geral do Estado de Pernambuco. Cartilha de Estruturação e Implementação da Gestão de Riscos. Pernambuco: SCGE-PE, 2022.

SALVADOR. Decreto nº 37.836 de 28 de novembro de 2023. Estabelece as diretrizes gerais da Gestão de Riscos no âmbito do Poder Executivo do município de Salvador. Diário Oficial do Município: Decretos numerados, Salvador - Ba, ano 37, n.

8670, p. 9-12, 29 nov. 2023.

SALVADOR. Decreto nº 37.837 de 28 de novembro de 2023. Institui a Política de Governança no âmbito do Poder Executivo do município de Salvador. Diário Oficial do Município: Decretos numerados, Salvador - Ba, ano 37, n. 8670, p. 12-14, 29 nov. 2023.

THE INSTITUTE OF INTERNAL AUDITORS (IIA). As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles. IIA, 2013.

THE INSTITUTE OF INTERNAL AUDITORS (IIA). Modelo das Três linhas do IIA 2020 – Uma atualização das Três Linhas de Defesa. IIA, 2020.

UNIVERSIDADE FEDERAL DO CEARÁ. Plano de Gestão de Riscos 2023-2027. Ceará: UFC, 2022.

ZILLER, Henrique Moraes; BORGES, Mara Nunes Silva; CRISPIM, Luís Henrique; CASTRO, Adriano Abreu de. Gestão de Riscos na Prática: Conceitos, Desafios e Resultados no Estado de Goiás. 1. ed. Belo Horizonte: Fórum, 2023. 219 p.