MANUAL DE GESTÃO DE RISCOS

2023

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

Ficha Técnica

Controlador Geral do Município

Daniel Gustavo Falcão Pimentel dos Reis

Chefe de Gabinete

Thalita Abdala Aris

Elaboração

Claudia Valente
Luis Felipe Nogueira Giacomello
Paula Yoshie Maeda
Thais Almeida Valvassoura

Revisão e Edicão

Wagner Luiz Taques Da Rocha
Renata Figueiredo Andrade de Oliveira
Thalita Abdala Aris
José Maurício Linhares Barreto Neto
Kelvin Peroli dos Reis
Jardel Soares Fernandes
Fabio Fernandes Libonati

Diagramação

Thiago Henrique Pereira

SUMÁRIO

APRESENTAÇÃO

Criada pela Lei nº 15.764, de 27 de maio de 2013, a Controladoria Geral do Município de São Paulo (CGM) é órgão central tanto do sistema de controle interno dos órgãos municipais e das entidades da administração indireta quanto do Sistema de Corregedorias e do Sistema de Ouvidorias. Entre as suas principais finalidades estão a promoção do controle interno da administração, o suporte ao Prefeito, no desempenho de suas atribuições quanto aos assuntos e providências que, no âmbito do Poder Executivo, sejam atinentes à defesa do patrimônio público, ao controle interno, à auditoria pública, à correição, à prevenção e ao combate à corrupção, às atividades de ouvidoria e da promoção da ética no serviço público, o incremento da moralidade e da transparência e o fomento ao controle social da gestão, no âmbito da Administração Municipal.

Dentro de suas competências, a CGM busca implementar ferramentas e mecanismos capazes de modernizar seus processos de trabalho, de modo a torná-los cada vez mais eficientes na condução de sua missão institucional. É nesse sentido que a CGM elaborou a Política de Gestão de Riscos (PGR), um instrumento fundamental para o aprimoramento da gestão pública municipal.

Estruturada com base nas principais referências sobre o tema (ISO 31000:2018 e COSO ERM) e das experiências realizadas por outros órgãos da administração pública federal e municipal nos últimos anos, a Política de Gestão de Riscos apresenta a sua metodologia estruturada em etapas que facilita a sua realização e que apresenta uma série de ferramentas que auxiliam os trabalhos. Junto com a gestão de riscos, como parte do processo este manual apresenta também conceitos e modelos de gestão de processos. Assim, além de identificar, corrigir e tratar os riscos existentes nos processos de trabalho adotados no âmbito do órgão, diminuindo a quantidade de eventos que possam afetar, direta ou indiretamente, o alcance dos objetivos traçados no seu planejamento estratégico, ela facilita a distribuição de tarefas e responsabilidades para cada agente envolvido.

Com base no exposto acima, o objetivo deste manual é apresentar a Política de Gestão de Riscos da Controladoria Geral do Município de São Paulo, em especial, a sua estrutura e metodologia, com vistas a orientar a sua implementação, em conformidade com a Portaria 49/2023, e demais normativos e boas práticas de governança.

POLÍTICA DE GESTÃO DE RISCOS

A. INTRODUÇÃO

Risco é definido como a possibilidade de que um evento ocorra e afete, positivamente (risco positivo) ou negativamente (risco negativo), os objetivos pretendidos. Assim, percebe-se que os riscos estão presentes tanto no cotidiano das pessoas quanto no das organizações. Para uma pessoa, essas ameaças ou oportunidades podem influenciar o andamento de suas atividades, levando-a a uma direção completamente diferente daquela inicialmente planejada. Do mesmo modo, isso também ocorre no mundo corporativo. Diariamente, as organizações são expostas a uma série de incertezas, provenientes tanto de fatores internos quanto externos, que tornam duvidoso o êxito do atingimento das metas dos projetos ou das atividades durante a busca para agregar valor aos negócios.

Uma maneira de reduzir esse problema a níveis aceitáveis de riscos e assegurar o alcance dos objetivos das instituições é por meio da implementação de um sistema de gestão de riscos. Suas ferramentas e metodologias permitem a identificação antecipada dos possíveis eventos que poderiam ameaçar o atingimento das metas, o cumprimento dos prazos, das leis e regulamentos, entre outros. Em resumo, a gestão de riscos pode ser descrita como o conjunto de técnicas e ferramentas coordenadas que têm como objetivo gerenciar e controlar uma organização em relação a potenciais ameaças, seja qual for a sua manifestação (econômica, social, legal, tecnológica, operacional etc.), e que afetam os seus trabalhos. Isso implica no planejamento e uso dos recursos humanos e materiais para minimizar os riscos ou, então, tratá-los, mantendo-os compatíveis com o apetite a risco da organização, bem como na melhoria contínua dos processos organizacionais. Portanto, nota-se que a adoção dessas práticas é necessária em todas as entidades, especialmente nas públicas, visando resguardar os bens e recursos públicos, evitar seu mau uso e garantir a eficácia na execução das políticas públicas.

Nas organizações públicas, a busca pela eficiência e foco no cidadão são fatores diretamente relacionados, já que não se pode falar em atenção ao cidadão sem a prestação de serviços públicos de qualidade e a custos compatíveis com os orçamentos previamente aprovados. Isto é, a principal maneira para que os órgãos e entidades públicas cumpram com as suas missões e objetivos é mediante a busca crescente por melhorias no sentido de alcançar a excelência operacional. Assim, a inclusão da gestão de riscos na cultura de trabalho das entidades públicas só tem a contribuir, pois a mitigação de riscos, se implementada com a racionalidade e foco adequados, aumenta a certeza de atingimento dos objetivos da gestão, com benefícios diretos e imediatos para a sociedade.

Para que isso se torne uma realidade na administração pública municipal, foram elaborados os seguintes documentos: a Política de Gestão de Riscos da Controladoria Geral do Município

de São Paulo, a Portaria 49/2023, e o presente manual, o qual representa um instrumento importante para sua implementação. A metodologia nele desenvolvida tem como objetivo auxiliar o gestor na tomada de decisão com vistas a prover razoável segurança no cumprimento da missão e no alcance dos objetivos institucionais. Além disso, fornece condições para que seja capaz de identificar os principais riscos e as várias possíveis respostas a cada um deles, sendo uma ferramenta importante de apoio na busca por ganhos de eficiência, de eficácia, e de melhoria na qualidade dos serviços prestados. Em termos de conteúdo, aborda os objetivos, os princípios da gestão de riscos na CGM, sua governança e seu funcionamento, o processo de gestão de riscos propriamente dito e um glossário com a definição dos principais termos utilizados.

B. OBJETIVOS

A Política de Gestão de Riscos foi construída com base em objetivos claros e alinhados diretamente com os trabalhos de implementação, desenvolvimento e disseminação da metodologia de gestão de riscos. São eles:

I. Fomentar o ambiente íntegro e confiável, alinhado aos valores éticos compartilhados pela sociedade;
II. Prezar a conformidade legal e normativa, incluindo políticas, programas, planos, procedimentos e normas internas dos órgãos e entidades;
III. Ampliar o desenvolvimento do controle interno e das boas práticas de governança;
IV. Subsidiar a tomada de decisões, zelando pelo atingimento de metas e resultados;
V. Mitigar os efeitos de eventos que representem riscos negativos que impactam no alcance da missão e dos objetivos traçados no Planejamento Estratégico;
VI. Melhorar os controles de riscos existentes;
VII. Estimular uma gestão proativa que antecipe ocorrências e previna impactos no desempenho;
VIII. Desenvolver uma gestão dos recursos eficaz e eficiente;
IX. Promover a integração e a melhoria contínua dos processos organizacionais;
X. Fortalecer a cultura da gestão de riscos, de controles internos e de comportamento ético;

C. PRINCÍPIOS

As atividades de gestão de riscos, bem como seus instrumentos e ferramentas, encontram suporte nos seguintes princípios da Política de Gestão de Riscos:

I. Zelar pelos valores éticos, de integridade e pelas boas práticas de governança;
II. Ser parte integrante dos processos organizacionais;
III. Ser sistemática, estruturada e oportuna;
IV. Utilizar as melhores informações disponíveis;
V. Estar alinhada com o contexto interno e externo e com o perfil do risco organizacional;
VI. Considerar os fatores humanos e culturais;
VII. Ser transparente e integrada;
VIII. Ser dinâmica, interativa e capaz de reagir a mudanças;
IX. Agregar valor à instituição;
X. Subsidiar a tomada de decisões;
XI. Promover melhorias contínuas;
XII. Ter o comprometimento de todos os servidores, em especial, o da alta administração.

D. ESTRUTURA

A implantação de um sistema efetivo de Gestão de Riscos demanda adaptações e ajustes na estrutura organizacional do Município para explicitar o papel, responsabilidades, tarefas e inter-relações desempenhados por cada agente público envolvido.

As orientações aqui apresentadas têm por premissa o desenvolvimento de um sistema de gestão de riscos abrangente, e que funcione de forma harmônica e sinérgica, propiciando o amadurecimento do sistema de modo eficiente e consistente.

A estrutura deve ser concebida em harmonia com o modelo de 3 linhas desenvolvido pelo Instituto de Auditoria Interna, representado na Figura 01, o qual vem sendo implementado com sucesso em inúmeras organizações, desde sua propositura em 2013, sob a premissa de evitar a duplicação de estruturas com responsabilidades concorrentes, bem como evitar a existência de vácuos estruturais que impeçam a aplicação bem-sucedida do modelo de gestão de riscos.

Figura 01: Modelo de 3 Linhas do IIA. Fonte: IIA Brasil[1]

Apresenta-se, abaixo, a estrutura da Gestão de Riscos das Unidades da Prefeitura do Município de São Paulo com base no Modelo de Três Linhas (figura 02). Ela contempla três instâncias principais: o Comitê de Gestão de Riscos, o Núcleo Especializado de Gestão de Riscos, e os Gestores dos Riscos.

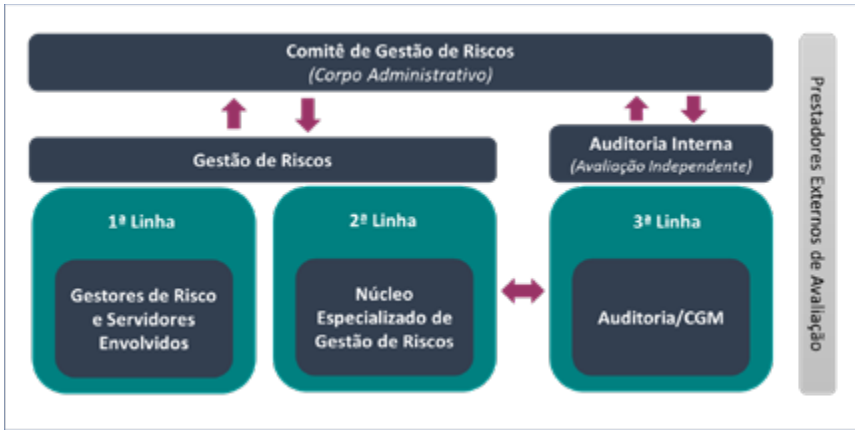

Figura 02: Estrutura de Gestão de Riscos aplicada às Unidades da PMSP[2]

[1] Fonte: https://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/20200758glob-th-editorHTML-00000013-20082020141130.pdf

[2] Elaboração própria, com base no Modelo de 3 Linhas do IIA. Idem, Op. Cit..

a) Comitê de Gestão de Riscos

O Comitê de Gestão de Riscos representa a alta gestão do órgão ou entidade, bem como os agentes definidores de seu planejamento estratégico.

Para a sua implementação de uma política de gestão de riscos, é necessário desenvolver um planejamento estratégico e definir os objetivos do órgão ou entidade. Assim, a Alta Gestão deve formalizar a estrutura do Comitê de Gestão de Riscos, conforme descrito na Portaria 49/2023, que abarque as seguintes responsabilidades:

- Definir os objetivos e metas do planejamento estratégico da Entidade;
- Acompanhar e avaliar relatórios periódicos dos órgãos ou entidades, estabelecer diretrizes e aprovar as atividades do Núcleo Especializado de Gestão de Riscos;
- Decidir, com base em parecer do Núcleo Especializado de Gestão de Riscos, sobre o apetite a risco organizacional, definindo referências, limites e critérios para a mensuração de resultados;
- Aprovar os riscos que excedam o apetite definido e os riscos aceitos pelo órgão ou entidade;
- Revisar periodicamente o apetite ao risco da instituição, além dos riscos aceitos que superem esse apetite, garantindo direcionamento claro para a gestão de riscos do órgão ou entidade;
- Monitorar a implementação das deliberações do próprio Comitê de Gestão de Riscos, assegurando apoio institucional para a efetivação da Gestão de Riscos;
- Definir e revisar periodicamente o nível de maturidade em gestão de riscos desejados no órgão ou entidade;
- Estabelecer parcerias com outras instituições para mitigar riscos compartilhados.

b) Núcleo Especializado de Gestão de Riscos

Abaixo do Comitê, encontra-se o Núcleo Especializado de Gestão de Riscos, ao qual cabe a efetiva implementação da Gestão de Riscos e deve ser presidido pelo Responsável pelo Controle Interno (RCI) do órgão ou entidade. Esse grupo terá as seguintes responsabilidades:

- Assegurar que informações sobre riscos e controles internos cheguem aos membros do Comitê de Gestão de Riscos e que as decisões do comitê sejam disseminadas em toda a instituição;
- Dirigir a aplicação da metodologia de gestão de riscos e coordenar a revisão periódica do processo visando sua melhoria contínua;
- Coordenar o mapeamento dos processos- chave relacionados aos objetivos, cujos

riscos possuem classificação mais crítica;

· Identificar contexto e nível do apetite ao risco conforme planejamento estratégico do órgão ou entidade e metodologia aplicável;

· Apreciar respostas aos riscos, controles e planos de ação propostos;

· Consolidar plano de gerenciamento de riscos do órgão ou entidade de acordo com a resposta ao risco definida, avaliar grau de maturidade e monitorar seu desempenho;

· Coordenar implementação de plano de ação e/ou controles internos, bem como ferramentas de gestão de riscos do órgão ou entidade;

· Monitorar a evolução dos níveis de riscos e a efetividade das medidas de controles implementadas;

· Orientar, monitorar e capacitar gestores de riscos da Unidade, bem como os responsáveis por demais funções no processo de gestão de riscos do órgão ou entidade;

· Auxiliar no agendamento, pauta, organização e documentação das reuniões realizadas pelo Comite;

· Atuar ativamente na disseminação da cultura de gestão de riscos por meio de reuniões, palestras, oficinas, cursos, dentre outros eventos;

. Coordenar o trâmite e arquivamento de documentos relevantes ao processo de gestão de riscos, preferencialmente em unidade própria no Sistema Eletrônico de Informações (SEI);

· Executar outras tarefas determinadas pelo Comitê de Gestão de Riscos.

c) Gestores de Riscos

Os Gestores dos Riscos usualmente são os gestores diretos dos servidores que executam as atividades relacionadas aos riscos. Eles devem ter alçada suficiente para orientar e acompanhar as etapas de identificação, análise, avaliação e implementação das respostas aos riscos assim como tomar decisões relacionadas as respostas, planos de ação e implementação de controles internos. Suas principais atribuições são:

- Direcionar e orientar o mapeamento dos processos e sua gestão;
- Identificar, analisar e avaliar os riscos dos processos sob sua tutela;
- Propor respostas e respectivas medidas de controle para os processos organizacionais de sua competência;
- Desenvolver os controles e os planos de ações aprovados pelo Comitê de Gestão de Riscos para o tratamento dos riscos;
- Atuar para garantir a mitigação dos níveis de riscos e a efetividade das medidas de controles implementadas;
- Comunicar ao Núcleo Especializado de Gestão de Riscos as ações realizadas e emitir relatórios periódicos dos indicadores de riscos da unidade;
- Informar o Núcleo Especializado de Gestão de Riscos sobre mudanças significativas nos processos organizacionais sob sua responsabilidade e demais informações relevantes;
- Atender às solicitações do Núcleo Especializado de Gestão de Riscos;
- Designar os servidores que auxiliarão na elaboração dos mapeamentos dos processos e na execução de outras tarefas;
- Orientar e incentivar servidores responsáveis pelos processos para atuação com foco na gestão de riscos.

E. METODOLOGIA DE GESTÃO DE RISCOS

A metodologia apresentada a seguir foi estruturada para atender o processo de gerenciamento de riscos desde sua implementação até seu amadurecimento e aprimoramento ao longo dos anos nos órgãos e entidades. Ela é composta por sete etapas interligadas (Figura 03), que engloba todas as fases da gestão de riscos, com objetivo de reduzir ou manter riscos a níveis aceitáveis, garantindo o alcance dos objetivos com razoável confiabilidade.

Os órgãos e entidades devem aplicar a estrutura descrita em ciclos (a cada dois anos) ou após a revisão do planejamento estratégico, caso ocorra primeiro. É vital que todas as fases sejam realizadas envolvendo os responsáveis adequados e pessoas com expertise nos tópicos abordados.

Em sua execução, devem ser considerados os projetos em andamento e os previstos, os processos de trabalho, os sistemas informatizados, bem como a gestão orçamentária, patrimonial, financeira e de pessoal do órgão ou entidade, visando minimizar ameaças ou capitalizar oportunidades.

Figura 03: Estrutura de Gestão de Riscos[3]

Etapas do Processo de Gestão de Riscos

Na Figura 04, são apresentadas as etapas do processo de gestão de riscos que definem o ciclo a ser seguido para a aplicação da metodologia baseada na norma ISO 31000 no órgão ou entidade:

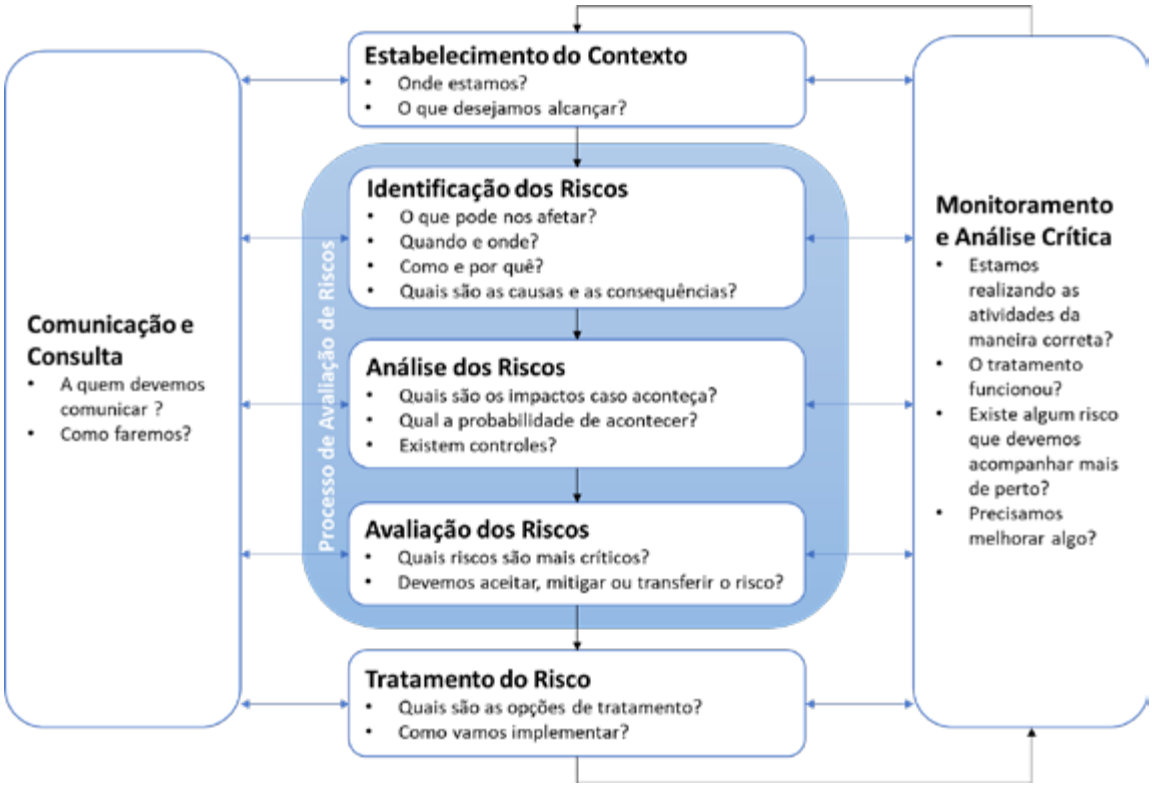

Figura 04: Processo de Gestão de Riscos baseada na norma ISO 31000[4]

[3] Fonte: ISO 31000/2018.

[4] Elaboração própria, com base no Modelo de 3 Linhas do IIA. Idem, Op. Cit.

1. Análise do contexto

A aplicação do gerenciamento de riscos deve começar com a etapa de estabelecimento do contexto. Nela a entidade deve realizar uma avaliação global do cenário no qual está inserida, partindo da identificação dos fatores relacionados tanto ao ambiente interno quanto ao externo.

De acordo com a ABNT NBR ISO 31.000/2018, "O propósito do estabelecimento do escopo, contexto e critérios é personalizar o processo de gestão de riscos, permitindo um processo de avaliação de riscos eficaz e um tratamento de riscos apropriado".

Desse modo, além de permitir um entendimento das principais características internas, a análise do contexto promove uma compreensão do momento em que a organização se encontra, como, por exemplo, a sua posição estratégica no município, seu relacionamento com os servidores e demais colaboradores, indícios acerca do futuro e da continuidade de seus serviços esperados pelos seus principais usuários, entre outros. Esta atividade é fundamental na metodologia de gestão de riscos; com base nela, definem-se os riscos a tratar conforme o grau de ameaça ou oportunidade.

1.1 Apresentação da Estrutura da Organização

Para estabelecer o contexto, é necessário levantar a estrutura organizacional visando, pelo menos, identificar:

- A própria estrutura organizacional;
- A regulamentação vigente;
- As principais atividades desempenhadas; e
- Os instrumentos normativos chave relacionados à gestão de riscos.

1.2 Estabelecimento do Ambiente Interno

Para uma gestão de riscos personalizada e eficaz, é crucial compreender os valores centrais da organização e os fatores estratégicos que a guiam em direção aos seus objetivos. Assim, torna-se necessário definir:

a) Missão

Representa o propósito e a razão de ser da organização. Por meio dela, deve-se responder perguntas como:

- Quem somos?
- Qual é o nosso propósito?
- O que fazemos para reconhecer, antecipar e responder ao nosso propósito?
- Quais são os valores culturais e filosofias que nos guiam?
- O que nos diferencia e nos torna e únicos?

b) Visão

Representa aonde a organização quer chegar e o que pretende alcançar com suas atividades. A visão manifesta os ideais e aspirações para o futuro, sendo uma fonte de motivação, uma direção geral e uma filosofia que orienta os seus membros. Ela norteia respostas para questões como:

- Em que a organização quer se tornar?
- Qual direção seguir?
- O que a organização aspira a ser?
- Em que devo focar meus esforços?
- Que futuro estou ajudando a construir?
- Para qual direção os recursos investidos estão conduzindo a organização?

c) Valores

Representam as crenças, atitudes e padrões de comportamento valorizados pela organização. Por meio dos valores, a cultura organizacional se conecta aos processos internos e alinha seus agentes e atividades aos objetivos estratégicos.

d) Objetivos

Os objetivos representam as intenções que orientam a organização de forma clara e concisa, visando alcançar sua visão. Constituem a definição dos resultados que se busca atingir em um determinado período, ancorados no planejamento estratégico, tático e operacional.

O estabelecimento dos objetivos é crucial na gestão de riscos. As demais etapas se baseiam no definido aqui para orientar suas atividades. Quando realizado corretamente, esse processo potencializa ótimos resultados ao seu término. Durante sua execução, deve-se observar:

- Os objetivos devem ser claros, específicos e detalhistas, refletindo o que a organização realmente busca.;
- É essencial que os objetivos sejam mensuráveis, com referências claras para aferir seu alcance;
- Embora possam ser desafiadores, os objetivos devem ser realistas;
- Objetivos muito extensos podem se desdobrar em partes menores, com metas intermediárias.

e) Modelo de Negócio

O modelo de negócio refere-se à forma como a organização cria, entrega e captura valor em diversos contextos, como econômicos, sociais e culturais. Representa a estruturação dos elementos e etapas que determinam sua atuação e atividades.

1.3 Análise do Ambiente Interno e Externo (SWOT)

Após o levantamento do ambiente interno e das informações estratégicas, é essencial compreender a relação da organização com tais fatores. . Nesse contexto, emprega-se a análise SWOT. Ela identifica forças (Strengths) e fraquezas (Weaknesses) do ambiente interno e oportunidades (Opportunities) e ameaças (Threats) do ambiente externo. Esta análise pode ser adaptada tanto para o município quanto para o órgão ou entidade que adotará a gestão de riscos. Esses termos são assim definidos:

- Forças - vantagens internas;
- Fraquezas - desvantagens internas;
- Oportunidades - aspectos externos positivos que podem potencializar os resultados da área/atividade;

· Ameaças - aspectos externos negativos que podem pôr em risco os resultados da área/atividade.

Com base nas definições acima, pode-se elaborar a matriz SWOT:

Figura 05: Análise SWOT (criação própria baseada na metodologia SWOT)

1.4 Mapeamento dos processos

Após a análise inicial da organização, o passo seguinte é o mapeamento de processos. Para aumentar a eficiência e efetividade da gestão de riscos, é essencial selecionar os processos-chave com base nas atividades operacionais, táticas e estratégicas. De acordo com a evolução da maturidade da organização e a sua capacidade de monitoramento, pode-se expandir o escopo aos demais processos e projetos desenvolvidos, garantindo que a qualidade dos trabalhos não seja comprometida. O objetivo principal desta etapa é retratar o funcionamento da organização, mostrando de forma clama os seus processos. Para alcançar essa meta, é fundamental seguir a metodologia, considerando pelo menos as etapas a seguir:

[5] Criação própria baseada na metodologia SWOT

· Identificação dos objetivos e etapas dos processos: detalhar as etapas de cada processo, indicando seus respectivos objetivos;
· Recursos humanos envolvidos: divisões do órgão ou entidade e agentes públicos que atuam em cada etapa de processo;
· Recursos Físicos e Tecnológicos: infraestrutura física e tecnológica utilizada em cada etapa (Exemplo: “hardware” e “software” utilizados para documentação de informações em formatos digitais);
· Métodos de comunicação e compartilhamento: modo de como os recursos humanos se comunicam e como as informações são compartilhadas entre as etapas;
· Informações e documentação por etapa: lista de documentos e informações geradas ou compartilhados em cada fase de um processo.

Em situações em que, após uma decisão, uma etapa possa se desmembrar em diferentes etapas ou faça referência a outras, é possível sequenciar as etapas:
1. com subitens (exemplo:, etapa 2.1 e etapa 2.2, seguintes à etapa 1); e
2. com remissão à(s) etapa(s) precedente(s) ou sucessora(s).

Essa análise deverá ter como descritivos:
· Um resumo que contemple as principais etapas, atos e resultados;
· Definição dos objetivos gerais e específicos;
· Especificação dos recursos humanos empregados em cada etapa;
· Detalhamento dos recursos físicos e tecnológicos empregados em cada etapa;
· Listagem dos normativos pertinentes para execução da atividade;
· Identificação das áreas e cargos encarregados da execução;
· Descrição do cenário atual de realização dos processos, incluindo aspectos como prazos, quantidades, valores, objetos entre outros.;
· Relação de documentos consultados e/ou gerados em cada etapa do processo.

2. Processo de Avaliação dos Riscos

Neste momento, a metodologia de gestão de riscos entra em seu principal macroprocesso, constituído de três etapas: a identificação, a análise e avaliação dos riscos críticos, isto é, aqueles riscos que podem impactar de maneira significativa os processos e projetos atrelados aos objetivos organizacionais.

Essas atividades são essenciais para a administração integral dos riscos, visto que, a partir dos seus resultados, serão estruturados os procedimentos apropriados e a natureza de resposta a ser dada a um risco específico, baseando-se no apetite por risco definido pela organização.

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

2.1 Identificação dos Riscos

A etapa de identificação de riscos pode ser caracterizada como o processo de levantamento, identificação e descrição dos riscos, tendo por base as informações obtidas durante a Análise do Contexto, e contando com a comunicação e consulta contínua das equipes envolvidas e outras partes interessadas. O principal objetivo é elaborar um registro abrangente de riscos, isto é, uma relação detalhada dos eventos que, caso ocorram, podem influenciar na realização dos objetivos institucionais.

Os responsáveis por essa etapa devem realizá-la mediante a realização de reuniões, desenvolvimento de atividades e conversas, junto aos demais servidores indicados - que necessitam ter profundo conhecimento dos processos-chave mapeados e visão abrangente da entidade e/ou setor –sempre com o suporte e orientação do Núcleo Especializado de Gestão de Riscos. Para facilitar a implementação, é viável dividir a etapa em fases, adotando uma abordagem que vai do geral para o específico. Isto é, primeiro inicialmente são identificados os riscos que permeiam os processos mais críticos e estratégicos em um nível mais amplo, servindo como ponto de inicial para, posteriormente, analisar-se os riscos de forma mais minuciosa, replicando esse método para os processos de menor prioridade.

Para o desenvolvimento do levantamento de riscos, as equipes podem utilizar dados históricos, análises teóricas, opiniões de especialistas, assim como as seguintes técnicas de coleta de informação:

· **Chuva de ideias (Brainstorming):** Nesta técnica, os servidores que estão diretamente ligados aos processos centrais são convocados para compartilhar suas perspectivas, sem necessidade de um consenso inicial. O intuito é compilar uma gama de riscos percebidos na organização em avaliação, utilizando como referência as informações coletadas na anterior.

· **Análise SWOT** (strengths, weaknesses, opportunities and threats analysis): Com base na análise SWOT elaborada na fase de Análise de Contexto, os responsáveis devem identificar possíveis eventos, tanto internos quanto externos, que poderiam resultar em problemas financeiros, legais, operacionais, de imagem, entre outros, para a organização ou entidade.

· **Análise da causa-raiz:** Nesta técnica a equipe envolvida busca identificar problemas existentes e os passíveis de acontecer no futuro, e descobrir os eventos de riscos que levam e/ou levariam a eles.

· **Entrevistas:** Esta técnica baseia-se na formulação prévia de um conjunto de perguntas que são apresentadas nas entrevistas feitas com os agentes mais envolvidos nos processos e especialistas no assunto. Ela tem como finalidade garantir que todos os entrevistados abordem os mesmos assuntos na identificação de riscos e evitar a influência da opinião de outros participantes do grupo nas respostas.

De acordo com o grau de maturidade de cada organização, pode-se adotar diferentes metodologias das presentes acima e/ ou haver a combinação entre elas. Para aqueles que ainda estão iniciando o processo de gestão de riscos, sugere-se a combinação do brainstorming, Análise SWOT, junto à utilização de entrevistas no final para acrescentar informações adicionais, pois sua aplicação possui baixa complexidade, sempre direcionadas aos processos-chave previamente mapeados.

Após a atividade de identificação, a equipe deve fazer o descritivo dos riscos encontrados com os seus detalhes. Exemplo:

Risco Crítico	Descritivo do Risco
Incêndio	Ocorrência de Incêndio de grande porte no prédio onde fica localizado o órgão, com destruição dos equipamentos e documentos existentes.
Colapso no sistema de Informação	Colapso no sistema de informação, que impede a gestão de acompanhar os processos por um período significativo (de 1 semana até 1 mês).

Tabela 01: Exemplo de descritivo de risco.

Em seguida, deve-se classificá-los segundo as seguintes categorias:

· **Operacional:** refere-se aos eventos que podem comprometer as atividades diárias da instituição, seja por questões técnicas ou operacionais;

· **Orçamentário:** envolve os eventos que, ao se materializem, podem afetar o orçamento da organização, impactando em receitas ou despesas;

· **Imagem:** diz respeito aos eventos que têm a possibilidade de impactar de maneira significativa a reputação da organização, afetando, em consequência, a opinião pública (incluindo a população e a imprensa) sobre a entidade e/ou governo;
· **Conformidade:** engloba os eventos que podem impedir a organização de atender à legislação vigente, como leis, decretos, portarias e outros atos normativos;
· **Social:** abarca os eventos que têm o potencial de afetar diretamente na execução de políticas públicas com um claro dano social, seja na educação, saúde, moradia etc.;
· **Integridade:** abrange os eventos que ameaçam os valores e princípios éticos da organização, relacionados a atos de corrupção, fraude, irregularidades e/ou desvios éticos, de conduta e conflitos de interesse.

No caso de o evento de risco esteja associado a duas ou mais categorias de classificação, deve-se escolher a categoria que reflete o aspecto mais relevante em relação ao impacto que o evento de risco poderá trazer, caso se materialize. Para padronização e otimização das análises, será adotada a planilha apresentada no anexo 03 como modelo de documento para Gestão de Riscos.

Por último, as equipes precisam analisar os riscos previamente descritos e classificados e, então, listar as possíveis causas de sua ocorrência, assim como suas consequências. As causas são condições (falhas) que dão origem à possibilidade de um evento ocorrer, também chamadas de fatores de riscos e podem ter origem no ambiente interno e externo. Já as consequências são o resultado (impacto) de um evento de risco sobre os objetivos do processo.

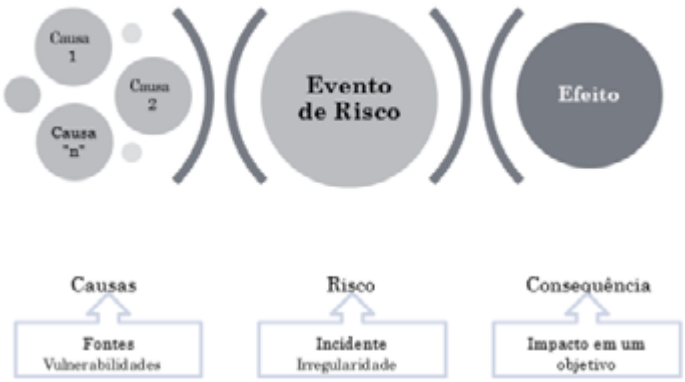

Figura 06: Componentes dos eventos de risco. Fonte: Manual de Gestão de Riscos, Controles Internos e Integridades do Ministério do Desenvolvimento Regional [6]

[6] BRASIL, Ministério do Desenvolvimento Regional. Manual de Gestão de Riscos, Controles Internos e Integridade. Disponível em: https://www.gov.br/mdr/pt-br/acesso-a-informacao/governanca/MANUALDEINTEGRIDADEGESTAODERISCOSECONTROLESINTERNOSMDR_V9F.pdf.

Como forma de auxílio na reflexão e desenvolvimento desta etapa, apresenta-se a seguinte síntese:

Devido à **<CAUSA>**, poderá acontecer **<EVENTO DE RISCO>**, o que poderá levar à **<IMPACTO>**, constrangendo o **<OBJETIVO DO PROCESSO>**

De acordo com o grau de maturidade de cada organização, diferentes metodologias também podem ser adotadas e/ou haver a combinação entre elas, de modo a auxiliar na identificação das causas e impactos dos riscos. Abaixo, seguem as principais técnicas de diagrama.

· **Diagramas de causa e efeito** (também conhecidos como Ishikawa ou espinha de peixe): É uma ferramenta gráfica, com o formato de espinha de peixe, que tem como finalidade ajudar as equipes a identificar as causas dos riscos e definir alguns potenciais impactos.

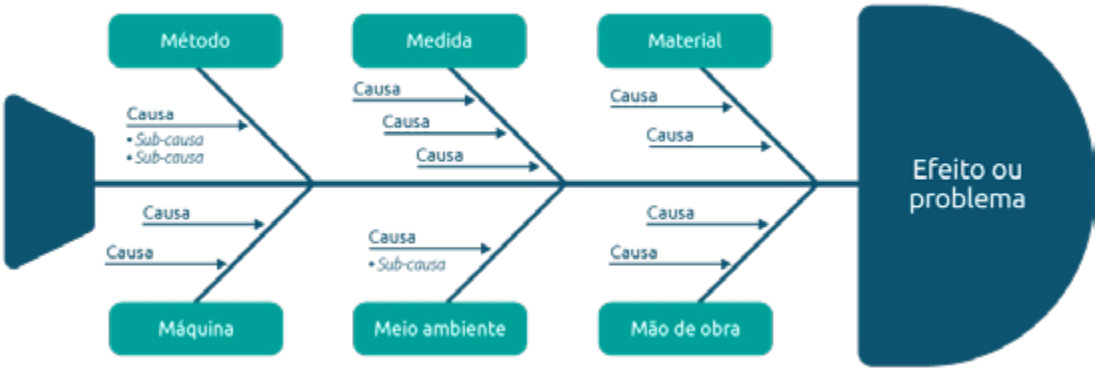

Figura 07: Modelo diagrama de causa e efeito [7]

· **Fluxograma:** É uma representação gráfica do percurso ou caminho percorrido pelo evento de risco, geralmente com o uso de figuras geométricas e setas as unindo. Desse modo, demostra como os vários elementos de um sistema se inter-relacionam, bem como seus mecanismos de causalidade.

· **Diagramas de Influência:** É uma representação gráfica que demonstra os relacionamentos dos eventos, deixando claro as suas influências de causalidade, a ordem dos eventos no tempo e outras relações entre variáveis e resultados.

Bow Tie (gravata borboleta): É um diagrama que serve para descrever os riscos e analisar suas trajetórias, desde as causas até as consequências. Seu foco está nas barreiras que mediam as causas e o risco, e o risco e as consequências. As seguintes etapas são consideradas para este método:

[7] Fonte: https://pt.slideshare.net/ythkar/ppt-ao-corretiva-e-no-conformidadepptx

1. Identificação dos riscos a serem analisados, representando o nó principal da gravata borboleta;
2. Elaboração de uma descrição das causas do evento, baseando-se nos riscos apontados;
3. Estabelecimento do mecanismo pelo qual a fonte do perigo principal leva a um evento crítico;
4. Elaboração de desenho de linhas que conectam as causas e o evento, criando o lado esquerdo da gravata borboleta;
5. Definição de barreiras que evitariam consequências não desejadas;
6. Identificação de possíveis consequências e delineamento de linhas demostrando como o evento pode se propagar;
7. Representação de barreiras que que previnem a propagação das consequências, concluindo o lado direito da gravata.

Para as unidades que estão iniciando o processo de gestão de riscos, recomenda-se a aplicação do método Bow Tie demonstrado abaixo, dado que sua implementação possui baixa complexidade

Figura 08: Modelo diagrama Bow tie. Fonte: http://www.arrudaconsult.com.br/. [8]

[8] Fonte: http://www.arrudaconsult.com.br/2020/03/analise-de-risco-tecnica-bow-tie.html

2.2 Análise dos Riscos

Esta etapa possui como objetivo principal a análise profunda de cada risco, especialmente quanto à probabilidade de ocorrência e os potenciais impactos nos objetivos organizacionais. Considera-se **probabilidade** as chances reais do risco identificado ocorrer, sendo fundamentada na análise de dados históricos do processo. Já o **impacto** de um risco pode ser caracterizado como qualquer repercussão financeira, operacional, de imagem, dentre outras, que se manifestem após a sua materialização.

Com base nesta análise, realiza-se a classificação dos riscos de maneira mais efetiva e precisa, assim como a elaboração de cada plano de ação e/ou estratégia de controle interno a ser implementada, visando corresponder adequadamente a cada risco identificado.

Para efetivar a prática, sugere-se que a classificação dos riscos quanto ao seu impacto e à sua probabilidade seja feita de maneira colegiada por um time designado para essa finalidade. Além disso, deve-se adotar um procedimento pré-estabelecido: inicia-se com a avaliação do risco inerente (risco bruto, sem considerar qualquer controle), em seguida, parte para a análise do(s) controle(s) já existente(s) e, por fim, é concluída por meio da verificação do risco residual (considerando os controles identificados e avaliados quanto ao desenho e a sua execução).

2.2.1 Análise dos Riscos Inerentes

O risco inerente pode ser definido como aquele presente na organização antes de qualquer ação de mitigação ou tratamento ser levada em conta. Sua análise é feita com relação à **probabilidade** de ocorrência e aos possíveis **impactos** gerados, podendo ser fundamentada em uma avaliação **quantitativa** e/ou **qualitativa**, e pode abranger diversos graus de detalhamento dependendo do tipo de risco, da finalidade, da análise e das informações, dados e recursos disponíveis. É recomendável estabelecer um método padrão para que fatores como a divergência de opinião entre os envolvidos, a incerteza, e a disponibilidade e a qualidade dos dados sejam levados em consideração. Além disso, a metodologia deve assegurar que a quantidade e a pertinência das informações não promovam limitações sobre a modelagem.

Com base no exposto anteriormente, foi desenvolvido um procedimento de simples aplicação e que gera bons resultados no estudo dos riscos inerentes. Ele consiste em três

atividades: a obtenção da probabilidade e impacto do risco, a realização de seus enquadramentos e a classificação na matriz de risco

Obtenção da Probabilidade e Impacto do Risco

Inicialmente, verifica-se a **probabilidade** de ocorrência de cada tipo de risco e os possíveis **impactos** caso se concretize. Para a determinação da probabilidade, a equipe encarregada pode recorrer a duas fontes de dados:

· Quantitativos – trata-se de uma abordagem que se coleta dados concretos e estatísticos dos eventos de risco, seja por meio de buscas em pesquisas científicas e em informações teóricas, ou nos registros históricos da entidade sobre riscos já materializados, em determinado período ou média histórica disponível.

· Qualitativos – é uma abordagem na qual se reúne informações sobre os riscos por intermédio de descrições, impressões pessoais, opiniões e pontos de vista. Para isso, utilizam-se técnicas de apoio à coleta estruturada de informações para a obtenção dos conhecimentos técnicos e das experiências vivenciadas pelos envolvidos no processo avaliado como, por exemplo, um questionário com perguntas preestabelecidas.

Como resultado dessa análise, será obtido um descritivo da probabilidade como o exemplo abaixo:

Risco Crítico	Descritivo da Probabilidade
Incêndio	Nunca ocorreu um incêndio nas instalações, mas de forma inesperada ou casual poderá ocorrer.
Colapso no sistema de Informação	Diversas falhas no sistema de informação já ocorreram no passado e de forma até esperada. Existe 80% de chance de falhas segundo o fornecedor. É provável que o colapso ocorra.

Tabela 02: Exemplo de Descritivo de Probabilidade [9]

Em relação aos impactos significativos de cada risco, a equipe deve utilizar-se, principalmente, de dados qualitativos para a sua obtenção, aplicando as técnicas explicadas anteriormente, como o brainstorming e o questionário com perguntas preestabelecidas. Contudo, os dados quantitativos representam também fontes importantes de informação, como as estimativas orçamentárias e análises baseadas no histórico da organização.

[9] Fonte tabela: criação própria

Do mesmo modo, será obtido como resultado dessa análise um descritivo dos impactos com a particularidade de que para cada risco poderá ou não ter mais de um impacto relevante. Entretanto, nesta fase será necessário um procedimento adicional, isto é, realizar o enquadramento dos impactos nas seguintes categorias:

· **Operacional:** afetam as atividades diárias da instituição, sejam de natureza técnica ou operacional;
· **Orçamentário:** influenciam o orçamentário da entidade, seja em receitas ou despesas;
· **Imagem:** impactam diretamente a reputação da organização e, em consequência, a opinião pública (população, imprensa etc.) sobre a entidade e/ou governo;
· **Social:** afetam a execução de políticas públicas com um dano social evidente, seja na educação, saúde, moradia etc.;
· **Integridade:** representam uma ameaça aos valores e princípios éticos da entidade, e estão relacionados a atos de corrupção, fraude, irregularidades e/ou desvios éticos e de conduta;

Como a administração pública deve sempre observar o princípio da legalidade em seus atos, é compreendido que todos os riscos terão impacto ligado à Conformidade. Necessitamos focar em nossa análise no PRINCIPAL impacto, levando em consideração a fonte do risco para determinarmos a devida classificação conforme as descrições acima. Na hipótese de não enquadramento do risco em nenhuma das categorias acima, é compreendido que o impacto de conformidade deva ser utilizado mediante justificativa.

Risco Crítico	Categoria	Descritivo do Impacto
Incêndio	Operacional	Compromete as atividades diárias da instituição pela destruição de equipamentos e arquivos armazenados fisicamente no local do escritório.
	Financeira	Afeta diretamente o orçamentário da organização em decorrência das despesas não previstas para compra de novos equipamentos e infraestrutura.

Tabela 03. Exemplo de Descritivo de Impacto.

Vale ressaltar que, para este trabalho, é desejável que a consistência das percepções de probabilidade e impacto seja sustentadas por evidências registradas, como dados históricos, documentos, relatórios e documentos constantes no SEI, por exemplo.

Realização dos Enquadramentos

Logo após a identificação e a descrição, realiza-se o enquadramento dos resultados obtidos conforme o nível de ocorrência (probabilidade) e de gravidade (impacto).

A classificação da probabilidade de cada risco é feita em: **muito baixa, baixa, média, alta e muito alta**, conforme a tabela 04.

Escala de Probabilidades

Probabilidade	Descrição da Probabilidade	Frequência	Peso
Muito baixa	**Improvável**. Evento nunca ocorreu e em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade	<= 20%	1
Baixa	**Rara**. Evento nunca ocorreu, mas de forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade	> 20% e <=40%	2
Média	**Possível**. Evento já ocorreu no passado e de alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade	>40% e <=60%	5
Alta	**Provável**. Evento já ocorreu no passado e de forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	> 60% e <= 80%	8
Muito alta	**Praticamente certa**. De forma inequívoca, o evento está ocorrendo ou já ocorreu e as circunstâncias indicam claramente que poderá ser recorrente em um curto espaço de tempo.	>80%	10

Tabela 04: Escala de Probabilidades [10]

Já para a avaliação de cada impacto, deve-se fazer o enquadramento em **muito baixo, baixo, médio, alto e muito alto**, respeitando sempre a categoria estabelecida anteriormente (tabela 05). E, em seguida, anotando o seu peso (tabela 06).

Impacto	Muito Baixo	Baixo	Médio	Alto	Muito Alto
Impacto Operacional	Atividades suspensas por poucas horas e/ou sem perda de dados.	Atividade suspensa por pelo menos um dia E/OU poucos dados perdidos com possibilidade de recuperação total.	Atividades suspensas por uma semana E/OU grande perda de dados com possibilidade de recuperação.	Atividades suspensas por um mês E/OU perda de dados com possibilidade de recuperação parcial.	Atividades suspensas por tempo indeterminado E/OU perda de dados sem recuperação.
Impacto Orçamentário	Queda na arrecadação previstas em orçamento sem impacto em despesas.	Aumento em despesas previstas em orçamento sem impacto na arrecadação.	Queda na arrecadação não previstas em orçamento sem impacto em despesas.	Aumento em despesas não previstas em orçamento sem impacto na arrecadação.	Queda na arrecadação E aumento em despesas fora da previsão orçamentária.
Impacto de Imagem	Imagem prejudicada entre servidores do próprio órgão.	Imagem prejudicada entre servidores da PMSP.	Imagem prejudicada para os servidores e/ou parte da sociedade.	Imagem prejudicada para toda a sociedade com envolvimento de mídia.	Imagem prejudicada com envolvimento da CGM.
Impacto Social	Atraso na execução de política pública sem danos sociais/ambientais.	Impossibilidade da entrega da política pública sem danos sociais/ambientais.	Dano social/ambiental com possibilidade de reversão.	Dano social/ambiental com possibilidade de reversão parcial.	Dano social/ambiental irreversível.
Impacto de Integridade	Evento não acarreta penalidades previstas no estatuto do servidor.	Evento acarreta repreensão ou suspensão de acordo com Art. 184 do estatuto do servidor.	Evento acarreta demissão/cassação de aposentadoria conforme art. 184 do estatuto do servidor.	Evento acarreta, além de alguma das penalidades previstas no estatuto do servidor, punição de acordo com a LAC.	Evento acarreta punição de acordo com estatuto do servidor, LAC e/ou processo criminal e civil.
Impacto de Conformidade	Descumprimento de políticas e processos internos de maneira reversível.	Descumprimento de políticas e processos internos de maneira irreversível.	Descumprimento de atos normativos municipais de maneira reversível.	Descumprimento de atos normativos municipais de maneira irreversível.	Descumprimento de atos normativos estaduais e federais.

Tabela 05: Classificação de Impacto por categoria [11]

Escala de Impactos (substituir pela tabela abaixo)

Impacto	Peso
Muito baixo	1
Baixo	2
Médio	5
Alto	8
Muito alto	10

Tabela 06: Classificação de Impacto por categoria [12]

[11] Fonte tabela: criação própria baseada na metodologia TCU https://portal.tcu.gov.br/data/files/21/96/61/6E/05A1F6107AD96FE6F18818A8/Referencial_basico_gestao_riscos.pdf

[12] Fonte tabela: criação própria baseada na metodologia TCU https://portal.tcu.gov.br/data/files/21/96/61/6E/05A1F6107AD96FE6F18818A8/Referencial_basico_gestao_riscos.pdf

Dessa forma, será possível entender como cada risco pode afetar os objetivos estratégicos em cada uma das áreas categorizadas, de forma a facilitar o desenvolvimento dos respectivos planos de ação direcionados a cada um dos impactos que podem gerados.

Classificação na Matriz de Risco

Por fim, realiza-se a análise das informações conjuntamente para determinar a classificação final do risco inerente em **muito baixo, baixo, médio, alto e muito alto**, utilizando-se a **Matriz de Riscos**.

Dessa maneira, é preciso dispor de dois valores: o **peso da probabilidade** de cada risco e o **peso do impacto** de cada risco. O primeiro é alcançado diretamente como resultado das classificações feitas para a probabilidade (tabela 04). Já para a obtenção do segundo, realiza-se o **cálculo da média aritmética dos pesos anotados dos impactos de cada risco**, ou seja, para cada risco, realiza-se a soma dos pesos de seus impactos e o resultado é dividido pelo número de impactos, conforme a fórmula abaixo:

$$Média\ dos\ Impactos = Impacto1 + Impacto2 + ImpactoN / N$$

A classificação final do risco inerente é obtida a partir da multiplicação do valor da probabilidade pelo valor da média do impacto, e de acordo com o enquadramento do produto nas tabelas 07 e 08.

$$Risco\ Inerente = Probabilidade \times Média\ dos\ Impactos$$

MATRIZ DO RISCO INERENTE						
IMPACTO	MUITO ALTO (10)	10 RM	20 RM	50 RA	80 RE	100 RE
	ALTO (8)	8 RB	16 RM	40 RA	64 RA	80 RE
	MÉDIO (5)	5 RB	10 RM	25 RM	40 RA	50 RA
	BAIXO (2)	2 RB	4 RB	10 RM	16 RM	20 RM
	MUITO BAIXO (1)	1 RB	2 RB	5 RB	8 RB	10 RM
		MUITO BAIXA (1)	BAIXA (2)	MÉDIA (5)	ALTA (8)	MUITO ALTA (10)
		PROBABILIDADE				

Risco Extremo

Risco Alto

Risco Médio

Risco Baixo

Tabela 07: Classificação final do risco [13]

Escala de Nível de Risco Inerente

Nível de Risco	Risco Baixo (RB)	Risco Médio (RM)	Risco Alto (RA)	Risco Extremo (RE)
Pontuação	0 a 9,99	10 a 39,99	40 a 79,99	80 a 100

Tabela 08: Classificação do risco inerente [14]

O resultado obtido será uma tabela preenchida com o exemplo abaixo:

Riscos Identificados	Probabilidade	Impacto	Nível de Risco Inerente
Risco 1	Alta-8	M. Alto-10	RE-80
Risco 2	M.Alta-10	Alto-8	RE-80
Risco 3	Alta-8	Alto-8	RA-64
Risco 4	Baixa-2	Médio-5	RM-10

Tabela 09: Exemplo de registro de riscos inerentes calculados [15]

[13] Fonte tabela: criação própria baseada na metodologia TCU

[14] Fonte tabela: criação própria baseada na metodologia TCU

[15] Fonte tabela: criação própria baseada na metodologia TCU
(https://portal.tcu.gov.br/data/files/21/96/61/6E/05A1F6107AD96FE6F18818A8/Referencial_basico_gestao_riscos.pdf)

2.2.2 Análise dos Controles Existentes

A próxima etapa é a avaliação dos controles existentes. Após a mensuração do risco inerente, deve-se identificar e avaliar os controles internos que incidam sobre os riscos detectados.

Os controles constituem-se em ações, políticas, práticas, procedimentos ou quaisquer outras medidas adotadas com o objetivo de diminuir o nível de exposição a riscos. São mecanismos de controle comumente encontrados e que podem ter aplicação no gerenciamento de riscos:

- Utilização de checklists;
- Mecanismos de atribuição de competências com limites de alçadas;
- Prescrições de capacitação e treinamento para realização de determinadas funções;
- Normas de formalização e publicação de atos;
- Implementação de manuais e padronização de procedimentos;
- Práticas que conferem rastreabilidade a serviços e produtos;
- Relatórios de acompanhamento intermediário;
- Monitoramento de indicadores de desempenho e realização de testes de conformidade;
- Práticas de revisão e aprovação de tarefas;
- Segregação e rotação de funções;
- Uso de sistemas informatizados e automatizados;
- Implementação de estruturas de proteção físicas (ambiente fechado) ou digitais (senhas individuais).

Para a realização do levantamento dos controles, a equipe encarregada pode utilizar-se dos mapeamentos prévios realizados dos processos, assim como as técnicas de entrevistas e questionários com os responsáveis pela execução das tarefas, considerando que existe a possibilidade de alguns controles (operacional, tático e estratégico), estão interligados e entrelaçados.

É costumeiro que controles gerenciais sejam consolidados a partir de dados coletados em tarefas operacionais.

Após o levantamento de controles existentes, faz-se necessária a consideração de seu funcionamento em relação aos riscos que afetam. Destaca-se que um risco pode ter mais de um controle, e os controles podem afetar mais de um risco. Convém que os seguintes aspectos dos controles sejam considerados:

· Responsável pela execução do processo e pela execução do controle (segregação de função);
· O mecanismo pelo qual os controles se destinam a modificar o risco (são preventivos ou detectivos?);
· Se os controles existentes são capazes de operar como planejado e se estão alcançando os resultados esperados;
· Identificação de deficiências no projeto dos controles ou na forma como eles são aplicados;
· Lacunas ou sobreposições nos controles;
· Se os controles funcionam independentemente ou se precisam funcionar coletivamente para serem eficazes;
· Se existem fatores, condições, vulnerabilidades ou circunstâncias que podem reduzir ou eliminar a eficácia do controle (tais como possibilidade de fraude ou outros fatores);
· Se os próprios controles introduzem riscos adicionais;
· O alinhamento do controle com os objetivos do órgão ou entidade;
· Forma de execução do controle (manual ou automatizada).

Uma outra ferramenta bastante valiosa para entendimento do funcionamento dos controles em relação aos eventos de risco é o diagrama Bow Tie, elaborado nas etapas anteriores. Nele são levantados os principais eventos de risco identificados, suas possíveis causas e consequências, os controles existentes relacionados e as atividades que suportam o funcionamento dos controles.

Após a listagem dos controles existentes e a análise de seus relacionamentos com os riscos verificados nas etapas anteriores, a equipe responsável pelo levantamento deve encaminhar as informações aos Gestores de risco para que realizem a determinação de um fator de avaliação dos controles internos para cada risco indicado na etapa de identificação dos riscos, conforme a escala abaixo:

Nível de Confiança	Descrição	Fator de Avaliação dos Controles Internos
Inexistente	Os controles são inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	1
Fraco	Os controles existentes têm abordagens ad hoc, ou seja, tendem a ser aplicados caso a caso, e a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	0,8
Mediano	Os controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	0,6
Satisfatório	Os controles implementados são sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	0,4
Forte	Os controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco.	0,2

Tabela 10: Avaliação da Maturidade (2018) [16]

Os controles podem ser considerados **inexistentes, fracos, medianos, satisfatórios e fortes**, devendo ser investigada a conveniência de sua manutenção, substituição, modificação, supressão ou institucionalização. Esta etapa pode evidenciar algumas oportunidades de aperfeiçoamento dos controles existentes, as quais deverão ser retomadas e ter sua implementação avaliada na etapa de definição de respostas aos riscos, considerando o apetite ao risco definido, recursos demandados e prioridades estabelecidas nas etapas subsequentes.

Ressalta-se que todo o processo de Gestão de Riscos deve observar os controles sob a perspectiva de custo-benefício, visando aperfeiçoar a alocação de recursos e fomentar um maior alcance do valor público gerado. Como regra geral, o custo de um controle não deve superar os benefícios gerados ou esperados.

2.2.3 Avaliação dos Riscos Residuais

Após analisar o nível de confiança dos controles existentes, é necessário determinar o nível de Risco Residual. Isto é, deve-se avaliar a influência desses controles nos riscos identificados, podendo melhorar ou agravar a sua situação no processo de gestão de riscos. A determinação é realizada por meio da

[16] Fonte Tabela: Exemplo de escala para avaliação de controles (adaptado de DANTAS et al, 2010; AVALOS, 2009, adaptado).

Fonte: TCU https://portal.tcu.gov.br/data/files/21/96/61/6E/05A1F6107AD96FE6F18818A8/Referencial_basico_gestao_riscos.pdf

multiplicação do Risco Inerente pelo Fator de Avaliação dos Controles Internos, conforme a fórmula abaixo:

Risco Residual=Risco Inerente x Fator de Avaliação dos Controles Internos

Com o valor em mãos, deve-se fazer o seu enquadramento, verificando em qual quadrante da Escala de Nível de Risco Residual (tabela 11) ele estará inserido.

Nível de Risco	Risco Baixo (RB)	Risco Médio (RM)	Risco Alto (RA)	Risco Extremo (RE)
Pontuação	0 a 9,99	10 a 39,99	40 a 79,99	80 a 100

Tabela 11: Nível de risco residual [17]

No final da atividade, a equipe envolvida obterá como produto uma tabela preenchida com todos os valores alcançados até momento, incluindo os das etapas anteriores como, por exemplo, o quadro abaixo.

Riscos Identificados	Probabilidade	Impacto	Nível de Risco Inerente	Nível de Confiança do Controle	Fator de Avaliação do Controle Interno	Nível de Risco Residual
Risco 1	Alta-8	M. Alto-10	RE-80	Inexistente	1	RE-80
Risco 2	M.Alta-10	Alto-8	RE-80	Fraco	0,8	RA-64
Risco 3	Alta-8	Alto-8	RA-64	Mediano	0,6	RM-38,4
Risco 4	Baixa-2	Médio-5	RM-10	Satisfatório	0,4	RB-4

Tabela 12: Exemplo de registro de riscos parcial com níveis de risco residual calculados [18]

Antes de prosseguir para a próxima etapa, é importante que os valores dos riscos residuais também sejam validados com os gestores dos riscos.

[18] Fonte tabelas: criação própria baseada na metodologia TCU
[18] Fonte tabelas: criação própria baseada na metodologia TCU https://portal.tcu.gov.br/data/files/21/96/61/6E/05A1F6107AD96FE6F18818A8/Referencial_basico_gestao_riscos.pdf

3. Resposta aos Riscos

A Avaliação dos Riscos Residuais, assim como todas as etapas realizadas anteriormente, visa orientar a Resposta aos Riscos, facilitando a tomada de decisões sobre quais riscos requerem tratamento, que tipo de tratamento será aplicado e a prioridade para a implementação do tratamento. A atividade envolve comparar o **Nível de Risco Residual** com os **Critérios Para Priorização e Tratamento de Risco** (tabela 13) para então determinar o **Tipo de Resposta ao Risco**, ou seja, se a sua magnitude é aceitável ou tolerável ou se é necessário algum tratamento (tabela 14).

Priorização dos Riscos Identificados e Avaliados

Na priorização dos riscos, verifica-se qual foi o nível de risco residual encontrado na etapa de Análise dos Riscos e, então, classifica-se segundo o apetite ao risco da organização. O apetite a risco é o nível de exposição a perdas que a organização vê como aceitável, dados os seus objetivos e recursos, ou seja, é a quantidade e os tipos de riscos que a organização está disposta a assumir para atingir os seus objetivos.

Ressalta-se que os gestores possuem autonomia para a definição do apetite ao risco de cada órgão ou entidade de acordo com suas atividades, mas devem estar cientes que esta decisão impacta no processo de gestão de riscos da entidade. Por exemplo, ao declarar que sua organização aceita trabalhar com riscos altos, o gestor de riscos está dizendo que não haverá a obrigatoriedade de planejamento de ações para mitigar tais riscos. Neste caso, se o evento de risco se concretizar (alta probabilidade) o problema gerado poderá causar danos irreparáveis à organização (alto impacto).

Com relação à administração pública municipal, para se evitar uma visão extremamente conservadora de aceitar apenas riscos baixos, o que poderia impedir as Pastas de exercerem as suas obrigações, e uma visão arrojada de aceitar riscos altos, o que não convém ao utilizar dinheiro público, sugere-se um apetite a risco que aceite os riscos classificados como baixos e médios e exija respostas para os riscos altos e extremos como padrão. As respostas aos riscos de cada unidade devem levar em conta o apetite ao risco previamente definido. Deste modo, a priorização dos riscos e, consequentemente, o estabelecimento de tratamento serão baseados nos critérios abaixo.

NÍVEL DE RISCO	CRITÉRIOS PARA PRIORIZAÇÃO E TRATAMENTO DE RISCOS	RESPOSTA AO RISCO
Risco Extremo Absolutamente *(Inaceitável)*	Nível de risco muito além do apetite ao risco. Qualquer risco neste nível deve ser comunicado à autoridade máxima da unidade e ao Comitê. É necessária a elaboração de planos de ação para evitar ou eliminar as causas e/ou consequências, bem como considerar a necessidade de mobilização imediata de recursos, materiais e pessoal capacitado, com vistas ao tratamento deste risco.	Evitar, eliminar reduzir, compartilhar
Risco Alto *(Inaceitável)*	Nível de risco além do apetite ao risco. Qualquer risco neste nível deve ser comunicado à autoridade máxima. É necessária a elaboração de planos de ação para evitar ou eliminar as causas e/ou consequências.	Evitar, eliminar reduzir, compartilhar
Risco Médio *(Aceitável)*	Nível de risco dentro do apetite ao risco. Geralmente nenhuma medida é necessária, porém requer atividades de monitoramento específico e atenção da gerência na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custo adicional.	Aceitar, evitar, eliminar reduzir, compartilhar
Risco Baixo *(Aceitável)*	Nível de risco dentro do apetite ao risco, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custo-benefício, como diminuir o nível de controles.	Aceitar, evitar, eliminar, reduzir, compartilhar

Tabela 13: Exemplo de priorização e tratamento de riscos em função do apetite ao risco [20]

É importante ressaltar que, mesmo para os riscos baixos e médios, deve ser feita uma avaliação caso a caso sobre a aceitação do risco. Esse cuidado deve ser tomado porque sempre existirão oportunidades de melhorias para os processos da entidade, contudo, o custo relacionado não poderá ultrapassar o benefício proporcionado.

Tipo de Resposta aos Riscos

Neste momento serão propostas as ações a serem implementadas para o tratamento de cada um dos riscos identificados e analisados. Dentre as possíveis respostas, estão as seguintes: eliminar; evitar; reduzir ou mitigar; compartilhar ou transferir; aceitar e potencializar ou explorar.

[20] Fonte tabela: criação própria baseada na metodologia TCU https://portal.tcu.gov.br/data/files/21/96/61/6E/05A1F6107AD96FE6F18818A8/Referencial_basico_gestao_riscos.pdf

Respostas ao Risco	Descrição
Evitar ou Eliminar	Um risco normalmente é evitado quando é classificado com **Alto ou Extremo**, mas a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação. Exemplo: mudança de processo ou descontinuidade do processo que causa o risco.
Reduzir ou Mitigar	Um risco é mitigado quando é classificado como **Alto ou Extremo**. A implementação de controles, neste caso, apresenta um custo/benefício adequado. Exemplo: aprovações, checklist de conferência, assinaturas etc.
Compartilhar ou Transferir	Um risco normalmente é compartilhado quando é classificado como **Alto ou Extremo**, mas a implementação de controles não apresenta um custo/benefício adequado. Exemplo: Contratação de seguros.
Aceitar	Um risco normalmente é aceito quando seu nível está nas faixas de **Baixo ou Médio**. Nesta situação, nenhum novo controle precisa ser implementado para mitigar o risco. Toda aceitação de risco, independentemente de sua classificação, deve ser documentada e aprovada pelo gestor de risco do órgão bem como pela alta administração.
Potencializar ou Explorar	Um risco pode ser potencializado quando existe no ambiente uma oportunidade a ser explorada. Trata-se de riscos positivos que terão um bom impacto no objetivo da unidade.

Tabela 14: Tipos de Tratamento do Risco [21]

Portanto, para os níveis de risco crítico e alto, a resposta deverá sempre ser evitar, reduzir ou compartilhar. Para os níveis moderado e pequeno, de maneira geral, deve-se aceitar. Entretanto, a depender da situação, a unidade poderá decidir por outra resposta que não seja essas, sempre considerando o custo-benefício da implementação ou melhoria dos controles. Para estes casos, deverá ser devidamente justificado e registrado nos documentos.

Após um risco receber como resposta a mitigação, ou seja, a redução de impacto e/ou probabilidade de materialização, espera-se que controles internos sejam incorporados nos processos administrativos impactados pelo risco. Um controle interno pode ter algumas classificações:

a. **Manual** – executado por um ou mais servidores dentro do órgão;

b. **Automático** – feito via sistema, sem intervenção humana;

c. **Preventivo** – o controle ocorre antes do risco se materializar, diminuindo, portanto, sua probabilidade de ocorrência;

d. **Detectivo** – são controles que ocorrem após a materialização do risco, sendo utilizado pela unidade para corrigir temporalmente os erros eventualmente cometidos diminuindo, portanto, a escala de impacto do risco.

[21] Fonte tabela: criação própria

Vale ressaltar que os controles internos precisam ser reproduzíveis e gerar evidências de execução. Ao elaborar uma matriz de controles internos na unidade, sugere-se que se tenha a participação do responsável por riscos e controles envolvido. E, após a sua aprovação, sugere-se que seja compartilhada com as demais instâncias responsáveis pelo seu acompanhamento.

A consolidação dos tratamentos gerados pelo processo de gerenciamento de riscos do processo organizacional juntamente com os controles internos sugeridos desse processo organizacional é o Plano de Tratamento de riscos, que deve ser validado pelo Núcleo Especializado de Gestão de Riscos e aprovado pelo Comitê de Gestão de Riscos.

A responsabilidade final pelo processo de gerenciamento de risco é da Alta Gestão da Entidade, porém são as áreas gerenciais e operacionais (1ª Linha) que irão implementar o Plano de Tratamento, por isso, é necessário definir os responsáveis (servidores ou cargos) pela implementação de cada iniciativa. Também serão responsáveis pelo monitoramento e do reporte do andamento das iniciativas

Além dos procedimentos realizados acima, deve-se atentar para as etapas de **Monitoramento e Análise Crítica**, **e de Comunicação e Consulta,** as quais devem ser realizadas durante **toda a Gestão de Risco.**

4. Monitoramento e Análise Crítica

A etapa de monitoramento e análise crítica é fundamental para a gestão de riscos. Segundo a ABNT 2018 [21], seu propósito é assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultado do processo. Como consequência, ela deve ser contínua, ocorrer em todos os estágios e envolver todas as instâncias da estrutura de Gestão de Riscos.

.

Desse modo, ela abrange desde o planejamento, coleta e análise de informações, até o registro de resultados e o fornecimento de retorno, garantindo, em cada decisão, a compreensão de todos os agentes envolvidos sobre os riscos existentes e promovendo a eficácia dos controles.

4.1 Monitoramento dos Riscos

Realizar o monitoramento de uma atividade ou de um processo significa agir no sentido de acompanhar o seu regular andamento. Isto implica checar o seu progresso por meio de uma observação sistemática e com propósitos definidos.

O Monitoramento dentro do processo de gestão de riscos visa assegurar que as etapas estão sendo realizadas, de modo correto, que o ambiente de controle se mantém efetivo ao longo do tempo, e que os riscos de nível crítico, considerados intoleráveis, recebem uma atenção mais concentrada. Dado que ambiente interno e externo das organizações se alteram com o passar do tempo, os procedimentos estabelecidos e as respostas a riscos que se mostravam válidos anteriormente podem se tornar ineficazes, as atividades de controle podem deixar de ser executadas, ou os objetivos da própria organização podem evoluir. Em face dessas alterações, a administração necessita avaliar se o funcionamento do gerenciamento de riscos permanece eficaz.

É pertinente destacar que o monitoramento não tem apenas a finalidade de verificar a execução das atividades relacionadas à gestão de risco e controles por si só, uma vez que estes fatores não são suficientes para assegurar que os objetivos dos órgãos sejam alcançados. Adicionalmente, é necessário promover o acompanhamento do engajamento das equipes, bem como garantir o respeito aos limites estabelecidos, a área de atuação de cada servidor, e a clareza das suas responsabilidades. Esses pontos são essenciais para que cada um dos participantes compreenda como o seu cargo se integra na estrutura corporativa de gestão de riscos e controles.

Com base no explicitado acima, as equipes devem desenvolver procedimentos formais de registro e acompanhamento das informações, tais como:

· Implementação de estruturas de proteção físicas (ambiente fechado) ou digitais (senhas individuais).

· Elaboração de relatórios que documentem as atividades realizadas e seus achados durante a aplicação da metodologia de gestão de riscos;

· Desenvolvimento e implementação de indicadores que evidenciem a evolução da gestão de riscos implementada e a efetividade dos controles estabelecidos;

· Inclusão dos documentos em processos no SEI;

· Remessa da documentação às instâncias responsáveis (diretor, coordenador, Núcleo Especializado de Gestão de Riscos, Comitê Interno de Governança etc.) e seguindo um fluxo predeterminado de comunicação.

4.2 Análise Crítica

Logo após a coleta de dados e informações, deve-se seguir para a próxima fase deste estágio, ou seja, realizar a análise crítica dos dados monitorados. A realização de uma análise crítica significa engajar-se em um exercício de reflexão ou estudo minucioso dos resultados obtidos, visando a identificação de aspectos positivos e negativos. Os positivos são indicadores de que o trabalho foi desenvolvido de forma adequada e os controles mantêm-se eficazes, gerando resultados no gerenciamento de riscos. Os negativos, por outro lado, sinalizam possíveis pontos de atenção e melhorias, bem como problemas a serem solucionados.

No que diz respeito aos aspectos negativos, há um que se destaca e requer acompanhamento contínuo por parte dos gestores: o risco de nível crítico. Para este, é imperativo estabelecer procedimentos de comunicação e ação imediata, além de um monitoramento mais frequente e rigoroso. Assim, quando o gestor identificar qualquer indício de perigo, deverá acionar os protocolos previamente estabelecidos e adotar as medidas cabíveis, prevenindo a materialização do risco.

Também vale ressaltar que, após implementados os controles, o gestor deverá monitorá-los continuamente, tanto no desenho quanto na operação, assegurando que o controle esteja ativo e operante. Esse acompanhamento contínuo é vital, pois visa a verificar se os controles estão menos eficazes ou obsoletos, o que os tornaria inadequados para mitigar o risco. Nesse cenário, uma nova avaliação deve ser conduzida e, se necessário, devem ser implementados novos planos de ação e controles.

Para facilitar a operacionalização da análise crítica, as equipes, seus gestores, devem estabelecer indicadores que evidenciem a evolução do processo de gestão de riscos aplicado e a efetividade dos controles implementados que, demonstrando, com uma frequência mínima trimestral, o percentual de controles efetivos por meio de autoavaliações de conformidade realizadas pela área.

5. Comunicação e Consulta

A ISO 31000:2018 ressalta a necessidade de acesso a informações confiáveis, íntegras e tempestivas para que a gestão de riscos seja adequada e eficaz na realização de seus objetivos.[22] As comunicações devem percorrer em todas as direções e ser claras. Isso facilita que sejam acessíveis, assertivas e ágeis, promovendo a disseminação de informações e direcionamentos estratégicos originários do Comitê de Gestão de Riscos e do Núcleo Especializado de Gestão de Riscos a todo o órgão ou entidade.

A comunicação interna da organização pode ser classificada como vertical e horizontal. A comunicação vertical, que ocorre de baixo para cima ou vice-versa dentro da estrutura organizacional, deve respeitar a hierarquia da organização e manter um caráter mais formal. Já a comunicação horizontal, que acontece entre as indivíduos ou equipes, precisa ser ágil e oportuna como, por exemplo, por meio de envios de e-mails. Além disso, sendo um instrumento de gestão, as informações internas obtidas e processadas durante o processo de gerenciamento de riscos devem ter caráter restrito. Apenas os relatórios finais e Planos de Gestão de Riscos elaborados serão divulgados pela alta administração.

As informações externas pertinentes aos processos de trabalho também devem ser consideradas e distribuídas de maneira apropriada. Do mesmo modo, a comunicação voltada para a sociedade deve ser alvo de monitoramento e controle, minimizando riscos de respostas não alinhadas às expectativas da população.

Para instituir um bom fluxo de comunicação eficaz, é imperativo que cada agente envolvido compreenda a sua função individual no gerenciamento de riscos, bem como as atividades pessoais que interagem com o trabalho dos outros. Visando facilitar o entendimento desta fase, introduz-se a Matriz de RACI para o processo de Gestão de Riscos da CGM.

		Dirigente da Unidade	Comitê de Gestão de Riscos	Nucleo Especializado de Gestão de Riscos	Gestor do Risco	Servidores da CGM
Atividades / Produtos	Objetivos e Metas do Planejamento Estratégico da CGM	A	R	C	I	I
	Diretrizes do trabalho do NEGR	C	R	C		
	Parecer sobre o Apetite ao risco	C	I	R	C	I
	Definição do apetite a Risco organizacional	A	R	C	I	I
	Estabelecimento do Contexto	I	C	R	C	I
	Identificação dos Riscos	A	I	C	R	C
	Análise dos Riscos	A	I	C	R	C
	Avaliação dos Riscos	A	I	C	R	C
	Priorização dos Riscos	A	C	C	R	I
	Elaborar Plano de gerenciamento de risco			C	R	
	Validar o Plano de Gerenciamento de Risco		RA	C	I	
	Executar o Tratamento dos riscos		I	C	R	R
	Estabelecer indicadores de risco		A	C	R	I
	Registrar a ocorrência de riscos			I	R	I
	Monitorar a execução do plano de Resposta			R	C	I
	Monitorar os indicadores de Risco		I	R	C	I
	Elaborar Relatórios de Riscos			A	R	I
	Submeter os Relatórios de Riscos	I	A	R	I	I
	Comunicar a existencia de Riscos Extremos Imediatamente	I	I	R	R	R

Tabela 15: Matriz RACI.

Legenda:

R: Responsável – quem executa a atividade

A: Autoridade – quem aprova a tarefa ou produto. Pode delegar a função, mas mantém a responsabilidade

C: Consultado: quem pode agregar valor ou é essencial para a implementação; e

I: Informado: quem deve ser informado de resultados ou ações tomadas, mas não precisa se envolver na decisão.

Entre os pontos citados anteriormente, é crucial enfatizar a necessidade e o caráter mandatório da notificação urgente sobre riscos de nível crítico, vistos como inaceitáveis, ao Comitê de Gestão de Riscos. Desta forma, possibilita-se que medidas rápidas e oportunas sejam implementadas, e que os riscos sejam monitorados conforme a urgência requerida.

[22] Fonte tabela RACI - Criação própria baseada em metodologia.

BIBLIOGRAFIA

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). ISSO/TR 31004:2015, Gestão de riscos: Diretrizes. Rio de Janeiro, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). NBR ISO 31000:2018, Gestão de riscos: Guia para implementação da ABNT NBR ISSO 31000. Rio de Janeiro, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). NBR IEC 31010:2021, Gestão de riscos - Técnicas para o processo de avaliação de Riscos. Rio de Janeiro, 2021.

AUDITORIA GERAL DO ESTADO. Manual do Programa de Gestão de Riscos. SEFAZ BAHIA, 2020 Disponível em: http://www.sefaz.ba.gov.br/administracao/controle_interno/OT_02_2020_manual_programa_gestao_riscos.pdf Acesso em 26/09/2022

CONTROLADORIA GERAL DO MUNICÍPIO DO RIO DE JANEIRO. Política de Gerenciamento de Riscos (PGR). CGM-Rio, 2022. Disponível em: https://www.rio.rj.gov.br/web/cgm/apresentacao Acesso em 26/09/2022

BELO HORIZONTE. Portaria CTGM N° 013 de 4 de abril de 2018. Dispõe sobre a Política de Gestão de Riscos da Controladoria-Geral do Município de Belo Horizonte e dá outras providências. Prefeitura do Município de Belo Horizonte, 2018 Disponível em: https://prefeitura.pbh.gov.br/sites/default/files/estrutura-de-governo/controladoria/2018/documentos/LEGISLA%C3%87AO%20CTGM/PORTARIA%20CTGM%20N%C2%BA%20013.2018.pdf Acesso em: 20 de set. 2022.

INSTITUTO DOS AUDITORES INTERNOS DO BRASIL (IIA Brasil). Modelo das 3 linhas do IIA 2020, IIA Brasil, 2021. Disponível em: https://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/20200758glob-th-editorHTML-00000013-20082020141130.pdf . Acesso em 15/09/2022

TRIBUNAL DE CONTAS DA UNIÃO. Referencial Básico de Gestão de Riscos TCU, 2018. Disponível em: https://portal.tcu.gov.br/referencial-basico-de-gestao-de-riscos.htm Acesso em 26/09/2022

Gestão de Riscos. Portal de Gestão de Riscos do Distrito Federal, 2022. Disponível em: http://www.gestaoderiscos.cg.df.gov.br/index.php/conceitos/ Acesso em 26/09/2022

Técnica Bow Tie: Aprenda a usar e baixe grátis Arruda Consult, 2020 .Disponível em http://www.arrudaconsult.com.br/2020/03/analise-de-risco-tecnica-bow-tie.html Acesso em 26/09/2022

ANEXO I – TERMOS E DEFINIÇÕES

Apetite ao risco: é a quantidade e os tipos de riscos que a organização está disposta a aceitar para atingir os seus objetivos;

Tolerância ao risco: é o nível de variação aceitável quanto à realização de um objetivo, podendo ser para mais ou para menos. Está relacionada à resiliência da organização;

Causa: 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. São considerados os "porquês" da ocorrência do evento;

Consequência: possíveis efeitos resultantes da ocorrência de um evento sobre os objetivos do processo de trabalho ou da organização;

Controles Internos: conjunto de regras, procedimentos, diretrizes, entre outros, operacionalizados de forma integrada pelos colaboradores, e que têm como objetivo a gestão dos riscos e o fornecimento de razoável segurança na consecução da missão da entidade;

Gestão de riscos: é o conjunto de ações direcionadas ao desenvolvimento, disseminação e implementação de metodologias de gerenciamento de riscos institucionais, objetivando apoiar a melhoria contínua de processos de trabalho, projetos e a alocação e utilização eficaz dos recursos disponíveis, contribuindo para o cumprimento dos objetivos da entidade;

Gerenciamento de riscos: processo contínuo que consiste no desenvolvimento de um conjunto de ações destinadas a identificar, analisar, avaliar, priorizar, tratar e monitorar eventos capazes de afetar, positiva ou negativamente, os objetivos, processos de trabalho e projetos da organização, nos níveis estratégico, tático e operacional;

Processos de trabalho: conjunto de atividades inter-relacionadas ou interativas que representam os métodos de execução de um trabalho necessário para alcançar um objetivo;

Nível de risco: o nível de criticidade do risco, ou seja, o quanto um risco pode afetar os objetivos, processos de trabalho e projetos da entidade, a partir de escala predefinida de criticidades possíveis;

Impacto: o grau ou importância dos efeitos da ocorrência de um risco, estabelecido a partir de uma escala pré-definida de consequências possíveis;

Probabilidade: é a chance de o risco acontecer, estabelecida a partir de uma escala predefinida de probabilidades possíveis;

Processos-chave: são os processos relevantes para a entidade relacionados a sua atividade-fim e/ou aos objetivos estratégicos definidos no Planejamento Estratégico;

Risco: a possibilidade de que um evento ocorra e afete, positiva (risco positivo) ou negativamente (risco negativo), os objetivos estratégicos da organização, por meio dos seus processos de trabalho ou projetos desenvolvidos;

Risco inerente: é o nível de risco ao qual uma organização está exposta antes de qualquer ação de mitigação ou qualquer controle preexistente ter sido levado em conta;

Risco residual: é o nível de risco ao qual uma organização está exposta mesmo depois de serem consideradas as ações de mitigação e os controles preexistentes; e

Dimensões do risco: classificação dos tipos de riscos que podem afetar o alcance dos objetivos da organização, observadas as características de sua área de atuação e as particularidades do setor.

ANEXO II – MODELO DE PLANILHA DE GESTÃO DE RISCOS

	Classificar o risco conforme abrangência. Exemplo: Auditoria Interna; Administração e Finanças; Outros.	Escolher melhor categoria para classificar o risco.	Explicar resumidamente do que se trata o risco.	Descrever a falha que pode levar à ocorrência do risco.	Descrever qual o impacto: o que pode ocorrer caso o evento risco ocorra.
Nº	PROCESSO	CATEGORIA DO RISCO	DESCRIÇÃO DO RISCO	DESCRIÇÃO DA(S) CAUSA(S)	DESCRIÇÃO DA(S) CONSEQUÊNCIAS(S)
1			Risco 1: Descrever risco.	1) falta de funcionários; 2).... 3)	1) dano à imagem da PMSP; 2)
2			Risco 2: Descrever risco.		
3			Risco 3: Descrever risco.		
4			Risco 4: Descrever risco.		
5			Risco 5: Descrever risco.		
6			Risco 6: Descrever risco.		
7			Risco 7: Descrever risco.		
8			Risco 8: Descrever risco.		
9			Risco 9: Descrever risco.		
10			Risco 10: Descrever risco.		
11			Risco 11: Descrever risco.		
12			Risco 12: Descrever risco.		
13			Risco 13: Descrever risco.		
14			Risco 14: Descrever risco.		
15			Risco 15: Descrever risco.		

Escolher o nível de impacto se o evento ocorrer. Pesos: Muito baixo (1); Baixo (2); Médio (5); Alto (8); Muito Alto (10).	Escolher a probabilidade de ocorrência do evento risco. Pesos: Muito baixa (1); Baixa (2); Média (5); Alta (8); Muito Alta (10).	Cálculo automático. Em caso de erro multiplicar Probabilidade de Ocorrência do Risco x Impacto do Risco.	Resposta automática.	Breve justificativa sobre a avaliação realizada.
IMPACTO (PESO)	**PROBABILIDADE (PESO)**	**Nível do Risco Inerente (NRI)**	**TIPO DE RISCO INERENTE**	**JUSTIFICATIVA DA AVALIAÇÃO: IMPACTO E PROBABILIDADE**
10	10	100	Risco Extremo - RE	
8	8	64	Risco Alto - RA	
5	10	50	Risco Alto - RA	
2	1	2	Risco Baixo - RB	
2	5	10	Risco Médio - RM	
8	8	64	Risco Alto - RA	
		0		
		0		
		0		
		0		
		0		
		0		
		0		
		0		

Descrever os controles existentes para que o evento risco não ocorra (deixar em branco se não existir qualquer controle).	Julgar a efetividade dos controles em relação ao risco. Inexistente (1); Fraco (0,8); Mediano (0,6); Satisfatório (0,4); Forte (0,2).	Cálculo automático.	Resposta automática.	Breve justificativa sobre a avaliação realizada.	Responder.
DESCRIÇÃO DOS CONTROLES	FATOR DE AVALIAÇÃO DOS CONTROLES INTERNOS	NÍVEL DO RISCO RESIDUAL (NRR)	TIPO DE RISCO RESIDUAL	JUSTIFICATIVA DA AVALIAÇÃO: CONTROLES INTERNOS	O RISCO SERÁ INCLUÍDO EM PLANO DE AÇÃO?
1) Manual Operacional xyz; 2) descrição...	1	100	Risco Extremo - RE		Não
	0,8	51,2	Risco Alto - RA		Sim
	0,6	30	Risco Médio - RM		Não
	0,4	0,8	Risco Baixo - RB		Não
	0,2	2	Risco Baixo - RB		Sim
	1	64	Risco Alto - RA		Sim
		0			
		0			
		0			
		0			
		0			
		0			
		0			
		0			
		0			