Conselho Administrativo de Defesa Econômica

Metodologia de Gestão de Riscos

CADE
Conselho Administrativo de Defesa Econômica

Ficha Institucional

PRESIDENTE

Alexandre Cordeiro Macedo

CONSELHEIROS

Gustavo Augusto Freitas de Lima

Victor Oliveira Fernandes

SUPERINTENDENTE-GERAL

Alexandre Barreto de Souza

PROCURADORA-CHEFE

Juliana Oliveira Domingues

ECONOMISTA-CHEFE

Lílian Santos Marques Severino

DIRETOR DE ADMINISTRAÇÃO E PLANEJAMENTO

Ricardo Lovatto Balttes

Ficha Técnica

COORDENAÇÃO

Beatriz Leal dos Reis

REDAÇÃO E REVISÃO

Adriana da Silva Pereira

Ana Gabriela de Carvalho Costa

Beatriz Leal dos Reis

Cristina Pinheiro Castilho Portela

COLABORADORES

Paulo Eduardo Silva de Oliveira

Equipe da Auditoria Interna do Cade

Equipe da SG/CGAA10

SUMÁRIO

Apresentação

Prever e controlar eventos que podem ou não vir a ocorrer não é uma tarefa fácil. No entanto, cada vez mais as organizações se deparam com fatores internos e externos que tornam incerto o alcance de seus objetivos e, por isso, precisam estar preparadas para enfrentar os possíveis efeitos dessas ocorrências.

A probabilidade de ocorrência e o impacto de eventos imprevistos, bem como a pronta condição de resposta, contudo, podem ser eficientemente trabalhadas com a adequada aplicação de uma metodologia de gestão de riscos.

A gestão de riscos no Cade tem por objetivo permitir aos gestores lidar de modo eficaz com a incerteza e os riscos e as oportunidades a ela associados, reforçando a capacidade da autarquia de criar valor público, além de oferecer uma sinalização à sociedade do fortalecimento do compromisso e zelo com a coisa pública, a partir de uma gestão preventiva que se antecipa, no possível, aos eventos incertos.

É importante ressaltar que a gestão de riscos é um elemento essencial para a boa governança, pois contribui para reduzir as incertezas que envolvem a definição da estratégia e o alcance dos objetivos institucionais.

Por isso, este Comitê de Governança, Riscos e Controles (Corisc) aprovou, do Despacho Decisório nº 4/2023/DICOR/DAP/CADE, a Metodologia de Gestão de Riscos do Cade.

A Metodologia aprovada tem por objetivo orientar as unidades do Cade a implementar a gestão de riscos em conformidade com a Política instituída pela Portaria Cade nº 97, de 24 de março de 2022. Contudo, para que a gestão de riscos seja exitosa é preciso que ela faça parte da cultura desta autarquia, o que depende do envolvimento de todos.

Assim, convidamos os gestores, servidores e colaboradores do Cade a utilizar amplamente esta ferramenta e a incorporar a visão da gestão de riscos aos seus processos de trabalho.

Comitê de Governança, Riscos e Controles

CAPÍTULO I

- Planejamento Estratégico
- Cadeia de Valor
- Estrutura de Governança

1. Introdução

Este guia tem como objetivo apresentar a metodologia e os procedimentos a serem adotados, por todas as unidades do Cade, na gestão de riscos associados aos diversos processos de trabalho, bem como conceitos e referências amplamente utilizados para tratar do tema.

A gestão de riscos é a forma pela qual as instituições buscam sistematicamente identificar antecipadamente possíveis eventos que poderiam impactar seus objetivos, seja de forma positiva ou negativa.

Portanto, gerenciar riscos deve ser intrínseco ao planejamento estratégico e incorporado aos processos contínuos e estruturados.

Em 2021 o Cade iniciou um novo ciclo de planejamento estratégico para o quadriênio 2021-2024. Nesse novo ciclo, a visão de futuro foi reformulada a fim de refletir os efeitos de um ambiente concorrencial saudável na competitividade nacional. Assim, o Cade tem como visão "**Ser agente indutor do aumento da competitividade no Brasil"**.

O Mapa Estratégico é uma representação gráfica da estratégia adotada pelo Cade por meio da alocação de objetivos estratégicos nas perspectivas: fundamentos, habilitadores e resultados à sociedade.

Figura 1 - Mapa Estratégico do Cade

Fonte: RG 2022

O Planejamento Estratégico do Cade, para o ciclo 2021-2024, procura traduzir a visão organizacional em Objetivos Estratégicos relacionados em uma lógica de causa e efeito que abrange desde as entregas finais para a sociedade até os aspectos internos da organização, desenvolvidos para viabilizar a execução da estratégia.

A partir da Missão e da Visão de Futuro do Cade foram estabelecidos os resultados à sociedade, que são oriundos dos processos de trabalho finalísticos. Definidos os resultados, foi possível identificar o que seria necessário para alcançá-los. Isso é feito por meio dos objetivos habilitadores, ou seja, o que habilita o Cade a entregar os resultados esperados. Por último, para construir as bases para cumprir a Missão e entregar os resultados à sociedade, foram definidos os fundamentos deste novo Plano Estratégico.

Todos esses elementos podem ser facilmente visualizados na figura que representa o Mapa Estratégico do Cade 2024: Por um Brasil mais competitivo.

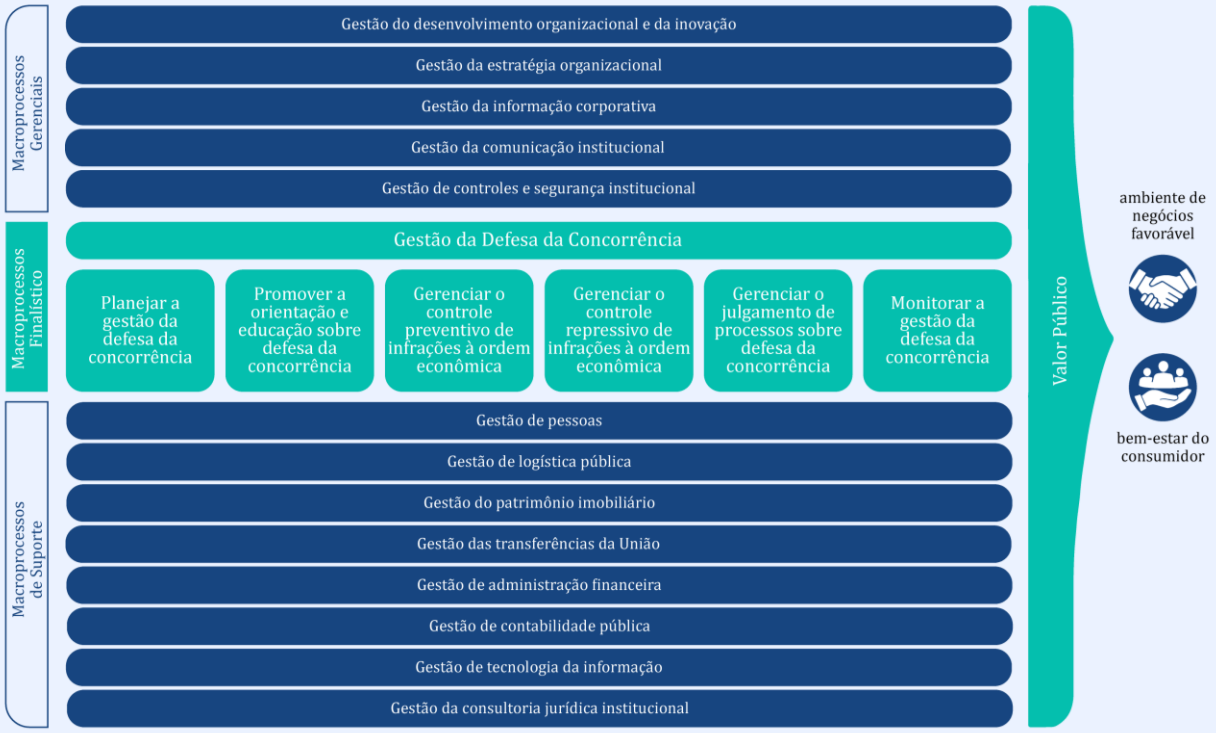
Adicionalmente, o Plano Estratégico do Cade está alinhado com a Estratégia Nacional de Desenvolvimento Econômico e Social (Endes 2020-2031), em seu eixo econômico, com vistas a ampliar a competitividade do Brasil de forma a se aproximar das economias desenvolvidas e aumentar a produtividade da economia brasileira

A gestão de riscos também se associa à Endes 2020-2031, pois objetiva mitigar possíveis eventos que possam afetar o alcance das estratégias setoriais relativas à ampliação da competitividade do Brasil.

Outro instrumento importante que todos devem tomar conhecimento é a Cadeia de Valor do Cade. Trata-se também de uma representação gráfica que busca demonstrar o que a autarquia faz para gerar valor público à sociedade. Se o Mapa Estratégico é desdobrado em iniciativas e projetos estratégicos, a Cadeia de Valor se desdobra em macroprocessos e processos, que estão agrupados em finalísticos, gerenciais e de suporte. Eles se integram e se complementam de maneira que a instituição possa ser vista por uma forma integrada.

A atual Cadeia de Valor do Cade aponta para dois principais ganhos para a sociedade: o bem-estar do consumidor e o ambiente de negócios favorável ao investimento.

Figura 2 - Cadeia de Valor



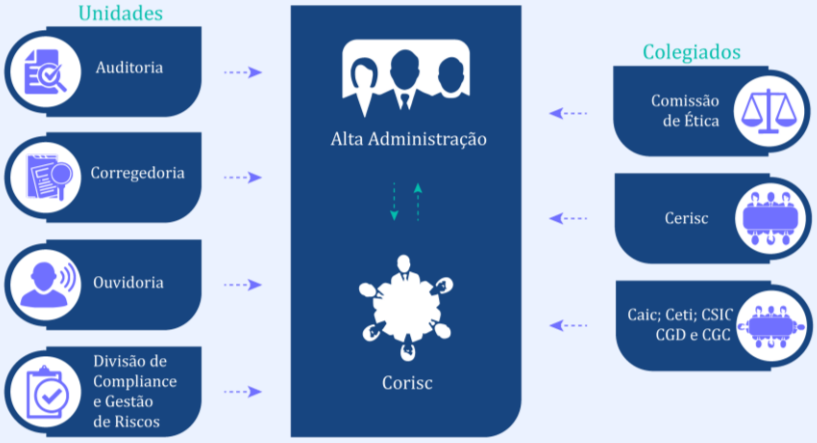
Fonte: RG 2022

A representação da Cadeia de Valor permite uma visão lógica dos processos organizacionais. O mapeamento dos processos, processos de trabalho e atividades é essencial para que a aplicação da metodologia de gestão de riscos tenha maior efetividade.

Nesse contexto, a gestão de riscos, além de estar associada ao planejamento estratégico e aos processos de trabalho, integra a governança, pois se aplicada de forma sistemática, estruturada e oportuna, fornece informações que dão suporte à tomada de decisão e contribui para a otimização do desempenho organizacional.

A estrutura de governança do Cade foi revista em 2021 com o objetivo de aprimorar a condução de temas estratégicos e o processo decisório da autarquia.

Figura 3 - Estrutura de Governança do Cade



Fonte: RG 2022

No centro da figura, estão a alta administração e o Corisc. A alta administração é a responsável por implementar e manter mecanismos e práticas de governança e o Corisc auxilia a alta administração na implementação e na manutenção de processos, estruturas e mecanismos adequados à incorporação dos princípios e das diretrizes da governança. Há, ainda, as instâncias internas de apoio que prestam suporte à implementação da política de governança no Cade e possuem a atribuição de zelar pelas boas práticas de governança, gestão de riscos e integridade. Observe na figura que tanto as unidades como os colegiados ali listados compõem as instâncias de apoio à governança.

A governança define o norte a ser seguido pela instituição, reforça a importância da gestão de riscos e estabelece as responsabilidades de cada instância.

Por fim, esta Metodologia foi elaborada com o propósito de orientar a identificação, a avaliação e a adoção de respostas aos eventos de risco que tenham potencial de impactar o alcance dos objetivos estratégicos do Cade, além de tratar do monitoramento e dos mecanismos de comunicação.

Neste documento serão apresentados os principais conceitos, as referências, as técnicas e algumas exemplificações para a gestão de riscos, lembrando que se trata de um processo contínuo de melhoria e aprendizagem, sempre buscando a adequação às normas vigentes e as melhores práticas de gestão.

CAPÍTULO II

- Legislação Aplicável
- Normativos Internos
- Referencial Teórico

2. Referenciais Normativos

No âmbito da Administração Pública federal existe um conjunto de normas e regulamentações que dispõem e orientam a aplicação da gestão de riscos nas organizações públicas.

Além disso, existem outras iniciativas amplamente reconhecidas e que têm sido base para a implementação da gestão de riscos em grande parte das organizações em todo o mundo.

Neste tópico serão apresentados, de forma sucinta, os principais atos normativos e o referencial teórico que conduzem a gestão de riscos no Poder Executivo federal.

2.1 Legislação Aplicável

Instrução Normativa Conjunta nº 1, de 10 de maio de 2016

Expedida pelo Ministério do Planejamento, Desenvolvimento e Gestão (MP) e pela Controladoria-Geral da União (CGU), a Instrução Normativa Conjunta nº 1, de 2016 dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal.

Decreto nº 9.203, de 22 de novembro de 2017

Este Decreto estabelece a política de governança da Administração Pública direta, indireta, autárquica e fundacional e, em seu art. 17, estão elencadas as atribuições da alta administração para a gestão de riscos:

> A alta administração das organizações da Administração Pública federal direta, autárquica e fundacional 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, observados os seguintes princípios:
>
> I - implementação e aplicação de forma sistemática, estruturada, oportuna e documentada, subordinada ao interesse público;
>
> II - integração da gestão de riscos ao processo de planejamento estratégico e aos seus desdobramentos, às atividades, aos processos de trabalho e aos projetos em todos os níveis da organização, relevantes para a execução da estratégia e o alcance dos objetivos institucionais;

> III - estabelecimento de controles internos proporcionais aos riscos, de maneira a considerar suas causas, fontes, consequências e impactos, observada a relação custo benefício; e
>
> IV - utilização dos resultados da gestão de riscos para apoio à melhoria contínua do desempenho e dos processos de gerenciamento de risco, controle e governança.

2.2 Normativos Internos de Gestão de Riscos

Portaria Cade nº 499, de 23 de novembro de 2021

A partir da edição do Decreto nº 10.139, de 28 de novembro de 2019, que dispõe sobre a revisão e a consolidação dos atos normativos inferiores a decreto, os normativos do Cade passaram por uma revisão, o que resultou na atualização da política de governança, gestão de riscos e integridade no âmbito da autarquia.

Assim, foi publicada a Portaria Cade nº 499, de 2021, que dispõe sobre a estrutura de governança da autarquia, sua composição e competências. Nas disposições finais, a Portaria remete à necessidade de edição de normas complementares para a regulamentação da gestão de riscos, controles internos e integridade.

Portaria Cade nº 97, de 24 de março de 2022

Em decorrência da edição da Portaria Cade nº 499, de 2021, foi publicada a Portaria Cade nº 97, de 2022, que dispõe sobre a Política de Gestão de Riscos no âmbito da autarquia.

A Portaria Cade nº 97, de 2022, é o atual referencial normativo da gestão de riscos no Cade e estabelece princípios, diretrizes e responsabilidades mínimas a serem observados para a gestão de riscos, bem como a necessidade de operacionalização por meio de uma metodologia específica.

A seguir estão transcritos os princípios, diretrizes e objetivos constantes da Portaria Cade nº 97, de 2022, que foram utilizados como norte na elaboração deste documento.

> Art. 3º Constituem-se princípios da Gestão de Riscos no Cade:
>
> I - a integração ao processo de planejamento estratégico;
>
> II - a aplicação de forma contínua e integrada aos processos de trabalho e aos projetos, em todos os níveis da organização;

III - a implementação e a aplicação de forma sistemática, estruturada, oportuna e documentada, subordinada ao interesse público;

IV - a direção, o apoio, a supervisão e o monitoramento pela alta administração; e o engajamento de todo o corpo funcional;

V - o subsídio à tomada de decisão e ao aperfeiçoamento do planejamento estratégico;

VI -a utilização dos resultados da gestão de riscos para a melhoria contínua do desempenho e dos processos, controles e governança;

VII - a aderência à integridade e aos valores éticos; e

VIII - a consideração dos fatores humanos e culturais.

Art. 4º São diretrizes da Gestão de Riscos no Cade:

I - promover a cultura de gestão de riscos em todas as unidades e em todos os níveis da autarquia;

II - promover a contínua capacitação do corpo funcional em gestão de riscos e em outras competências técnicas correlatas;

III - acompanhar e avaliar o contexto interno e externo;

IV - fixar parâmetros e definir instrumentos de medição de desempenho da gestão de riscos;

V - definir responsabilidades e competências dos agentes envolvidos no processo de gerenciamento de riscos; e

VI - promover a avaliação da maturidade da gestão de riscos periodicamente.

Art. 5º São objetivos da Gestão de Riscos no Cade:

I - auxiliar a tomada de decisão com vistas a prover razoável segurança no cumprimento da missão e no alcance dos objetivos institucionais;

II - identificar e avaliar os riscos e definir respostas, dentre elas os controles a serem implementados; e

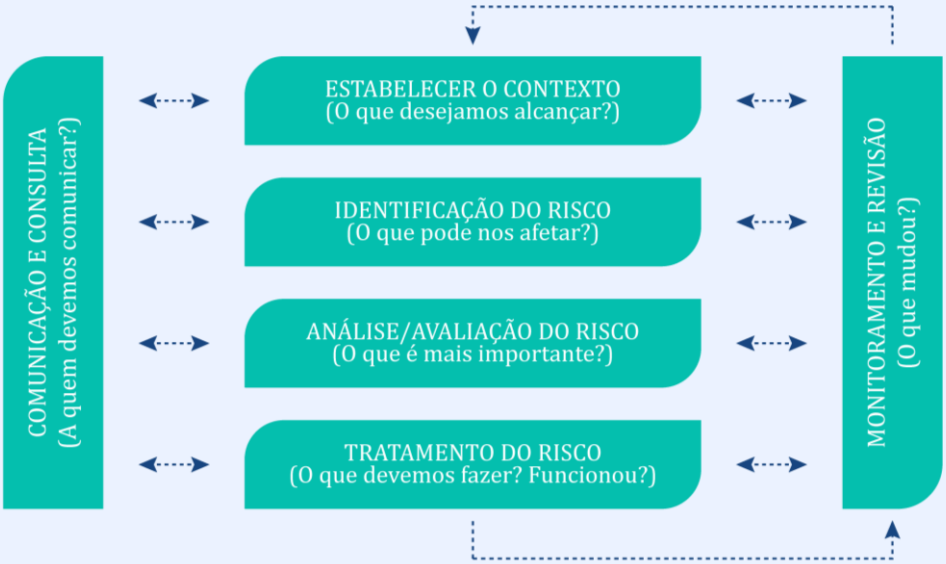
III - utilizar a gestão de riscos para aprimorar os controles internos da gestão e a alocação de recursos.

Nesse contexto, pode-se observar que a evolução da gestão de riscos no Cade buscou o alinhamento com a legislação vigente e outros conteúdos amplamente reconhecidos sobre o tema.

2.2 Referencial Teórico

As metodologias de gestão de riscos possuem diversas similaridades entre si pelo fato de identificarem e tratarem as incertezas de forma sistemática para que haja uma comunicação precisa ao longo do processo de avaliação de riscos. De modo geral ao longo da execução da gestão de riscos existe um conjunto de questões encadeadas nas quais uma pergunta leva naturalmente à próxima, formando um processo genérico de gestão de riscos. Estas questões, retratadas na Figura 4, estão presentes durante a execução das etapas contidas nas principais metodologias.

Figura 4 - Processo genérico de gestão de riscos



Fonte: Hillson (2017, p. 9), com adaptações

A seguir são abordadas as referências em gestão de riscos utilizadas para o desenvolvimento da Metodologia do Cade.

2.2.1 COSO ERM

Um dos principais modelos internacionais de referência em gestão de riscos aplicável às organizações públicas é o do COSO - *Committee of Sponsoring Organizations of the Treadway Commission*. O material publicado tem por objetivo ajudar empresas e outras organizações a avaliar e aperfeiçoar seus sistemas de controle interno.

De acordo com o COSO ERM, com base na missão ou visão definida, a administração estabelece os principais planos e a estratégia e determina o alinhamento dos objetivos nos níveis da organização.

Dessa forma, foi concebido um cubo que relaciona dimensões de objetivos, de unidades de negócio e as oito etapas da condução da gestão de riscos.

Na dimensão dos objetivos, a estrutura de gerenciamento de riscos é orientada a fim de alcançar os objetivos da organização e são classificados em quatro componentes:

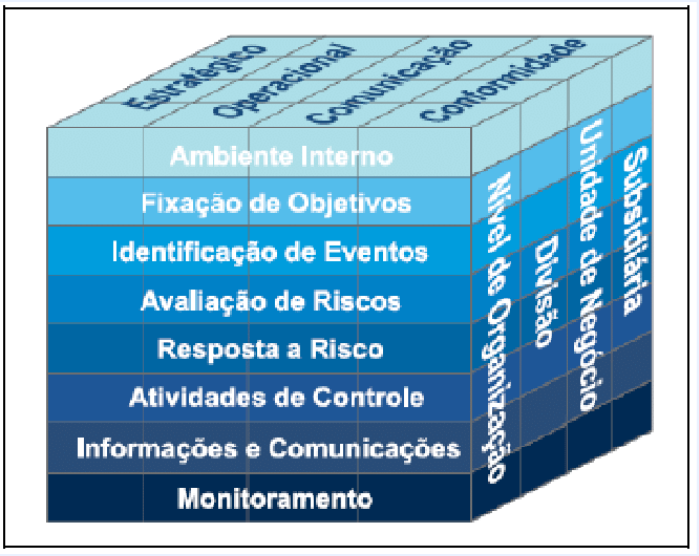
- Estratégico: objetivos e metas alinhados à missão da entidade;
- Operacional: utilização eficaz e eficiente dos recursos;
- Comunicação: confiabilidade dos relatórios;
- Conformidade: cumprimento das leis e regulamentos aplicáveis.

O modelo avançou na inclusão de objetivos estratégicos, pois de nada adiantaria ter operações eficientes, relatórios confiáveis e regulamentos sendo cumpridos, se a organização não sabe onde quer chegar.

Em relação às etapas para a condução da gestão de risco, foram definidos oito componentes: Ambiente Interno; Fixação de Objetivos; Identificação de Eventos; Avaliação de Riscos; Resposta aos Riscos; Atividades de Controle; Informação e Comunicação e Monitoramento.

A figura abaixo ficou conhecida como o Cubo COSO ERM, indicando a relação entre a dimensão dos objetivos da instituição, a dimensão dos níveis da organização e os oito componentes dessa estrutura:

Figura 5 - Metodologia de Gestão de Riscos do ERM-COSO – ERM-CUBE



Fonte: ERM-COSO (2004, p. 7)

Resumidamente, o ambiente interno está relacionado ao núcleo de qualquer organização, o pessoal. Aqui estão os atributos individuais, como integridade, valores éticos e competência, e o ambiente no qual operam. Todos os níveis da organização devem ter objetivos fixados e comunicados alinhados à missão e compatíveis ao apetite a riscos. Já os eventos são situações que ainda não ocorreram, mas que podem causar impacto no alcance dos objetivos e por isso precisam ser identificados.

A avaliação de riscos, sob a perspectiva de probabilidade e impacto, serve como subsídio para o desenvolvimento de estratégias de resposta aos riscos. A resposta ao risco pode ser evitar, aceitar, compartilhar ou reduzir e vai depender do apetite a risco da organização. As atividades de controle são expressas em políticas e procedimentos estabelecidos para assegurar que as ações necessárias para gerenciar o risco estão sendo implementadas.

O componente informação e comunicação permite a coleta e troca de informações necessárias para conduzir, gerenciar e controlar as operações.

Por último, o monitoramento tem o objetivo de avaliar a qualidade da gestão de riscos e controle internos ao longo do tempo, verificando seu funcionamento e se é possível realizar modificações para seu aprimoramento.

Na parte superior do cubo estão os quatro objetivos: estratégico; comunicação; operacional; e conformidade. E na dimensão lateral está a ideia de que a gestão de riscos perpassa todas as unidades da organização.

Em resumo, a dimensão superior do cubo representa os objetivos que são objeto da gestão de riscos, a dimensão lateral os níveis da organização pelos quais perpassa a gestão de riscos e a dimensão frontal são os oitos componentes abordados sinteticamente acima.

A metodologia possui ainda uma seção definindo papéis e responsabilidades quanto à gestão de riscos, já que está presente em toda organização.

2.2.2 COSO 2017

A nova versão, COSO ERM – *Integrating with Strategy and Performance*, também denominado como *Framework*, destaca a importância de considerar os riscos tanto no processo de estabelecimento da estratégia quanto na melhoria do desempenho operacional.

> O gerenciamento de riscos corporativos não é uma função ou departamento. É a cultura, os recursos e as práticas que as organizações integram com a estratégia definida e executada, com o objetivo de gerenciar o risco na criação, preservação e valorização. (COSO, 2017)

O modelo revisado reduziu de oito para cinco os componentes do gerenciamento de riscos e adotou princípios associados aos componentes. Assim, são 20 princípios organizados em cinco componentes inter-relacionados:

A figura a seguir ilustra o novo modelo de gestão de riscos corporativos, COSO 2017:

Figura 6 - Modelo de Gestão de Riscos Corporativos

Fonte: COSO *Enterprise Risk Management – Integrating with Strategy and Performance* (COSO, 2017) – tradução livre.

Legenda:

a) **Governança e Cultura**: a governança estabelece o tom da organização, intensifica a importância e define responsabilidades de supervisão sobre a gestão de riscos. A cultura consiste em valores éticos, comportamentos esperados e entendimento do risco em todos os níveis da organização. Princípios relacionados: i) exercer a supervisão de riscos pelo Conselho; ii) estabelecer estruturas operacionais; iii) definir a cultura desejada; iv) demonstrar comprometimento aos valores fundamentais; e v) atrair, desenvolver e reter pessoas capacitadas;

b) **Estratégia e Definição de Objetivos**: a gestão de riscos corporativos está integrada ao plano estratégico da organização por meio do processo de definição da estratégia e dos objetivos de negócio. O apetite a risco é definido e alinhado com a estratégia. Os objetivos de negócios colocam em prática a estratégia, além de constituírem alicerce para a identificação, avaliação e resposta aos riscos. Princípios relacionados: i) analisar o contexto dos negócios; ii) definir o apetite a riscos; iii) avaliar estratégias alternativas; e iv) formular objetivos de negócio;

c) **Desempenho**: é necessário identificar e avaliar os riscos que podem afetar a execução da estratégia e dos objetivos de negócios. Os riscos devem ser priorizados de acordo com o grau de severidade e do apetite a risco. A organização seleciona as respostas aos riscos e obtém uma visão consolidada do portfólio e do montante de riscos assumidos. Princípios relacionados: i) identificar riscos; ii) avaliar a severidade dos riscos; iii) priorizar riscos; iv) implementar respostas aos riscos; e iv) desenvolver visão de portfólio;

d) **Revisão**: a análise do desempenho permite refletir sobre o funcionamento dos componentes do gerenciamento de riscos corporativos, dentro do contexto de mudanças, além de possibilitar os ajustes necessários. Princípios relacionados: i) avaliar mudanças relevantes; ii) revisar riscos e desempenhos; e iii) perseguir melhorias na gestão de riscos;

e) **Informação, Comunicação e Reporte**: é um processo contínuo de obtenção e compartilhamento de informações. A informação provém de fontes internas e externas, potencializadas por sistemas de tecnologia da informação e utilizadas para apoiar a gestão de riscos. Princípios relacionados: i) alavancar informações e tecnologia; ii) comunicar informações sobre riscos; e iii) reportar sobre riscos, cultura e desempenho.

Interessado no COSO 2017?
Clique no link para acessar:

2017-COSO-ERM-*Integrating-with-Strategy-and-Performance-Executive-Summary*

2.2.3 ISO 31000

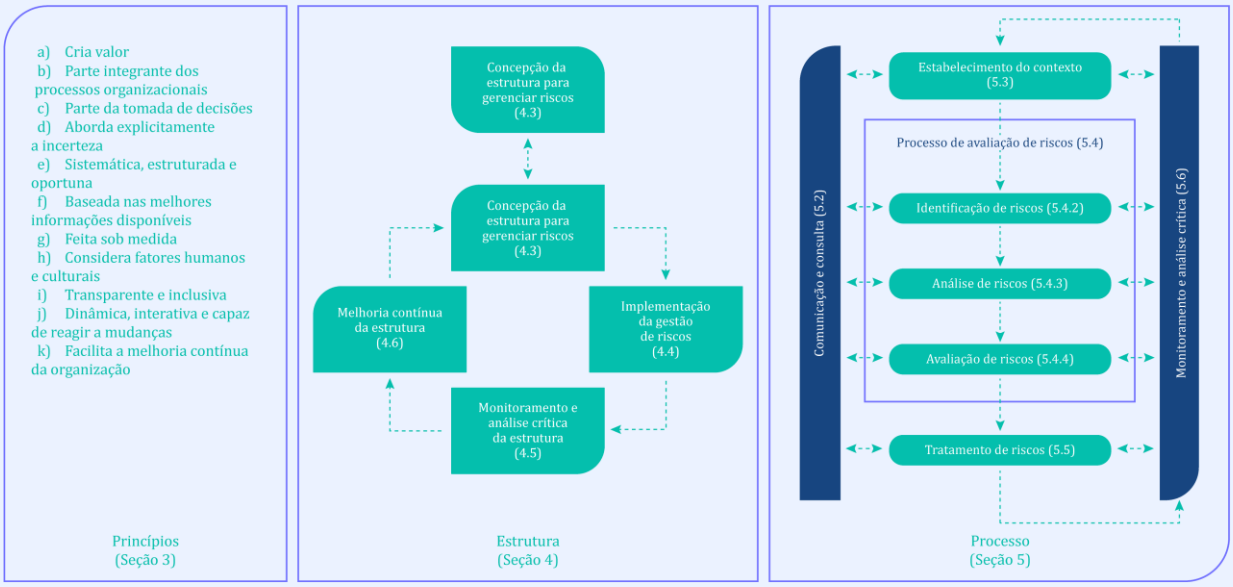
A ABNT NBR ISO 31000 foi elaborada pela Comissão de Estudo Especial de Gestão de Riscos (CEE- 63) com o objetivo de disseminar princípios e diretrizes para gestão de riscos, aplicáveis a organizações de qualquer setor.

Em complemento foi publicada a ISO Guia 73, que buscou definir conceitos sobre gestão de riscos e padronizar terminologias. Em 2009, foi publicada a ISSO/IEC 31010 – Gestão de Riscos – Técnicas de Avaliação de Riscos, norma de apoio à ISO 31000, que fornece orientação detalhada sobre a seleção e aplicação de técnicas de identificação e avaliação de riscos.

A definição de risco da ISO 31000 é bastante simples: “risco é o efeito da incerteza nos objetivos, é um desvio em relação ao esperado, podendo ser positivo ou negativo”. Aqui uma diferença em relação a outras normas que consideram o risco como algo negativo, chamando de oportunidade o evento positivo.

A norma está dividida em três componentes: definição de princípios, estrutura e processo.

Figura 7 - Metodologia de Gestão de Riscos da ISO 31000



Fonte: ABNT NBR ISO 31000 (2009, p. vii)

De acordo com a norma, para a gestão de riscos ser eficaz deve atender aos seguintes princípios:

I - a gestão de riscos cria e protege valor: contribui para a realização dos objetivos e melhoria do desempenho organizacional;

II - é parte integrante de todos os processos organizacionais: não pode ser vista como responsabilidade de uma pessoa ou departamento;

III – é parte da tomada de decisão: esse é um dos objetivos da gestão de riscos, auxiliar o gestor de qualquer nível a tomar as melhores decisões;

IV – aborda explicitamente a incerteza: leva em consideração a incerteza e como ela pode ser tratada;

V - é sistemática, estruturada e oportuna: contribui para a eficiência e para os resultados consistentes, comparáveis e confiáveis;

VI - baseia-se nas melhores informações disponíveis: fontes de informação, tais como dados históricos, experiências, retroalimentação das partes interessadas, observações, previsões, e opiniões de especialistas;

VII - é feita sob medida: está alinhada com o contexto interno e externo da organização e com o perfil do risco. O modelo de gestão de riscos deve ser construído de acordo com a estrutura e a complexidade de cada organização;

VIII - considera fatores humanos e culturais: reconhece as capacidades, percepções e intenções do pessoal interno e externo que podem facilitar ou dificultar a realização dos objetivos da organização;

> IX - é transparente e inclusiva: envolve as partes interessadas e os tomadores de decisão;
>
> X - é dinâmica, iterativa e capaz de reagir a mudanças: percebe e reage às mudanças e aos eventos externos e internos; e
>
> XI - facilita a melhoria contínua da organização: as organizações desenvolvem e implementam estratégias para melhorar a sua maturidade na gestão de riscos juntamente com os demais aspectos da organização.

Por fim, segundo a ISO 31000, convém que o processo de gestão de riscos seja parte integrante da gestão, incorporado na cultura e nas práticas e adaptado aos processos de negócios da organização.

2.2.4 Três linhas de defesa

O modelo das três linhas de defesa surgiu para atender diversas questões relacionadas à governança, à gestão de riscos e ao controle, definindo responsabilidades entre os diversos órgãos de controle interno e possibilitando a interação desses órgãos para melhor gestão dos riscos em uma organização.

É uma forma simples e eficaz de melhorar a comunicação do gerenciamento de riscos e controle por meio do esclarecimento dos papéis e responsabilidades essenciais.

Na primeira linha estão as funções que gerenciam os riscos e têm a propriedade sobre eles. Essa linha é responsável por implementar ações corretivas para resolver deficiências em processos de trabalho e controles. Em uma organização pública, essa primeira linha é aquela realizada por cada agente público no exercício de suas atividades. A gerência operacional é responsável por manter controles internos eficazes e por conduzir procedimentos de risco e controle diariamente.

Na segunda linha estão as funções que apoiam a implementação e monitoram a gestão de riscos, sendo representada pela unidade responsável e pelos comitês temáticos da instituição. Tem a atribuição de facilitar a implementação de práticas eficazes de gestão de riscos e auxiliar os proprietários dos riscos a identificar e reportar adequadamente informações relacionadas ao risco.

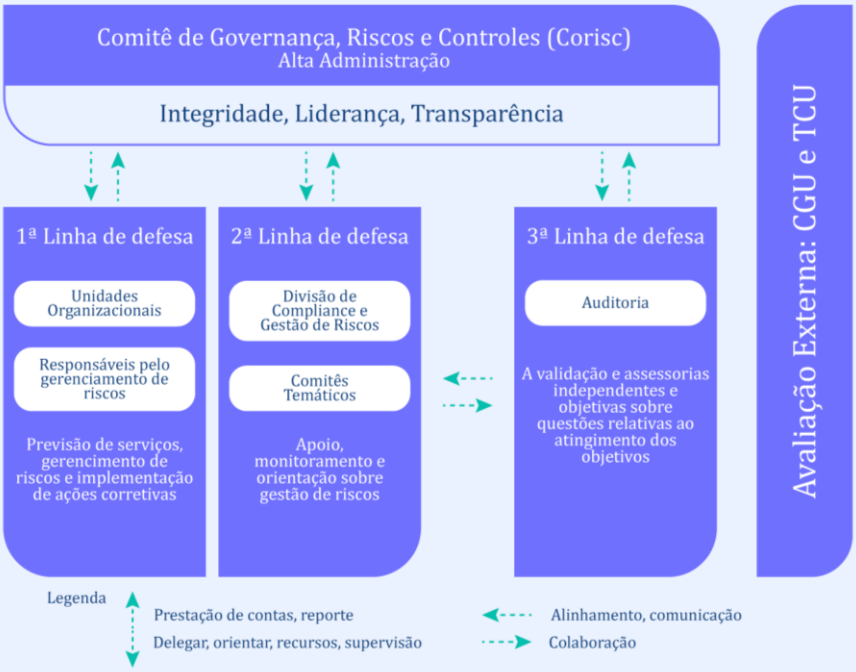
Na terceira linha está a Auditoria Interna, que realiza avaliações objetivas e independentes quanto à adequação e à eficácia da governança e da gestão de riscos (incluindo controles internos) para apoiar o alcance dos objetivos organizacionais, bem como para promover e facilitar a melhoria contínua dos processos de trabalho. Presta serviços de avaliação e consultoria com base nos pressupostos de autonomia técnica e objetividade, a fim de contribuir para o aprimoramento da atuação da organização.

O órgão máximo de governança e a alta administração são as principais partes interessadas atendidas pelas linhas e estão em melhor posição para ajudar a garantir que o modelo seja aplicado aos processos de gestão de riscos e controle da organização.

Cada uma das três linhas desempenha um papel distinto dentro da estrutura mais ampla de governança da organização.

O Cade adota o modelo de três linhas, como pode ser observado na imagem abaixo:

Figura 8 - Três Linhas de Defesa



Fonte: elaboração própria, com base no modelo do IIA 2020.

Para conhecer mais sobre o modelo das três linhas de defesa, acesse o documento:

Modelo das Três Linhas do IIA 2020

CAPÍTULO III

Metodologia de Gestão de Riscos do Cade

3 A Gestão de Riscos no Cade

Para implantar a gestão de riscos em uma organização, primeiro é preciso conhecer seus principais componentes, isto é, a estrutura que fornece os fundamentos e os arranjos institucionais que permitem a execução de uma gestão de riscos eficiente.

No Cade os riscos são geridos de forma integrada, conforme determinado pela Portaria Cade nº 97, de 2022, que dispõe sobre a Política de Gestão de Riscos, definindo instâncias e responsabilidades, bem como a necessidade de uma metodologia e de instrumentos, tanto para a implementação quanto para o acompanhamento da gestão de riscos.

3.1 Instâncias de Gestão de Riscos

As instâncias de gestão de riscos instituídas pela Portaria Cade nº 97, de 2022 são:

- Comitê de Governança, Riscos e Controles (Corisc): é o órgão colegiado de decisão máxima na estrutura de governança do Cade, ao qual compete aprovar a política, a metodologia e os mecanismos para a implantação e o monitoramento da gestão de riscos e controles internos, bem como acompanhar a evolução da gestão de riscos no Cade, especialmente dos riscos de maior relevância e que possam vir a afetar as estratégias setoriais e organizacionais;
- Comitê Executivo de Gestão de Riscos (Cerisc): responsável por apoiar o Corisc na gestão de riscos, incluindo a análise de políticas, diretrizes, definição de limites de exposição e metodologia, além de monitorar os riscos que podem comprometer o alcance dos objetivos, bem como apoiar as unidades na gestão de riscos no Cade;
- Divisão de *Compliance* e Gestão de Riscos (Dicor): é a unidade competente para propor a Metodologia de Gestão de Riscos e apoiar a implementação e o monitoramento da gestão de riscos, podendo i) promover outras ações relacionadas à implementação e à execução da gestão de riscos, em conjunto com as demais unidades do Cade; e ii) solicitar diretamente às unidades organizacionais do Cade documentos e informações necessários à execução de suas atividades. A Dicor poderá

ainda orientar os gestores de risco na aplicação da metodologia, bem como avaliar o adequado preenchimento do Mapa de Gestão de Riscos; e

- Gestores de Riscos: cada risco mapeado e avaliado deve estar associado a um gestor de riscos formalmente identificado. São responsabilidades do gestor de riscos: i) assegurar que o risco seja gerenciado de acordo com a política de gestão de riscos do Cade, conforme o Plano de Gestão de Riscos da própria unidade; ii) monitorar o risco ao longo do tempo, de modo a garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados, de acordo com a política de gestão de riscos; e iii) garantir que as informações adequadas sobre o risco estejam disponíveis em todos os níveis da autarquia. O gestor de risco também é responsável por comunicar a identificação de novos riscos associados ao processo e até mesmo a extinção de riscos anteriormente identificados, seguindo o fluxo de comunicação disposto no item 3.2.7.

Portanto, a gestão de riscos não pode ser considerada atribuição apenas de uma unidade ou cargo específico. Ela deve ser aplicada por todos os servidores e colaboradores do Cade nos processos de trabalho e na execução de suas atividades diárias.

3.2 Metodologia de Gestão de Riscos do Cade

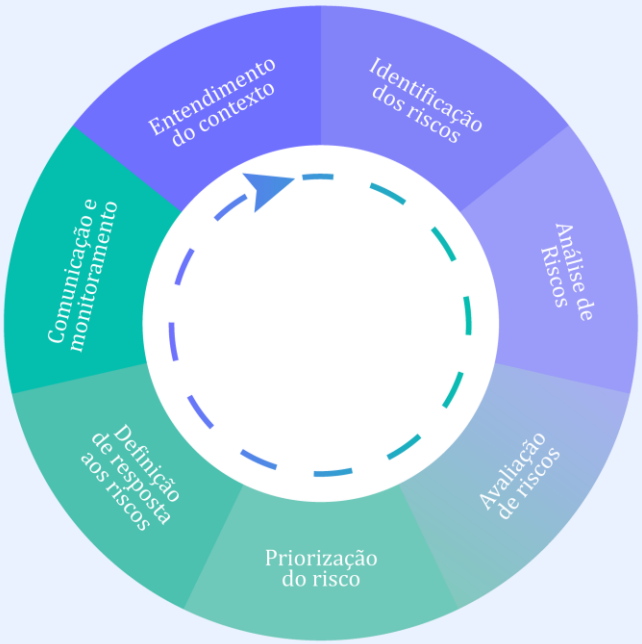
É necessário que sejam executadas algumas atividades antes de se iniciar as etapas da gestão de riscos. O mapeamento de processos contribui para que a informação seja disseminada de forma clara e que os participantes saibam o que fazer, quando fazer, como fazer, e qual é o resultado esperado para determinado processo. Contudo, como nem sempre todos os processos estão mapeados pode-se pensar minimamente em quais entregas estão sendo realizadas por uma unidade, o que é necessário para que ocorra essa entrega e quais requisitos as entregas precisam oferecer. Pode-se usar a técnica Sipoc (*Supplyer, Input, Process, Output, Customer* – Fornecedor, Entrada, Processo, Resultado ou Saída, Cliente) para se ter um melhor entendimento destes processos.

Na prática, a técnica Sipoc começa pela identificação dos “fornecedores” ou os responsáveis por darem início a uma demanda, podendo ser internos ou externos. Em seguida, verifica-se quais são as “entradas” que geram uma demanda, isto é, recursos ou informações que dão início ao processo. Já os “processos” são as principais ações a serem colocadas em prática e as “saídas” são os produtos do processo, as entregas. Por fim, os “clientes” são aqueles beneficiados com a realização do processo. Assim, mesmo sem um mapeamento completo, é possível documentar um processo do começo ao fim.

A Metodologia de Gestão de Riscos do Cade foi dividida em sete etapas, sendo que algumas delas poderão ser realizadas concomitantemente.

Trata-se de um ciclo contínuo que se retroalimenta:

Figura 9 - Etapas da Metodologia



3.2.1 Entendimento do Contexto

O entendimento do contexto tem a finalidade de colher informações para apoiar a identificação de eventos de risco e envolve conhecer os principais fatores do ambiente interno e externo que podem impactar o alcance dos objetivos institucionais.

- Ambiente interno: envolve aspectos como governança, estrutura organizacional, funções, alçadas e responsabilidades, políticas, estratégias, capacidades, competência, sistemas de informação, processos decisórios, cultura organizacional, etc.
- Ambiente externo: inclui aspectos como social, político, legal, regulatório, financeiro, tecnológico, econômico, ambiental, relações com partes interessadas externas, etc.

Inicialmente, é preciso conhecer o processo que se está trabalhando. Caso o processo ainda não tenha sido mapeado, elabore uma descrição resumida, buscando identificar minimamente os seguintes elementos:

Tabela 1 - Orientativa

Processo:	Nome do Processo Organizacional
Unidade Organizacional:	unidade que é a principal responsável pela execução do processo.
Unidade(s) Interveniente(s):	outra(s) unidade(s) que participa(m), em algum momento, do processo.
Objetivo Estratégico:	objetivo estratégico associado ao processo.
Objetivo do Processo:	o que se pretende alcançar com esse processo, podendo se dar na perspectiva estratégica, temporal, relacional, financeira, orçamentária, metas, entre outras.
Sistema Tecnológico:	existe algum sistema informatizado que apoia o processo?
Partes Interessadas:	quais atores estão envolvidos no processo (tanto interno quanto externo)?
Informações do Ambiente Interno:	pontos fortes e fracos na avaliação do ambiente interno (realizado em conjunto com a equipe).
Informações do Ambiente Externo:	oportunidades e ameaças na avaliação do ambiente externo (realizado em conjunto com a equipe).

Um ponto importante é a identificação do objetivo do processo, pois irá facilitar a identificação dos riscos. Deve-se considerar também, além do objetivo do processo, os estabelecidos no planejamento estratégico organizacional e os objetivos setoriais. Para isso, responda a seguinte questão: “O que deve ser atingido nas diversas dimensões para se concluir que o processo ocorreu com sucesso?” (CGU, 2018).

Os objetivos estratégicos definidos no planejamento do Cade orientam o trabalho e estabelecem uma base para os objetivos operacionais, visando a criação de valor público.

A gestão de riscos não dita os objetivos que a administração deve escolher, mas proporciona um processo que alinha os objetivos estratégicos com a missão da organização e com os demais objetivos correlatos, como os setoriais e operacionais.

Como executar na prática a primeira etapa da metodologia?

1. O principal responsável pelo processo levanta as informações básicas.
2. A equipe que executa o processo se reúne para discutir o fluxo e as atividades que compõem o processo. Aqui também é possível convidar representantes das unidades intervenientes que participam em algum momento do processo.
3. A equipe irá trazer novas informações e validar as já levantadas pelo responsável principal.
4. É importante levantar o maior número possível de informações sobre o ambiente interno e externo.
5. Podem ser realizadas tantas reuniões quanto necessárias até o contexto estar claramente construído.

Técnicas que podem ser empregadas nesta etapa

Brainstorming ou “tempestade de ideias”

É uma técnica de coleta de dados. A técnica se baseia em princípios como foco em quantidade, ausência de críticas e combinação de ideias. Principais etapas para uma sessão produtiva dessa técnica:

i. Para a reunião de *brainstorming* é preciso escolher um facilitador da atividade. O papel dele é garantir que o ambiente seja confortável e que não haja espaço para ridicularização ou julgamento. O facilitador também deve ficar responsável por anotar todas as ideias sugeridas;

ii. Explicar o objetivo: é importante que o coordenador/facilitador informe o objetivo da reunião. Dessa forma, ninguém perde o foco conforme as ideias surgirem;

iii. Não criticar ou julgar as ideias dos outros. Esta é uma oportunidade para opinar sobre o processo que está tendo seus riscos levantados e, portanto, não deve haver censura, pois isto acaba inibindo a participação e prejudicando a identificação dos riscos existentes;

iv. Focar na quantidade: quanto mais ideias, melhor. O objetivo do *brainstorming* é coletar o máximo de ideias possível e anotá-las para depois analisá-las e escolher as melhores;

v. Aprimorar as ideias: é comum que durante a atividade, uma pessoa fale uma ideia e outra pessoa a complemente. Portanto, não se deve haver constrangimento para combinar ideias e melhorá-las; e

vi. Controlar o tempo: determine um limite de tempo para a sessão. Se poucas ideias surgirem durante esse período, deixe que os participantes pensem individualmente em mais ideias após a atividade coletiva.

Análise SWOT

Técnica utilizada para a identificação dos pontos fortes e fracos, bem como para a análise e o registro das possíveis oportunidades e ameaças. Esta técnica é utilizada para fazer análise de cenário sobre o ambiente interno e externo, contribuindo para a identificação dos riscos e para a escolha das respostas aos riscos.

A imagem abaixo sintetiza a aplicação da análise SWOT:

Figura 10 - Análise SWOT

i. Forças: são as vantagens que a organização possui, o que ela tem de mais forte. Pense em como o serviço é prestado à sociedade, na qualidade técnica, nos recursos humanos, tecnológicos etc. São exemplos de pontos fortes: existência de servidores capacitados para execução das atividades, processo estruturado e eficiente, normativos internos claros e objetivos, emprego de tecnologias e sistemas adequados, controles internos efetivos etc.;

ii. Fraquezas: são pontos que podem prejudicar e/ou interferir negativamente no andamento da organização. Pense no oposto das Forças citadas anteriormente;

iii. Oportunidades: são as forças externas que impactam positivamente a organização. Não se pode controlá-las, elas podem surgir a qualquer momento e o ideal é estar preparado. São exemplos de oportunidades: criação de parcerias com outros órgãos e entidades, realização de eventos para aperfeiçoar a relação com o público externo, atos normativos que

favoreçam a realização das atividades, disponibilidade de recursos financeiros e orçamentários etc.; e

iv. Ameaças: são forças externas que influenciam negativamente ou possíveis eventos que prejudicariam o andamento do processo. Exemplos: crise econômica, mudanças drásticas no ambiente externo com impacto negativo, aumento de judicializações relacionadas ao processo, influência política externa que prejudique a execução das atividades, normas regulamentadoras que causem impactos negativos nas atividades etc.

Entrevistas

A utilização de entrevistas é uma importante ferramenta para auxiliar a obtenção de conhecimento de indivíduos sobre eventos passados e potenciais. Além de servidores do Cade, podem ser entrevistados especialistas da área em que se busca fazer o levantamento de riscos. Com a diversidade de experiência e especialidade de cada um consegue-se atingir um maior número de apontamentos no processo de identificação de riscos.

Atenção:

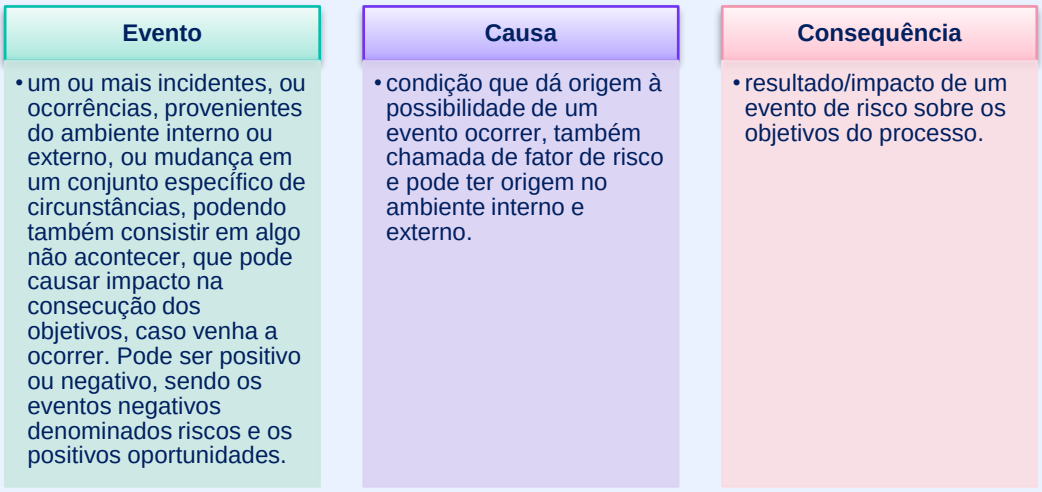
Como fonte de informação adicional, deve-se verificar também a existência de algum acórdão ou recomendação dos órgãos de controle (TCU e CGU) e da Auditoria Interna, análises ou estudos da OCDE, bem como processos judiciais, denúncias ou reclamações na Ouvidoria relacionados ao processo sob análise.

Estabelecido o contexto, torna-se mais fácil a identificação dos riscos na próxima etapa.

3.2.2 Identificação de Riscos

Esta etapa tem por finalidade identificar e registrar tanto os eventos de risco como as causas e as consequências de cada um deles. É importante ressaltar que um evento de risco pode ter, e geralmente tem, mais de uma causa e consequência.

Figura 11 - Identificação e Registro



Faz-se necessário considerar tanto a possibilidade de ocorrência de riscos quanto de oportunidades, pois uma boa gestão de riscos possibilita identificar oportunidades de melhoria (inclusive a redução e a otimização de controles já existentes), bem como minimizar os impactos de um possível risco pela existência conjunta de uma oportunidade.

Por isso, além dos eventos com potencial negativo deve-se levar em conta aqueles que representam oportunidades a serem aproveitadas e que podem, inclusive, vir a se tornar uma forma de resposta a um risco identificado. Portanto, o gestor precisa estar preparado para aproveitar as oportunidades que surgirem.

Assim, considerando o resultado da etapa de Entendimento do Contexto e a partir da experiência da equipe deve-se construir uma lista abrangente de eventos que podem evitar, atrasar, prejudicar ou impedir o cumprimento dos objetivos.

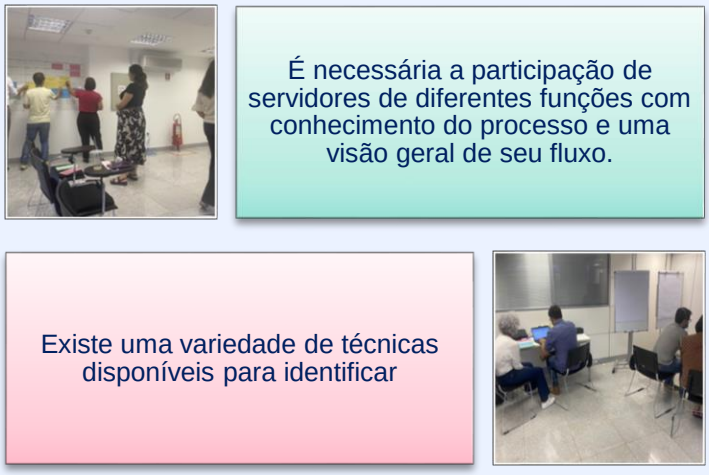
E como podemos identificar os eventos de riscos?

Para facilitar a identificação dos eventos de risco devem ser utilizadas as informações coletadas na etapa anterior.

Além disso, devem ser identificadas as ações ou sistemas que atuam como controle preventivos (que reduzem a probabilidade de ocorrência da causa e do evento de risco), assim como os controles corretivos (ações que reduzem ou eliminam as consequências previstas caso o evento de risco ocorra).

Antes de começar é preciso saber que:

Figura 12 - Idenficação de Eventos de Riscos



Fotos: 1ª Oficina Metodologia de Gestão de Riscos - Cade

Bow tie ou gravata-borboleta

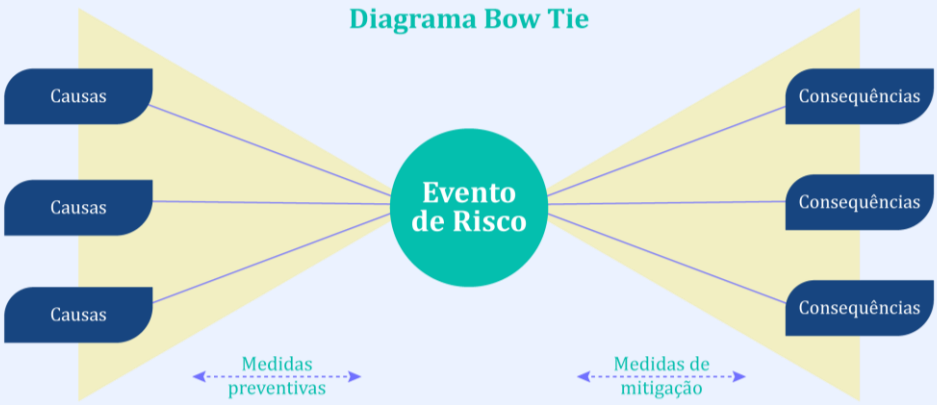
Nesta metodologia iremos apresentar a técnica *bow tie* ou gravata-borboleta, mas ela não é de aplicação obrigatória, podendo ser substituída por outra técnica.

A técnica *bow tie* consiste em identificar e analisar os possíveis caminhos de um evento de risco, dado que um problema pode estar relacionado a diversas causas e produzir diferentes consequências. Neste momento pode ser que as causas identificadas ainda não contem com controles preventivos e, da mesma forma, para cada consequência podem ou não existir controles corretivos ou medidas mitigadoras.

A figura abaixo representa a relação entre as causas, os controles preventivos, o risco, os controles corretivos e as consequências.

Figura 13 - Relação Causa, Evento e Consequência

Figura 14 - *Bow tie*



Fonte: Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão, do Ministério do Planejamento e Gestão, p. 28, 2017 (com adaptações)

No desenho acima, é possível visualizar que determinada CAUSA poderá levar à ocorrência de um EVENTO DE RISCO, o que poderá gerar uma CONSEQUÊNCIA (o que pode acontecer se tal evento se concretizar), impactando os objetivos. As medidas preventivas e de mitigação correspondem aos controles ou barreiras, que são elementos utilizados para reduzir a chance de que o evento ocorra ou mitigar as consequências, se ocorrer.

Como aplicar a técnica *bow tie*?

1. Primeiro, a partir das informações levantadas na etapa anterior, devem ser identificados os riscos associados à atividade em análise (riscos já conhecidos, riscos novos e outros que tenham potencial de afetar o processo e os objetivos propostos), utilizando a técnica *brainstorming*, por exemplo.

Ao descrever o evento de risco observe que:

Risco não é apenas o não alcance do objetivo. A descrição do risco deve proporcionar informações sobre o que pode dar errado, o fato que pode prejudicar o alcance do objetivo.

2. Os riscos podem ser identificados a partir de perguntas simples, como: Quais eventos podem EVITAR/ATRASAR/PREJUDICAR/IMPEDIR o alcance de um ou mais objetivos do processo organizacional? As respostas comporão uma lista que deverá ser analisada e consolidada. Aqui, é importante não confundir o evento de risco, o fato que prejudica o processo, com suas causas ou consequências.
3. Escolha um risco específico para análise. Ele ficará no centro, representando o nó central de uma *bow tie*.
4. Em seguida, liste as causas do evento de risco que vão dar origem ao nó central, isto é, o que poderia levar a ocorrência de um evento. As causas, também chamadas de fatores de risco, podem ter origem no ambiente interno e/ou externo. Geralmente, a falta de recursos (humanos, materiais, tecnológicos, financeiros) não é um risco, mas sim a possível causa. Por exemplo, o risco de não cumprir os prazos/metas de um processo pode ter como causa a falta/alta rotatividade de servidores.
5. Entre cada causa e o evento de risco são traçadas linhas, formando o lado esquerdo da *bow tie*. Podem existir controles/ações (medidas preventivas) que reduzem a possibilidade de determinada causa levar a uma consequência indesejada. Os controles são mostrados como barras verticais cruzando a linha.

6. No lado direito da *bow tie*, a possível ocorrência do evento de risco gera consequências ou efeitos potenciais que podem impactar o alcance dos objetivos. Aqui também são traçadas linhas para irradiar as consequências até o evento de risco. Deve-se pensar nas consequências como aquilo que ocorreria com o processo caso o risco se concretize. Por exemplo, o não cumprimento dos prazos legais de análise de atos de concentração geraria prejuízo ao processo e à imagem do Cade.
7. Para reduzir os impactos das consequências podem existir barreiras/ações (medidas de mitigação), representadas por barras verticais que cruzam as linhas.
8. Cada evento de risco deve ser examinado, ou seja, existe uma barreira (medida preventiva ou medida de mitigação) que evita, impede, controla ou limita este evento?

Atenção!

Só devem ser registradas na *bow tie* as medidas preventivas e as de mitigação que já existem no processo. Não devem ser listadas as medidas ainda não implantadas, as quais serão consideradas na etapa de definição de respostas aos riscos.

Por fim, o risco deve ser enquadrado em uma categoria de riscos. Como a categorização de riscos não encontra consenso na literatura, listamos neste documento as mais comumente utilizadas:

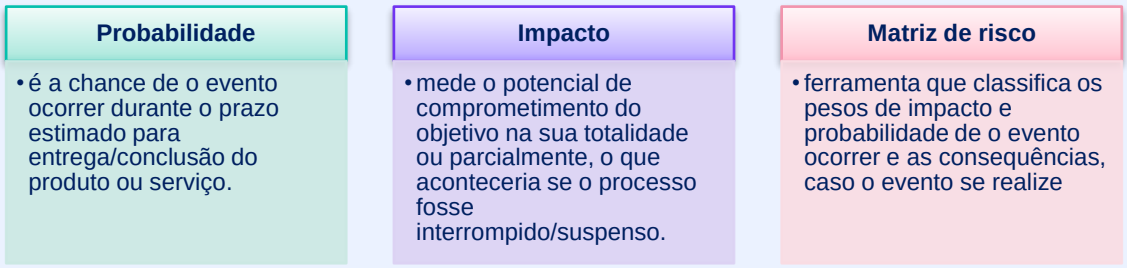
- Regulatório: leis ou regulamentos externos que podem impactar a organização no alcance dos objetivos, bem como os procedimentos internos de trabalho.
- Estratégico: eventos que possam impactar na missão, nas metas ou nos objetivos estratégicos da autarquia, caso venham ocorrer.
- Operacional: podem comprometer as atividades da unidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas, afetando o esforço da gestão quanto à eficácia e eficiência dos processos organizacionais.

- ❖ Orçamentário/Financeiro: eventos que podem comprometer a capacidade de contar com os recursos orçamentários necessários à realização das atividades ou possam comprometer a própria execução orçamentária.
- ❖ Imagem/Reputação: eventos que podem comprometer a confiança da sociedade em relação à capacidade do Cade em cumprir sua missão institucional, interferem diretamente na imagem da autarquia.
- ❖ Integridade: podem afetar a probidade da gestão de recursos públicos e as atividades da organização, causados pela falta de honestidade e desvios éticos.
- ❖ Conformidade: eventos que podem afetar o cumprimento de leis, normas e demais regulamentos aplicáveis. Seria o não cumprimento de uma disposição normativa.

3.2.3 Análise de Riscos

Nesta etapa, são calculados os níveis dos riscos identificados pela equipe técnica a partir de critérios de probabilidade e impacto. Para isso, iremos utilizar uma matriz de probabilidade x impacto, usualmente chamada de Matriz de Risco.

Figura 15 - Impacto, Probabilidade e Matriz de Risco



Antes de seguir para a forma como a matriz de riscos é elaborada, é preciso tomar conhecimento de dois conceitos muito importantes:

a) Risco inerente: é o risco que a organização irá enfrentar na falta de medidas preventivas, ou seja, o risco quando não há nenhum controle aplicado.

b) Risco residual: é o risco que remanesce depois de considerado o efeito das ações mitigadoras, incluindo os controles existentes.

No entanto, cabe apontar que não é consenso na literatura sobre a necessidade de utilização do risco inerente na análise, em razão da maior dificuldade em se medir o impacto e a probabilidade em uma situação de total ausência de controles. Por isso, é comum encontrar metodologias de gestão de risco que utilizam apenas o risco residual na análise, ou seja, aquele que permanece mesmo contando com controles, por ser mais próximo da realidade de quem está lidando com o processo.

Nesta metodologia, iremos analisar o impacto e a probabilidade de ocorrência de um evento de risco considerando o histórico do processo e sua situação atual, ou seja, com os controles existentes e implantados até então.

Como elaborar uma Matriz de Risco?

A matriz define o nível de riscos a partir da combinação de probabilidade e de impacto, utilizando escalas numéricas, como apresentado a seguir:

Escala de probabilidade (1 a 5):

1 – muito baixa: um risco que acontece apenas em situações excepcionais. Não há indícios que sinalizem sua ocorrência.

2 - baixa: aponta para baixa frequência de ocorrência no prazo associado ao objetivo.

3 - média: acontece com frequência razoável ou há indícios que possa ocorrer durante o prazo de execução do processo.

4 - alta: há muitos indícios que ocorrerá no prazo de execução do processo.

5 – muito alta: ocorrência praticamente garantida de ocorrência do evento.

Escalas de impacto (1 a 5):

1 – muito baixo: a ocorrência compromete minimamente, não altera o alcance do objetivo.

2 - baixo: pouco relevante, não impede o alcance da maior parte do objetivo.

3 - médio: compromete razoavelmente o alcance do objetivo.

4 - alto: compromete fortemente o atingimento do objetivo.

5 - muito alto: compromete totalmente ou quase o atingimento do objetivo.

Simplificando:

Tabela 2 – Escala de Probabilidade

Probabilidade	Descrição da probabilidade	Frequência	Peso
Muito alta	**Praticamente certa**. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	> = 90%	5
Alta	**Provável**. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	>= 75%<= 90%	4
Média	**Possível.** De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade	>= 40% <75%	3
Baixa	**Rara.** De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	>= 10% <40%	2
Muito baixa	**Improvável.** Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade	< 10%	1

Fonte: Elaboração própria com base na Metodologia de Riscos 2021 da CGU - Disponível em: **https://repositorio.cgu.gov.br/bitstream/1/65535/6/Metodologia_de_riscos_2_0.pdf**.

Tabela 3 - Escala de Impacto

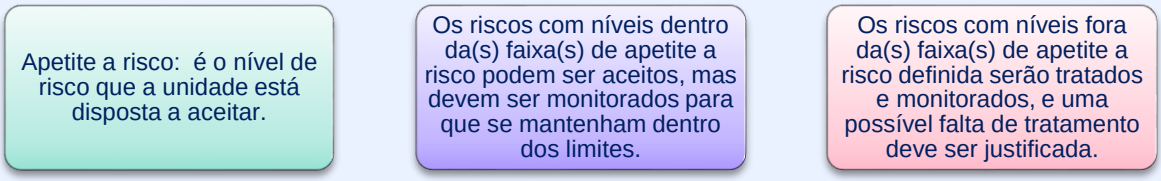
Impacto	Descrição do impacto nos objetivos, caso o evento ocorra	Peso
Muito alto	**Catastrófico** impacto nos objetivos do processo, de forma irreversível.	**5**
Alto	**Significativo** impacto nos objetivos do processo, de difícil reversão.	**4**
Médio	**Moderado** impacto nos objetivos do processo, porém recuperável.	**3**
Baixo	**Pequeno** impacto nos objetivos do processo.	**2**
Muito Baixo	**Mínimo** impacto nos objetivos do processo	**1**

Fonte: Elaboração própria com base na Metodologia de Riscos 2021 da CGU - Disponível em: **https://repositorio.cgu.gov.br/bitstream/1/65535/6/Metodologia_de_riscos_2_0.pdf**.

Os níveis de risco são o resultado da combinação entre os dois pesos (da probabilidade e do impacto). Assim, multiplicando o peso do impacto com o peso da probabilidade encontramos o nível de risco para cada evento identificado.

Mas, primeiro, é preciso conhecer o apetite a risco da organização.

Figura 16 - Apetite a Risco



O nível de risco representa o apetite a risco da organização, conforme abaixo:

Tabela 4 - Apetite de Risco

Nível	Faixa	Definição
Risco Crítico (RC)	20 – 25	Acima do apetite a risco e requer um plano de ação imediato. Não se admite postergar o tratamento.
Risco Alto (RA)	12 – 19,99	Acima do apetite a risco. Requer um plano de ação para um período determinado.
Risco Médio (RM)	5 – 11,99	Dentro do apetite a risco. Não é necessária medida especial, porém requer monitoramento e atenção para a manutenção dos controles.
Risco Baixo (RB)	0 – 4,99	Dentro do apetite a risco. Não é preciso adotar novas medidas para tratamento do risco.

Fonte: Elaboração própria com base na Metodologia de Riscos 2021 da CGU - Disponível em: **https://repositorio.cgu.gov.br/bitstream/1/65535/6/Metodologia_de_riscos_2_0.pdf**.

Importante: Cabe ao Corisc a definição do apetite a risco do Cade. Nesta Metodologia propomos a faixa superior de 12 pontos como acima do apetite à risco, mas essa pontuação pode ser revista, a partir de uma deliberação do Corisc.

Tabela 5 - Matriz de Risco

IMPACTO	5	Risco Médio (5)	Risco Médio (10)	Risco Alto (15)	Risco Crítico (20)	Risco Crítico (25)
	4	Risco Baixo (4)	Risco Médio (8)	Risco Alto (12)	Risco Alto (16)	Risco Crítico (20)
	3	Risco Baixo (3)	Risco Médio (6)	Risco Médio (9)	Risco Alto (12)	Risco Alto (15)
	2	Risco Baixo (2)	Risco Baixo (4)	Risco Médio (6)	Risco Médio (8)	Risco Médio (10)
	1	Risco Baixo (1)	Risco Baixo (2)	Risco Baixo (3)	Risco Baixo (4)	Risco Médio (5)
		1	2	3	4	5
		PROBABILIDADE				

Fonte: Elaboração própria com base na Metodologia de Riscos 2021 da CGU - Disponível em: **https://repositorio.cgu.gov.br/bitstream/1/65535/6/Metodologia_de_riscos_2_0.pdf**

Ao final desta etapa, por meio da matriz de riscos, é possível ter uma visão geral dos níveis de risco dos eventos identificados.

3.2.4 Avaliação de Riscos

Após os riscos identificados e analisados, eles precisam ser avaliados. A avaliação de riscos consiste em comparar os resultados da análise com os níveis de riscos para determinar se o risco da ocorrência do evento é aceitável.

Portanto, a unidade irá definir seu plano de ação para as possíveis respostas, de acordo com os níveis de riscos identificados:

- Riscos acima do limite de exposição: risco alto e crítico – exigem uma atuação imediata ou em um prazo determinado. Não admite postergação;
- Riscos com necessidade de monitoramento: risco médio – acompanhar e avaliar a necessidade de novos controles ou ações; e
- Riscos que podem ser aceitos: risco baixo – poderão ser aceitos sem novas medidas a serem tomadas (os controles existentes já são suficientes e efetivos).

A finalidade da avaliação é subsidiar a tomada de decisão e o estabelecimento de prioridade na implementação das medidas de tratamento dos riscos.

O que devo fazer para avaliar os riscos da unidade?

Primeiro, considerando que o limite de exposição aceitável vai até o nível médio, podemos seguir os seguintes passos:

1. Identificar, na matriz de riscos, os níveis que estão acima do limite de exposição a risco (crítico e alto).
2. Identificar os riscos que estão no nível médio para monitoramento.
3. Os riscos que se encontram no nível baixo, poderão ser aceitos, pois não são relevantes ou já existem controles suficientes.

Nesta etapa deve-se avaliar também a existência de controles internos ou ações que respondam aos riscos identificados. Os controles são expressos em forma de políticas, regras, procedimentos, entre outros, operacionalizados de forma integrada, destinados a enfrentar os riscos e fornecer segurança razoável de que os objetivos organizacionais serão alcançados.

Ainda que existam controles formalmente definidos, é necessário avaliar sua efetividade, isto é, se estão sendo aplicados adequadamente e se são suficientes.

A tabela abaixo apresenta uma síntese de como analisar os controles existentes:

Tabela 6 – Classificação dos Controles

Classificação	Descrição
Controles preventivos	Controles existentes e que atuam sobre as possíveis causas do risco, com o objetivo de prevenir a sua ocorrência. Exemplos de controles preventivos: requisitos / checklist definidos para o processo e capacitação dos servidores envolvidos no processo.
Controles de atenuação e recuperação	Controles existentes executados após a ocorrência do risco com o intuito de diminuir o impacto de suas consequências. Exemplos de controles de atenuação e recuperação: plano de contingência; tomada de contas especiais; procedimento apuratório.
Controles detectivos	Controles existentes que atuam na detecção da materialização de um risco ou de sua iminência. Exemplos de controles de detecção: indicadores; termômetros; sensores.

Fonte: Elaboração própria com base na Metodologia de Riscos 2021 da CGU - Disponível em: **https://repositorio.cgu.gov.br/bitstream/1/65535/6/Metodologia_de_riscos_2_0.pdf**

A avaliação de riscos é um processo dinâmico, pois os riscos são constantemente influenciados pelo ambiente interno e externo, indo desde a rotatividade da equipe que executa o processo até a alteração na legislação vigente.

Portanto, a avaliação dos riscos irá fornecer subsídios para a tomada de decisão, cabendo ao gestor, diante da lista de riscos ordenados por nível de risco, decidir/priorizar quais merecerão ações mitigadoras.

3.2.5 Priorização de Riscos

Com base na avaliação, serão definidos quais riscos terão prioridade na implementação das medidas de tratamento ou definição de respostas aos riscos.

E como fazer essa priorização?

1. Primeiro, a unidade deverá verificar quais riscos foram classificados nos níveis alto e crítico (cores amarelo e vermelho na matriz). Estes riscos serão priorizados.
2. Para cada risco nesses níveis deverão ser implementadas ou aperfeiçoadas medidas de tratamento ou respostas e sua não implantação deverá ser justificada.
3. Os riscos que estão nos níveis baixo e médio geralmente não requerem uma medida especial, porém devem ser monitorados para averiguar se os controles existentes são suficientes para manter o risco nesse nível ou possam ser reduzidos sem custos adicionais.

A priorização dos riscos cabe ao gestor do risco, pois é ele que tem condições de avaliar os riscos do processo e quais medidas são possíveis de serem implementas.

3.2.6 Definição de Respostas aos Riscos

A resposta ou o tratamento de riscos envolve a proposição de uma ou mais alternativas para evitar, reduzir, compartilhar ou aceitar os riscos. Uma vez implementado, fornece novos controles ou modifica os atuais.

Para selecionar a medida mais adequada, deve-se equilibrar os custos e esforços empregados com os benefícios decorrentes de sua implementação.

As respostas usualmente empregadas para o tratamento de riscos são:

- Evitar: Eliminar a fonte do risco. A seleção desta resposta significa encerrar determinada atividade ou processo. Entretanto, a descontinuidade é uma decisão nem sempre possível no setor público, pois o governo pode ser o único provedor ou se tratar de uma determinação legal.
- Reduzir/Mitigar: Controlar, implementar ações ou ferramentas para reduzir a probabilidade ou impacto ou ambos. Exemplos: criação de lista de verificação; monitoramento de cenários, a fim de se antecipar a eventuais mudanças no panorama político; elaboração de planos de contingência, com o objetivo de preparar a organização caso determinado cenário previsto se concretize.
- Compartilhar: Transferir o risco. Redução da probabilidade ou impacto dos riscos pela transferência de uma porção do risco. Exemplos: terceirização de atividades e contratação de seguros.
- Aceitar: Não fazer nada. A exposição ao risco é tolerável, não sendo necessária qualquer ação. Significa que, após uma avaliação do custo-benefício, concluiu-se que não valeria a pena a implementação de medidas de redução ou compartilhamento do risco.

Para identificar as medidas de resposta ao risco, respondas as seguintes questões:

1. Que medidas poderiam ser adotadas para reduzir a probabilidade de ocorrência do risco?
2. Que medidas poderiam ser adotadas para reduzir o impacto do risco no objetivo/resultado?

Para responder essas questões, volte um pouco nas etapas anteriores e considere as fontes e causas dos riscos. As respostas que atacam as causas do risco reduzem a probabilidade de ocorrência e os planos de contingência amenizam os impactos, caso o risco se concretize, ou pode ser adotada uma combinação das duas abordagens.

Várias opções de respostas podem ser implementadas individualmente ou combinadas. As medidas mitigadoras podem envolver a adoção de controles, o redesenho de processos, a realocação de pessoas, a realização de ações de capacitação, o desenvolvimento ou aperfeiçoamento de soluções de TI, a adequação da estrutura organizacional, entre outros.

Deve-se buscar construir respostas aos riscos que sejam factíveis, isto é, que possam ser implementas pelos responsáveis. É importante lembrar que essas ações serão objeto de monitoramento da gestão de riscos e serão acompanhadas pela alta administração.

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

Atenção!

Não há uma relação direta entre um risco e uma resposta. É possível que uma única ação seja utilizada para reduzir/mitigar vários riscos assim como um determinado risco pode requerer diversas ações de tratamento.

Plano de Gestão de Riscos

O plano de gestão de riscos é um documento que consolida o resultado da aplicação da metodologia e as ações necessárias para adequar os níveis de risco, por meio da adoção de novos controles ou da otimização dos controles existentes, bem como outras medidas preventivas ou corretivas.

O plano será elaborado para aqueles eventos de risco que receberão tratamento, conforme definido na priorização, e deverá contar com as ações necessárias para assegurar que as repostas aos riscos sejam executadas, bem como os prazos e responsáveis pelas ações.

A elaboração do plano deve se iniciar concomitantemente à identificação dos riscos, sendo periodicamente atualizado. Portanto, as informações resultantes de cada etapa devem ir sendo registradas e, assim, ao final da aplicação da metodologia o Plano estará pronto.

Para facilitar a elaboração do plano, sugere-se a utilização do seguinte modelo:

Tabela 7 - Modelo Plano de Gestão de Risco

PLANO DE GESTÃO DE RISCOS	
UNIDADE	
PROCESSO	
DATA DA AVALIAÇÃO	

Fonte: Dicor/DAP

Preencher as informações abaixo para cada evento de risco associado ao processo:

Tabela 8 - Modelo Informações Evento de Risco

Risco	Descrever o evento de risco identificado
Causa	O que pode fazer um evento ocorrer (pode ter origem no ambiente interno e externo)
Consequência	É o resultado ou impacto de um evento de risco
Controles ou ações existentes	São as ações, controles ou medidas que já existem para reduzir/mitigar o risco
Nível de Risco	Crítico, alto, médio, baio
Resposta ao Risco	Evitar, Reduzir/Mitigar, Compartilhar, Aceitar
Ações/medidas propostas	Descrição da ação que será realizada para reduzir/mitigar o risco. O que vai ser feito e como vai ser feito
Prazo	Data de início e fim previstos para a implementação das respostas
Responsável	Nome ou cargo do principal responsável pela ação proposta
Intervenientes	Outras áreas que participam de alguma forma na execução da ação proposta
Resultado	A ação foi implementada? As ações diminuíram a probabilidade de ocorrência do risco ou alteraram o impacto do evento?

Fonte: Dicor/DAP

Para cada processo avaliado poderão ser encontrados (e geralmente são) mais de um risco associado. Portanto, a segunda parte do modelo deverá ser replicada quantas vezes for necessário para contemplar todos os riscos identificados em cada processo.

Veja o modelo no “ANEXO I – PLANO DE GESTÃO DE RISCOS”

Cabe destacar que o Plano de Gestão de Riscos não é um documento estático e, portanto, deve ser constantemente atualizado. A periodicidade de atualização deve ser definida pelos gestores, de acordo com os riscos identificados e as ações propostas.

Contudo, sugere-se um período mínimo de revisão anual que pode resultar em:

- manutenção do Plano vigente, tendo em vista que se mantém fiel à realidade do setor e à metodologia adotada;
- atualização do Plano vigente, em decorrência da alteração das respostas ao risco, do nível de exposição ao risco ou outra mudança pontual;
- elaboração de um novo Plano, por não atender mais à realidade do setor ou à metodologia recomendada.

A revisão anual do Plano oferece ao setor a oportunidade de realizar uma avaliação sobre seu processo de gestão de riscos, possibilitando que se mantenha coerente aos objetivos institucionais e adequado ao contexto de cada unidade e às medidas adotadas.

3.2.7 Comunicação e Monitoramento

Comunicação

É importante que a comunicação flua em todos os níveis da organização, facilitando a troca de informações pertinentes e confiáveis. Pode se dar por meio de troca de mensagens, documentos, notificações e até mesmo pelo uso de sistemas automatizados de gestão de riscos quando disponível.

A comunicação entre as unidades e as instâncias de gestão de riscos ocorre em níveis: i) operacional, representado pelo gestor do processo e por sua chefia imediata e/ou da unidade, a quem cabe executar a gestão de riscos; ii) tático, que é a unidade responsável pelo monitoramento da gestão de riscos e por apoiar às unidades do Cade; e iii) estratégico, no qual a alta administração, representada pelo Corisc, irá deliberar e orientar as unidades do Cade na condução das ações para a gestão de riscos.

Para facilitar o entendimento, separamos a comunicação em dois fluxos:

1. **Comunicação padrão**: formalmente estabelecida, com periodicidade definida, para reporte das informações derivadas da aplicação da Metodologia de Gestão de Riscos para subsidiar o monitoramento da gestão de riscos no Cade; e
2. **Comunicação eventual**: reporte de eventos sensíveis, que podem causar um impacto significativo no alcance dos objetivos institucionais e, portanto, precisam ser do conhecimento imediato da alta administração.

O detalhamento dos fluxos pode ser visualizado no “ANEXO II – FLUXO DE COMUNICAÇÃO”.

Monitoramento

O monitoramento consiste no acompanhamento das ações propostas pelo gestor responsável como respostas aos riscos identificados. Monitorar faz parte do processo de gestão de riscos e tem como objetivo:

a) obter informações adicionais para melhorar o processo de gestão de riscos;

b) detectar mudanças no contexto interno e externo;

c) analisar eventos, mudanças, tendências, sucessos, fracassos, lições aprendidas; e

d) acompanhar a evolução dos níveis de riscos e a implementação das respostas aos riscos.

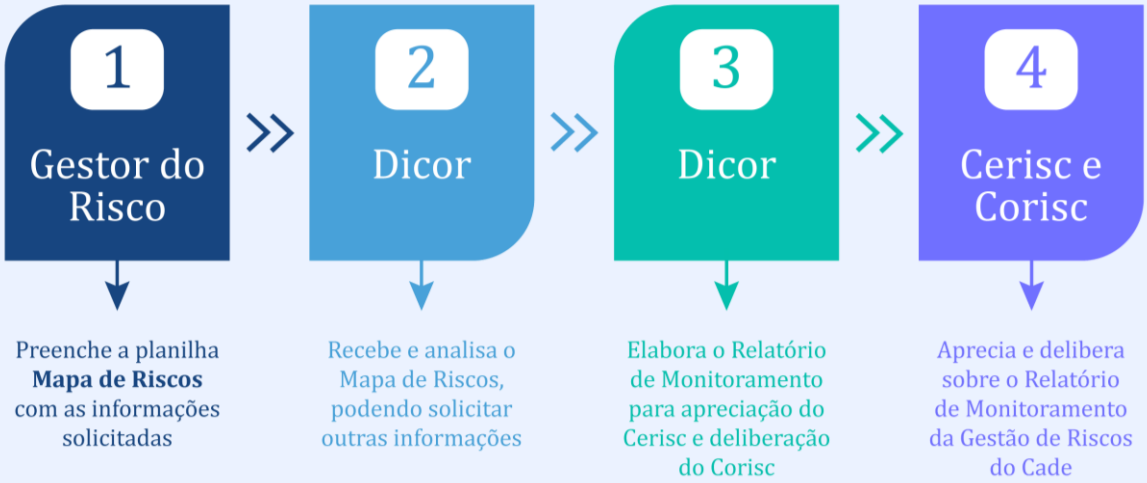
As informações para o monitoramento devem ser registradas pelo gestor do processo no modelo de planilha constante do “ANEXO III – MAPA DE GESTÃO DE RISCOS” na periodicidade solicitada pela unidade responsável pelo apoio à gestão de riscos.

O preenchimento do Mapa de Riscos pelo gestor do risco tem por objetivo informar à alta administração a evolução da gestão de riscos durante todo o ciclo de vida do processo. Todas as informações que irão compor o Mapa de Riscos podem ser extraídas da aplicação das técnicas disponíveis nesta Metodologia.

O fluxo de monitoramento da gestão de riscos no Cade se inicia pelo preenchimento do Mapa de Riscos pelos gestores de risco nos meses de fevereiro e setembro de cada ano. A seguir, o Mapa é encaminhado à Dicor para análise e elaboração do Relatório de Monitoramento da Gestão de Riscos do Cade, de forma a proporcionar tempo hábil para a apreciação quadrimestral pelo Cerisc e deliberação do Corisc.

O fluxo de monitoramento pode ser sintetizado da seguinte forma:

Figura 17 - Fluxo Monitoramento



O Mapa de Risco é a principal ferramenta de monitoramento da gestão de riscos. É a partir dele que serão extraídas e analisadas as informações que irão compor o Relatório de Monitoramento que será encaminhado para conhecimento e deliberação da alta administração do Cade.

Atenção!

Ainda que as informações para a gestão de riscos estejam relacionadas ao processo sob análise e, normalmente, não adentrarem no conteúdo de casos específicos, é preciso ficar atento e evitar o registro de alguma informação sigilosa, restrita ou sensível.

No decorrer da aplicação da Metodologia, caso se identifique alguma informação sigilosa, restrita ou de conteúdo sensível, procure reescrever de forma genérica e se não for possível utilizar um código, como "informação restrita".

CAPÍTULO IV

- Considerações Finais
- Referências Bibliográficas
- Glossário
- Anexos

Considerações Finais

A gestão de riscos pode ser entendida como o processo de identificar, avaliar, tratar e monitorar os riscos existentes em uma organização, unidade, processo ou atividade específica. Tem como objetivo minimizar a possibilidade de impactos negativos sobre os objetivos pretendidos, caso algum dos riscos analisados venha a se concretizar, bem como perceber e aproveitar possíveis oportunidades.

A publicação desta metodologia, além de atender determinação do Corisc, conforme disposto na Portaria Cade nº 97, de 2022, busca auxiliar as unidades do Cade na identificação e mitigação de possíveis ocorrências de eventos de riscos, utilizando conceitos e técnicas apresentados de forma sistematizada, simples e abrangente.

Esta metodologia tem a finalidade de agregar valor aos processos organizacionais e facilitar a implantação da gestão de riscos no Cade, trazendo conceitos, exemplificações, modelos, técnicas e outras informações importantes sobre o tema. Fornece ferramentas para o registro de dados sobre riscos, bem como para viabilizar um melhor gerenciamento desses dados. Permite que o gestor tenha uma visão crítica de seus processos e assim possa estabelecer correções e aprimoramentos.

Importante apontar que o propósito da implantação de uma gestão de riscos não constitui um mero atendimento às demandas normativas, mas sim uma mudança cultural da gestão com a adoção de ferramentas que possam servir de apoio para o alcance dos objetivos institucionais.

Por fim, cabe destacar que a gestão de riscos é um processo dinâmico e deve ser aprimorada continuamente para se adaptar às melhores práticas, bem como ser incorporada à cultura organizacional do Cade.

Referências Bibliográficas

BERMEJO, Paulo Henrique et all. ForRisco: gerenciamento de riscos em instituições públicas na prática. Brasília: Editora Evobiz, 2018.

BRASIL. Controladoria-Geral da União. Instrução Normativa Conjunta nº 1, de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal. Brasília, 2016.

_____. Decreto nº 9.203, de 22 de novembro de 2017. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Brasília, 2017.

_____. Controladoria-Geral da União. Metodologia de Gestão de Riscos, 2021.

_____. Ministério da Infraestrutura. Manual de Gestão de Riscos dos Processos de Trabalho. Brasília, 2021.

_____. Ministério da Justiça e Segurança Pública. Manual de Gerenciamento de Riscos e Controles Internos. Brasília, 2020.

_____. Tribunal de Contas da União. Manual de Gestão de Riscos do TCU – um passo para a eficiência. 2ª Edição, Brasília, 2020.

_____. Agência Nacional de Aviação Civil. Manual de Referência de Gestão de Riscos dos Processos Organizacionais. Brasília, 2019.

_____. Ministério da Justiça. Assessoria Especial de Controle Interno. Manual de Gerenciamento de Riscos e Controles Internos. Brasília, 2018.

_____. Ministério da Transparência e Controladoria-Geral da União. Metodologia de Gestão de Riscos. Brasília, 2018.

_____. Ministério do Planejamento, Desenvolvimento e Gestão. Assessoria Especial de Controles Internos. Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão. Brasília. V1.1.2, 2017.

GOVERNO DO ESTADO DE MINAS GERAIS. Guia Metodológico de Gestão de Riscos Estratégicos. Belo Horizonte, 2020.

MIRANDA, Rodrigo Fontenelle. Implementando a Gestão de Riscos no Setor Público. Belo Horizonte, 2017.

Glossário

Para fins deste documento, consideram-se os seguintes conceitos extraídos da Portaria Cade nº 97/2022:

- **apetite a risco**: nível de risco que uma organização está disposta a aceitar.
- **controle interno da gestão**: conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados, de forma integrada, destinados a enfrentar os riscos e fornecer segurança razoável para a consecução dos objetivos da organização.
- **evento**: um ou mais incidentes, ou ocorrências, provenientes do ambiente interno ou externo, ou mudança em um conjunto específico de circunstâncias, podendo também consistir em algo não acontecer.
- **gerenciamento de riscos**: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza quanto ao alcance dos objetivos da organização.
- **gestor do risco**: responsável com autoridade e competência para gerenciar riscos.
- **planos de gestão de riscos**: documentos que identificam os riscos, suas causas e consequências, as ações de mitigação e os responsáveis por gerenciá-los, bem como o processo de implementação, acompanhamento e avaliação.
- **risco**: possibilidade de ocorrência de um evento que tenha impacto no atingimento dos objetivos da organização.

Outros conceitos importantes para a gestão de riscos:

- **análise SWOT**: análise que permite avaliar quesitos internos e externos de uma organização. Seu nome é um acrônimo da sigla em inglês para forças (Strengths), fraquezas (Weaknesses), oportunidades (Opportunities) e ameaças (Threatens).
- **governança no setor público**: compreende essencialmente os mecanismos de liderança, estratégia e controle postos em prática para

avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade.

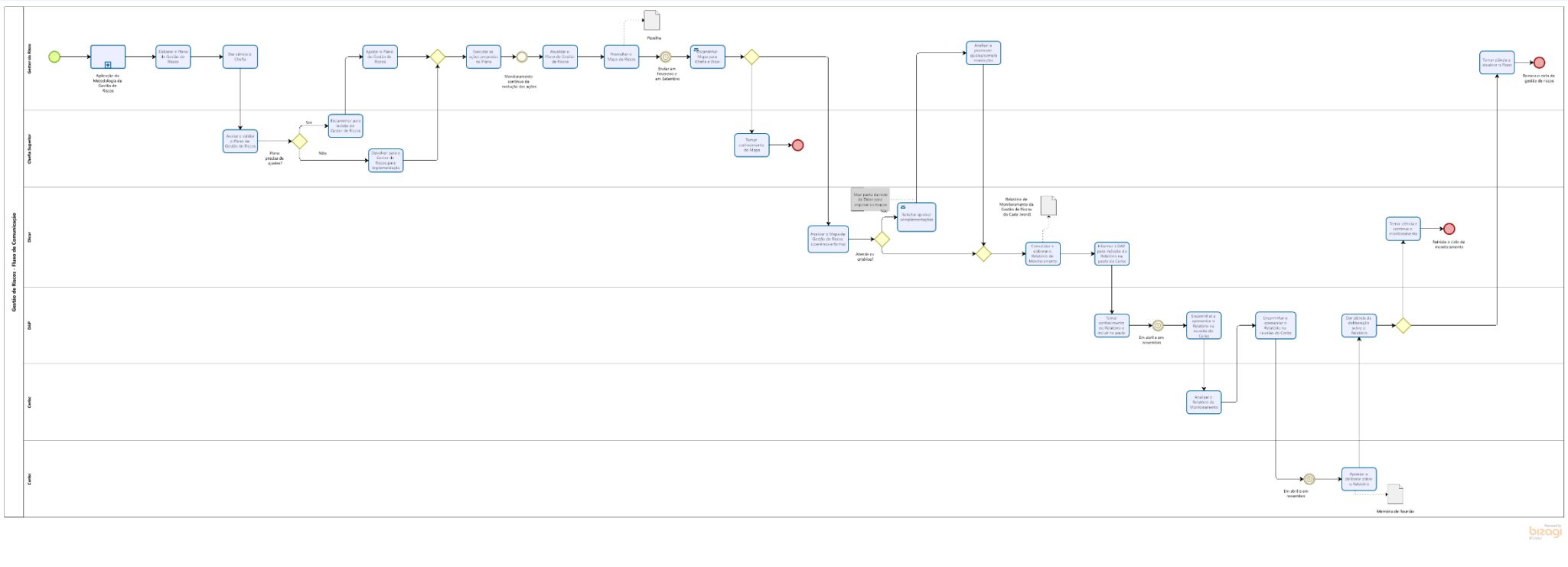
- **medida de controle**: medida aplicada pela organização para tratar os riscos, aumentando a probabilidade de que os objetivos e as metas organizacionais estabelecidos sejam alcançados.
- **nível de risco**: magnitude de um risco, expressa em termos da combinação de suas consequências e probabilidades de ocorrência.
- **objetivos (estratégicos):** os desafios a que a organização se propõe para cumprir sua missão e alcançar sua visão de futuro no cumprimento do seu papel institucional.
- **objeto de gestão de risco:** qualquer processo de trabalho, atividade, projeto, iniciativa ou ação de plano institucional, assim como os recursos que dão suporte à realização dos objetivos.
- **oportunidade**: possibilidade de que um evento afete positivamente o alcance de objetivos.
- **processo:** conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar produto, resultado ou serviço predefinido.
- **projetos:** são definidos como um esforço temporário, com início e término definidos, cujo objetivo resulta em uma entrega formal de um produto ou serviço único.
- **risco** inerente: risco a que uma organização está exposta sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto.
- **risco residual:** risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco.

ANEXO I – PLANO DE GESTÃO DE RISCOS

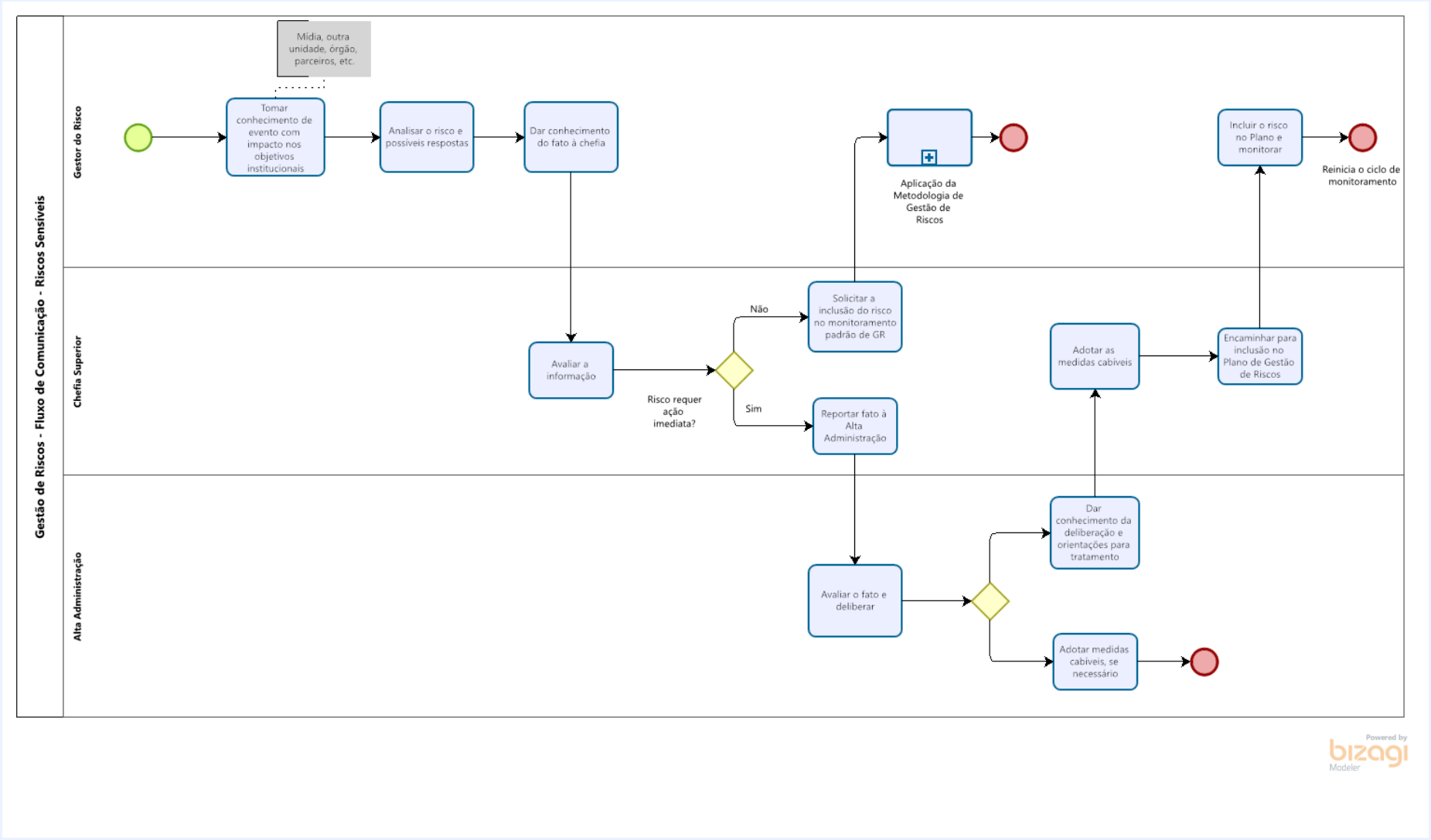
UNIDADE										
PROCESSO										
DATA DA AVALIAÇÃO										
Risco	**Causa**	**Consequência**	**Controles ou ações existentes**	**Nível de Risco**	**Resposta ao Risco**	**Ações/medidas propostas**	**Prazo**	**Responsável**	**Intervenientes**	**Resultado**
Descrever o evento de risco identificado	O que pode fazer um evento ocorrer (pode ter origem no ambiente interno e externo)	É o resultado ou impacto de um evento de risco	São as ações, controles ou medidas que já existem para reduzir/mitigar o risco	Crítico, alto, médio, baio	Evitar, Reduzir/ Mitigar, Compartilhar, Aceitar	Descrição do controle preventivo, das medidas mitigadoras, do plano de contingência ou outras ações para reduzir/mitigar o risco	Data de início e fim previstos para a implementação das respostas	Nome ou cargo do principal responsável pela ação proposta	Outras áreas que participam de alguma forma na execução da ação proposta	Qual a situação do risco após a conclusão da implementação das respostas. As ações diminuíram a probabilidade de ocorrência ou alteraram o impacto do evento?

ANEXO II – FLUXO DE COMUNICAÇÃO

Fluxo de Comunicação Padrão



Fluxo de Comunicação Eventual



ANEXO III – MAPA DE GESTÃO DE RISCOS

Priorização do Risco	Risco-Chave Descrição	Unidade (Sigla)	Categoria do Risco	Causas Prováveis	Controle Identificados e Ações Existentes	Classificação dos Controles	Consequências	Probabilidade	Impacto	Resultado Automático	Nível de Risco	Resposta ao Risco	Ações/medidas propostas	Responsável	Prazo	Intervenientes	Situação	Resultado
R1										0	Baixo							
R2										0	Baixo							
R3										0	Baixo							
R4										0	Baixo							
R5										0	Baixo							

Observações**:**

Macroprocesso – Identifica o macroprocesso finalístico, gerencial ou de suporte de acordo com a Cadeia de Valor do Cade.

Processo – nome do processo que representa o conjunto de atividades correlacionadas, desenvolvidas com o objetivo de gerar resultados à organização e que envolvem um ordenamento lógico para transformar entradas (insumos) em saídas, buscando o alcance de uma meta ou objetivo.

Risco – o que pode prejudicar/atrapalhar/impedir o cumprimento dos objetivos?

Nível de risco – Crítico, alto, médio ou baixo.

Controles ou ações existentes – Controles, ações ou medidas já existentes que atuam sobre o risco identificado.

Resposta ao risco – Evitar, reduzir, compartilhar, aceitar.

Ações/medidas propostas- Descrição do que será feito para reduzir/mitigar a ocorrência do risco ou seu impacto.

Situação: A iniciar, em andamento ou concluída.

Resultado - O risco foi mitigado? O que realmente aconteceu após a implantação das medidas.

ANEXO IV – APLICAÇÃO DA METODOLOGIA

Colocar a Metodologia em prática pode gerar muitas dúvidas: como organizar a equipe; encontros presenciais, remotos ou híbridos; como estimar o tempo para as atividades?

Essas são algumas questões levantadas na organização dos pilotos realizados para a validação desta Metodologia. Por isso, preparamos algumas dicas, bem como disponibilizamos roteiros e *templates* prontos para utilização, além de outros materiais de apoio.

Vamos lá:

1. Defina quem vai participar, se apenas a equipe ou se serão convidadas pessoas de outras áreas.
2. Crie um grupo no Microsoft Teams para a troca de informações entre os participantes.
3. Escolha uma data e encaminhe o convite para os participantes com antecedência, juntamente com as informações iniciais sobre o processo que vai ser trabalhado e o documento da Metodologia de Gestão de Riscos do Cade. Em eventos remotos lembre-se de encaminhar o link da reunião e de acesso à ferramenta para a construção coletiva (o Miro, por exemplo).
4. Caso se opte por encontros presenciais, deve-se reservar a sala com equipamento para projeção, verificar se materiais como cartelas coloridas, pincéis, fita crepe, flip chart etc estão disponíveis em quantidade suficiente.
5. Defina os papéis: quem vai fazer a abertura, quem vai ser o facilitador e quem vai apoiar as atividades.
6. Descreva o passo a passo, detalhando cada atividade, horários de início e fim e quem faz o que (recepção dos participantes, abertura e contextualização, forma de execução das etapas, intervalo, encerramento). Deve-se estimar um tempo para cada item. Utilize o modelo de roteiro disponibilizado no grupo “Metodologia de Gestão de Riscos” do Microsoft Teams.

7. Salve os *templates,* materiais e anotações utilizados nas etapas da gestão de risco em um local de fácil acesso (pasta na rede, pen drive, nuvem, Teams). Caso for utilizada a ferramenta Miro o salvamento é automático no *board.*
8. No formato remoto, pode-se utilizar a ferramenta Miro para trabalho colaborativo, de acesso livre. Foi aberto o Processo nº 08700.007351/2023-61 com *templates* que podem ser utilizado para as atividades.
9. Faça testes de uso das ferramentas e da qualidade de sua conexão para o formato virtual.
10. Nos encontros remotos, explique as principais funcionalidades da ferramenta que será utilizada e como se dará a participação virtual (como se deslocar pela área de trabalho, colar *post-it* nos *templates* com as ideias, como será realizada a discussão e consolidação etc)
11. Durante o encontro, muitas vezes será preciso fazer intervenções, direcionar a discussão para que não se perca o foco do trabalho. Esteja preparado e fique atento ao tempo para cumprir o cronograma proposto.
12. Registre todas as informações levantadas, pois elas são o resultado da aplicação da Metodologia.
13. Se possível, tire fotos, grave o evento.
14. Ao final, solicite que os participantes façam uma avaliação da atividade.

Os materiais de apoio para a aplicação da Metodologia estão disponíveis no Processo nº 08700.007351/2023-61:

- *Templates*
- Apresentação Contextualização da Gestão de Riscos
- Modelos
- Roteiro de Organização das Oficinas
- Guia de Facilitação Remota (Enap)
- Guia para aplicação da Metodologia de Gestão de Riscos no Miro

Atenção! O objetivo da prática anteriormente descrita é apoiar os gestores de risco para a implementação da Metodologia, auxiliando no planejamento das atividades e na execução de forma colaborativa, tanto no formato presencial quanto virtual.

Contudo, enfatizamos que as técnicas e ferramentas apresentadas são opcionais, bem como o formato de aplicação. Cabe ao gestor do risco definir a forma de trabalho que melhor se adapta às características do processo e da equipe, seja por meio de encontros presenciais ou reuniões virtuais, pelo uso de ferramentas sofisticadas ou uma simples planilha Excel.

O importante é a criação de uma cultura que incorpore a gestão de riscos na rotina de trabalho das unidades do Cade.

ANEXO V – SÍNTESE DA METODOLOGIA DE GESTÃO DE RISCOS

Ao longo deste documento buscou-se abordar os principais aspectos relacionados à gestão de riscos, a partir da apresentação de uma metodologia baseada em referencial amplamente reconhecido e adotado no setor público, bem como a apresentação de técnicas e práticas para facilitar sua implementação, independente do tipo ou complexidade do processo.

As etapas de gestão de riscos estão definidas na Portaria Cade nº 97, de 2022, e servem de base para a aplicação da metodologia. As etapas foram descritas de forma a assegurar um embasamento teórico para a implantação da gestão de riscos e seu detalhamento teve por objetivo oferecer subsídios aos gestores de risco, de modo que a operacionalização vá evoluindo gradualmente.

Na aplicação prática é comum a junção de etapas que possuem conteúdos próximos, como as que são referentes ao Entendimento do Contexto, Identificação dos Riscos e Análise do Riscos, que podem formar um bloco, assim como Avaliação, Priorização e Definição de Respostas aos Riscos outro bloco. O ritmo e a forma de aplicação da metodologia devem estar de acordo com as características do processo, da experiência e do conhecimento da equipe.

Cabe destacar que as técnicas apresentadas, como *brainstorming*, *bow tie*, análise SWOT, entre outras, servem como apoio, principalmente para quem está iniciando a jornada na gestão de riscos. Elas são opções comumente utilizadas, mas outras técnicas e ferramentas podem ser adotadas para auxiliar na identificação, avaliação e tratamento dos riscos.

Sinteticamente, a Metodologia de Gestão de Riscos do Cade consiste em:

1. Entendimento do Contexto;
2. Identificação dos Riscos;
3. Análise dos Riscos;
4. Avaliação dos Riscos;
5. Priorização do Risco;
6. Definição de Respostas aos Riscos;
7. Comunicação e Monitoramento.

Os itens que se seguem trazem a síntese que teve por objetivo fornecer uma visão rápida da Metodologia de Gestão de Riscos, principalmente para aqueles que já possuem alguma experiência com o tema.

Contudo, ressaltamos que a Metodologia foi projetada para apoiar o gestor na operacionalização, de modo a oferecer referências, técnicas e ferramentas para facilitar a implantação da gestão de riscos no Cade

V.1 Entendimento do Contexto

Esta etapa reúne as informações para a identificação do processo, como o nome, a unidade responsável, a(s) unidade(s) interveniente(s), os objetivos estratégico e do processo, a existência de sistema tecnológico e as partes interessadas.

Aqui devem ser levantadas informações sobre o ambiente interno (pontos fortes e fracos) e externo (oportunidades e ameaças).

As forças representam o que a organização tem de mais forte, como um processo bem definido, a qualidade técnica da equipe, os recursos tecnológicos etc. São exemplos de pontos fortes: existência de servidores capacitados, processo estruturado e eficiente, normativos internos claros e objetivos, tecnologias e sistemas adequados, controles internos efetivos etc.

As fraquezas são os pontos do ambiente interno que podem prejudicar e/ou interferir negativamente no alcance dos objetivos da organização. Pode-se pensar no oposto das forças citadas anteriormente.

As oportunidades são encontradas no ambiente externo e impactam positivamente a organização. São exemplos de oportunidades: parcerias com outros órgãos e entidades, realização de eventos para aperfeiçoar a relação com o público externo, atos normativos que favoreçam a realização das atividades, disponibilidade de recursos financeiros e orçamentários etc.

As ameaças são forças do ambiente externo que influenciam negativamente a organização. Exemplos: crise econômica, mudanças drásticas no ambiente externo com impacto negativo no processo, aumento de judicializações relacionadas ao processo, influência política externa que prejudique a execução das atividades, normas que causem impactos negativos nas atividades etc.

Nesta etapa deve-se utilizar diversas fontes para o levantamento de um cenário completo.

V.2 Identificação dos Riscos

A partir das informações do contexto, devem ser identificados os riscos associados ao processo em análise (riscos já conhecidos, riscos novos e outros que tenham potencial de afetar o processo e os objetivos propostos).

Para isso, responda a seguinte pergunta: Quais eventos podem EVITAR/ATRASAR/PREJUDICAR/IMPEDIR o alcance de um ou mais objetivos do processo organizacional? As respostas comporão uma lista que deverá ser analisada e consolidada. Aqui, é importante não confundir o evento de risco, o fato que prejudica o processo, com suas causas ou consequências.

Depois de listar os riscos, devem ser identificadas as causas e as consequências de cada evento de risco e por fim os controles preventivos (antes da ocorrência do risco) e os controles corretivos (depois da ocorrência do risco). Atenção para listar apenas os controles ou ações já existentes.

Causa é aquilo que poderia acontecer para determinado risco vir a ocorrer, o motivo que explica a ocorrência do risco. Geralmente, a falta de recursos (humanos, materiais, tecnológicos, financeiros) não é um risco, mas sim a possível causa. Por exemplo, o risco de não cumprir os prazos ou as metas de um processo pode ter como causa a falta ou alta rotatividade de servidores.

Consequência é o resultado ou o efeito produzido por um evento de risco sobre os objetivos. Deve-se pensar nas consequências como aquilo que ocorreria com o processo caso o risco se concretize. Por exemplo, o não cumprimento dos prazos legais poderia gerar a prescrição ou nulidade de um processo.

Os riscos identificados devem ser classificados de acordo com a categorização proposta:

I. **regulatório**: leis ou regulamentos externos que podem impactar o alcance dos objetivos e/ou os procedimentos internos de trabalho;

II. **estratégico**: eventos que possam impactar na missão, nas metas ou nos objetivos estratégicos da autarquia, caso venham ocorrer;

III. **operacional**: eventos que podem comprometer as atividades da unidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas;

IV. **orçamentário/financeiro**: comprometimento da capacidade de contar com recursos orçamentários ou da própria execução orçamentária;

V. **imagem/reputação**: pode comprometer a confiança da sociedade em relação à capacidade do Cade em cumprir sua missão institucional, afeta a imagem da autarquia;

VI. **integridade**: relacionado à probidade da gestão de recursos públicos e as atividades da organização, causados pela falta de honestidade e desvios éticos; e

VII. **conformidade**: relaciona-se ao descumprimento de leis e demais normas aplicáveis.

V.3 Análise dos Riscos

Tem por objetivo mensurar a probabilidade de o risco vir a ocorrer e o potencial de seu impacto, caso ocorra, determinando a magnitude do risco (nível de risco).

Os níveis de risco são definidos pela alta administração que irá estabelecer o apetite a risco, isto é, até que nível de risco a instituição está disposta a aceitar, conforme abaixo:

Tabela 9 - Nível de Risco

Nível	Pontuação	Definição
Risco Crítico (RC)	20 – 25	Acima do apetite a risco e requer um plano de ação imediato. Não se admite postergar o tratamento.
Risco Alto (RA)	12 – 19,99	Acima do apetite a risco. Requer um plano de ação para um período determinado.
Risco Médio (RM)	5 – 11,99	Dentro do apetite a risco. Não é necessária medida especial, porém requer monitoramento para a manutenção dos controles.
Risco Baixo (RB)	0 – 4,99	Dentro do apetite a risco. Não é preciso adotar novas medidas para tratamento do risco.

Fonte: Elaboração própria com base na Metodologia de Riscos 2021 da CGU - Disponível em: **https://repositorio.cgu.gov.br/bitstream/1/65535/6/Metodologia_de_riscos_2_0.pdf**.

Obs.: Os níveis de riscos são aprovados e atualizados por deliberação do Corisc.

Para calcular o nível de risco, deve-se atribuir um peso para a probabilidade e outro para o impacto do risco em análise, utilizando uma escala de 1 a 5, como apresentado a seguir:

Tabela 10 – Probabilidade

Probabilidade	Descrição da probabilidade	Frequência	Peso
Muito alta	**Praticamente certa**. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	> = 90%	5
Alta	**Provável**. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	>= 75%<= 90%	4
Média	**Possível.** De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade	>= 40% <75%	3
Baixa	**Rara.** De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	>= 10% <40%	2
Muito baixa	**Improvável.** Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade	< 10%	1

Fonte: Elaboração própria com base na Metodologia de Riscos 2021 da CGU - Disponível em: **https://repositorio.cgu.gov.br/bitstream/1/65535/6/Metodologia_de_riscos_2_0.pdf**.

Tabela 11 - Impacto

Impacto	Descrição do impacto nos objetivos, caso o evento ocorra	Peso
Muito alto	**Catastrófico** impacto nos objetivos do processo, de forma irreversível.	**5**
Alto	**Significativo** impacto nos objetivos do processo, de difícil reversão.	**4**
Médio	**Moderado** impacto nos objetivos do processo, porém recuperável.	**3**
Baixo	**Pequeno** impacto nos objetivos do processo.	**2**
Muito Baixo	**Mínimo** impacto nos objetivos do processo	**1**

Fonte: Elaboração própria com base na Metodologia de Riscos 2021 da CGU - Disponível em: **https://repositorio.cgu.gov.br/bitstream/1/65535/6/Metodologia_de_riscos_2_0.pdf**

A partir da atribuição dos pesos para cada risco identificado, deve-se multiplicar o peso da probabilidade com o peso do impacto para encontrar o nível de risco.

Ao final, com o resultado da probabilidade x impacto, será possível ter uma visão geral e apontar aqueles riscos que estão no nível crítico, alto, médio e baixo.

V.4 Avaliação dos Riscos

Consiste em comparar o resultado da análise com os níveis de risco para determinar se o risco do evento é aceitável. Assim a unidade poderá definir as possíveis respostas, de acordo com os níveis de riscos identificados:

- Riscos classificados como crítico e alto: exigem uma atuação imediata ou em um prazo determinado;
- Riscos de nível médio: devem ser acompanhados para verificar se os controles são suficientes ou necessitam aprimoramento; e
- Riscos de nível baixo: poderão ser aceitos sem novas medidas a serem tomadas (os controles existentes já são suficientes e efetivos).

Nesta etapa deve-se avaliar também a existência de controles internos que respondam aos eventos de riscos identificados. Ainda que existam controles formalmente definidos, é preciso avaliar sua efetividade, isto é, se estão sendo aplicados adequadamente e se são suficientes.

A tabela abaixo apresenta uma síntese de como analisar os controles existentes:

Tabela 12 – Classificação dos Controles

Classificação	Descrição
Controles preventivos	Controles existentes e que atuam sobre as possíveis causas do risco, com o objetivo de prevenir a sua ocorrência. Exemplos de controles preventivos: requisitos / checklist definidos para o processo e capacitação dos servidores envolvidos no processo.
Controles de atenuação e recuperação	Controles existentes executados após a ocorrência do risco com o intuito de diminuir o impacto de suas consequências. Exemplos de controles de atenuação e recuperação: plano de contingência; tomada de contas especiais; procedimento apuratório.
Controles detectivos	Controles existentes que atuam na detecção da materialização de um risco ou de sua iminência. Exemplos de controles de detecção: indicadores; termômetros; sensores.

Fonte: Elaboração própria com base na Metodologia de Riscos 2021 da CGU - Disponível em: **https://repositorio.cgu.gov.br/bitstream/1/65535/6/Metodologia_de_riscos_2_0.pdf**

A finalidade da avaliação é subsidiar a tomada de decisão e o estabelecimento de prioridade na implementação das medidas de tratamento aos riscos.

V.5 Priorização do Risco

Com base na avaliação, serão definidos quais riscos terão prioridade na implementação das medidas de tratamento ou definição de respostas aos riscos. Os riscos classificados nos níveis crítico e alto devem ser priorizados.

Cabe ao gestor do risco definir a priorização e as formas de tratamento, tendo em vista que é ele quem melhor conhece o processo.

V.6 Definição de Respostas aos Riscos

Compreende o planejamento e a realização de ações para modificar o nível do risco.

As respostas usualmente empregadas para o tratamento de riscos são evitar, reduzir/mitigar, compartilhar e aceitar.

- **Evitar**: Eliminar a fonte do risco. Significa encerrar determinada atividade ou processo. Entretanto, a descontinuidade é uma decisão nem sempre possível no setor público, pois o governo pode ser o único provedor ou se tratar de uma determinação legal.
- **Reduzir/Mitigar**: Controlar, implementar ações ou ferramentas para reduzir a probabilidade ou impacto ou ambos.
- **Compartilhar**: Transferir o risco. Exemplos: terceirização de atividades e contratação de seguros.
- **Aceitar**: Não fazer nada. A exposição ao risco é tolerável, não sendo necessária qualquer ação.

Na definição de respostas busca-se propor ou aprimorar ações para reduzir a probabilidade de ocorrência do risco ou seu impacto.

Várias opções de respostas podem ser implementadas individualmente ou combinadas. Não há uma relação direta entre um risco e uma resposta, isto é, uma resposta pode ser utilizada para tratar diferentes riscos assim como um risco pode requerer diversas respostas.

Deve-se buscar construir respostas aos riscos que sejam factíveis, isto é, que possam ser implementas pelos responsáveis. Tais ações serão objeto de monitoramento da gestão de riscos e acompanhadas pela alta administração.

Na redação da resposta ao risco deve-se ser sucinto, mas sem ser demasiado genérico. Por exemplo, uma ação proposta pode ser “capacitação”. Transmite a ideia geral, mas não é suficiente para descrever a ação: que tipo de capacitação, tema, público-alvo, carga horária, etc. Pense no “como” fazer e não apenas no “o que fazer”.

O tratamento de riscos pressupõe a elaboração de um Plano de Gestão de Riscos que estabelece, minimamente, o que será feito, qual ação será implementada ou aperfeiçoada, o prazo de implementação e os responsáveis pela ação.

Veja o modelo no “ANEXO I – PLANO DE GESTÃO DE RISCOS”

V.7 Comunicação e Monitoramento

A comunicação deve fluir em todos os níveis da organização, facilitando a troca de informações pertinentes e confiáveis.

No Cade foram estabelecidos dois fluxos para a comunicação da gestão de riscos:

I. **comunicação padrão**: formalmente estabelecida, com periodicidade definida, para reporte das informações derivadas da aplicação da Metodologia de Gestão de Riscos para subsidiar o monitoramento da gestão de riscos no Cade; e

II. **comunicação eventual**: reporte de eventos sensíveis, que podem causar um impacto significativo no alcance dos objetivos institucionais e, portanto, precisam ser do conhecimento imediato da alta administração.

O detalhamento dos fluxos pode ser visualizado no “ANEXO II – FLUXO DE COMUNICAÇÃO”.

O monitoramento consiste no acompanhamento da implementação da gestão de riscos no Cade. As informações para o monitoramento da gestão de riscos são registradas no Mapa de Riscos.

O fluxo de monitoramento se inicia pelo preenchimento do Mapa de Riscos pelos gestores nos meses de fevereiro e setembro de cada ano. Em seguida, o Mapa é encaminhado à Dicor para análise e elaboração do Relatório de Monitoramento da Gestão de Riscos do Cade, de forma a proporcionar tempo hábil para a apreciação quadrimestral pelo Cerisc e deliberação do Corisc.

O modelo de Mapa de Riscos está disponível no Anexo III.


CADE
Conselho Administrativo de Defesa Econômica