SEFIN
Secretaria de Estado de Finanças

RONDÔNIA
Governo do Estado

METODOLOGIA DE GESTÃO DE RISCOS

2025

METODOLOGIA DE GESTÃO DE RISCOS

LUÍS FERNANDO PEREIRA DA SILVA
Secretário de Estado de Finanças

FRANCO MAEGAKI ONO
Secretário de Estado de Finanças Adjunto

Responsável pela relatoria/consolidação do conteúdo:

PEDRO HENRIQUE ARAÚJO E ARAÚJO
Chefe do Núcleo de Gerenciamento de Riscos

Responsável pela revisão do conteúdo:

DOUGLAS CARREIRO DA HORA
Controlador Interno

SEFIN
Secretaria de Estado de Finanças
RONDÔNIA
Governo do Estado

INTRODUÇÃO

Este documento estabelece o compromisso da Secretaria de Estado de Finanças (SEFIN) com a governança e a gestão de riscos, visando aprimorar a eficiência no cumprimento de suas metas institucionais. Ele delineia a metodologia a ser adotada para identificar, analisar e tratar riscos, alinhando-se às diretrizes de sua Política de Gestão de Riscos, instituída por meio da Portaria n.º 1073, de 28 de novembro de 2023.

A Gestão de Riscos da SEFIN objetiva, entre outros, o cumprimento do objetivo estratégico que consta no seu Plano Estratégico para o período de 2025-2026, definido por meio da Resolução n.º 5, de 20 de maio de 2025:

> OBJETIVOS ESTRATÉGICOS DE RESULTADO (OKRs): definem o que deve ser alcançado. São significativos, concretos, orientados por ações e representam a realidade futura almejada. Cada objetivo contém um conjunto de resultados-chave (KRs).

A metodologia de gestão de riscos apresentada considera o processo de gestão de riscos em levantamentos estruturados relativos à gestão estratégica e operacional, orçamentária e financeira, contábil, patrimonial, de contratações públicas, de convênios e operacional, conforme modelo de Relatório Anual de Controle Interno (RACI) para o exercício de 2025.

Ademais, essa metodologia visa orientar a operacionalização da Gestão de Riscos na SEFIN, em consonância com as diretrizes da Política de Gestão de Riscos em vigor. Será adotada para gerenciar riscos nas diversas áreas da instituição, e o detalhamento do processo de gestão de riscos adotado por esta está estabelecido na Política..

Quanto à abrangência, a presente metodologia aplica-se a todas as unidades administrativas da SEFIN, incluindo autarquias vinculadas e órgãos auxiliares, devendo ser observada na gestão de seus processos organizacionais, projetos estratégicos, programas institucionais, atividades finalísticas e de apoio. Sua observância é obrigatória nos procedimentos relacionados à identificação, análise, avaliação, tratamento e monitoramento de riscos, bem como na elaboração de relatórios e planos de ação, nos termos estabelecidos neste documento.

Assim, apresenta elementos conceituais e metodológicos relacionados à gestão de riscos, além de um cronograma com as ações prioritárias voltadas à administração de riscos na Secretaria para o seu período de vigência, visando aumentar a probabilidade de alcance dos objetivos da organização, reduzindo os riscos a níveis aceitáveis e, ainda, agregar valor à organização por meio da melhoria dos processos de tomada de decisão e do tratamento adequado dos riscos e dos impactos negativos decorrentes de sua materialização.

LEVANTAMENTO E

Avaliações de Ações Pretéritas

Para subsidiar a estruturação da Metodologia de Gerenciamento de Riscos da SEFIN, inicialmente foi necessário compreender, de forma detalhada, o processo de Gerenciamento de Processos, conforme tramitado no processo SEI n.º 0030.005086/2025-76. Para isso, foram selecionados processos organizacionais-chave, visando avaliar e compreender a metodologia de gestão de riscos atualmente adotada pela instituição.

Na sequência, procedeu-se ao levantamento de informações relativas a eventos de risco ocorridos no período de 2018 a 2025, com o intuito de avaliar sua natureza, frequência, impactos gerados e a eficácia da medida de mitigação ou tratamento adotado. Esse levantamento contemplou oito categorias de riscos institucionais, conforme tipificação adotada no âmbito da SEFIN, alinhada às boas práticas de governança pública, a saber: estratégicos, orçamentários/fiscais, de integridade, de conformidade, reputacionais, operacionais, tecnológicos e políticos.

As principais fontes de informação utilizadas foram:

- Relatórios internos de gestão de riscos das unidades;
- Informações fornecidas por áreas finalísticas e administrativas;
- Atas de reuniões institucionais e documentos de planejamento estratégico.

De maneira geral, o trabalho permitiu identificar pontos de melhoria relevantes, os quais serão incorporados à nova metodologia de gestão de riscos. Destacam-se, entre eles:

- A necessidade de maior clareza quanto às etapas e fluxos dos processos;
- O aprimoramento do papel dos atores institucionais no processo de gestão de riscos;
- A otimização das etapas metodológicas, com foco em eficiência e padronização;
- A instituição de um ciclo semestral de monitoramento, com a elaboração de relatório técnico analítico destinado à alta administração.

Por fim, concluiu-se que a SEFIN dispõe de uma metodologia de gestão de riscos em uso, contudo ainda não disseminada de forma uniforme entre as unidades setoriais, o que compromete o monitoramento das ações e afeta a qualidade da gestão de riscos, tanto pelas unidades executoras quanto pela instância responsável pela supervisão e controle desses processos.

METODOLOGIA

de Gestão de Riscos

A base teórica-conceitual da Metodologia de Gestão de Riscos da SEFIN está pautada basicamente em frameworks internacionais e em normativos e referências nacionais de gestão de riscos e controles internos, dos quais se destacam:

Decreto Estadual n.º 23.277, de 16 de outubro de 2018 — Dispõe sobre o Sistema Estadual de Controle Interno;

Portaria n.º 217/CGE-RO, de 08 de dezembro de 2021 — Estabelece a metodologia de gestão de riscos no âmbito do Poder Executivo Estadual;

Portaria n.º 1073, de 28 de novembro de 2023 — Política de Gestão de Riscos da SEFIN;

Portaria n.º 314, de 17 de dezembro de 2024 — Aprova o modelo de Relatório Anual de Controle Interno - RACI, das unidades da Administração Pública Direta, Autarquias e Fundações do Poder Executivo do Estado de Rondônia;

Instrução Normativa Conjunta CGU/MP n.º 01, de 10/5/2016 — Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal;

Gerenciamento de Riscos Corporativos (2017) — COSO ERM: Enterprise Risk Management;

Metodologia de Gestão de Riscos da Controladoria Geral da União (CGU) — 2.ª versão (2021);

ABNT NBR ISO 31000, de 28/03/2018 — Diretrizes da Gestão de Riscos;

ABNT NBR IEC 31010, de 30/08/2021 — Técnicas para o processo de avaliação de riscos;

ABNT NBR ISO 31073, de 14/07/2022 — Gestão de Riscos: vocabulário;

Modelo das Três Linhas de Defesa (2020) — Instituto dos Auditores Internos do Brasil (IIA).

Destarte, a implementação da Gestão de Riscos na SEFIN busca garantir alinhamento metodológico com as principais referências nacionais e internacionais, promovendo a convergência entre boas práticas, normativos legais e os princípios constitucionais da administração pública.

No âmbito do Poder Executivo Estadual, o marco regulatório que orienta os órgãos e as entidades públicas à estruturação de mecanismos de controles internos, gestão de riscos e governança é a Portaria n.º 217/CGE-RO, de 8 de dezembro de 2021, em que são apresentados conceitos, princípios, objetivos e responsabilidades relacionados aos temas.

Com vistas ao cumprimento dessa Portaria e utilizando como parâmetros os frameworks citados acima, a SEFIN publicou a sua Política de Gestão de Riscos, por meio da Portaria n.º 1073, de 28 de novembro de 2023. Essa Portaria aborda conceitos básicos, princípios, objetivos, operacionalização e competências no âmbito da Gestão de Riscos da Secretaria.

Conforme a Controladoria Geral da União (CGU), a Gestão de Riscos consiste na arquitetura (princípios, objetivos, estrutura, competências e processo) necessária para se gerenciar riscos eficazmente. Trata-se de um sistema institucional de natureza permanente, estruturado, monitorado e direcionado às atividades de identificar, analisar e avaliar riscos, decidir sobre estratégias de resposta e ações para tratamento desses riscos, além de monitorar e comunicar sobre o processo de gerenciamento dos riscos organizacionais.

Dessa forma, entende-se que o gerenciamento de riscos também deve ser utilizado como uma ferramenta para promover a simplificação dos procedimentos relacionados à prestação de serviços, garantindo que apenas os controles essenciais sejam aplicados, conforme os limites de exposição a riscos definidos pela Secretaria, e serem eliminados controles desnecessários ou economicamente ineficientes.

Nesse sentido, para operacionalização do gerenciamento de riscos, a SEFIN deverá seguir as etapas de Estabelecimento e Supervisão da Gestão de Riscos e Processo de Gerenciamento de Riscos, conforme detalhamento abaixo:

ETAPAS DE ESTABELECIMENTO E SUPERVISÃO DA GESTÃO DE RISCOS	ETAPAS DO PROCESSO DE GESTÃO DE RISCOS
• Fortalecimento do ambiente interno; e • Supervisão da gestão de riscos.	• Análise de ambiente e dos objetivos; • Identificação dos riscos; • Avaliação dos riscos; • Respostas aos riscos; e • Monitoramento e comunicação

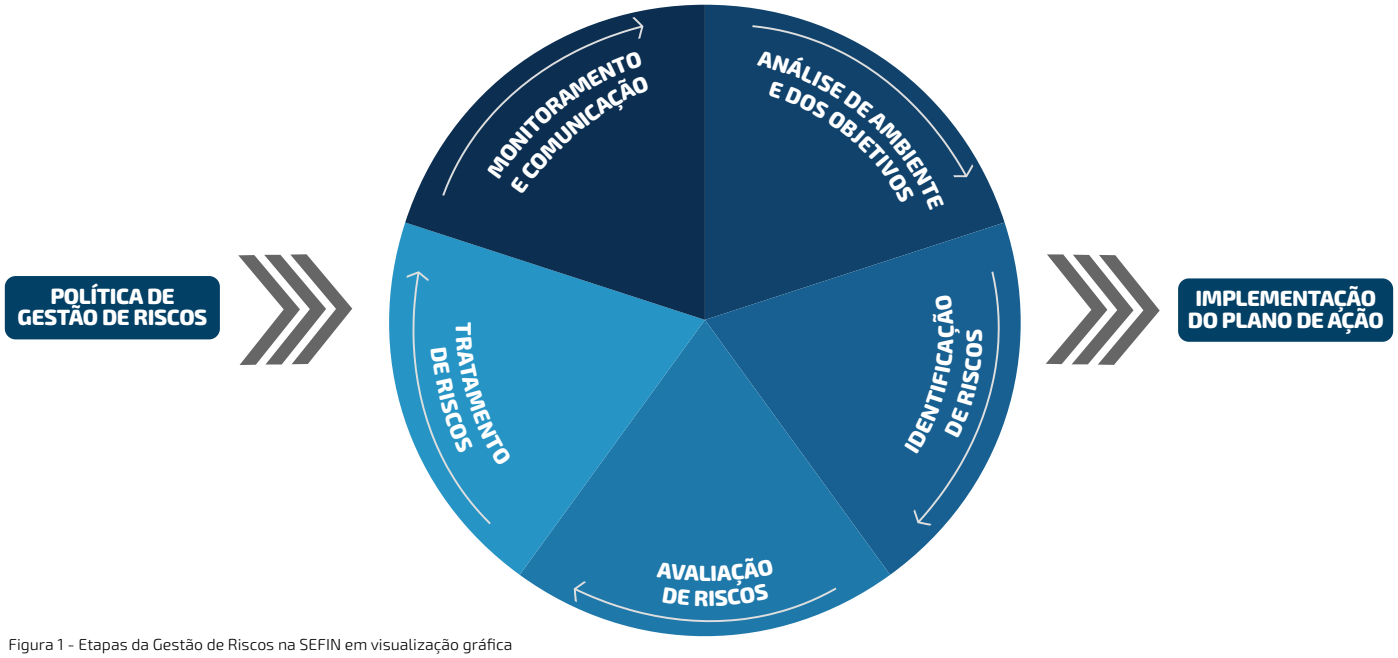


Figura 1 - Etapas da Gestão de Riscos na SEFIN em visualização gráfica

As etapas de Estabelecimento e Supervisão da Gestão de Riscos servem de base para o gerenciamento de riscos ao nível organizacional, atividades tipicamente desempenhadas pelo Comitê de Gestão de Riscos. Essas atividades permeiam e impactam todos os passos do processo de gerenciamento de riscos, enquanto desenvolvem as competências e fornecem os parâmetros necessários para sua condução. As demais etapas compreendem o processo operacional de gerenciamento de riscos.

A execução dessas etapas cabe aos gestores e servidores responsáveis pela execução da metodologia. A seguir estão apresentadas as etapas de "Estabelecimento e Supervisão da Gestão de Riscos" do "Processo de Gerenciamento de Riscos".

Fortalecimento do ambiente interno

O ambiente interno refere-se ao conjunto de elementos e fatores internos de uma organização que influenciam como ela identifica, avalia, trata e monitora riscos. Para fortalecê-lo, a SEFIN desenvolverá uma cultura de gestão de riscos, com a implantação da Política, Metodologia e Planos de Ação de Gestão de Riscos; promoverá comunicação eficiente para que os servidores possam relatar riscos organizacionais às unidades responsáveis; e monitorar e avaliar continuamente o ambiente interno, a fim de identificar ameaças e oportunidades e ajustar os processos de gestão de riscos conforme necessário.

Supervisão da Gestão de Riscos

A supervisão da Metodologia e do Plano de Gestão de Riscos tem como finalidade acompanhar o desenvolvimento e o desempenho das ações de gerenciamento de riscos nos diversos níveis de atuação. Busca-se, por meio da supervisão, avaliar a efetividade da política e práticas de Gestão de Riscos em vigor da SEFIN.

Ademais, a supervisão do processo de gerenciamento de riscos deverá ser realizada diretamente pelo Núcleo de Gerenciamento de Riscos e Núcleo de Monitoramento, subordinados à Assessoria de Controle Interno, enquanto unidades da Segunda Linha de Defesa.

Etapas do Processo de Gerenciamento de Riscos

O processo de gerenciamento de riscos consiste em um conjunto ordenado de atividades que permitem avaliar o contexto organizacional e identificar, analisar, avaliar, tratar, monitorar e comunicar os riscos de cada objetivo estratégico ou processo organizacional selecionado. A partir da seleção dos objetivos estratégicos e/ou processos definidos, cada unidade deve dar início à operacionalização das etapas do processo de gerenciamento de riscos, mas o gestor da unidade poderá à priori designar formalmente o responsável pelo gerenciamento de riscos nela e as equipes técnicas envolvidas. Tais equipes devem ser compostas por servidores com conhecimento aprofundado sobre o objeto de análise, isto é, o objetivo estratégico ou processo.

Ademais, diferentes equipes poderão ser designadas conforme o objetivo

estratégico ou processo organizacional em análise. No caso de objetivos estratégicos, a equipe técnica designada deve ser composta por membros do corpo diretivo, que detenham responsabilidades sobre as ações estratégicas relacionadas.

Para processos organizacionais, os membros podem ser designados ao nível operacional, desde que conheçam o fluxo do processo, seus objetivos, contexto interno e externo, atores envolvidos e controles já existentes.

Cumpre destacar que o resultado de cada etapa, descrito na sequência, deve ser acompanhado pelo dirigente da unidade.

Etapa 1: análise do ambiente e dos objetivos

Etapa em que são identificados os objetivos relacionados ao processo organizacional e definidos os contextos externo e interno a serem levados em consideração ao gerenciar riscos. São levantadas, no mínimo, as seguintes informações: fluxo de processo; infraestrutura utilizada; legislação correlacionada; principais objetivos do processo; principais problemas no passado que podem a ser riscos no futuro; recurso humano utilizado, incluindo o nível de conhecimento exigido para operacionalizar os processos; sistemas informatizados; partes interessadas internas e externas; e ambiente (ex.: análise SWOT).

Assim, quanto ao ambiente interno, a SEFIN encontra-se atualmente nas seguintes perspectivas:

- Atribuição de autoridade e de responsabilidade: Regimento Interno Institucionalizado, conforme Portaria n.º 720, de 31 de agosto de 2022;

- Integridade e valores éticos: Código de Ética institucionalizado, conforme Portaria n.º 506, de 12 de junho de 2024;

- Comprometimento da alta administração: cultura organizacional estruturada para apoio às decisões de gestão de risco, por meio das competências institucionalizadas do Comitê de Gestão de Riscos, conforme Portaria n.º 1078 de 29 de novembro de 2023;

- Filosofia de gerenciamento de riscos: a maturidade de gestão de riscos ainda é baixa, mas tem iniciado esforços para padronizar e institucionalizar o processo de gestão de riscos, com implementação de cronograma para capacitação de gestão de riscos. Ainda que não esteja em uma maturidade razoável de gerenciamento de riscos, a SEFIN institucionalizou, por meio da Portaria n.º 1073, de 28 de novembro de 2023, a Política de Gestão de Riscos, que estabelece os princípios, diretrizes, competências e responsabilidades para a gestão de riscos a serem observados e seguidos para sua implementação no âmbito da secretaria.

Assim, a primeira etapa do processo de gerenciamento de riscos consiste em examinar minuciosamente os cenários internos e externos da organização, e

posteriormente fixar os objetivos dos processos e macroprocessos (estratégicos e correlatos) que se deseja alcançar com o processo de gerenciamento de risco, nos quais devem estar alinhados ao apetite e a tolerância a riscos da SEFIN.

No que se refere a quanto à SEFIN está disposta a correr risco para atingir os objetivos organizacionais, o apetite a riscos da secretaria foi aprovado pelo Comitê de Gestão de Riscos, e será publicado nos meios oficiais da SEFIN.

Consoante a referida resolução, a Declaração de Apetite de Riscos é um importante instrumento que sintetiza a cultura de risco e direciona o plano estratégico da SEFIN, norteando os demais planos e permitindo que a Alta Administração otimize a alocação de recursos orçamentários, humanos e tecnológicos, dentre outros.

"A SEFIN apresenta apetite moderado ao risco e, portanto, tem um apetite médio ao risco em todas as categorias consideradas.

Salienta-se que o Apetite a Riscos será acompanhado pelo Comitê de Gestão de Riscos e monitorados permanentemente pela Assessoria de Controle Interno (ASCOINT), junto ao Núcleo de Gerenciamento de Riscos (NGR).

No que tange à fixação de objetivos, todos os departamentos da SEFIN devem ter objetivos fixados e comunicados, estando diretamente relacionados ao Plano Estratégico da organização. Esse procedimento é necessário para identificação de eventos que potencialmente impeçam a sua consecução.

Para os objetivos estratégicos, é necessário vislumbrar os objetivos específicos relacionados, os indicadores, as ações estratégicas e outras informações que permitam uma visão ampla e consubstanciada do contexto interno e externo relacionado.

No caso dos processos organizacionais, é importante fixar os objetivos de cada processo. Se for possível, devem ser indicados o objetivo geral e os objetivos específicos do processo, considerando as perspectivas estratégica, temporal, legal, financeira/orçamentária, entre outras.

Uma vez fixados os objetivos (gerais e específicos), pode-se iniciar a identificação e análise dos eventos de riscos que podem impactar o alcance do objetivo. Esse procedimento deverá analisar quais os processos deverão ser priorizados para serem mapeados e gerenciados, definindo critérios para selecionar quais processos serão mapeados. Um inventário de riscos depende da identificação dos processos de trabalho, não necessariamente do mapeamento de todos eles.

Nessa etapa, é importante elaborar mapa de processos organizacionais (governança, finalísticos e/ou) de suporte a fim de analisar se há riscos relacionados a redundância de informações, separação de responsabilidades, etapas burocráticas que impedem a organização de atingir seus objetivos, etc. Assim, para a melhoria dos processos de trabalho e visualização de fluxos, sugere-se a utilização de ferramentas que utilizem a notação internacional BPMN (Business

Process Model and Notation), como o Bizagi, Miro e Lucidchart.

Como resultado esperado da integração de gestão de riscos à gestão de processos, espera-se: melhor entendimento das etapas, dos fluxos dos processos e do papel dos atores nos processos; otimização das etapas dos processos; dimensionamento do custo operacional e temporal dos processos; automação de partes dos processos.

Etapa 2: Identificação de riscos

Esta etapa envolve reconhecer e catalogar os riscos ou eventos potenciais que possam impactar o alcance dos objetivos da organização, do processo ou atividade objeto da gestão de riscos, considerando os diversos níveis da organização. Envolve também a identificação de fontes de risco, eventos, suas causas e seus efeitos potenciais, num esforço de compreensão da natureza de determinado risco inerente.

A Política de Gestão de Riscos da secretaria define como:

a. Risco: possibilidade de ocorrência de um evento que tenha impacto no atingimento dos objetivos da organização.

b. Evento: ocorrência ou mudança em um conjunto específico de circunstâncias.

Ademais, os eventos, quando influenciam favoravelmente a realização dos objetivos, chamamos de oportunidades; e, quando influenciam negativamente ou dificultam a execução das ações planejadas, são eventos de risco.

Nesse sentido, os responsáveis pelos objetivos e processos/projetos devem construir uma lista abrangente de eventos de risco que possam comprometer o alcance dos objetivos gerais e específicos estabelecidos na Etapa 1.

Uma das principais técnicas para identificação de riscos é o brainstorming, que envolve estimular e incentivar o livre fluxo da conversação entre um grupo de pessoas, cuja imaginação é provocada pelos pensamentos e declarações de outras pessoas. Essa técnica propõe que o grupo se reúna e utilize a diversidade de pensamentos e experiências para gerar soluções inovadoras, sugerindo qualquer pensamento ou ideia que vier à mente a respeito do tema tratado.

Assim, deve-se levantar os objetivos do processo e verificar quais eventos poderiam impactar no objetivo. Todo risco levantado deve ser correlacionado a qual objetivo do processo está impactando de forma mais significativa.

A identificação e mensuração dos riscos devem ocorrer por meio de reuniões estruturadas com servidores envolvidos no processo de gestão estratégica, inclusive chefes ou membros de departamentos e, com isso, permite-se construir matrizes de riscos que envolvam a dual oportunidade e ameaça (ex.: riscos podem ser de integridade e operacional conjuntamente).

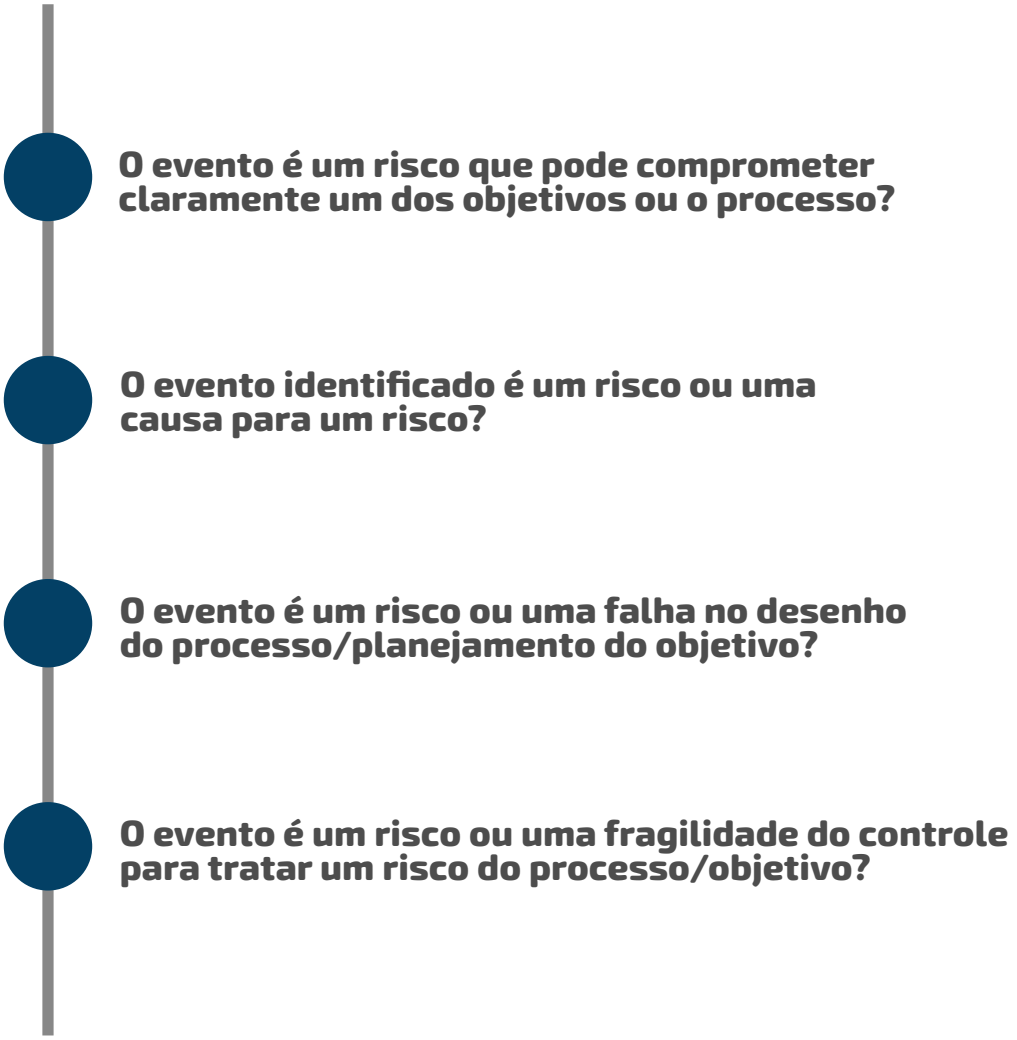
Além da autoavaliação dos riscos, poderá ser utilizada outra técnica para avaliação, como os Indicadores-Chave de Risco (KRI's) e o registro histórico de eventos.

Cada unidade deverá identificar e registrar no Mapa de Riscos os eventos de riscos relevantes que comprometem o alcance do objetivo do processo, bem como suas causas, seus efeitos, sua categoria e natureza.

Para a descrição do risco durante a sua identificação, pode ser utilizada a sintaxe do Tribunal de Contas da União, qual seja:

- **Devido a <CAUSA/FONTE>, poderá acontecer <DESCRIÇÃO DA INCERTEZA>, o que poderá levar a <DESCRIÇÃO DO IMPACTO, CONSEQUÊNCIA, EFEITO>, impactando no/na <DIMENSÃO DO OBJETIVO IMPACTADA>.**

Outrossim, eventos identificados inicialmente podem ser analisados, revisados e eliminados nesta etapa, e, para tanto, podem ser utilizadas as seguintes questões:



Os resultados dessa análise devem ser documentados na Matriz de Riscos, preenchendo os seguintes campos:

Processo/ Objetivo	Evento de risco	Categoria do Risco	Causas do risco	Consequências do risco
Descrição do processo, objetivo ou projeto (objeto da análise de riscos).	Descreve os eventos de riscos identificados, que podem evitar, atrasar, prejudicar ou impedir o cumprimento dos objetivos identificados na Etapa 1.	Caracterizado conforme parâmetros e categorias definidos no quadro 2 abaixo.	Descreve as possíveis causas, condições que dão origem à possibilidade de um evento ocorrer, também chamadas de fatores de risco, e podem ter origem no ambiente interno e externo. CAUSA = Fatores de Risco + Vulnerabilidade.	É o resultado da ocorrência do risco, afetando o objetivo do processo. A análise pode envolver: • relacionar as consequências do risco aos objetivos originais; e • levar em consideração os controles existentes para tratar as consequências, juntamente com todos os fatores contributivos pertinentes que tenham um efeito sobre as consequências.

Quadro 2: informações para a matriz de risco

Para eventos identificados e analisados como riscos do processo, deve-se indicar a categoria do risco dentre as definidas pela SEFIN, atentando-se da possível dualidade de classificação do risco:

Categoria dos riscos	Descrição
Estratégicos	Riscos que podem afetar negativamente na capacidade da secretaria em atingir os seus objetivos estratégicos definidos no Plano Estratégico da SEFIN, e poderão ter impactos positivos (oportunidades) ou negativos (ameças) para a organização.
Orçamentários e financeiros	Eventos que podem comprometer a capacidade da organização de contar com recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária.
Contábeis	Riscos que podem levar ao não atingimento dos objetivos da contabilidade pública no âmbito da SEFIN.
Patrimoniais	Eventos ou condições incertas que podem comprometer a integridade física, jurídica, contábil ou funcional dos bens públicos sob a responsabilidade do ente estatal, ocasionando perdas, danos, deteriorações, desvio de finalidade, subutilização ou desaparecimento desses ativos. Esses riscos afetam diretamente o controle, a proteção e a correta destinação do patrimônio público, impactando a prestação de serviços, o cumprimento de objetivos institucionais e a conformidade com os princípios da administração pública.
De contratações públicas	Eventos de riscos decorrentes de condutas fraudulentas, que podem impactar de forma adversa no alcance dos objetivos das contratações públicas, e na gestão dos contratos decorrentes dessas contratações.
De convênios	Riscos relacionados à concessão e gestão dos convênios, repasses ou instrumentos congêneres.
Operacionais	Riscos que podem comprometer as atividades da organização normalmente associados a falhas, deficiência ou inadequação de processos internos, normas legais, pessoas (integridade), conformidade, infraestrutura e sistemas.

Quadro 3: categoria de riscos e suas respectivas definições

Etapa 3: avaliação de riscos

A avaliação de riscos compreende a seguintes etapas:

Nessa etapa, os gestores de riscos das unidades devem avaliar os riscos para cada um dos eventos identificados na etapa 3. Essa avaliação deverá ser realizada considerando os critérios de probabilidade e de impacto.

Os componentes dessa etapa são:

I. **Nível de risco:** medida de importância ou significância do risco, quanto à sua criticidade, obtida a partir da combinação de dois fatores universais: probabilidade de ocorrência e impacto nos objetivos organizacionais. Quanto maior for a probabilidade e maior o impacto, maior é o nível do risco. Nível de Risco = Perda Estimada;

II. **Probabilidade:** associada a um incidente ou ocorrência potencial (chance de o evento ocorrer, a partir de fontes internas ou externas);

III. **Escala de probabilidade:** critérios que serão utilizados para o julgamento da probabilidade de ocorrência do evento;

IV. **Impacto:** associado à consequência do evento ocorrido (materialização o risco);

V. **Escala de impacto:** critérios que serão utilizados para o julgamento do impacto de ocorrência do evento;

VI. **Risco inerente:** risco a que a organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto, e é obtido por meio da pontuação

resultante da multiplicação da probabilidade pelo impacto a um evento de risco;

VII. **Classificação de Risco:** faixas de classificação utilizadas para o julgamento do nível de risco de cada evento;

VIII. **Matriz de Risco:** matriz de possíveis resultados da combinação das escalas de probabilidade e de impacto;

IX. **Controles internos:** mecanismos que reduzem ou podem reduzir a probabilidade de sua ocorrência, ou de seu impacto. Os controles preventivos atuam sobre possíveis causas do risco, visando prevenir sua ocorrência (ex.: requisitos, checklist, capacitação de servidores, etc.). Os controles de atenuação e recuperação são executados após a ocorrência do risco com o intuito de diminuir o impacto de suas consequências (ex.: plano de contingência, tomada de contas especiais, procedimento apuratório, etc.);

X. **Fator de Avaliação dos Controles:** pontuação atribuída a partir do julgamento da efetividade dos controles existentes conforme os critérios estabelecidos;

XI. **Risco residual:** nível de risco que se espera atingir com a implantação de novos controles propostos pela avaliação de riscos, obtido por meio da pontuação resultante da multiplicação do risco inerente pelo fator de avaliação dos controles.

Para cada evento identificado, a equipe técnica deve calcular o nível de risco, a partir dos critérios de probabilidade e de impacto, conforme demonstrado abaixo:

Escala da Probabilidade		
Classificação	**Descrição**	**Nível (peso)**
Muito Baixa	Evento extraordinário.	1
Baixa	Evento casual, inesperado. Existe histórico de ocorrência.	2
Média	Evento esperado de frequência reduzida. Histórico parcialmente conhecido.	3
Alta	Evento usual de frequência habitual. Histórico amplamente conhecido.	4
Muito Alta	Evento que se repete seguidamente. Interfere no ritmo das atividades.	5

Quadro 4: Escala de Probabilidade

Escala da Impacto		
Classificação	**Descrição**	**Nível (peso)**
Muito Baixa	Não afeta os objetivos.	1
Baixa	Afeta, de forma pequena, o alcance dos objetivos.	2
Média	Torna incerto e duvidoso o alcance do objetivo.	3
Alta	Torna improvável o alcance do objetivo, em vista de caracterizar-se por impacto de difícil reversão.	4
Muito Alta	Capaz de impedir o alcance do objetivo.	5

Quadro 5: Escala de Impacto

A multiplicação entre os valores de probabilidade e impacto irá definir o nível de risco, ou seja, o provável impacto nos objetivos do processo organizacional

NR = NP x NI	
NR	nível de risco
NP	nível de probabilidade do risco
NI	nível de impacto do risco

A partir do resultado do cálculo, o risco pode ser classificado dentro das seguintes faixas:

CLASSIFICAÇÃO DOS RISCOS	
Classificação	**Faixa**
Risco Baixo - RB	1 a 2
Risco Médio - RM	3 a 6
Risco Alto - RA	8 a 12
Risco Crítico - RC	15 a 25

Quadro 6: Cálculo de riscos organizacionais

A seguir, a Matriz de Probabilidade X Impacto representa os possíveis resultados da combinação das escalas de probabilidade e impacto dos eventos:

Matriz Probabilidade x Impacto						
IMPACTO	**Muito Alto 5**	5 RM	10 RM	15 RA	20 RC	25 RC
	Alto 4	4 RB	8 RM	12 RA	16 RA	20 RC
	Médio 3	3 RB	6 RM	9 RM	12 RA	15 RA
	Baixo 2	2 RB	4 RB	6 RM	8 RM	10 RM
	Muito Baixo 1	1 RB	2 RB	3 RB	4 RB	5 RM
Legenda do Nível de Risco Crítico Alto Médio Baixo		**Muito Baixa 1**	**Baixa 2**	**Média 3**	**Alta 4**	**Muito Alta 5**
		PROBABILIDADE				

Quadro 7: Matriz de riscos probabilidade x impacto

Após a identificação e classificação dos riscos conforme a matriz de probabilidade e impacto, deve-se avaliar os controles existentes a fim de verificar a eficácia desses na mitigação dos riscos identificados e aferir o risco residual. Assim, nessa terceira etapa, devemos avaliar o risco inerente, os controles e o risco residual.

No quadro abaixo, são apresentados os fatores de avaliação dos controles internos existentes a serem considerados nessa etapa:

Descrição	Classificação
Controles existentes mal desenhados ou mal implantados, isto é, não funcionais.	**Inexistente**
Controles têm abordagens ad hoc (provisórias/pontuais), tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	**Fraco**
Controles implementados que mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a eficiências no desenho ou nas ferramentas utilizadas.	**Mediano**
Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	**Satisfatório**
Controles implementados que podem ser considerados a “melhor prática”, mitigando todos os aspectos relevantes do risco.	**Forte**

Quadro 8: Fatores de avaliação dos controles internos existentes

Ademais, o valor do risco residual é identificado por meio da multiplicação do valor do risco inerente x o fator de avaliação dos controles, podendo ser reclassificado no Mapa de Riscos.

RISCO RESIDUAL
=
RISCO INERENTE X FATOR DE AVALIAÇÃO DOS CONTROLES

Ressalta-se que nem todos os riscos precisam e/ou devem ser controlados. Quando a probabilidade de um risco é baixa e o impacto nos objetivos organizacionais (em decorrência do risco) também é baixo, pode-se aceitar o risco e não estabelecer controles.

Outrossim, o mapa de riscos deverá ser ajustado após a avaliação dos controles existentes para os riscos em análise, tendo em vista que o nível de risco estabelecido a partir da análise servirá como referência para o planejamento, priorização e avaliação dos riscos em comparação aos limites de exposição a risco definidos.

Essa fase também compreende comparar o nível do risco identificado com o limite de exposição a riscos definidos pela organização. O limite de exposição a riscos estabelece quais riscos devem ser aceitos, tratados, monitorados ou não tolerados. Os controles planejados para tratamento dos riscos inerentes devem ter potencial para reduzir os riscos residuais a níveis aceitáveis.

Portanto, envolve comparar os níveis de risco identificados com os limites de exposição aos riscos estabelecidos pela SEFIN. Com base nessa comparação, decide-se quais riscos devem ser aceitos, mitigados, compartilhados, monitorados ou evitados.

Ato contínuo, os limites de exposição a risco a serem observados na avaliação dos riscos estão estabelecidos abaixo por categoria de risco, bem como os parâmetros para a tomada de decisão em relação à aceitação, à mitigação ou ao tratamento dos riscos. Esses limites foram definidos conforme a criticidade dos riscos e seu impacto potencial sobre a missão, os objetivos estratégicos e a continuidade operacional da instituição, conforme demonstrado na tabela a seguir:

CATEGORIA	LIMITE DE EXPOSIÇÃO	AÇÃO NEESSÁRIA
Estratégicos	Risco classificado como "Alto" ou "Crítico" (pontuação > 12 na matriz de risco).	Implementar plano de contingência e ações corretivas imediatas; reportar ao Comitê de Gestão de Riscos.
Orçamentários e Financeiros	Variações dentro da margem de erro prevista nas metas fiscais são consideradas Médias; descumprimento da Lei de Responsabilidade Fiscal (LRF), queda severa de arrecadação ou aumento abrupto das despesas obrigatórias são “Altos”.	Avaliação das metas fiscais, ajustes nos fluxos de caixa, revisão de cenários e contenção de despesas.
Contábeis	Eventos que impactem mais de 2% do orçamento contratual ou envolvam fraude, corrupção ou erro material relevante são considerados "Altos" ou "Críticos".	Reforço dos controles contábeis e conciliação periódica de contas; comunicação imediata à alta gestão em caso de inconsistências relevantes.
Patrimoniais	Riscos que possam causar perda, deterioração, desvio de finalidade ou sanções legais relevantes são considerados "Altos" ou "Críticos".	Ações imediatas de correção e apuração; revisão periódica da conformidade legal e inventário patrimonial.
De contratações públicas	Qualquer evento que comprometa a integridade do processo ou gere dano à imagem institucional será classificado como "Crítico".	Investigação imediata; comunicação à Assessoria Jurídica e Comissão de Ética; revisão dos controles contratuais.
De convênios	Desvios na aplicação de recursos, inadimplência ou falhas na prestação de contas superiores a 5% do valor conveniado são classificados como “Altos”.	Revisão dos controles de repasse, capacitação dos gestores, bloqueio preventivo e instauração de apuração.
Operacionais	1. Incidentes que afetam a continuidade de serviços essenciais ou resultem em interrupções superiores a 24h são considerados “Altos” ou “Críticos”.	Implantação de plano de continuidade; revisão de sistemas e fluxos operacionais; plano de recuperação de desastres.
	2. Indícios de condutas irregulares, conflito de interesse, fraude ou corrupção são considerados “Críticos”, mesmo sem impacto financeiro imediato.	Ação imediata de apuração, aplicação de sanções disciplinares e revisão dos controles internos preventivos.
	3. Descumprimento reiterado de normas legais, regulamentos internos ou recomendações de controle é considerado “Alto”.	Adequação normativa, responsabilização funcional e reforço da capacitação das unidades envolvidas.

Quadro 9: Limites de exposição a riscos

Os limites de exposição admitem a aceitação de riscos classificados até o nível médio, desde que monitorados e devidamente justificados pelas unidades responsáveis. Riscos classificados como alto ou crítico deverão ser obrigatoriamente tratados com medidas corretivas ou mitigadoras, conforme plano de ação específico, sob acompanhamento do Núcleo de Gerenciamento de Riscos e reporte ao Comitê de Gestão de Riscos.

Como resultado desta etapa, deve ser elaborado o mapa de riscos da unidade, conforme o modelo da tabela a ser disponibilizado pelo Núcleo de Gerenciamento de Riscos da SEFIN.

Etapa 4: tratamento de riscos (Plano de Ação)

Etapa em que, a cada risco identificado e avaliado, poderaão ser elaboradas propostas de ação com medidas (respostas ao risco) para sua mitigação, na forma de Plano de Ação. O nível do risco pode ser modificado por meio de medidas de resposta ao risco que mitiguem, transfiram ou evitem esses riscos. Somente devem ser objeto de tratamento os riscos priorizados.

A identificação das medidas de resposta ao risco, assim como a identificação de riscos, deve ser realizada em oficinas de trabalho ou, conforme o caso, pelo próprio gestor do risco, com a participação de pessoas que conheçam bem o objeto de gestão de riscos.

Assim, nessa fase, devem ser levados em conta os valores dos níveis de riscos residuais obtidos na etapa 4 (análise de riscos), a fim de identificar quais riscos terão prioridade para tratamento e o tipo de resposta apropriada para cada situação. Ademais, devem ser analisados e priorizados os riscos residuais, em que todos os riscos, cujos níveis estejam aceitáveis (BAIXO e MÉDIO), podem ser aceitos, e uma possível priorização para tratamento deve ser justificada. Os riscos fora dos níveis aceitáveis (ALTO e CRÍTICO) deverão ser tratados e monitorados, e uma possível inexistência de tratamento deve ser justificada, conforme o quadro abaixo:

CLASSIFICAÇÃO	AÇÃO NECESSÁRIA	EXCEÇÃO
Risco baixo	Nível de risco dentro do apetite a risco, mas é possível existirem oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custo x benefício, como diminuir o nível de controles.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Médio	Nível de risco dentro do apetite a risco, mas é possível existirem oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custo x benefício, como diminuir o nível de controles.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Alto	Nível de risco além do apetite a risco. Os riscos nesse nível devem ser comunicados ao dirigente máximo da unidade, e ter uma ação tomada para implementação de controles imediatos e com período determinado.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.

CLASSIFICAÇÃO	AÇÃO NECESSÁRIA	EXCEÇÃO
Risco Crítico	Nível de risco muito além do apetite a risco. Os riscos nesse nível devem ser objeto do Cálculo do Nível de Riscos e ser comunicados ao Comitê de Gestão de Risco e ao dirigente máximo da unidade, com uma resposta imediata. Postergação de medidas apenas com autorização desse Comitê.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo dirigente máximo da unidade e pelo Comitê de Gestão de Riscos.

Quadro 10: Atuação conforme classificação

O tratamento de riscos envolve a seleção de uma ou mais opções para modificar os riscos e a implementação dessas opções. Uma vez implementado, fornece novos controles ou modifica os existentes. Assim, as respostas a riscos dizem respeito aos controles internos (procedimentos e normas estabelecidas pela SEFIN) ajustados ou criados pelos gestores em um Plano de Ação (Plano de Tratamento de Riscos), identificando os responsáveis pelas medidas a serem implementadas e os prazos para implementação.

As opções de tratamento (respostas aos riscos) são as estabelecidas no quadro abaixo:

Opções de tratamento	Descrição
Mitigar	Mitigar um risco significa implementar controles que possam diminuir as causas ou as consequências dos riscos, identificadas na etapa de identificação e análise de riscos. Um risco é normalmente mitigado quando é classificado como "Alto" ou "Crítico". A implementação de controles, neste caso, apresenta um custo/benefício adequado.
Transferir (compartilhar)	Um risco é normalmente compartilhado quando é classificado como “Alto” ou “Crítico”, mas a implementação de controles não apresenta um custo/benefício adequado. Pode-se compartilhar o risco por meio de terceirização ou apólice de seguro (seguro de vida), por exemplo.
Evitar	Um risco é normalmente evitado quando é classificado como “Alto” ou “Crítico”, e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco com a SEFIN. Evitar o risco significa encerrar o processo, objetivo ou projeto organizacional. Nesse caso, essa opção deve ser aprovada pelo Comitê de Gestão de Riscos da secretaria.
Aceitar	Um risco é normalmente aceito quando seu nível está nas faixas de apetite a risco. Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco.

Quadro 11: Possibilidades de tratamento dos riscos

Neste contexto, a seta “Implementação do Plano de Ação” no processo de gestão de riscos tem a função de representar o esforço necessário para o desenvolvimento e implementação das respostas que ainda não estão em vigor. Ou seja, enquanto a fase 4 marca o momento de decisão sobre como tratar o risco, a seta externa indica que, caso a resposta necessária ainda não esteja implementada, será elaborado um plano de ação para viabilizar essa implementação.

Assim, as duas representações coexistem com funções

distintas:

- No ciclo interno, indica-se o ponto em que se avaliam e definem as respostas necessárias;

- Na seta externa, destaca-se o fluxo de implementação daquelas respostas que exigem ações adicionais para serem efetivadas.

Essa separação é relevante para garantir clareza metodológica e apoiar o acompanhamento da execução das ações planejadas.

Etapa 5: monitoramento e comunicação

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

a. auxiliar a estabelecer o contexto apropriadamente e assegurar que as visões e percepções das partes interessadas, incluindo necessidades, suposições, conceitos e preocupações sejam identificadas, registradas e levadas em consideração;

b. auxiliar a assegurar que os riscos sejam identificados e analisados adequadamente, reunindo áreas diferentes de especialização; e

c. garantir que todos os envolvidos estejam cientes de seus papéis e responsabilidades, e avalizem e apoiem o tratamento dos riscos.

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

De acordo com a ISO 31000/18, o monitoramento é parte integrante e essencial da gestão de riscos, cuja finalidade é:

a. detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco e no próprio risco, que podem requerer revisão dos tratamentos atualmente adotados e suas prioridades, e levar à identificação de riscos emergentes;

b. obter informações adicionais para melhorar a política, a estrutura e o processo de gestão de riscos;

c. analisar eventos - incluindo os "quase incidentes", mudanças, tendências, sucessos e fracassos e aprender com eles; e

d. garantir que os controles sejam eficazes e eficientes no desenho e na operação.

As competências e responsabilidades pelo monitoramento do Plano de Gestão de Riscos da SEFIN são apresentadas no quadro abaixo:

Aspectos a serem monitorados	Núcleo de Gerenciamento de Riscos (NGR)	Coordenadores setoriais	Servidores envolvidos
Execução do Plano de Gestão de Riscos	• Requisitar aos responsáveis pela gestão de riscos dos processos organizacionais as informações necessárias para a consolidação dos dados e a elaboração de relatórios gerenciais; e	• Validar e monitorar, no seu âmbito de atuação, a execução do Plano de gestão de Riscos e das medidas decorrentes de sua implementação;	-
	• Consolidar os resultados das diversas áreas em relatórios gerenciais	• Manter atualizadas as informações relativas à execução das medidas de tratamento de riscos.	
Riscos identificados	Solicitar às unidades informações sobre o andamento das etapas referentes ao gerenciamento de riscos.	Monitorar, ao longo do tempo, os riscos mapeados a partir das informações fornecidas pelos gestores responsáveis pelo gerenciamento de riscos, de modo a garantir que as respostas adotadas resultem na manutenção dos riscos em níveis aceitáveis.	Reportar imediatamente ao responsável pelo gerenciamento de riscos do processo qualquer mudança que possa requerer revisão dos controles e/ou do Plano de Tratamento.
Controles Internos	• Realizar o acompanhamento da implementação dos controles internos definidos em cada unidade da SEFIN; e	Propor respostas e respectivas medidas de controle a serem implementadas nos processos organizacionais sob sua responsabilidade.	Implementar os controles internos estabelecidos.
	• Dar suporte aos gestores (1ª linha) na implementação e monitoramento contínuo dos controles internos destinados a tratar os riscos identificados.		
Níveis de riscos	Monitorar a evolução dos níveis de riscos, considerando o monitoramento realizado pelos setores da secretaria.	Monitorar a evolução dos níveis de riscos nos processos organizacionais sob sua responsabilidade.	Participar nos processos em que estiverem envolvidos.
Planos de ações de medidas de controle	Monitorar as medidas de controle implementadas para tratamento de riscos, considerando o monitoramento realizado pelas unidades.	Monitorar a evolução da da implementação das medidas de controles dos riscos organizacionais sob sua responsabilidade.	Participar nos processos em que estiverem envolvidos.

Quadro 12: Competências e responsabilidades das unidades

Ademais, a norma ISO 31000/2018 ressalta a importância da Alta Administração assegurar a atribuição das instâncias e responsabilidades vinculadas à gestão de risco a todas as autoridades pertinentes, com a comunicação e divulgação em todos os níveis da organização.

Assim, para assegurar a responsabilidades dos atores do processo de gestão de riscos na SEFIN, será utilizada a Matriz RACI (acrônimo para Responsável (Responsible), Autoridade (Accountable), Consultado (Consulted) e Informado (Informed), a qual constitui um instrumento gráfico que permite definir os responsáveis pela execução do gerenciamento de riscos, quem deve assumir as consequências, quem deve ser consultado e quem deve ser informado, de forma tempestiva e eficaz.

Dessa forma, a matriz de responsabilidades da SEFIN será aplicada da seguinte maneira:

MATRIZ DE RESPONSABILIDADES							
ATIVIDADE	**RESPONSÁVEIS**						
	Secretário de Finanças	**Comitê de Gestão de Riscos**	**Núcleo de Gerenciamento de Riscos (NGR)**	**Controladoria Interna / Núcleo de Avaliação de Controles Internos (NACIN)**	**Coordenadores setoriais de Gerenciamento de Riscos**	**Gestores de riscos e demais servidores**	**Diretoria Executiva**
Garantir o apoio para promover as ações institucionais de estruturação do sistema e política de gestão de riscos, e o desenvolvimento contínuo dos servidores da área de gestão de riscos.	RESPONSÁVEL	CONSULTADO	CONSULTADO				INFORMADO
Aferir a efetividade do gerenciamento de riscos, fornecendo ao Secretário e ao Comitê de Gestão de Riscos avaliações abrangentes e independentes.	AUTORIDADE	INFORMADO	CONSULTADO	RESPONSÁVEL	CONSULTADO		INFORMADO
Orientar e propor as áreas responsáveis pelos riscos no desenvolvimento e implementação de processos e controles para mitigar os riscos.			CONSULTADO	RESPONSÁVEL	INFORMADO	INFORMADO	
Definir os níveis de apetite a riscos e a periodicidade máxima do ciclo do processo de gerenciamento de riscos	AUTORIDADE	RESPONSÁVEL	CONSULTADO		INFORMADO	INFORMADO	CONSULTADO
Propor a revisão de Política de Gestão de Riscos e Metodologia para o Processo de Gerenciamento de Riscos, bem como melhorias futuras.		CONSULTADO	RESPONSÁVEL	INFORMADO	INFORMADO	INFORMADO	AUTORIDADE
Coordenar e assessorar a implementação e a operação do Sistema de Gestão de Riscos.		CONSULTADO	RESPONSÁVEL		INFORMADO	INFORMADO	AUTORIDADE
Identificar, analisar, avaliar os riscos, elaborar e implementar plano de tratamento dos riscos.		CONSULTADO	CONSULTADO		RESPONSÁVEL	RESPONSÁVEL	INFORMADO
Coordenar e apoiar os gestores de riscos vinculados à área de atuação, no processo de Gerenciamento dos riscos, elaboração de planos de tratamento e acompanhar a evolução da implementação das medidas de controle.			CONSULTADO		RESPONSÁVEL		AUTORIDADE
Monitorar a evolução da implantação dos planos de tratamento dos riscos junto aos coordenadores setoriais.	INFORMADO	INFORMADO	RESPONSÁVEL		CONSULTADO		INFORMADO
Acompanhar a evolução da implementação das medidas de controle relacionados aos riscos da área de atuação junto às unidades e gestores de riscos.			CONSULTADO		RESPONSÁVEL	RESPONSÁVEL	AUTORIDADE

Legenda:
AUTORIDADE: quem valida a tarefa ou produto (pode delegar a função, mas mantém a responsabilidade);
RESPONSÁVEL: quem realiza a atividade;
CONSULTADO: quem fornece informações importantes ou que pode agregar valor à implementação do processo;
INFORMADO: quem deve ser comunicado dos resultados ou ações tomadas, mas não precisa participar da decisão.

Quadro 13: Matriz de responsabilidades aplicada à gestão de riscos

Com base nas tabelas acima, as unidades da SEFIN deverão monitorar os riscos de suas competências de forma contínua e sistemática, com foco na avaliação da efetividade das ações de tratamento adotadas, da atualização dos riscos mapeados e da adequação dos controles implementados. Além disso, o NGR atuará como segunda linha, fornecendo suporte para gestão de riscos eficaz e eficiente e monitorando ações e atividades por meio de relatórios periódicos.

No que se refere às ações e atividades, serão monitoradas pelo NGR por meio do seguinte rito:

as unidades preencherão a planilha de gestão de riscos a ser disponibilizada pelo NGR por meio de um sistema próprio, o qual será continuamente atualizado para atender mudanças culturais e normativas internas e externas quanto ao gerenciamento de riscos;

os resultados deverão ser formalizados no sistema SEI! e encaminhados ao NACIN, para consolidação e reporte à Alta Administração, ao Comitê de Governança e aos órgãos de controle, quando aplicável.

O relatório do monitoramento do NGR será realizado semestralmente, baseado nas informações de atividades gerenciais contínuas (pelos próprios gestores de riscos, no âmbito dos seus processos); avaliações independentes (realizadas pela Controladoria Geral do Estado) e ações de competência do Núcleo de Acompanhamento de Controles Internos (NACIN). Assim, será possível identificar possíveis falhas nas etapas anteriores e componentes que estruturam o gerenciamento de risco, bem como avaliar se os riscos que haviam sido identificados continuam no mesmo grau de importância.

Dessa forma, a frequência pela qual o NGR e o NACIN apresentarão tais relatórios seguirá os seguintes parâmetros:

TIPO DE AVALIAÇÃO	PERIODICIDADE	OBSERVAÇÕES
Ordinária	Semestral	Para riscos estratégicos e críticos
Anual	Anual	Todos os riscos registrados deverão ser reavaliados
Extraordinária	Sempre que necessário	Situações imprevistas, mudanças estruturais ou normativas

Ademais, a efetividade no alcance das ações propostas deverá ser realizada com base em indicadores definidos em plano de ação de riscos e subsidiado por relatórios técnicos das unidades gestoras.

Para auxiliar na visualização, entendimento de dados e processo de tomada de decisão, serão criados dashboards interativos para visualização dinâmica de indicadores, de forma a segmentar dados por filtros (como período e tipo de processo), realizar análises comparativas e drill-down, além de análises preditivas para identificar padrões e detectar possíveis inconsistências.

VIGÊNCIA E ATUALIZAÇÃO

da Metodologia de Gestão de Riscos

A presente metodologia poderá ser revista e atualizada periodicamente, com vistas ao seu aprimoramento contínuo e à incorporação de boas práticas, inovações tecnológicas ou alterações normativas.

Sugestões de aprimoramento poderão ser encaminhadas pelas unidades ao NGR, o qual avaliará a viabilidade técnica e a necessidade de atualização da metodologia, mediante aprovação do Comitê de Gestão de Riscos.

DISPOSIÇÕES

Finais

Esta metodologia entra em vigor na data de sua aprovação por meio de portaria, e deverá ser amplamente divulgada às unidades da Secretaria de Estado de Finanças, com vistas à sua implementação integral e gradativa.

As situações omissas serão resolvidas pelo Núcleo de Gestão de Riscos, em articulação com o Comitê de Gestão de Riscos, sempre que necessário.

Referências

ABNT. **Gestão de Riscos – Princípio e diretrizes. NBR ISO 31000**. Associação Brasileira de Normas Técnicas. 2018.

ABNT. **Gestão de Riscos – Técnicas para o processo de avaliação de riscos**. NBR ISO 31010. Associação Brasileira de Normas Técnicas. 2021.

ABNT. **Gestão de Riscos – Vocabulário. NBR ISO 31073**. Associação Brasileira de Normas Técnicas. 2022.

BRASIL. I**nstrução Normativa Conjunta MP/CGU N.º 01**, de 10 de maio de 2016, que estabelece a adoção de uma série de medidas para a sistematização de práticas relacionadas a gestão de riscos, controles internos e governança.

BRASIL. Controladoria-Geral da União. **Metodologia de Gestão de Riscos**. Abril de 2021.

BRASIL. Ministério da Transparência e Controladoria-Geral da União. **Gestão de Riscos e Controles Internos no Setor Público**. Abril de 2017.

BRASIL. Tribunal de Contas da União. **Gestão de Riscos – Avaliação da Maturidade. Janeiro de 2018**.

COSO. Committee of Sponsoring Organizations of the Treadway Commission. **Gerenciamento de Riscos Corporativos – Estrutura Integrada. 2017**.

COSO. Committee of Sponsoring Organizations of the Treadway Commission. **Risk Assessment in Practice**.

IIA. The Institute of Internal Auditors. **Modelo das 3 três linhas do IIA 2020 – Uma atualização das três linhas de defesa**.

FONTENELLE, Rodrigo. **Implementando a Gestão de Riscos no Setor Público**. Editora Fórum, 3ª Edição. Brasília. 2024.

CONTROLADORIA-GERAL DO ESTADO DE MINAS GERAIS. **Guia Metodológico de Gestão Integrada de Riscos**. Belo Horizonte: CGE-MG, 2024. Disponível em: https://cge.mg.gov.br/download/category/34-manuais-e-cartilhas. Acesso em: 16/07/2025.