PARANÁ
GOVERNO DO ESTADO
SECRETARIA DA FAZENDA

DESENVOLVIMENTO

DE METODOLOGIA

SERVIÇOS DE CONSULTORIA PARA IMPLANTAÇÃO DE SISTEMÁTICA DE GESTÃO DE RISCOS NA SEFA/PR

CONTRATO: Nº 2970/2022-SEFA/PR

Sumário

1. APRESENTAÇÃO

Este documento apresenta os fundamentos, a estrutura e a Metodologia de Gestão de Riscos da Secretaria da Fazenda do Estado do Paraná (SEFA/PR), com o objetivo de orientar a implementação da Política de Gestão de Riscos (PGR) da SEFA/PR, publicada por meio da Resolução nº 1298/2022.

Conforme conceito registrado na PGR da SEFA/PR, a Gestão de Riscos é composta por uma arquitetura (princípios, objetivos, estrutura, competências e processo) necessária para gerenciar riscos de maneira eficaz.

1.1 Composição do Documento:

- Fundamentos da Gestão de Riscos SEFA/PR, contendo os conceitos básicos, os referenciais legais e teóricos, bem como os princípios e objetivos que norteiam a Gestão de Riscos da SEFA/PR;
- Estrutura da Gestão de Riscos da SEFA/PR, onde são apresentadas as competências e responsabilidades, a forma de integração dos processos organizacionais, os recursos necessários e os mecanismos de comunicação para a Gestão de Riscos;
- Metodologia de Gestão de Riscos da SEFA/PR, com detalhes das etapas do processo de gerenciamento de riscos e acompanhamento das ações de mitigação.
- As demais informações operacionais, referentes à Gestão de Riscos da SEFA/PR, serão apresentadas no manual de gestão de riscos.

2. FUNDAMENTOS DA GESTÃO DE RISCOS DA SEFA-PR

2.1 Parâmetros Legais e *Framework*

A construção desta metodologia se baseou na legislação vigente e em referenciais teóricos como normas, regulamentos e modelos, a seguir discriminados, constituindo um *framework* de gestão de risco.

2.1.1 *COSO*

No ano de 1992, por meio do guia *Internal Control – Integrated Framework,* publicado pelo *Committee of Sponsoring Organizations of the Treadway Commission (COSO)*, a gestão de riscos tomou ênfase nas organizações que passaram a ser orientadas para o aprimoramento dos sistemas de controle interno. O *COSO*, estabelece que esses sistemas são formados por componentes integrados, incluindo a avaliação de riscos. Em 2004, com ênfase na avaliação de riscos foi publicado pelo COSO o Enterprise *Risk Management - Integrated Framework* (COSO-ERM), que sugere componentes, princípios e conceitos para a gestão de riscos corporativos.

2.1.2 ISO 31000:2018

Foi utilizada também a norma da Associação Brasileira de Normas Técnicas (ABNT) Norma Brasileira Regulamentadora (NBR) ISO 31000:2018 Gestão de Riscos – Diretrizes, que fornece diretrizes para gerenciar riscos enfrentados pelas organizações e pode ser personalizada para qualquer organização e seu contexto.

2.1.3 Modelo de Linhas de Defesa

O Modelo de Linhas de Defesa do *Institute of Internal Audit* (IIA) 2020, ajuda as organizações a identificar estruturas e processos que melhor auxiliam no atingimento dos objetivos e facilitam uma forte governança e gerenciamento de riscos. O modelo é aplicável a todas as organizações.

3. TERMOS, CONCEITOS E DEFINIÇÕES

Esse documento considera os termos, conceitos e definições a seguir descriminados, extraídos da PGR da SEFA/PR, NBR ISO 31000:2018, do COSO e do IIA.

Apetite a risco: nível de risco que uma organização está disposta a aceitar;

Controle: medida que está mantendo e/ou modificando o risco. Os controles incluem, mas não estão limitados a qualquer processo, política, dispositivo, prática ou outras ações que mantém e/ou modificam o risco. Os controles nem sempre conseguem exercer o efeito de modificação pretendido ou presumido;

Controle interno da gestão: processo que engloba o 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 de que os objetivos organizacionais serão alcançados;

Consequência: resultado de um evento que afeta os objetivos. Uma consequência pode ser certa ou incerta e pode ter efeitos positivos ou negativos, diretos ou indiretos nos objetivos. As consequências podem ser expressas qualitativa ou quantitativamente. Consequências podem escalar por meio de efeitos cascata e cumulativos;

Evento: a ocorrência ou mudança em um conjunto específico de circunstâncias. Um evento pode consistir em uma ou mais ocorrências e pode ter várias causas e várias consequências. Um evento pode também ser algo que é esperado, mas não acontece, ou algo que não é esperado, mas acontece. Um evento pode ser uma fonte de risco.

Fonte de risco: elemento que, individualmente ou combinado, tem o potencial para dar origem ao risco, pode ser relacionado a um problema ou fragilidade existente no processo;

Gerenciamento de risco: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações e fornecer segurança razoável no alcance dos objetivos organizacionais;

Gestão de riscos: São atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos, composta por uma arquitetura (princípios, objetivos, estrutura, competências e processo) necessária para se gerenciar riscos eficazmente;

Gestor do risco: servidor com responsabilidade e autoridade para gerenciar um risco ou processo;

Governança: combinação de processos e estruturas implantadas pela alta administração da organização, para informar, dirigir, administrar, avaliar e monitorar atividades organizacionais, com o intuito de alcançar os objetivos e prestar contas das atividades para a 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; e

Meta: alvo ou propósito com que se define um objetivo a ser alcançado;

Objetivo organizacional: situação que se deseja alcançar de forma a se evidenciar êxito no cumprimento da missão e no atingimento da visão de futuro da organização;

Parte interessada: pessoa ou organização que pode afetar, ser afetada, ou perceber–se afetada por uma decisão ou atividade;

Probabilidade: chance de algo acontecer, pode ser objetiva ou subjetiva, quantitativa ou qualitativa, descrita a partir de termos matemáticos ou gerais. Na terminologia de gestão de riscos, a palavra “probabilidade” é utilizada para referir-se à chance de algo acontecer, não importando se definida, medida ou determinada, ainda que objetiva ou subjetivamente, qualitativa ou quantitativamente, e se descrita utilizando-se termos gerais ou matemáticos (como probabilidade ou frequência durante um determinado período de tempo);

Processo: conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar produto, resultado ou serviço predefinido;

Risco: efeito da incerteza nos objetivos. Um efeito é um desvio em relação ao esperado, que pode ser positivo, negativo ou ambos. Os objetivos podem ter diferentes aspectos (como financeiros, de saúde, segurança, ambientais entre outros) e podem ser aplicar em diferentes níveis da organização (estratégico, tático, operacional, projeto, produto e processo) e são usualmente expressos em termos de fontes de risco, eventos potenciais, suas consequências e suas probabilidades;

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.

4. OBJETIVOS E PRINCÍPIOS

4.1. Objetivos da gestão de riscos

Essa metodologia observa os objetivos da Gestão de Riscos na SEFA/PR, estabelecido na Política de Gestão de Riscos, por meio da Resolução 1298/2022, descritos no art. 6º - A Gestão de Riscos tem por objetivos:

I Aumentar a probabilidade de atingimento dos objetivos estratégicos;

II Fomentar a gestão proativa e a inovação;

III Identificar e tratar riscos em todas as áreas da Secretaria;

IV Facilitar a identificação de oportunidades e ameaças;

V Prezar pelas conformidades legal e normativa dos processos organizacionais;

VI Melhorar a prestação de contas à sociedade;

VII Melhorar a governança;

VIII Estabelecer uma base confiável para a tomada de decisão e o planejamento;

IX Melhorar o controle interno da gestão;

X Alocar e utilizar eficazmente os recursos para o tratamento de riscos;

XI Melhorar a eficácia e a eficiência operacional;

XII Melhorar a prevenção de perdas e a gestão de incidentes;

XIII Minimizar perdas;

XIV Melhorar a aprendizagem organizacional; e

XV Aumentar a capacidade da organização de se adaptar a mudanças.

Observa também os objetivos da gestão de riscos da Instrução Normativa Conjunta nº 01/2016 da CGU e do MPOG, descritos no artigo 15.

I Assegurar que os responsáveis pela tomada de decisão, em todos os níveis do órgão ou entidade, tenham acesso tempestivo a informações suficientes quanto aos riscos aos quais está exposta a organização, inclusive para determinar questões relativas à delegação, se for o caso;

II Aumentar a probabilidade de alcance dos objetivos da organização, reduzindo os riscos a níveis aceitáveis;

III 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;

4.2. Princípios da gestão de riscos da SEFA/PR

Este documento observa os princípios estabelecidos no art. 4º, da PGR da SEFA/PR, alinhados à norma ABNT NBR ISO 31000:2018 e a seguir detalhados:

I Criação e proteção do valor público gerado: melhora o desempenho, encoraja a inovação e apoia o alcance de objetivos;

II Ser parte integrante dos processos organizacionais: integra todas as atividades da SEFA/PR;

III Ser sistemática, estruturada e abrangente: contribui para resultados consistentes e comparáveis;

IV Personalizada: é adequada e proporcional aos contextos externo e interno da SEFA/PR e relacionadas aos seus objetivos;

V Inclusiva: o envolvimento apropriado e oportuno das partes interessadas possibilita que seus conhecimentos, pontos de vista e percepções sejam considerados, que resulta na melhor conscientização e gestão de riscos fundamentada;

VI Dinamismo, iteração e capacidade de reagir a mudanças: antecipa, detecta, reconhece e responde as mudanças dos contextos externo e interno e aos eventos de maneira apropriada e oportuna;

VII Uso efetivo das melhores informações disponíveis e da transparência: considera quaisquer limitações e incertezas associadas a estas informações e expectativas. A informação deve ser oportuna, clara e disponível para a SEFA/PR e partes interessadas;

VIII Consideração dos fatores culturais, humanos e sociais: o comportamento humano e a cultura da SEFA/PR influenciam significativamente todos os aspectos da gestão de riscos em cada nível e estágio;

IX Melhoria institucional contínua: é melhorada continuamente por meio do aprendizado e experiências.

5. A ESTRUTURA DE GOVERNANÇA DA GESTÃO DE RISCOS DA SEFA/PR

Conforme a NBR ISO 3100:2018, o desenvolvimento da estrutura engloba integração, concepção, implementação, avaliação e melhoria da gestão de riscos através da organização.

A NBR ISO 3100:2018 trata, também, dos componentes da estrutura da gestão de riscos como: mandato e comprometimento, concepção da estrutura para gerenciar riscos, implementação da gestão de riscos, monitoramento e análise crítica da estrutura e melhoria contínua da estrutura.

Na estrutura da SEFA/PR o componente Mandato e Comprometimento é demonstrado pelas ações da alta administração e do Comitê de Gestão de Riscos, especialmente quanto ao patrocínio e à promoção do gerenciamento de risco da SEFA/PR, por meio da publicação da PGR da SEFA/PR, com a definição das competências e responsabilidades para o gerenciamento de riscos no âmbito do órgão, englobando assim a concepção da estrutura para gerenciar riscos.

No que tange ao monitoramento e à análise crítica da estrutura de gestão de riscos, fica estabelecido nesta metodologia que deve ser realizado, constantemente, por meio da comparação da Gestão de Riscos da SEFA/PR com as bases normativas, *frameworks*, contextos internos e externos, percepção das partes interessadas, com vistas à melhoria contínua da Gestão da Riscos.

5.1. Modelo de Três Linhas de Defesa

O Modelo de Três Linhas de Defesa, publicado pelo IIA, utilizado nas organizações como melhor prática de governança, estabelece a segregação das funções e das responsabilidades da gestão de riscos em três linhas de defesa. Neste modelo, a organização divide a responsabilidade da gestão de riscos em camadas. O modelo divide as funções que compõem o sistema de governança de riscos em três grupos:

- **primeira linha:** estão diretamente alinhados a entrega serviços e resultados, incluindo funções de apoio, responsáveis por identificar e tratar o risco diretamente por aqueles que executam o processo;
- **segunda linha:** fornecem assistência no gerenciamento de riscos, podendo ser atribuídos a especialistas, para fornecer conhecimentos complementares, apoio, monitoramento e questionamento àqueles com papéis de primeira linha. Os papéis de segunda linha podem se concentrar em objetivos específicos do gerenciamento de riscos, como: conformidade com leis, regulamentos e comportamento ético aceitável; controle interno; segurança da informação e tecnologia; sustentabilidade; e avaliação da qualidade. Como alternativa, os papéis de segunda linha podem abranger uma responsabilidade mais ampla pelo gerenciamento de riscos, como o gerenciamento de riscos corporativos (*enterprise risk management – ERM)*. No entanto, a responsabilidade pelo gerenciamento de riscos segue fazendo parte dos papéis de primeira linha e dentro do objetivo da gestão.
- **terceira linha:** prestam avaliação e assessoria independentes e objetivas sobre a adequação e eficácia da governança e do gerenciamento de riscos. Isso é feito através da aplicação competente de processos sistemáticos e disciplinados, expertise e conhecimentos. Reporta suas descobertas à gestão e ao órgão de governança para promover e facilitar a melhoria contínua. Ao fazê-lo, pode considerar a avaliação de outros prestadores internos e externos.

Fonte: Modelo de Três Linhas de Defesa - *The Institute of Internal Auditors,* 2020, adaptado.

A primeira linha de defesa é composta pelas unidades, gestores e servidores que são expostos diretamente ao risco por meio de seus processos. Atores dessa linha de defesa são responsáveis por manter controles eficazes e por conduzir procedimentos de gestão de riscos, por já estarem em contato direto com o processo.

Os responsáveis pela primeira linha de defesa identificam, avaliam, controlam e mitigam os riscos, com o desenvolvimento e a implementação de políticas, normas e procedimentos internos e assegurando que as atividades atendam objetivos estratégicos da SEFA/PR.

Por meio de uma estrutura de responsabilidades em camadas, os atores da primeira linha de defesa desenvolvem e implementam procedimentos detalhados que servem como controles e supervisionam a execução, no seu dia a dia, pelas equipes, incluindo terceiros.

A segunda linha de defesa, composta normalmente de áreas responsáveis pela supervisão da gestão de riscos específicos, tem o papel de atuar de forma transversal às áreas finalísticas, monitorando as ocorrências, a eficiência dos controles, os níveis de riscos e as perdas operacionais. Assim como apoiar os agentes da primeira linha de defesa, promover a educação dos gestores e padronizar os instrumentos utilizados para o gerenciamento de risco.

A terceira linha de defesa, composta pelas atividades independentes de avaliação e de consultoria realizada pela Secretaria de Transparência e Controle (STC) do Estado do Paraná, oferece avaliações independente e assessoramento à organização, destinados ao aprimoramento dos processos de gerenciamento de riscos, de controles internos, de integridade e de governança, de forma que controles mais eficientes e eficazes mitiguem os principais riscos que impedem os órgãos e as entidades de atingir seus objetivos estratégicos.

5.2. Responsabilidades e competências

As responsabilidades e competências são descritas nos capítulos VII e VIII da PGR da SEFA/PR, a seguir detalhadas as atividades de gerenciamento de risco para cada um dos atores integrantes da gestão de riscos dentro da Secretaria de Fazenda do Estado do Paraná:

Responsável	Descrição da atividade	Nível Linha de Defesa	Periodicidade
Todos os servidores e unidades da SEFA/PR	Monitoramento dos níveis de riscos e da efetividade das medidas de controles implementadas nos processos organizacionais, que estiverem envolvidos ou que tomarem conhecimento	Primeira	Permanente
	Cumprir as diretrizes da Política de Gestão de Riscos, da Metodologia de Gestão Risco e do Manual de Gestão de Riscos da SEFA/PR	Primeira	Permanente
Gestores das unidades estratégicas, táticas e operacionais	Difundir a importância da Gestão de Riscos na sua área, aculturando e disseminando responsabilidades e comprometimentos	Primeira	Permanente
	Registrar, monitorar e manter atualizada a Matriz de Riscos, a descrição dos processos, os fluxos e os controles sob sua responsabilidade	Primeira	Permanente
	Analisar sistematicamente os processos com o objetivo de identificar riscos existentes ou potenciais e propor planos de ação de mitigação	Primeira	Permanente
	Coletar, registrar, quantificar e informar os dados de perdas operacionais ocorridas nos processos	Primeira	Permanente

Responsável	Descrição da atividade	Nível Linha de Defesa	Periodicidade
	Assegurar a existência de informações abrangentes, adequadas, confiáveis, oportunas e acessíveis sobre os riscos pertinentes, reportando-as tempestivamente às unidades de segunda linha de defesa	Primeira	Permanente
	Formalizar a conformidade de novos produtos, serviços e sistemas com abordagem baseada em gerenciamento de riscos	Primeira	Permanente
	Elaborar e atualizar Plano de Tratamento de risco e melhoria de controles	Primeira	Permanente
Secretário da fazenda; Diretoria-Geral; Diretoria da Receita Estadual; Gabinete da Secretaria; Assessoria de TI; Assessoria Técnica; Diretoria do Tesouro; e Diretoria de Orçamento; e Diretoria de Contabilidade; e Assessoria de Modernização Fazendária.	Gerir os riscos de forma transversal às diversas unidades	Segunda	Permanente
	Dar suporte na análise de riscos transversais	Segunda	Permanente
	Definir controles de monitoramento de riscos transversais	Segunda	Permanente
	Monitorar riscos e controles de forma consolidada	Segunda	Permanente
	Elaborar e revisar indicadores de riscos em segunda linha de defesa	Segunda	Semestral
	Gerar reportes para Comitê de Gestão de Riscos	Segunda	Semestral
Assessoria de Modernização Fazendária	Divulgar e propor melhorias para a Política de Gestão de Riscos na SEFA/PR e a Metodologia de Gestão de Riscos da SEFA/PR	Primeira/Segunda	Permanente
	Elaborar e manter atualizado os manuais, procedimento e instrumentos apropriados que possibilitem a identificação, a avaliação, a mitigação, o controle e o reporte do risco e permitam a análise de impacto, elaboração, implantação, teste e monitoramento de planos de contingência	Primeira/Segunda	Permanente
	Assegurar que a cultura da Gestão de Risco seja difundida de forma ampla e completa entre todos os servidores da SEFA/PR	Primeira/Segunda	Permanente

Responsável	Descrição da atividade	Nível Linha de Defesa	Periodicidade
	Mensurar, reportar o grau de riscos assumidos pela SEFA/PR e submeter ao Comitê de Gestão de Riscos os limites consistentes com o apetite a riscos	Primeira	Semestral
	Elaborar o caderno de riscos que apresentem os aspectos qualitativos e quantitativos dos Riscos Relevantes da SEFA/PR	Primeira	Bimestral
	Reportar ao Comitê Gestão de Risco o grau de aderência da SEFA/PR à Política de Gestão de Riscos	Primeira	Semestral
	Apoiar os gestores das unidades na identificação dos processos críticos e na avaliação, monitoramento e controle, por meio da implementação dos instrumentos de gerenciamento de risco da SEFA/PR	Primeira	Permanente
	Informar e responder dúvidas das Partes Interessadas sobre riscos	Primeira	Permanente
	Implantar e gerenciar processos e procedimentos de controle, para garantir a aderência às políticas internas e às regulamentações externas sobre o Gerenciamento do Risco	Primeira	Permanente
	Disponibilizar ao Comitê de Gestão de Riscos informações relacionadas a operações que possam expor a SEFA/PR a perdas operacionais ou disrupções de serviços, o impacto resultante e a alternativas de recuperação	Primeira	Permanente
	Apoiar a análise e decisão sobre a alocação de recursos necessários para a Estrutura de Gerenciamento de Riscos	Segunda	Permanente
	Difundir o conceito do Risco e consolidar o seu gerenciamento, que são únicos para toda a SEFA/PR	Primeira/Segunda	Permanente
	Implantar e gerenciar processos e procedimentos de controle, para garantir a aderência às políticas internas e às regulamentações externas sobre o Gerenciamento do Risco	Segunda	Permanente
	Interagir com todas as áreas da SEFA/PR para garantir a aplicação eficiente das metodologias, modelos e ferramentas adotados para a Gestão do Risco	Primeira/Segunda	Permanente

Responsável	Descrição da atividade	Nível Linha de Defesa	Periodicidade
	Avaliar a possibilidade de ocorrência das perdas operacionais, o impacto resultante e as alternativas de recuperação, por meio da identificação dos riscos das atividades	Segunda	Permanente
	Realizar treinamentos periódicos apropriados, sendo responsável pela disseminação da cultura, do conhecimento e das práticas sobre Riscos na SEFA/PR	Primeira	Permanente
	Avaliar e recomendar a alocação de recursos necessários para a Estrutura de Gerenciamento de Riscos	Primeira	Permanente
	Monitorar as recomendações e orientações deliberadas pelo Comitê de Gestão de Riscos da SEFA/PR	Segunda	Mensalmente
	Elaborar o Relatório Geral de Riscos da SEFA/PR	Primeira	Trimestral
	Acompanhar o ciclo anual de gerenciamento de riscos da SEFA/PR	Primeira	Permanente
Comitê de Gestão de Riscos	Aprovar política, diretrizes, metodologias e mecanismos para comunicação e institucionalização da gestão de riscos e dos controles internos	Comitê	Anual
	Supervisionar o mapeamento e avaliação dos riscos chave que podem comprometer a prestação de serviços de interesse público	Comitê	Permanente
	Liderar e supervisionar a institucionalização da gestão de riscos e dos controles internos, oferecendo suporte necessário para sua efetiva implementação no órgão ou entidade	Comitê	Permanente
	Estabelecer limites de exposição a riscos globais do órgão, bem com os limites de alçada a nível de unidade, política pública ou atividade	Comitê	Anualmente, ou a cada ciclo de gerenciamento de risco
	Aprovar e supervisionar o método de priorização de temas e macroprocessos para gestão de riscos e implementação dos controles internos da gestão	Comitê	Anualmente, ou a cada ciclo de gerenciamento de risco
	Avaliar o desempenho da gestão de riscos por meio da comparação entre as avaliações de risco e a base de ocorrências	Comitê	Semestral

Responsável	Descrição da atividade	Nível Linha de Defesa	Periodicidade
	Emitir recomendação para o aprimoramento da governança, da gestão de riscos e dos controles internos	Comitê	Permanente
	Revisar as alçadas decisórias e responsabilidades relacionadas à estrutura de Gestão de Riscos	Comitê	Anual
	Instituir o processo de aculturamento do Risco para que o tema seja difundido de forma ampla e completa entre todos os servidores da SEFA/PR	Comitê	Anual
	Verificar o nível de aderência das metodologias e procedimentos de avaliação, mensuração e controle do Risco conforme descrito na Política de Gestão de Riscos	Comitê	Anual
	Acompanhar a implantação e a implementação das metodologias, dos modelos e das ferramentas de Gestão de Riscos, em conformidade com os dispositivos legais aplicáveis	Comitê	Permanente
Secretário(a) da	Estabelecer a estratégia de Gestão de Riscos e aprovar, em última instância, a política e respectivos manuais, fixando e dispondo as atribuições, poderes e responsabilidades sobre a manutenção, o monitoramento e o aperfeiçoamento dos controles internos da gestão; e	Alta Administração	Anual
SEFA-PR	Analisar os relatórios de Risco e avaliar a exposição ao risco e as medidas e planos adotados para sua prevenção ou mitigação.	Alta Administração	Semestral

6. METODOLOGIA DE GESTÃO DE RISCO

A Metodologia de Gestão de Riscos da SEFA/PR tem por objetivo detalhar e estruturar as etapas para a operacionalização da Gestão de Riscos na instituição, definida por meio do processo de gerenciamento de riscos, conforme estabelecido na PGR SEFA/PR.

A gestão de riscos deve ser compatível com o tamanho e a complexidade da organização, com objetivo de proporcionar melhores resultados entregues à sociedade, bem como proteger os valores e objetivos da instituição.

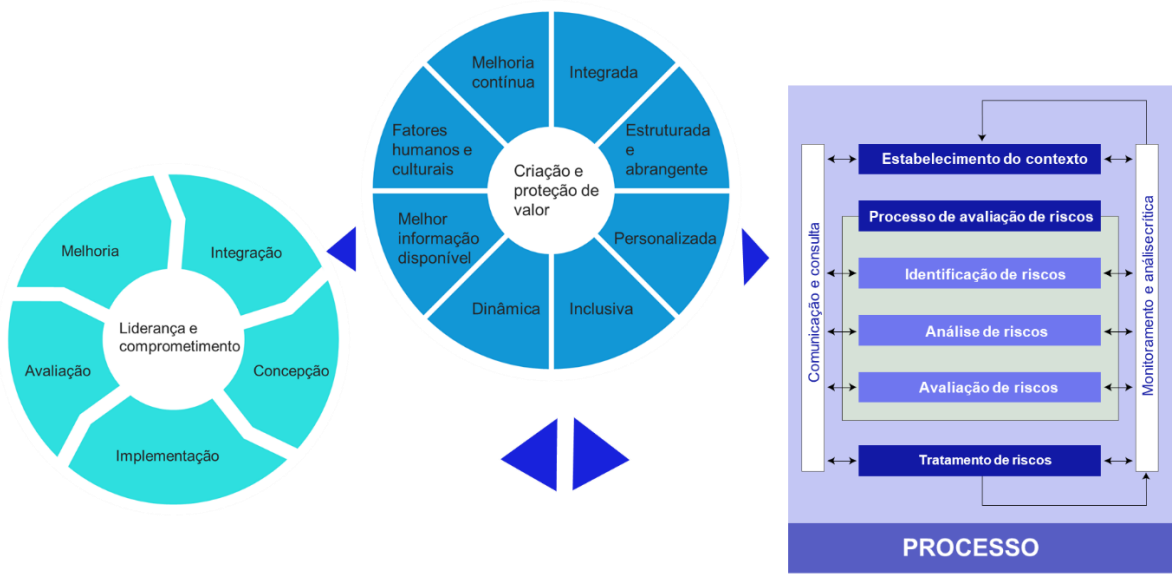
O processo de gerenciamento de risco deve identificar os eventos de riscos potenciais que podem afetar os objetivos da SEFA/PR, a partir de uma abordagem ativa, sistemática, holística e integrada, que permite gerenciar os riscos, modificando tanto a natureza de suas consequências como a probabilidade de que determinado efeito

ocorra, por meio da identificação, compreensão, atuação objetiva e comunicação de questões que envolvam riscos.

A gestão de riscos é aplicada, constantemente, em todos os níveis da organização, bem como a função, atividades e projetos específicos.

A arquitetura do gerenciamento de riscos da SEFA/PR, composta por princípios, estrutura e processo.

Na NRB ISO 31000:2018, a "gestão de riscos" refere-se à uma arquitetura para gerenciar riscos de maneira eficaz, composta por princípios, estrutura e processo, enquanto a expressão "gerenciar riscos" trata da aplicação dessa arquitetura para riscos específicos.



Fonte: Processos da Gestão de Riscos, ISO NBR 3100:2018

As etapas da Gestão de Riscos da SEFA/PR estão descritas no artigo 6 da PGR da SEFA/PR e serão detalhadas nessa Metodologia.

6.1 Definição do Plano de Gestão e Priorização de Riscos

O Plano de Gestão e Priorização de Riscos da SEFA/PR, é definido pelo Comitê de Gestão de Riscos da SEFA/PR, por meio da identificação e priorização dos riscos relevantes, contendo os processos organizacionais que comporão o referido plano.

Deve contemplar, também, os planos de tratamento no processo de gerenciamento de riscos, no qual devem ser priorizados os processos com maior vulnerabilidade considerando os objetivos declarados no planejamento estratégico e as tipologias de risco que a SEFA/PR pode estar sujeita.

A partir da decisão e escolha dos processos críticos, os responsáveis pelos processos, com apoio da AMF e do Comitê de Gestão de Riscos, aplicarão a Metodologia de Gestão de Riscos da SEFA/PR.

6.2. Seleção do Processo Organizacional

A seleção dos processos organizacionais tem por objetivo auxiliar na identificação do processo organizacional que será objeto do processo de gerenciamento de riscos, no qual deve ser apresentado, no mínimo:

- o responsável pelo gerenciamento de risco, com competência para orientar e acompanhar as etapas de identificação, análise, avaliação e implementação das respostas aos riscos;

- a equipe técnica responsável pelo processo de gerenciamento de riscos.

6.3. Entendimento do Contexto

No entendimento do contexto, o processo organizacional e seus objetivos são analisados em relação a seus ambientes interno e externo e identificados:

- descrição resumida do processo (breve relato do processo, que permite compreender o seu fluxo, os atores envolvidos e os resultados esperados);

- objetivos do processo organizacional;

- objetivos estratégicos da SEFA/PR alcançados pelo processo; e

- ciclo do processo de gerenciamento de riscos (o ciclo organizacional da SEFA/PR tem a duração de 12 a 24 meses);

- unidade demandante do processo de gerenciamento de riscos no processo organizacional (por exemplo a própria unidade, AMF ou Comitê de Gestão de Riscos);

- justificativa da implementação do gerenciamento de riscos no processo;

- unidade responsável pelo processo;

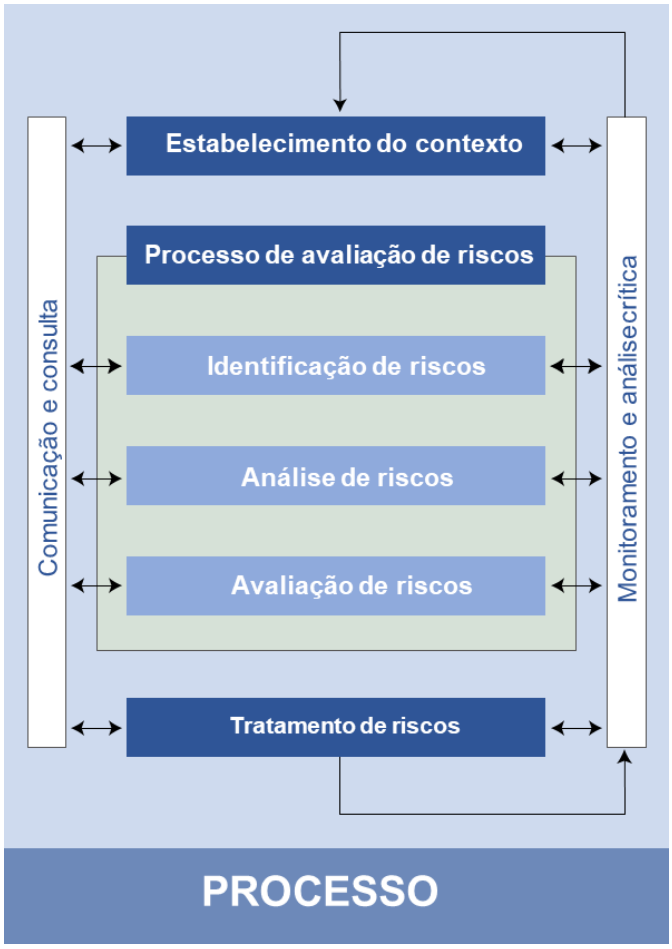
- partes interessadas no processo;

- informações do processo.

7. O PROCESSO DE GESTÃO DE RISCOS DA SEFA/PR

7.1. Visão geral do processo

O processo de gestão de riscos da SEFA/PR é orientado pelo *framework* da NBR ISO 31000:2018.



Fonte: Processos da Gestão de Riscos, ISO NBR 3100:2018

7.2. Identificação de escopo, contexto e critérios

7.2.1. Identificação de escopo

Com base na NBR ISO 3100:2018, a organização deve identificar o escopo, o contexto e estabelecer critérios de riscos, considerando a finalidade de personalizar o processo de gestão de riscos para permitir avaliação e tratamento de riscos de forma eficaz e apropriada às necessidades da SEFA/PR.

A identificação do escopo deve ser clara e alinhada aos objetivos organizacionais, especialmente em relação às(aos):

- objetivos e decisões que precisam ser tomadas;

- resultados esperados de cada etapa do processo;

- tempo, localização, inclusões e exclusões específicas;

- ferramentas e técnicas apropriadas para a avaliação dos riscos;

- recursos requeridos, responsabilidades e registros que serão mantidos; e

- relacionamento com outros projetos, processos e atividades.

7.2.2. Identificação do contexto externo e interno

Os contextos externo e interno são o ambiente no qual a organização opera para alcançar seus objetivos. Compreender o ambiente que a organização está inserida é essencial no processo de gerenciamento de riscos, pois a gestão de riscos ocorre no contexto dos objetivos e atividades da organização.

Deve-se observar, também, que fatores organizacionais podem ser fontes de risco, além disso o propósito e escopo do processo de gestão de risco estão inter-relacionados com os objetivos da organização como um todo.

A compreensão do contexto assegura que os objetivos e preocupações das partes interessadas sejam considerados no desenvolvimento dos critérios de risco. O contexto externo deve incluir, mas não está limitado a:

- fatores sociais, culturais, políticos, jurídicos, regulatórios, financeiros, tecnológicos, econômicos e ambientais, no âmbito internacional, nacional, regional ou local;

- direcionadores-chave e tendências que afetam os objetivos da organização;

- relacionamentos, percepções, valores, necessidades e expectativas das partes interessadas externas;

- complexidade das redes de relacionamento e dependências.

O contexto interno trata dos fatores que podem influenciar a maneira pela qual a organização gerenciará os seus riscos e deve incluir, mas não está limitado a:

- visão, missão e valores;

- governança, estrutura organizacional, papéis e responsabilizações;

- estratégia, objetivos e política;

- cultura da organização;

- normas, diretrizes e modelos adotados pela organização;

- capacidade em termos de recursos e conhecimentos (por exemplo, capital, tempo, pessoas, propriedade intelectual, processos, sistemas e tecnologias);

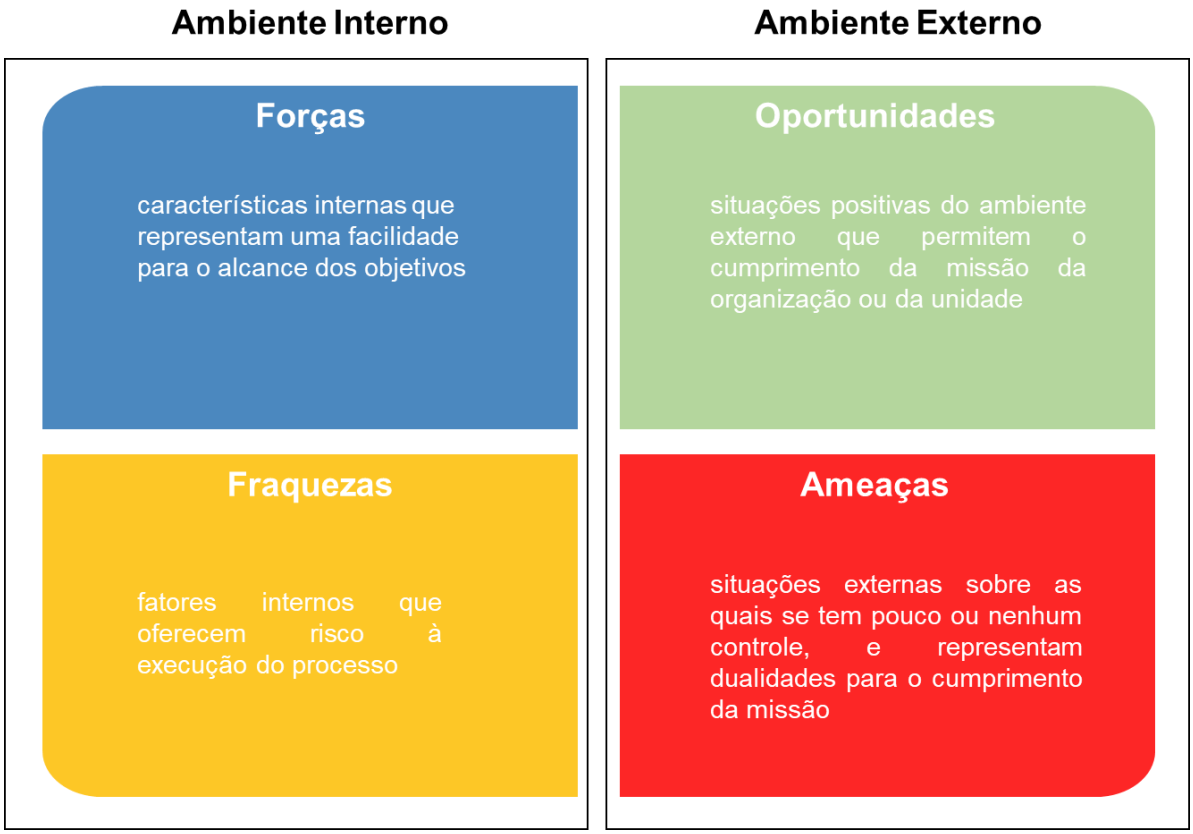
- dados, sistemas e fluxos de informação;

- relacionamentos com partes interessadas internas, suas percepções e valores;

- relações contratuais e compromissos; e

- interdependências e interconexões.

Para auxiliar na identificação do contexto, pode ser utilizada a análise do ambiente por meio da matriz SWOT, cuja sigla provém do inglês e busca identificar forças, fraquezas, oportunidades e ameaças da instituição ou das unidades, conforme demonstrado no diagrama a seguir.



7.2.3. Definição dos critérios de risco

Conforme a Política de Gestão de Riscos da SEFA/PR, o Comitê de Gestão Riscos da SEFA/PR é competente para definir os níveis de apetite a risco dos processos organizacionais, que deve ser estabelecido no início do processo de gerenciamento de riscos.

A definição dos critérios de risco, deve observar:

- a natureza e o tipo de incertezas que podem afetar resultados e objetivos (ainda que intangíveis);

- como as consequências e probabilidades serão medidas;

- fatores relacionados ao tempo;

- consistência no uso das medidas;

- como o nível de risco será determinado;

- como as combinações e sequências de múltiplos riscos serão levadas em consideração; e

- a capacidade da organização.

Os critérios de riscos devem ser estáveis o suficiente, de modo a permitir a comparabilidade entre riscos de diferentes processos organizacionais da SEFA/PR.

Após essa definição a unidade declara que:

- todos os riscos cujos níveis estejam dentro da(s) faixa(s) de apetite a risco podem ser aceitos, e uma possível priorização para tratamento deve ser justificada;

- todos os riscos cujos níveis estejam fora da(s) faixa(s) de apetite a risco serão tratados e monitorados, e uma possível falta de tratamento deve ser justificada.

7.3. Identificação de Riscos

A identificação dos riscos é a etapa na qual a organização identifica, reconhece e descreve os riscos e oportunidades de melhorias dos controles.

A partir do entendimento do contexto interno e externo é construída uma lista de riscos abrangente baseada em eventos, que podem criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos da SEFA/PR.

Para auxiliar na identificação do risco, podem ser utilizadas as seguintes questões:

- quais eventos podem criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos da SEFA/PR o atingimento de um ou mais objetivos do processo organizacional?

- o evento é um risco que pode comprometer claramente um objetivo do processo?

- o evento é um risco ou uma falha no desenho do processo organizacional?

- considerando os objetivos do processo organizacional, o evento identificado é um risco ou uma causa para um risco?

- o evento é um risco ou uma fragilidade em um controle para tratar um risco do processo?

A identificação abrangente deve ser crítica, uma vez que o risco que não é identificado nesta etapa não fará parte das demais etapas do processo de gerenciamento de risco.

E deve conter todos os riscos com impacto nos objetivos da SEFA/PR, incluindo suas fontes sob o controle ou não da SEFA/PR, ainda que as fontes e/ou causas não sejam evidentes. Durante a identificação dos riscos, pode ser verificado mais de um tipo de resultado, assim como uma variedade de consequências tangíveis e intangíveis.

No processo de identificação deve ser registrado objetivo do processo organizacional/etapa impactado pelo risco e realizada a categorização de riscos, no momento do mapeamento, que possibilita o reconhecimento dos riscos de forma minuciosa e as oportunidades de melhorias nos processos.

A tabela de categorias definida para aplicação na análise da SEFA/PR está disposta a seguir.

Tipo do Risco	Descrição	Exemplos
Operacional	eventos que podem comprometer as atividades, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas	- falhas de especificação dos produtos/serviços - negligência em relação às partes interessadas - problema crítico de desempenho - não entrega/atraso na entrega - qualidade da entrega - falha de sistemas - paralização da força de trabalho - acidentes - saúde e segurança
Legal	eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades da SEFA/PR	- problema crítico de desempenho - não entrega - qualidade da entrega - falha de sistemas

Tipo do Risco	Descrição	Exemplos
Financeiro/Orçamentário/Fiscal	eventos que podem comprometer a capacidade da SEFA/PR de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária	- perda de arrecadação - não execução orçamentária - atraso de pagamentos
Integridade	eventos relacionados a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta que podem comprometer os valores e padrões preconizados pela SEFA/PR e a realização de seus objetivos.	- fraudes - roubo - falsificação de documentos - entrada propositalmente errada de dados
Reputacional	eventos que podem comprometer a credibilidade da SEFA/PR	- divulgação de informações incorretas com prejuízo a credibilidade da organização - vazamento de informações sigilosas - não disponibilização de informações - discriminação ou assédio

Fonte: Metodologia de Gestão de Riscos da CGU, adaptado.

7.4. Análise de riscos

A análise de riscos tem como propósito compreender a natureza do risco, suas características e o nível de risco, quando apropriado. Essa etapa envolve a apreciação detalhada de incertezas, fontes de risco, suas consequências, probabilidade, eventos, cenários, controles e sua eficácia.

O propósito da análise, a disponibilidade e confiabilidade das informações e os recursos disponíveis determinam o grau de detalhamento e complexidade da análise.

A análise de riscos considera os seguintes fatores:

- probabilidade de eventos e consequências;

- natureza e magnitude das consequências;

- fatores temporais e volatilidade;

- eficácia dos controles existentes;

- sensibilidade e níveis de confiança.

Além da análise da eficácia dos controles internos existentes, a SEFA/PR deverá avaliar os controles com foco na simplificação e melhoria contínua.

Para auxiliar na análise do risco, podem ser levantadas as seguintes informações, como insumos o aprofundamento e análise dos problemas:

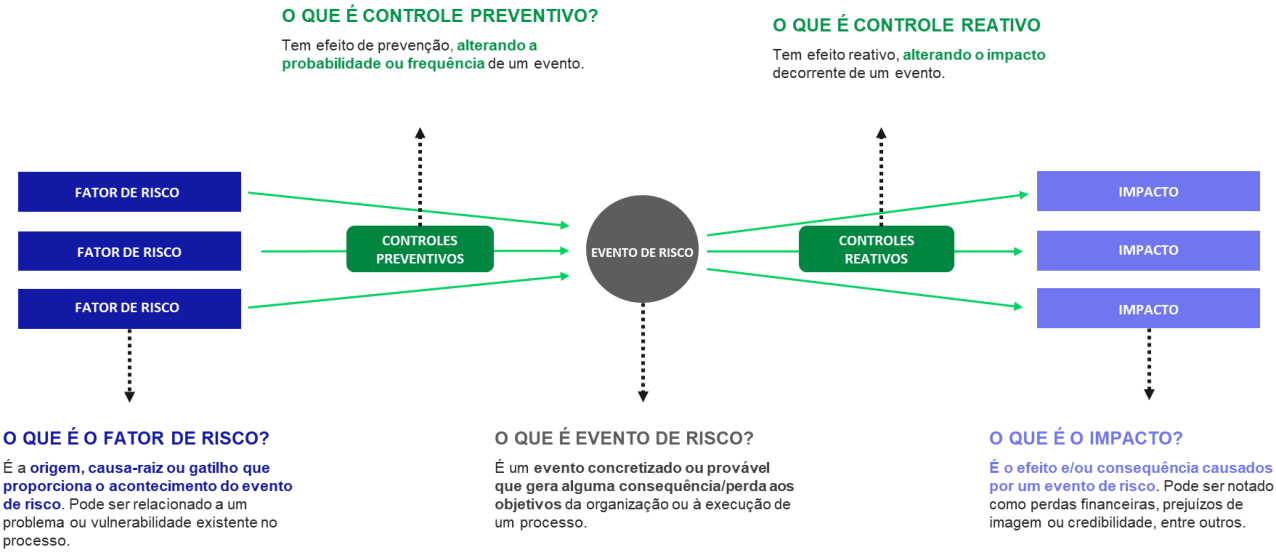
- causas: motivos que podem promover a ocorrência do risco;

- consequências: resultados do risco que afetam os objetivos;

- controles preventivos: controles existentes e que atuam sobre as possíveis causas do risco, como 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.

Como forma de representar e entender os riscos identificados, pode-se, também, utilizar uma ferramenta de diagrama da gravata borboleta que contempla as causas dos riscos, os eventos de riscos e os impactos dos riscos



Podem existir outras influências na análise que serão consideradas, documentadas e comunicadas eficazmente para os tomadores de decisão e, quando apropriado, as partes interessadas. Nos casos de eventos altamente incertos e difíceis de quantificar, a utilização de uma combinação de técnicas fornece maior discernimento.

Para o aprofundamento na análise do risco, os riscos levantados na SEFA/PR são classificados em Impacto e Probabilidade, de modo a determinar a sua posição e relevância no Mapa de Calor na etapa posterior de Avaliação do Risco.

Cada risco é avaliado qualitativamente conforme as descrições abaixo.

7.5. Avaliação de riscos

A avaliação de riscos é o processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou sua magnitude são aceitáveis ou toleráveis e apoiar decisões. Considera-se o contexto mais amplo e as consequências reais e percebidas pelas partes interessadas. Assim, com base nos resultados da análise de riscos, decide-se por:

- não fazer mais nada;

- considerar opções de tratamento de riscos

- realizar análises adicionais para melhor compreender o risco; ou

- manter os controles existentes, reconsiderar os objetivos.

O cruzamento das escalas de probabilidade e de impacto formam uma matriz de avaliação do risco ou mapa de calor do risco. Nessa matriz, cada evento de risco mapeado é posicionado conforme a sua maior avaliação dentro das escalas de impacto e probabilidade. A sua classificação máxima em uma escala de impacto determina o posicionamento do risco no sentido vertical e, sua classificação máxima em uma escala de probabilidade determinam sua posição horizontal.

Assim, com todos os riscos localizados, é possível realizar uma leitura visual da exposição a risco que a organização tem. Os gestores e as equipes, avaliando a pulverização dos riscos na matriz, podem definir qual resposta estaria à altura do perfil de cada risco e uma ideia de qual risco deve-se responder prioritariamente.

A multiplicação entre os valores de probabilidade e impacto define o nível do risco inerente, ou seja, o nível do risco sem considerar quaisquer controles que reduzem ou podem reduzir a probabilidade da sua ocorrência ou do seu impacto.

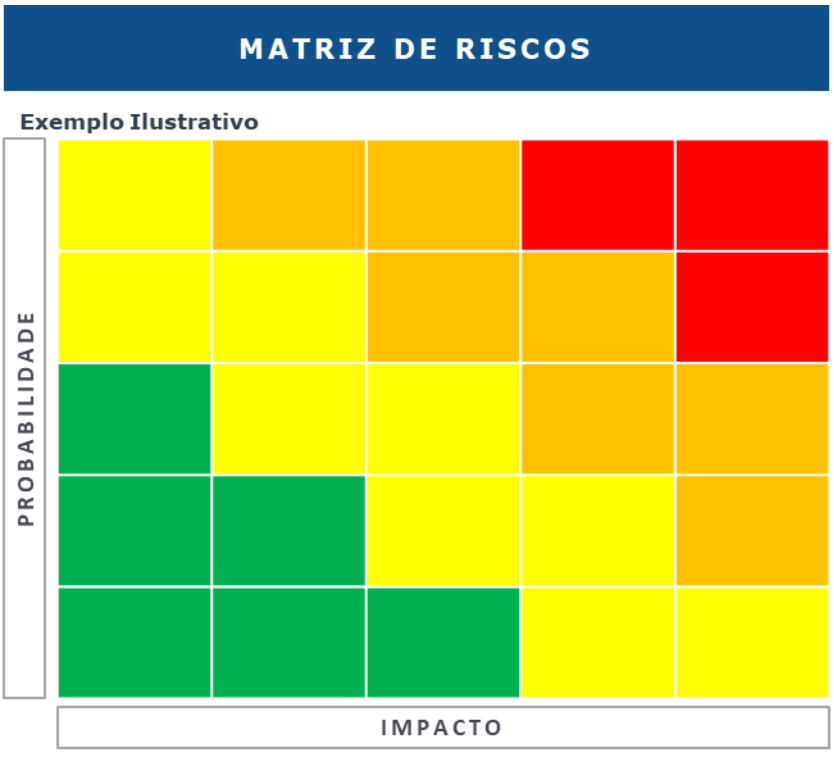
CLASSIFICAÇÃO DO NÍVEL DE RISCO (NR):

Risco Baixo	NR ≤ 4
Risco Médio	8 ≤ NR ≤ 16
Risco Alto	32 ≤ NR ≤ 64
Risco Extremo	NR ≥ 128

Fonte: Metodologia de Gestão de Riscos da CGU (adaptado)

A seguinte matriz representa os possíveis resultados da combinação das escalas de probabilidade e impacto.

Mapa de Calor dos Riscos



A cada ciclo de gerenciamento de risco deverá ocorrer a revisão do processo em novo ciclo do processo de gerenciamento de riscos, considerando o nível de risco inerente calculado no ciclo anterior e reavaliar os controles para o cálculo do risco residual. A comparação entre os níveis de riscos residuais de diferentes ciclos objetiva identificar se os controles definidos nos planos de tratamento estão sendo eficazes para tratar o risco.

Além da avaliação do nível de risco, deve ser avaliada a eficácia dos controles existentes, no desenho do processo e na operação, em relação aos objetivos do processo. Ou seja, é necessário verificar se os controles apontados durante a etapa de Identificação e Análise do risco, para subsidiar a de tratamento de riscos, para que seja adequado ao apetite de risco da SEFA/PR

Nível	Desenho	Operação de Controle
Inexistente	Não há procedimento de controles	Não há procedimento de controles
Fraco	Há procedimentos de controles, mas não são adequados e nem estão formalizados	Há procedimentos de controle, mas não são executados
Mediano	Há procedimentos de controles formalizados, mas não estão adequados (insuficientes)	Os procedimentos de controle estão sendo parcialmente executados
Satisfatório	Há procedimentos de controles adequados (suficientes), mas não estão formalizados	Os procedimentos de controle são executados, mas sem evidência de sua realização
Forte	Há procedimentos de controles adequados (suficientes) e formalizados	Procedimentos de controle são executados e com evidência de sua realização

Fonte: Gestão de Riscos – Avaliação da Maturidade (TCU, 2018, adaptado)

7.5.1 Priorização dos Riscos

Nesta etapa, considerando os valores dos níveis de riscos inerentes e residuais calculados na etapa anterior, serão identificados quais riscos serão priorizados para tratamento.

A faixa de classificação do risco residual deve ser considerada para a definição da atitude da unidade em relação à priorização do tratamento do risco.

Atitude esperada, perante o risco para cada classificação:

Classificação do Risco	Nível do Apetite	Ação necessária	Exceção
Extremo	Nível de risco muito além do apetite a risco	Comunicar ao Comitê de Gestão de Riscos, qualquer risco nesse nível deve ser objeto de Avaliação Estratégica. Realizar resposta imediata ao risco	Caso o risco não seja priorizado para implementação de medidas de tratamento, deve haver justificada pela unidade e aprovada pelo Comitê de Gestão de Riscos da SEFA/PR.
Alto	Nível de risco além do apetite a risco	Realizar resposta ao risco em período determinado. Comunicar ao Comitê de Gestão de Risco	
Médio	Nível de risco dentro do apetite a risco.	Realizar resposta e controles para reduzir ou mantê-lo, sem custos	Caso o risco seja priorizado para implementação de

Classificação do Risco	Nível do Apetite	Ação necessária	Exceção
		adicionais. Requer atividades de monitoramento específicas e atenção da unidade na manutenção de	medidas de tratamento, essa priorização deve ser justificada pela unidade e aprovada pela Assessoria de Riscos e Integridade
Baixo	Nível de risco dentro do apetite a risco.	Analisar se existem oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custo x benefício, como diminuir o nível de controles.	

Fonte: Gestão de Riscos – Avaliação da Maturidade (TCU, 2018, adaptado)

7.6. Tratamento de riscos

Nesta etapa, deve definir a opção mais apropriada de tratamento de riscos de forma a balancear os benefícios potenciais derivados em relação ao alcance dos objetivos, face aos custos, esforço ou desvantagens da implementação.

As opções de tratamento de riscos não são necessariamente mutuamente exclusivas ou adequadas em todas as circunstâncias.

As decisões levam em consideração os riscos que demandam um tratamento economicamente não justificável, como, por exemplo, riscos com grande consequência negativa, porém com probabilidade muito baixa. Além das considerações econômicas, considera-se também obrigações da SEFA/PR, compromissos voluntários e pontos de vista das partes interessadas. Ao selecionar as opções de tratamento de riscos, a organização considera os valores e as percepções das partes interessadas, e as formas mais adequadas para se comunicar com elas. Quando as opções de tratamento de riscos podem afetar o risco no resto da organização ou com as partes interessadas, todos os envolvidos participam da decisão.

Para cada risco priorizado deve ser relacionada a uma opção de tratamento, com base no nível do risco, contexto SEFA/PR e/ou custo do controle. As opções podem envolver uma ou mais das seguintes:

Opção de Tratamento	Descrição
Mitigar	Um risco normalmente é mitigado quando a implementação de controles, neste caso, apresenta um custo/benefício adequado, mitigar o risco significa implementar controles que possam remover as fontes de riscos, mudar a probabilidade ou mudar as causas ou as consequências dos riscos, identificadas na etapa de Identificação e Análise de Riscos.
Compartilhar	Um risco normalmente é compartilhado quando a implementação de controles não apresenta um custo/benefício adequado, pode-se compartilhar o risco por meio de terceirização ou apólice de seguro, por exemplo.
Evitar	Um risco normalmente é evitado quando a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco com a SEFA/PR. Evitar o risco significa encerrar o processo organizacional. Nesse caso, essa opção deve ser aprovada pelo Comitê de Gestão de Riscos da SEFA/PR.
Aceitar	Um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco. Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco.

Fonte: Metodologia de Gestão de Riscos da CGU (adaptado)

Caso a opção de tratamento do risco for “Mitigar”, o plano de tratamento deve ser capaz de diminuir os níveis de probabilidade e/ou de impacto do risco a um nível dentro ou mais próximo possível dos níveis aceitáveis de apetite a risco.

O plano de tratamento elaborado pelo responsável do processo para gerenciamento de riscos é um plano de ação para a implementação de medidas de tratamento dos riscos e deve conter, no mínimo:

- controle proposto;
- tipo de controle;
- objetivo do controle;
- unidade responsável pela implementação da iniciativa;
- responsável pela implementação;
- intervenientes: unidades corresponsáveis pela implementação da iniciativa, ou seja, unidades envolvidas na implementação do controle proposto;
- breve descrição sobre como será a implantado;
- data prevista para início da implementação; e
- data prevista para o término da implementação.

O controle proposto dever ter entregas intermediárias, nas quais permitam mensurar a evolução da implementação.

É importante que, em uma primeira abordagem da elaboração do Plano de Tratamento, avalie-se a necessidade de melhorar ou extinguir controles já existentes. Somente depois dessa avaliação, e se ainda identificada a necessidade de redução do nível do risco, podem ser propostos novos controles, observados sempre critérios de eficiência e eficácia da sua implementação.

Se as iniciativas definidas no Plano de Tratamento envolverem mais de uma unidade, o responsável pelo processo de gerenciamento de riscos deve encaminhar a proposta de Plano para que essas unidades validem as iniciativas de que participarem.

Se não houver opções de tratamento disponíveis ou se as opções de tratamento não modificarem suficientemente o risco, este deve ser registrado e mantido sob análise crítica e monitoramento contínuos.

Para garantir a conformidade e a segurança da implantação de melhorias nos controles, é importante garantir o alinhamento com as demais políticas institucionais da SEFA/PR.

Além disso, o tratamento pode não produzir os resultados esperados e pode produzir consequências não pretendidas. Um risco significativo pode derivar do fracasso ou da ineficácia das medidas de tratamento de riscos. O tratamento de riscos, por si só, pode introduzir novos riscos que precisam ser gerenciados. Monitoramento e análise crítica precisam ser parte integrante da implementação do tratamento de riscos, para assegurar que as diferentes formas de tratamento se tornem e permaneçam eficazes.

7.6.1 Aprovação do Plano de Ação (Matriz de Alçada)

O Plano de Tratamento deve ser aprovados pelas unidades competentes, que serão responsáveis por analisar se as ações propostas pelo responsável do gerenciamento do risco são suficientes para atender aos níveis de riscos enquadrados no apetite de risco da SEFA/PR.

Classificação	Alçada Competente
Extremo	Comitê de Gestão de Riscos SEFA/PR

Alto	Comitê de Gestão de Riscos da SEFA/PR
Médio	Superior Hierárquico da unidade responsável
Baixo	Superior Hierárquico da unidade responsável

A alçada competente poderá solicitar adequações nos planos de tratamentos propostos pelas unidades responsáveis pelo gerenciamento do risco, que devem atender a metodologia SMART, até que o plano de seja capaz de diminuir os níveis de probabilidade e/ou de impacto do risco a um nível dentro ou mais próximo possível dos níveis aceitáveis de apetite a risco.

7.7. Monitoramento e análise crítica

O monitoramento e a análise crítica periódicos asseguram a melhoria da qualidade e eficácia da concepção, implementação e resultados do processo. São partes planejadas do processo de gestão, com responsabilidades claramente definidas. Além disso, incluem todos os estágios do processo: planejamento, coleta e análise de informações, registro de resultados e fornecimento de retorno.

Monitorar e analisar criticamente o processo de gestão de risco é importante também para garantir que os controles sejam eficazes e eficientes no projeto e na operação, bem como para identificação de oportunidades de simplificação e desburocratização de controles

Os resultados do monitoramento e da análise crítica são registrados e reportados externa e internamente conforme apropriado, e convém que sejam utilizados como entrada para a análise crítica da estrutura de gestão de riscos.

Esses procedimentos tem finalidade detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco e no próprio risco, que podem requerer revisão dos tratamentos de riscos e suas prioridades, assim como identificar riscos emergentes; obter informações adicionais para melhorar a política, a estrutura e o processo de gestão de riscos; analisar eventos (incluindo os “quase incidentes”), mudanças, tendências, sucessos e fracassos e aprender com eles; e assegurar que os controles sejam eficazes e eficientes no projeto e na operação).

Na SEFA/PR, a responsabilidade para monitoramento e análise crítica está distribuída da seguinte forma:

Responsável	Descrição da atividade	Periodicidade
Todos os servidores da SEFA/PR	Monitoramento da evolução dos níveis de riscos e da efetividade das medidas de controles implementadas nos processos organizacionais em que estiverem envolvidos ou que tiverem conhecimento	Permanente
Comitê de Gestão de Riscos	monitoramento contínuo, com vistas a medir e reportar ao Comitê de Gestão de Riscos o desempenho da gestão de riscos, por meio de indicadores chave de risco, análise do ritmo de atividades, operações ou fluxos atuais em comparação com o que seria necessário para o alcance de objetivos ou manutenção das atividades dentro dos critérios de risco estabelecidos.	Anual
	análise crítica dos riscos e seus tratamentos, por meio de auto avaliação de riscos e controles	Anual
Controladoria do Estado do Paraná	avaliações independentes, seja por meio de auditorias, focando na estrutura e no processo de gestão de riscos, em todos os níveis relevantes das atividades organizacionais, ou seja, procurando testar os aspectos sistêmicos da gestão de riscos em vez de situações específicas.	Permanente

As atividades de monitoramento e análise crítica devem assegurar que o registro de riscos seja mantido atualizado, bem como que nele sejam documentados os resultados das ações mencionadas acima.

7.8. Registro e relato

O processo da gestão de risco e seus resultados serão documentados e relatados por meio de mecanismos apropriados. O registro e o relato visam:

- comunicar atividades e resultados de gestão de riscos em toda a organização;
- fornecer informações para a tomada de decisão;
- melhorar as atividades de gestão de riscos
- auxiliar a interação com as partes interessadas, incluindo aquelas com responsabilidade e com responsabilização por atividades de gestão de riscos.

As decisões sobre criação, retenção e manuseio de informação documentada levarão em consideração, mas não se limitam ao seu uso, a sensibilidade da informação e os contextos externo e interno. O relato é parte integrante da governança da SEFA/PR para melhorar o diálogo com as partes interessadas e apoiar a alta administração e os órgãos de supervisão a cumprirem suas responsabilidades.

7.9. Comunicação e consulta

A comunicação e consulta às partes interessadas são importantes na medida em que auxiliam esses atores na compreensão do risco, na base sobre a qual decisões são tomadas e nas razões pelas quais ações específicas são requeridas. A comunicação promove a conscientização e entendimento do risco e a consulta envolve obter retorno e informação para auxiliar a tomada de decisão. Ambas respeitam a confidencialidade e integridade da informação, bem como os direitos de privacidade.

Planos de comunicação devem abordar questões relacionadas com o risco propriamente dito, suas causas, suas consequências (se conhecidas) e as medidas que estão sendo tomadas para tratá-los. Comunicação e consulta visam a:

- reunir diferentes áreas de especialização para cada etapa do processo de gestão de riscos;
- assegurar que pontos de vista diferentes sejam considerados apropriadamente ao se definirem critérios de risco e ao se avaliarem riscos;
- fornecer informações suficientes para facilitar a supervisão dos riscos e a tomada de decisão;
- construir um senso de inclusão e propriedade entre os afetados pelo risco.

8. ACOMPANHAMENTO DAS AÇÕES DE GESTÃO DE RISCOS

O acompanhamento das ações de mitigação não se restringe à verificação da implementação das medidas metodológicas e ritos de governança, além disso a SEFA/PR deve se concentrar em verificar se o tratamento foi realizado de forma adequada aos riscos e se remediou a situação subjacente após um período razoável até chegar em um nível de maturidade aceitável.

8.1. Nível de Maturidade da Situação de Risco

A maturidade da organização em Gestão de Riscos pode variar desde aspectos processuais, pessoas, resultados e ambiente interno, como também determinar um nível de maturidade global, ao considerar todos os aspectos citados juntos.

Portanto, realizar a avaliação da maturidade da organização em relação ao gerenciamento de riscos deve funcionar de maneira integrada as ações de mitigação dos riscos, desde o planejamento estratégico da gestão até o nível de execução de todas as áreas.

8.2. Acompanhamento do Comitê de Gestão de Riscos

O Comitê de Riscos deve estar presente em toda a execução do plano de mitigação de riscos e realizar a análise crítica dos indicadores de desempenho que podem estar presentes nesses planos. Logo, se faz necessário o planejamento do acompanhamento

Uma vez planejado o monitoramento, a equipe analisará o relatório de auditoria, o plano de ação e outros documentos pertinentes. Na ocasião, deve-se destacar os indicadores de desempenho que serão aferidos para evidenciar a possível solução de problemas identificados na auditoria e as deliberações-chave, que seriam aquelas geradoras dos impactos considerados mais importantes, em termos financeiros ou qualitativos.

9. CULTURA E TREINAMENTO

9.1. Cultura

Uma cultura de risco refere-se ao conjunto de crenças, conhecimentos, entendimentos, atitudes, valores compartilhados e comportamentos que rege o dia a dia da organização frente as incertezas em suas atividades.

O comprometido da cultura de uma organização se inicia na Alta Administração da entidade e disseminando com o mesmo comprometimento para os operadores dos processos finalísticos, ou seja, a cultura de risco é um compromisso de todos.

A cultura de risco positiva é aquela em que o processo de gestão de risco de fato auxilia os atores a resolverem suas fragilidades de processo. O compromisso com a cultura de gerenciamento de risco desencadeia toda uma abordagem de resolução de problemas ágil, incentiva a intensificação da cultura e, por fim, é positivo para a organização.

Todas as interações têm foco em transformação e melhoria, ao invés de exposição de responsáveis e punição.

9.2. Treinamento

A divisão de responsabilidades da Gestão de Riscos é naturalmente pulverizada ao longo de toda a organização. Além disso, novas ameaças e tipos de incidentes surgem de forma dinâmica. Por fim, é importante reconhecer a dificuldade de manter uma cultura positiva, principalmente pelo cotidiano dos gestores e a distância e barreiras de comunicação entre as diversas áreas da organização.

Dessa forma, a capacitação permanente de todos os gestores da SEFA/PR se faz importante para que os processos de gestão consigam ser executados de maneira satisfatória. No ciclo anual de reavaliação, o Comitê de Gestão de Riscos da SEFA/PR delibera novos objetivos, apetite e tolerância ao risco, novas áreas de foco para implantação de controles e elaboração de planos de contingência.

Com essas diretrizes, a Assessoria de Riscos e Integridade da SEFA/PR identifica quais são os principais tópicos a serem reforçados na organização, define um público-alvo, elabora um material de treinamento e executa o plano através dos instrumentos apropriados de comunicação, de informação e de treinamento.

Assessoria de Riscos e Integridade da SEFA/PR, é responsável por manter os servidores da SEFA/PR periodicamente capacitados no que se diz respeito ao gerenciamento de riscos.

10. REFERÊNCIAS BIBLIOGRÁFICAS

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

AHP. ***Analytic Hierarchy Process***, Excel MS Excel 2010 (extensão xlsx). O modelo AHP foi desenvolvido por Goepel, Klaus D., modelo BPMSG AHP Excel, cuja versão é de livre uso. Disponível em http:// bpmsg.com

BRASIL. **Instrução Normativa Conjunta MP/CGU Nº 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. Ministério do Planejamento, Desenvolvimento e Gestão. Assessoria Especial de Controles Internos. **Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão.** Brasília. Brasília. V1.1.2 – 2017.

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. Referencial básico de Gestão de Riscos**. Abril de 2018.

BRASIL. Ministério da Transparência e Controladoria-Geral da União. **Portaria nº 915**, de 12 de abril de 2017, que institui a Política de Gestão de Riscos – PGR – do Ministério da Transparência, Fiscalização e Controladoria-Geral da União – CGU.

BRASIL. Ministério da Transparência e Controladoria-Geral da União. **Portaria nº 50.223**, de 04 de dezembro de 2015, que aprova o Planejamento Estratégico da CGU para o quadriênio 2016-2019.

BRASIL. Tribunal de Contas da União. **Gestão de Riscos**. Disponível em http://portal.tcu.gov.br/gestao-e-governanca/gestao-de-riscos/. Acesso em 02 de setembro de 2017.

BRASIL. Tribunal de Contas da União. **Gestão de Riscos – Avaliação da Maturidade**. Brasília. 164 p., 2018.

COSO. *Committee of Sponsoring Organizations of the Treadway Commission*. **Gerenciamento de Riscos Corporativos – Estrutura Integrada**. 2007. Tradução: Instituto dos Auditores Internos do Brasil (Audibra) e *Pricewaterhouse Coopers Governance, Risk and Compliance*, Estados Unidos da América, 2007.

COSO. *Committee of Sponsoring Organizations of the Treadway Commission*. **Risk Assessment in Practice**. Disponível em https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance -Risk-Compliance/dttl-grc-riskassessmentinpractice.pdf. Acesso em 20 de setembro de 2022.

IIA. *The Institute of Internal Auditors*. **As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles.** Disponível em https://na.theiia.org/translations/PublicDocuments/Three-Lines-Model-Updated-Portuguese.pdf . Acesso em 4 de setembro de 2022.