Secretaria de Fazenda

GOVERNO DO ESTADO
RIO DE JANEIRO

PLANO DE GESTÃO E GERENCIAMENTO DE RISCOS DA SEFAZ/RJ

COMITÊ PERMANENTE DE GOVERNANÇA E GERENCIAMENTO DE RISCOS

1ª Edição – janeiro de 2024

Sumário

Comitê Permanente de Governança e Gerenciamento de Riscos

Secretário de Estado de Fazenda

Leonardo Lobo

Subsecretário-Geral

Gustavo Tillmann

Subsecretário de Administração

Sérgio Henrique Jonas Fogaça

Subsecretária de Assuntos Jurídicos

Vanessa Huckleberry Portella Siqueira

Subsecretária de Contabilidade Geral

Yasmim da Costa Monteiro

Subsecretário de Controle Interno

Francisco Pereira Iglesias

Subsecretário de Estado de Receita

Adilson Zegur

Subsecretário de Política Tributária e Relações Institucionais

Thompson Lemos da Silva Neto

Subsecretário de Tecnologia da Informação e Comunicação

Gabriel Mac-Dowell Blum

Subsecretário do Tesouro Estadual

Bruno Schettini

Corregedor-Chefe da Corregedoria Tributária de Controle Externo

Flavio Müller Pupo

1. INTRODUÇÃO

Risco, conforme a ISO 31000, pode ser definido como o efeito das incertezas sobre os objetivos de uma organização, seja ela pública ou privada. Os efeitos podem ser positivos (oportunidades) ou negativos (ameaças). A SEFAZ, para efeitos deste documento, irá realizar a gestão dos riscos negativos que possam impactar no atingimento dos objetivos estratégicos.

Gerenciar riscos é uma atividade cada dia mais essencial, uma vez que uma gestão preventiva se antecipa a eventos incertos, ameaças e problemas e, dessa forma, melhora o desempenho da organização, encoraja a inovação e apoia o alcance de objetivos.

Este documento tem por objetivo detalhar o processo de gestão de riscos da SEFAZ-RJ, incorporando a visão de riscos à tomada de decisão, sendo documento complementar à Resolução SEFAZ n º 592, de 19 de dezembro de 2023, que instituiu a Política de Gestão de Riscos.

Importante observar que, como forma de acelerar a implementação da Gestão de Riscos na SEFAZ-RJ, foram utilizados materiais e troca de experiência com a Controladoria Geral do Estado de Goiás (CGE-GO).

2. BASE TEÓRICA

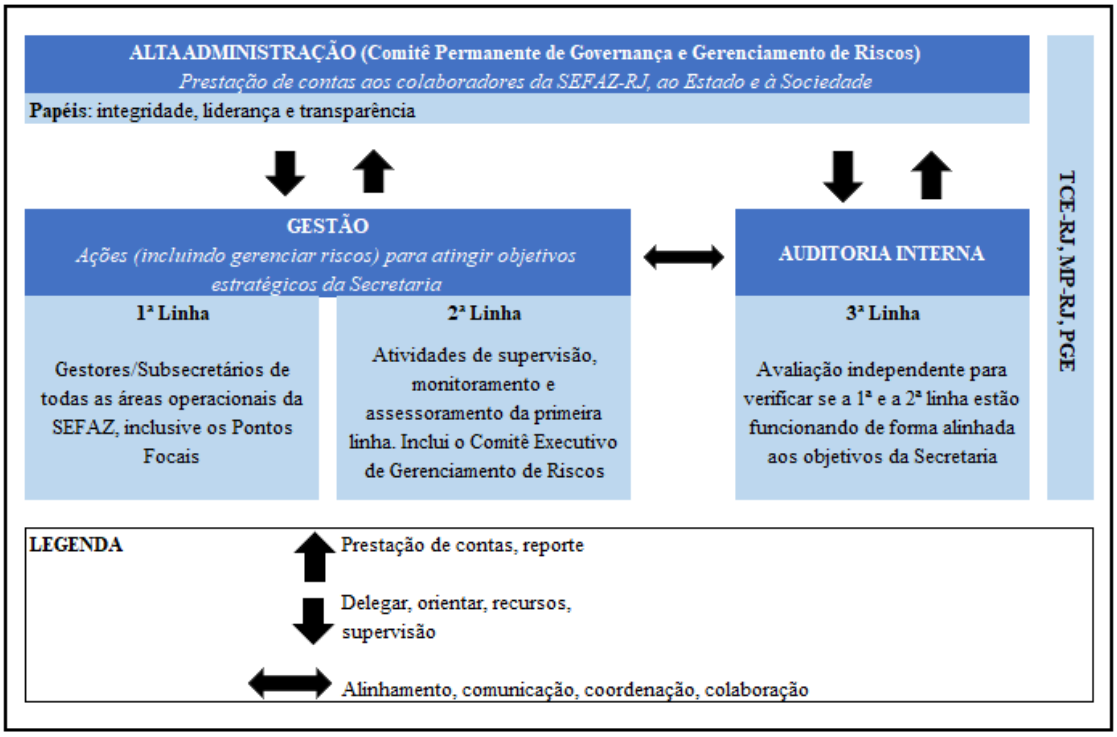
Existem diversas estruturas de gestão de riscos mundialmente reconhecidas e que são utilizadas como base em vários tipos de organizações, tanto na iniciativa privada quanto na esfera pública. A SEFAZ/RJ utilizou conceitos da estrutura da ABNT NBR ISO 31000 para estruturar seu processo de gerenciamento de riscos, além de considerar o Modelo das Três Linhas do IIA (The Institute of Internal Auditors) para melhorar a comunicação na gestão de riscos por meio do esclarecimento dos papéis e responsabilidades essenciais.

A adoção de uma metodologia de gestão de riscos traz inúmeros benefícios para uma organização, entre eles:

- Possibilita a identificação antecipada dos possíveis eventos que poderiam ameaçar o atingimento dos objetivos, o cumprimento de prazos, leis e regulamentos etc.;
- Permite uma implementação de estratégia efetiva de alocação de recursos para solução de problemas;
- Assegura que os responsáveis pela tomada de decisão, em todos os níveis da organização, tenham acesso tempestivo a informações suficientes quanto aos riscos aos quais ela está exposta;
- Aumenta a probabilidade de alcance dos objetivos da organização, trazendo os riscos a níveis aceitáveis; e
- Permite o aperfeiçoamento e a melhoria contínua dos processos organizacionais.

3. PAPÉIS ORGANIZACIONAIS

O modelo de Três Linhas do IIA (The Institute of Internal Auditors) não é uma estrutura de gerenciamento de riscos, mas propõe uma forma simples e eficaz de melhorar a comunicação do gerenciamento de riscos e controle por meio do esclarecimento dos papéis e responsabilidades essenciais. Neste modelo, cada uma das três "linhas" desempenha um papel distinto dentro da estrutura mais ampla de governança de uma organização. A imagem abaixo apresenta a esquematização deste modelo, adaptado à realidade da SEFAZ/RJ:



Primeira linha

Como primeira linha de defesa, os gestores operacionais gerenciam os riscos e tem propriedade sobre eles, isso porque tal gerenciamento pressupõe conhecimento detalhado do seu próprio processo de trabalho. Eles também são os responsáveis por implementar as ações corretivas para resolver deficiências em processos e controles.

Sendo assim, a gestão operacional é responsável por manter controles internos eficazes e por conduzir procedimentos de riscos e controle diariamente. Faz parte de suas atribuições identificar, avaliar, controlar e mitigar os riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos para garantir que as atividades estejam de acordo com as metas e objetivos.

Por meio de uma estrutura de responsabilidades em cascata, os gestores desenvolvem e implementam procedimentos detalhados que servem como controles e supervisionam a execução, por parte de seus colaboradores, desses procedimentos.

Os agentes públicos responsáveis pela condução de atividades e tarefas exercem o papel de primeira linha. Os pontos focais dão suporte na identificação, análise e avaliação dos riscos e auxiliam no monitoramento, na efetividade das medidas de controle e na identificação de indicadores de desempenho.

Segunda linha

O principal papel da segunda linha é facilitar e monitorar a implementação de práticas eficazes de gerenciamento de riscos por parte dos gestores operacionais. Além disso, ela também auxilia o Comitê Permanente de Governança e Gerenciamento de Riscos a definir a meta de exposição ao risco e a reportar adequadamente informações relacionadas a riscos em toda a SEFAZ/RJ.

O Comitê Executivo de Gerenciamento de Riscos exerce o papel da segunda linha no tocante ao gerenciamento de riscos da SEFAZ/RJ e auxiliará os gestores e subsecretários na implantação desta metodologia na Secretaria, via pontos focais.

Terceira linha

Responsável pela revisão independente sobre o gerenciamento dos riscos, a Auditoria Interna ajuda a organização a atingir os seus objetivos apresentando uma abordagem sistemática e disciplinada para avaliar e aprimorar a eficácia dos processos de gestão de riscos, controles e governança, fornecendo aos órgãos de governança e à Alta Administração avaliações abrangentes baseadas no maior nível de independência.

Opinam ainda sobre a forma como a Primeira Linha e a Segunda Linha alcançam os objetivos de sua atuação, contribuindo para o seu aprimoramento.

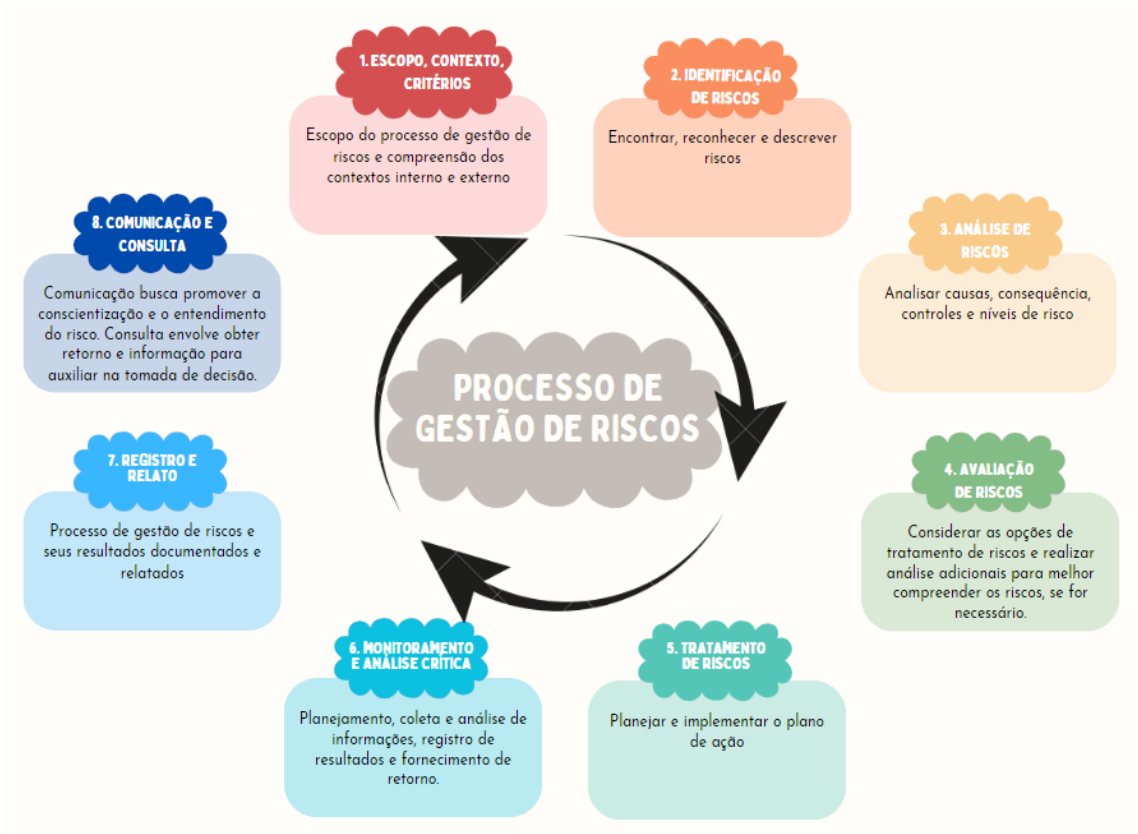
4. APETITE AO RISCO

Apetite a risco refere-se ao nível de riscos que a organização está disposta a aceitar para atingir seus objetivos. O detalhamento encontra-se no item 5.4.

A SEFAZ é conservadora e definiu o apetite ao risco como BAIXO.

5. DESENVOLVIMENTO DA METODOLOGIA

A metodologia de Gestão de Riscos apresenta o seguinte ciclo:



5.1. ESCOPO, CONTEXTO E CRITÉRIOS

Entender a estrutura da organização e seu contexto é essencial para personalizar o processo de gestão de riscos, permitindo um processo de avaliação de riscos eficaz e um tratamento de riscos apropriado.

Assim, todos os órgãos da SEFAZ deverão integrar em sua estrutura a atividade de gerenciamento de riscos, com o suporte dos pontos focais. Deverão ser priorizados os processos organizacionais que impactam diretamente no atingimento dos objetivos estratégicos da SEFAZ. Na ausência de planejamento estratégico, devem ser definidos quais objetivos devem ser alcançados pela Subsecretaria e qual o processo de trabalho relevante para o alcance desses objetivos.

Cabe aos Proprietário de Riscos escolher os processos de trabalho que devam ter os riscos gerenciados e tratados com prioridade em cada área técnica.

Nesta etapa devem ser identificados:

- ✓ Objetivos ou resultados que devem ser alcançados pela área, desdobrados do planejamento estratégico;
- ✓ Processos de trabalho relevantes para o alcance desses objetivos;
- ✓ Os principais fatores internos e externos que podem afetar o alcance dos objetivos/resultados (pessoas, sistemas informatizados, legislação, fatores políticos);

- ✓ Pessoas, unidades ou outras organizações envolvidas nesses processos.

5.2. IDENTIFICAÇÃO DE RISCOS

A etapa de identificação de riscos compreende encontrar, reconhecer e descrever riscos que possam impedir o alcance dos objetivos.

A correta identificação dos riscos demanda a adequada compreensão do seguinte conceito: “risco é o efeito da incerteza sobre os objetivos” (ABNT, 2018).

Para facilitar a identificação dos riscos podem ser levantadas informações como:

- ✓ Público alvo do processo
- ✓ Fluxo do processo
- ✓ Infraestrutura utilizada
- ✓ Legislação correlacionada
- ✓ Principais objetivos do processo
- ✓ Principais problemas do passado
- ✓ Recurso humano utilizado
- ✓ Sistemas informatizados
- ✓ Partes interessadas
- ✓ Ambiente externo (cenário político, social, financeiro, legal, tecnológico, econômico etc,)
- ✓ Tendências de mercado

Para facilitar a identificação dos riscos, podem ser empregadas ferramentas que facilitam a identificação de um maior número de riscos, tais como brainstorming, brainwriting, entrevistas, pesquisas etc. (TCU, 2020). Em um primeiro momento é importante que a utilização dessas técnicas seja realizada de maneira livre. Não é obrigatório o mapeamento do processo, mas mapear o processo ajuda a analisar o fluxo do processo através de uma representação esquemática, com o objetivo de compreender todas as inter-relações das entradas que o compõem, as tarefas, as saídas e as responsabilidades dos envolvidos. Após esse mapeamento os eventos afetam negativamente os processos podem ser identificados, analisados e mitigados.

Os riscos podem ser identificados a partir de perguntas, como:

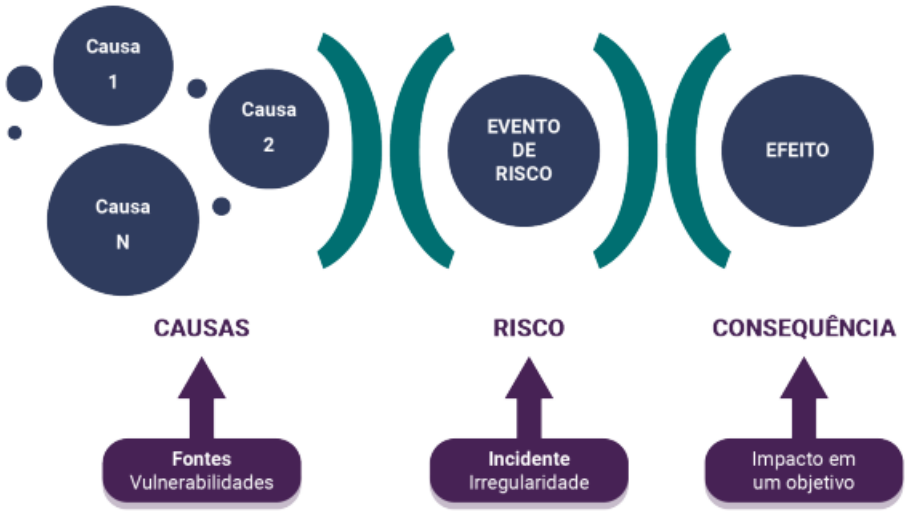
- ✓ Quais eventos podem EVITAR o atingimento de um ou mais objetivos do processo organizacional?
- ✓ Quais eventos podem ATRASAR o atingimento de um ou mais objetivos do processo organizacional?

- ✓ Quais eventos podem PREJUDICAR o atingimento de um ou mais objetivos do processo organizacional?
- ✓ Quais eventos podem IMPEDIR o atingimento de um ou mais objetivos do processo organizacional?

É importante que as técnicas sejam realizadas de forma coletiva, usando o conhecimento dos funcionários com maior experiência na área e conhecimento do processo de trabalho. Quanto mais especialistas no assunto estiverem juntos nesta etapa, melhor será o levantamento dos riscos.

5.3. ANÁLISE DE RISCOS

O propósito da análise dos riscos é compreender a natureza do risco e suas características, incluindo o nível de risco. Um evento de risco pode ter múltiplas causas e consequências e pode afetar múltiplos objetivos.



Fonte: ENAP

Causas são condições que dão origem à possibilidade de um evento ocorrer. Identificados os eventos que podem impedir ou dificultar a concretização dos objetivos do processo, projeto ou atividade, é preciso investigar as causas do evento de risco que podem se originar de diversas fontes, tais como:

- Processo - Decorrente de diretrizes estratégicas e da formalização/modelagem de processos, incluídos os métodos, procedimentos e regulamentações de planejamento, execução, controle e monitoramento. Os mecanismos de comunicação e repositório de conhecimento também se enquadram nesta fonte.

- Pessoas - Decorrente de operações humanas, onde são requeridas condutas apropriadas, competências, conhecimentos e habilidades.
- Externa - Decorrente do ambiente externo à organização como desastres naturais, conjuntura político-econômica, imprevisibilidade de fornecedores.
- Infraestrutura – Decorrente dos recursos de infraestrutura física ou lógica (sistemas de TI) da organização.
- Recursos humanos ou financeiros – Decorrente da disponibilidade de recursos humanos ou financeiros.

São exemplos de causa: pessoas sem capacitação, falta de legislação.

Consequência diz respeito ao efeito que o evento de risco terá sobre o alcance dos objetivos.

Algumas ferramentas tais como bow-tie e diagrama de causa e efeito ajudam a identificar as causas (e no caso da bow-tie também as consequências).

5.3.1. FERRAMENTAS

5.3.1.1. BRAINSTORMING

Brainstorming (tempestade de ideias) é uma técnica para rapidamente gerar tantas ideias quanto possível sobre um assunto ou problema no menor espaço de tempo. É muito importante que seja realizada de forma livre, sem críticas de forma que as pessoas não se sintam intimidadas ou com vergonha de expor suas ideias.

Regras:

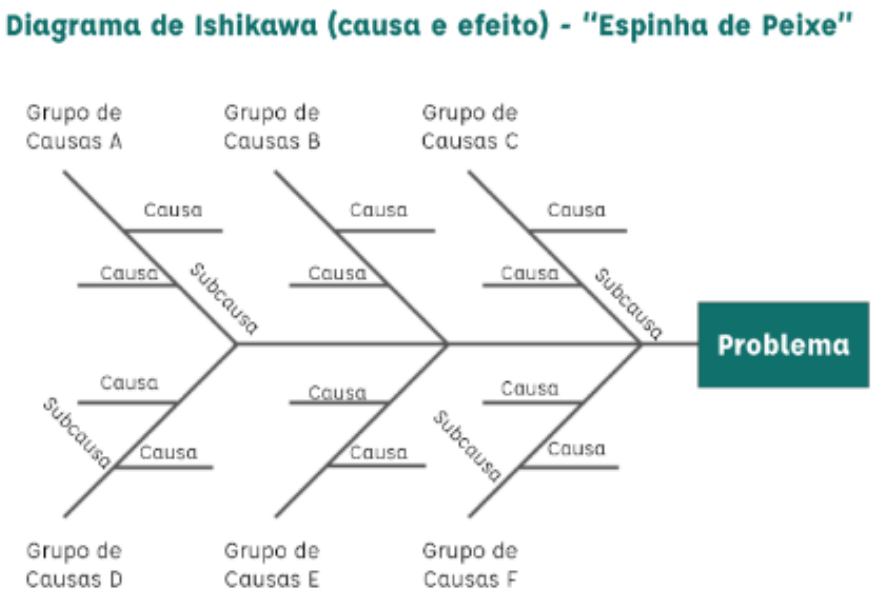
1. Escrever de forma clara o assunto a ser tratado (evento de risco) de modo que todos tenham um mesmo entendimento.
2. Cada participante deve colocar suas ideias de forma livre, sem críticas.
3. Anotar todas as ideias. A exposição de ideias serve de estímulo para novas ideias.
4. Rever todas as ideias colocadas de modo a eliminar as duplicadas.

O brainstorming pode ser usado para identificar os eventos de risco, bem como suas causas e consequências. Entretanto, é recomendável que seja utilizada a ferramenta bow-tie para facilitar a identificação do evento de risco, suas causas e consequências.

5.3.1.2. DIAGRAMA DE CAUSA E EFEITO (ISHIKAWA OU ESPINHA DE PEIXE)

O diagrama de causa e efeito, também conhecido como diagrama de Ishikawa ou diagrama espinha de peixe, representa a relação entre o “efeito” e todas as possíveis causas que podem contribuir para esse efeito.

As causas são agrupadas por categorias e semelhanças previamente estabelecidas, ou percebidas durante o processo de classificação.



Fonte: Assessoria de Comunicação Social - CGE-MG

Nos processos produtivos, geralmente as causas são agrupadas em mão-de-obra, meio ambiente, materiais, máquinas, medição e métodos. Em processos administrativos, os 6M podem ser substituídos por outras classificações tais como pessoas, políticas, procedimentos, meio ambiente, medição e lugar. As categorias são apenas sugestões. Pode ser usada qualquer classificação de categorias principais que ressalte ou auxilie as pessoas a pensarem criativamente.

Etapas:

1. Identificar o efeito que se deseja estudar, ou seja, a característica, medida ou problema para a qual se deseja estabelecer a relação causa-efeito.
2. Fazer um brainstorming das possíveis causas ou variáveis que afetem o “efeito”.
3. Classificar cada item do brainstorming numa das categorias do diagrama.

5.3.1.3. 5 POR QUÊS

Relaciona possíveis causas de um problema a fim de identificar a(s) causa(s) raiz apenas perguntando por que várias vezes (5 vezes é uma regra básica).

PROBLEMA: Tem uma mancha de umidade no forro da sala.

1. Por quê?

Porque a água está caindo no forro

2. Por quê?

Porque existe um buraco no canto do telhado

3. Por quê?

Passarinhos estão fazendo ninho neste local

4. Por quê?

Porque eles não conseguem fazer ninhos nas árvores

5. Por quê?

Porque as árvores não são altas o suficiente para eles ficarem fora do alcance do gato.

Foco deve ser em fechar os buracos no canto do telhado e colocar casa de passarinhos fora do alcance do gato.

5.3.1.4. BOW-TIE

A análise Bow Tie é uma maneira esquemática e simples de descrever e analisar os caminhos de um risco, desde as suas causas até as suas consequências. Após a identificação de um evento de risco, são identificadas as causas e consequências desse

evento de risco. Em segundo lugar, são identificadas as medidas de controle de prevenção que reduzem das chances de ocorrência do evento (antes do evento de risco se materializar) e medidas de mitigação (após o risco se materializar) que atenuam a severidade dos impactos derivados no evento.

A sintaxe abaixo pode ajudar também a verificar se o risco, suas causas e consequências estão corretos:

Descrição do risco: Devido à **CAUSA**, poderá haver **RISCO**, o que poderá ocasionar **CONSEQUÊNCIA**.

Importante também entender o que são controles de forma a facilitar o preenchimento da bow-tie. Os controles são qualquer processo, política, dispositivo, prática ou ação e medida adotada pela gestão" (...) com a finalidade de alcançar os objetivos organizacionais e proporcionar confiança no que diz respeito à eficácia e eficiência dos recursos, por meio da minimização dos riscos relevantes. (VIEIRA e BARRETO, 2019, p.143)

Os controles podem ser classificados em:

- Controles preventivos: controles existentes e que atuam sobre as possíveis causas do risco, com o objetivo de prevenir a sua ocorrência. Exemplos de controles preventivos: atribuição de autoridade e limites de alçada; procedimentos de autorização e aprovação; lista de verificação (checklists); segregação de funções ou atividades; rotatividade de funções; revisões; avaliações de desempenho operacional; avaliações de processos e atividades; supervisão direta; controles de acesso a recursos e registros.

- Controles de atenuação e recuperação: controles existentes executados após a ocorrência do risco com o intuito de diminuir o impacto de suas consequências.

Exemplos de controles de atenuação e recuperação: plano de contingência; tomada de contas especiais; procedimento apuratório.

- Controles detectivos: controles existentes que atuam na detecção da materialização de um risco ou de sua iminência. Exemplos de controles de detecção: indicadores; termômetros; sensores.

Após se identificar todos os controles associados aos riscos identificados é importante classificar os controles, conforme escala abaixo.

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

Antes de avaliar o risco, ainda é preciso classificá-lo quanto à sua categoria.

Quanto à categoria, os riscos serão classificados da seguinte forma: risco estratégico, operacional, financeiro/orçamentário, reputação, integridade, fiscal, conformidade.

Estratégico	Eventos que possam impactar na missão, nas metas ou nos objetivos estratégicos da SEFAZ/RJ, caso venham a ocorrer
Operacional	Eventos que podem comprometer as atividades da SEFAZ/RJ, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas, afetando o esforço da gestão quanto à eficácia e a eficiência dos processos
Financeiro/ Orçamentário	Eventos que podem comprometer a capacidade da SEFAZ/RJ de contar com os recursos orçamentários necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária
Reputação	Eventos que podem comprometer a confiança da sociedade em relação à capacidade da SEFAZ/RJ em cumprir sua missão institucional, interferem diretamente na imagem do órgão
Integridade	Eventos que podem afetar a probidade da gestão dos recursos públicos e das atividades da organização, causados pela falta de honestidade e desvios éticos
Fiscal	Eventos que podem afetar negativamente o equilíbrio das contas públicas
Conformidade	Eventos que podem afetar o cumprimento de leis e regulamentos aplicáveis

Após as etapas anteriores, deve-se realizar a análise dos níveis de risco. A matriz de nível de risco é uma ferramenta que apresenta o resultado visual em função da relação combinada da probabilidade e do impacto de cada evento.

PROBABILIDADE: chance de o evento de risco ocorrer

Critérios de probabilidade:

CRITÉRIO	PESO	DESCRIÇÃO
1) Raro	1	O evento pode ter acontecido anteriormente na organização ou em organizações similares. Entretanto, na ausência de outras informações ou circunstâncias excepcionais, não seria esperado que ocorresse na organização no futuro próximo. O evento pode ocorrer apenas em circunstâncias muito excepcionais. Ficaria surpreso se o evento ocorresse.
2) Improvável	2	O evento não ocorre de maneira frequente na organização ou organizações similares. Os controles atuais e as circunstâncias sugerem que a ocorrência seria considerada altamente não usual. O evento pode ocorrer em algum momento, mas é improvável.
3) Possível	3	O evento pode ter ocorrido ocasionalmente na organização ou em organizações similares. Os controles atuais ou as circunstâncias sugerem que há uma possibilidade plausível de ocorrência. O evento provavelmente ocorrerá em algumas circunstâncias.
4) Provável	4	O evento pode ocorrer regularmente na organização ou organizações similares. Com os controles atuais ou circunstâncias, pode-se esperar que ocorra ao longo de 1 ano. O evento provavelmente ocorrerá na maioria das circunstâncias.
5) Quase Certo	5	O evento ocorre frequentemente na organização ou com os controles ou circunstâncias espera-se sua ocorrência. É esperado que o evento ocorra na maioria das circunstâncias.

IMPACTO: o potencial comprometimento dos objetivos e resultados da unidade, possuindo relação direta com as consequências da ocorrência do risco.

Critérios de impacto:

CRITÉRIO	PESO	DESCRIÇÃO
1) Desprezível	1	O impacto do evento nos objetivos/resultados é insignificante, estando adstrito a procedimentos de determinado setor ou unidade.
2) Menor	2	O impacto do evento nos objetivos/resultados é pequeno, mas afetam de certa forma os procedimentos de determinada área ou setor influenciando os resultados obtidos
3) Moderado	4	O impacto do evento nos objetivos/resultados é médio e tem capacidade de afetar áreas ou unidades isoladas.
4) Maior	8	O impacto do evento sobre os objetivos/resultados da organização é de gravidade elevada, envolvendo áreas inteiras do órgão e/ou seu conjunto e é de difícil reversão.
5) Catastrófico	16	O impacto do evento sobre os objetivos/resultados da organização tem potencial desestruturante sobre todo o órgão e é irreversível.

O nível do risco será descoberto a partir da multiplicação do nível de probabilidade pelo nível de impacto. Ou seja, quanto maior a probabilidade e maior o impacto, maior será a severidade do risco. Estabelecer o nível de risco tem grande importância, pois, em regra, é a partir dela que será definido como o controle será exercido.

$$R = P \times I$$

Em que R = risco

P = probabilidade

I = impacto

Matriz de nível de risco:

IMPACTO	16	Catastrófico	Alto	Extremo	Extremo	Extremo	Extremo
	8	Maior	Médio	Alto	Alto	Extremo	Extremo
	4	Moderado	Baixo	Médio	Alto	Alto	Alto
	2	Menor	Baixo	Baixo	Médio	Médio	Alto
	1	Desprezível	Baixo	Baixo	Baixo	Baixo	Médio
	PESO		Raro	Improvável	Possível	Provável	Quase Certo
		PESO	1	2	3	4	5
			PROBABILIDADE				

Nível de severidade (classificação do risco):

Baixo	1 a 4
Médio	5 a 9
Alto	10 a 30
Extremo	31 a 80

5.4. AVALIAÇÃO DE RISCOS

O propósito da avaliação de riscos é apoiar decisões. A partir do apetite a riscos inicialmente definido, deve-se verificar quais riscos poderão ser aceitos e quais necessariamente deverão ser minimizados, ou seja, onde é necessária ação adicional, conforme tabela a seguir.

Tabela Apetite x Tolerância a Riscos

APETITE DA ORGANIZAÇÃO: BAIXO				
Nível de Risco	**Aceitação do Risco**	**Tratamento do Risco**	**Acompanhamento do Gerenciamento do Risco**	**Tolerância ao Risco**
EXTREMO	Inaceitável	Garantir que ações de controle sejam imediatamente implantadas, sem prejuízo do aprimoramento das ações de controle existentes, visando à redução do nível de risco. As ações de controle deverão ser sempre priorizadas em relação às demais ações de controle.	Comitê Permanente de Governança e Gerenciamento de Riscos	Nível de risco absolutamente intolerável
ALTO	Inaceitável	Garantir que ações de controle sejam implantadas, sem prejuízo do aprimoramento das ações de controle existentes, visando à redução do nível de risco, sempre que possível. As ações de controle deverão ser sempre priorizadas em relação àquelas dos riscos classificados no nível médio.	Subsecretário da Área	Nível de risco intolerável, excepcionalizando os casos em que a redução do nível de risco é impraticável ou seu custo é desproporcional à melhoria obtida.
MÉDIO	Inaceitável	Aprimorar as ações de controle existentes e/ou implementar ações complementares para tratar o risco residual, visando reduzir o nível de risco para o apetite definido.	Subsecretário da Área	Nível de risco tolerável se o custo da redução exceder a melhoria obtida.
BAIXO	Aceitável		Proprietário do Risco	Não se aplica. Nível de risco dentro do apetite definido.

Os riscos EXTREMOS serão acompanhados pelo Comitê Permanente de Governança e Gerenciamento de Riscos em reuniões periódicas, com periodicidade mínima de 2 (duas) vezes ao ano. Os riscos ALTO e MÉDIO serão acompanhados pelo Subsecretário da Área.

Os gestores operacionais devem assegurar que o risco se mantenha dentro do apetite desejado e observá-lo ao definir internamente os objetivos e metas inerentes às suas atividades.

Deve ser realizada a introdução de novos controles ou o aprimoramento dos existentes de forma a diminuir o nível do risco.

5.5. TRATAMENTO DE RISCOS

O tratamento de riscos envolve a seleção de uma ou mais opções para modificar o nível do risco (a probabilidade ou o impacto) e a elaboração de planos de ação que, uma vez implementados, implicarão na introdução de novos controles ou a modificação dos existentes. (TCU, 2017)

Formas de tratar riscos, não mutuamente exclusivas ou adequadas em todas as circunstâncias, incluem evitar, reduzir, compartilhar e aceitar o risco. Selecionar as opções mais apropriadas de tratamento envolve balancear os benefícios, face aos custos, ao esforço ou às desvantagens da implementação.

Fonte: ENAP

De maneira geral, riscos que possuam a classificação alto e extremo necessitam de controles mais rígidos, enquanto o risco médio mais moderado. Importante observar que riscos baixos geralmente não precisam de novos controles implementados, uma vez que seria desperdício de recursos.

A forma como preencher o plano de ação no modelo 2W2H na planilha de riscos encontra-se descrita no “GUIA PARA PREENCHIMENTO DA MATRIZ DE RISCOS”, anexado nos arquivos das Equipes do Teams. A evidência de concretização do produto deve ser periodicamente anexada/atualizada no Teams.

Tipos de Tratamento de Riscos:

Aceitar	A probabilidade e impacto do risco são tão baixos que não justificam a criação de controles para mitigação, ou os controles existentes já resguardam boa parte de suas consequências.
Reduzir	Reduzir a probabilidade e/ou impacto do risco, tornando-o menor ou mesmo removendo-o da lista dos principais riscos, que pode se materializar por meio da criação de novos controles ou da melhoria de controles existentes.
Compartilhar	Reduzir a probabilidade ou impacto da ocorrência do risco pela transferência de responsabilidade a terceiro.
Reduzir/ Compartilhar	Ações de controle combinadas, conforme definição acima.
Evitar	Envolve alterar o processo para evitar a ocorrência do risco.

5.6. MONITORAMENTO E ANÁLISE CRÍTICA

Durante todo o ciclo do processo de gestão de riscos deve haver uma efetiva comunicação entre as partes envolvidas para verificar o desempenho do processo de gestão de riscos, verificar os riscos identificados e as ações de controle propostas bem como reavaliar os riscos e ações.

Assim, a respectiva equipe no Teams deve ser utilizada pelo Comitê Executivo, pelos proprietários do risco bem como pelos pontos focais para:

a) preenchimento da matriz de riscos;
b) preenchimento do plano de ação;
c) inclusão de evidências que demonstrem a ação implementada;
d) disponibilização de materiais de referência que auxiliem os proprietários de risco e os pontos focais no levantamento dos riscos e no preenchimento da matriz de riscos.

Deverão ser realizadas reuniões periódicas entre o Comitê Executivo e as subsecretarias (via ponto focal) de forma a acompanhar o andamento do processo de gestão de riscos nas áreas e o preenchimento da matriz de riscos, bem como retirar dúvidas do processo. Para estas reuniões, também podem e devem ser levadas sugestões que visem a melhorar o processo de gestão de risco.

Como se trata de um processo rotineiro, o proprietário de riscos (via ponto focal) poderá periodicamente reavaliar seus riscos, registrando na matriz de risco a revisão realizada bem como os controles implementados. A identificação de novos riscos também deve ser realizada periodicamente. Importante que, antes da reunião do Comitê Executivo

com o Comitê Permanente de Governança e Gerenciamento de Riscos, os proprietários de riscos (via ponto focal) revisem suas respectivas matrizes de riscos e planos de ação para viabilizar a apresentação de uma “fotografia” mais atual ao Comitê Permanente.

5.7. REGISTRO E RELATO

Trata da documentação do processo de gestão de riscos, dos seus resultados e da apresentação de relatórios às partes interessadas, auxiliando as instâncias internas e externas de governança a cumprirem suas responsabilidades.

Pelo menos 2 vezes por ano, deverá ser realizada a reunião do Comitê Permanente de Governança e Gerenciamento de Riscos, quando o Comitê Executivo informará sobre o andamento da implementação da Gestão de Riscos nas áreas, a quantidade de riscos levantados por área, bem como sua classificação na matriz de risco. Além disso, serão detalhados os riscos extremos de forma a definir prioridades, inclusive alocação de recursos. Adicionalmente, poderão ser propostas melhorias no processo de Gestão de Riscos, visando à melhoria contínua.

Nesse sentido, devem ser desenvolvidos indicadores para monitorar o desempenho da gestão de riscos, pois “o que não se mede, não se gerencia”.

5.8. COMUNICAÇÃO E CONSULTA

O propósito da comunicação e consulta é auxiliar as partes interessadas pertinentes na compreensão do risco, fornecendo subsídio para a tomada de decisões.

O plano de comunicação será realizado em documento separado, de forma a trazer mais agilidade para o processo.

Referências Bibliográficas

ABNT. Gestão de Riscos – Princípio e diretrizes. NBR ISO 31000. Associação Brasileira de

Normas Técnicas. 2018.

Controladoria Geral do Estado de Goiás - Manual Orientativo Às Secretarias Executivas / Escritórios de Compliance. Disponível em https://www.controladoria.go.gov.br/files/New-Folder-6/Anexo1_14482.pdf

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

Tribunal de Justiça do Estado do Rio de Janeiro - Plano de Gestão de Riscos. Disponível em https://portaltj.tjrj.jus.br/documents/10136/182315962/Plano_de_Riscos.pdf/

ELABORADO POR

Subsecretário de Controle Interno

Francisco Pereira Iglesias

Assessora Especial de Controle Interno

Ana Caroline Rabelo Umbelino

Auditora Interna

Inah Sá Barretto Paraiso

Auditora Fiscal da Receita Estadual

Gabriela Menegassi Meilhac Ross

FORMATAÇÃO E PRODUÇÃO VISUAL

Auditor Fiscal da Receita Estadual

Fernando Salavracos Komatsu