Manual de
GESTÃO DE RISCOS

SECRETARIA DE ESTADO DE ECONOMIA DO DISTRITO FEDERAL

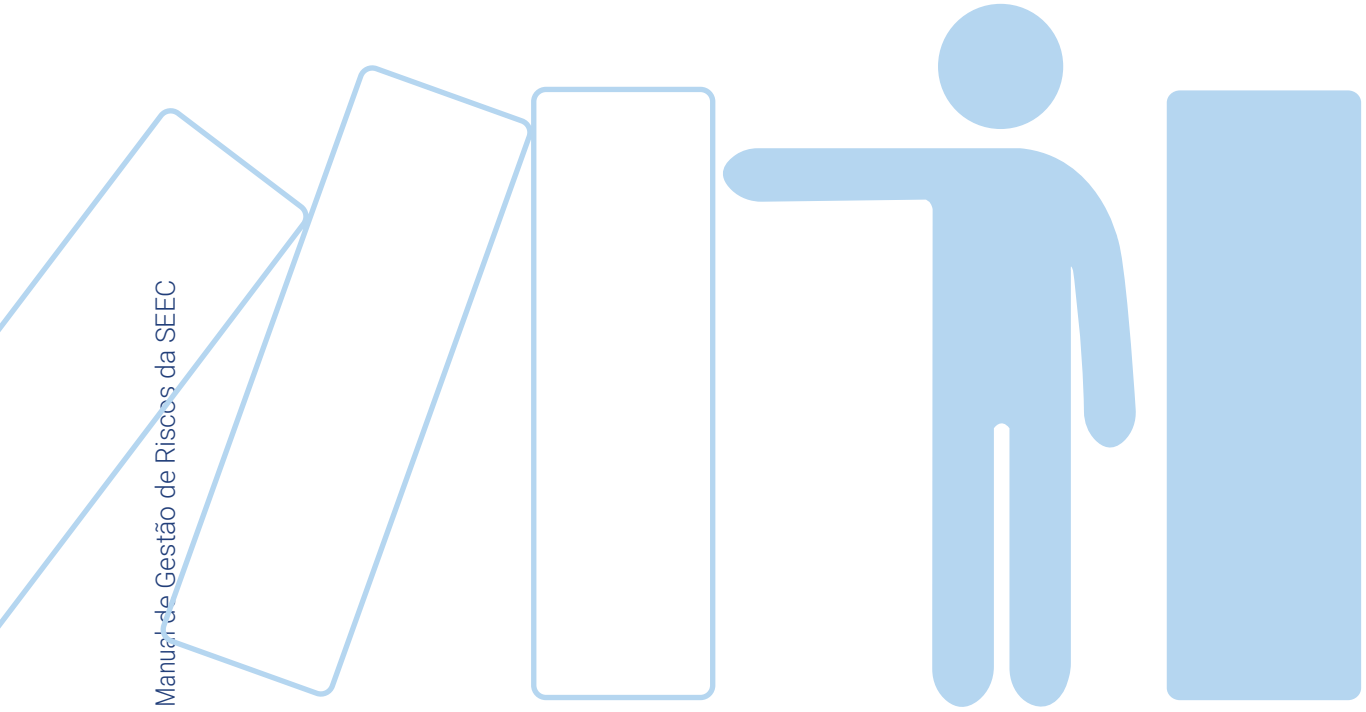
Sumário.

1. Apresentação

Este manual visa instruir sobre o Processo de Gestão de Riscos no âmbito da Secretaria de Estado de Economia do Distrito Federal (SEEC), com vistas à incorporação da análise de riscos à tomada de decisão, em conformidade com as boas práticas de governança adotadas no setor público.

As instruções contidas neste manual devem ser observadas por todas as áreas e os níveis de atuação da SEEC.

As atualizações deste manual serão identificadas e realizadas pela Subsecretaria de Governança, Análise e Avaliação da Estratégia (SUGEST) da Secretaria Executiva de Gestão da Estratégia (SGE) da SEEC.



2. Metodologia da Gestão de Riscos

2.1Diretrizes

A gestão de riscos, conforme definida pela Política de Governança Pública e Compliance no âmbito da Administração Direta, Autárquica e Fundacional do Poder Executivo do Distrito Federal[4], é processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar o órgão ou a entidade, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

A gestão de riscos no âmbito da Secretaria de Estado de Economia do Distrito Federal (SEEC) deverá ser permanente e observará a integração com as iniciativas e os processos estratégicos institucionais, bem como ser realizada de forma transparente e participativa.

Nesse sentido, a Política de Gestão de Riscos da SEEC será implementada de forma progressiva, incluindo avaliações periódicas e ajustes conforme necessário, alinhada ao Planejamento Estratégico Institucional (PEI).

Ademais, quanto ao assunto, recomenda-se a leitura dos seguintes normativos:

a) Decreto nº 37.302, de 29 de abril de 2016: estabelece os modelos de boas práticas gerenciais em Gestão de Riscos e Controle Interno a serem adotados no âmbito da Administração Pública do Distrito Federal;

b) Decreto nº 39.736, de 28 de março de 2019: dispõe sobre a Política de Governança Pública e Compliance no âmbito da Administração Direta, Autárquica e Fundacional do Poder Executivo do Distrito Federal;

c) Portaria nº 356, de 17 de maio de 2023: dispõe sobre a Política de Integridade Pública no âmbito da Secretaria de Estado de Economia do Distrito Federal (SEEC);

d) Decreto nº 45.933, de 20 de junho de 2024: dispõe sobre a composição e as competências das Unidades de Controle Interno do Poder Executivo do Distrito Federal, e dá outras providências;

e) Norma ABNT NBR ISO 31000:2018 - Gestão de Riscos;

f) Norma ABNT NBR ISO 19011:2011 - Diretrizes para Auditoria de Sistemas de Gestão; e

g) Controle Interno - Estrutura Integrada - 2013 do Comitê de Organizações Patrocinadoras da Comissão Treadway (COSO).

4 Decreto Nº 39.736, de 28 de março de 2019.

2.2 Papéis e Responsabilidades

2.2.1 Instâncias responsáveis pela Gestão de Riscos

São instâncias responsáveis pela Gestão de Riscos na Secretaria de Estado de Economia do Distrito Federal (SEEC):

I) Gerentes dos projetos, donos dos processos e seus respectivos substitutos;
II) Subsecretaria de Processos e de Projetos Institucionais e Inovação (SPPII);
III) Subsecretaria de Governança, Análise e Avaliação da Estratégia (SUGEST);
IV) Unidade de Controle Interno (UCI); e
V) Comitê Interno de Governança (CIG) da SEEC.

Considerando as instâncias responsáveis indicadas no item acima, são estabelecidas as seguintes competências:

I) Gerentes dos projetos e donos dos processos e seus respectivos substitutos:

a) Realizar a gestão dos riscos nos processos de trabalho, projetos e ações sob sua responsabilidade;
b) Elaborar a documentação e os artefatos pertinentes à operacionalização da gestão dos riscos nos processos de trabalho, projetos e ações sob sua responsabilidade;
c) Conduzir as reuniões com a equipe do processo de trabalho, projeto e/ou ação, para implementar controles de prevenção e tratamento de riscos;
d) Manter comunicação regular e tempestiva com as partes interessadas no gerenciamento dos riscos do processo de trabalho, projeto e/ou ação;
e) Assegurar o cumprimento dos eventuais prazos estabelecidos no âmbito do gerenciamento dos riscos; prestar informações e fornecer subsídios para auditorias, levantamentos, inspeções e monitoramentos acerca da gestão de riscos realizados no âmbito da unidade; e
f) Confeccionar relatórios e informativos para a SEEC, sempre que necessário e quando solicitado.

II) Subsecretaria de Processos e de Projetos Institucionais e Inovação (SPPII):

a) Monitorar o gerenciamento dos riscos referentes aos projetos e ações estratégicas do Planejamento Estratégico Institucional;
b) Prestar informações referentes ao monitoramento dos riscos dos projetos e ações estratégicas do Planejamento Estratégico Institucional à alta gestão;
c) Assistir aos gerentes de projetos e aos donos de processos no desempenho das funções relacionadas aos riscos de projetos e processos estratégicos sob sua responsabilidade; e
d) Promover a adoção de práticas que corroborem com a institucionalização do gerenciamento de riscos na gestão dos projetos estratégicos da Secretaria.

III) Subsecretaria de Governança, Análise e Avaliação da Estratégia (SUGEST):

a) Coordenar o processo de implementação da gestão de riscos na SEEC;

b) Propor a revisão do Manual de Gestão de Riscos da SEEC;

c) Consolidar os resultados da gestão de riscos das diversas unidades em relatórios gerenciais e encaminhá-los ao Comitê Interno de Governança (CIG) da SEEC;

d) Orientar, disseminar e promover temas pertinentes a gestão de riscos;

e) Promover a integridade de todo o processo de gerenciamento de risco; e

f) Coordenar a divulgação e comunicação do gerenciamento do risco na SEEC.

IV) Unidade de Controle Interno (UCI):

a) Apoiar a gestão no desenvolvimento de políticas e de processos de gerenciamento de riscos;

b) Apoiar a primeira linha na implementação de controles internos e práticas de gestão de riscos;

c) Monitorar os controles primários implementados pela primeira linha e a gestão de riscos a eles relacionados;

d) Monitorar o andamento da gestão de riscos, identificando se as ações e os projetos para tratamento dos riscos estão sendo implementados e gerando os efeitos esperados;

e) Recomendar aos atores da primeira linha a correção de falhas, omissões ou impropriedades identificadas;

f) ncentivar a formação e a capacitação dos agentes públicos envolvido no processo de gestão de riscos;

g) Sugerir melhorias nos procedimentos relativos à gestão de riscos, podendo propor ou até mesmo estabelecer novos controles, adequar os controles já existentes ou propor a remoção de controles ineficazes, ineficientes ou que se tornaram desnecessários;

h) Acompanhar, quando solicitado pelo gestor, o gerenciamento de riscos implementado pelas unidades orgânicas da Administração;

i) Apoiar auditorias, levantamentos, inspeções e monitoramentos acerca da gestão de riscos realizados no âmbito da unidade; e

j) Prestar colaboração técnica relativa à gestão de riscos na elaboração e na atualização de normas internas e de manuais.

V) Comitê Interno de Governança (CIG) da SEEC:

a) Promover a implementação e aplicação da gestão de riscos de forma sistemática, estruturada, oportuna e documentada;

b) Integrar a gestão de riscos ao processo de planejamento estratégico e aos seus desdobramentos;

c) Utilizar os resultados da gestão de riscos para apoio à melhoria contínua do desempenho e dos processos de gerenciamento de risco e governança;

d) Definir a tolerância ao risco dos processos organizacionais; e

f) Fomentar o desenvolvimento da cultura de gestão de riscos.

2.2.2 Modelo das Três Linhas

Na Secretaria de Estado da Economia do Distrito Federal (SEEC), os papéis e as responsabilidades referentes ao Processo de Gestão de Riscos serão operacionalizadas conforme o Modelo das Três Linhas do The IIA 2020 , indicado na imagem a seguir

Dessa maneira, o Instituto dos Auditores Internos do Brasil - IIA Brasil comunica que o Modelo das Três Linhas ajuda as organizações a identificar estruturas e processos que melhor auxiliam no atingimento dos objetivos e facilitam uma forte governança e gerenciamento de riscos.

A responsabilidade da gestão de atingir os objetivos organizacionais compreende os papéis da primeira e segunda linhas. Os papéis de primeira linha estão mais diretamente alinhados com a entrega de produtos e/ou serviços aos clientes da organização, incluindo funções de apoio. Os papéis de segunda linha fornecem assistência no gerenciamento de riscos.

Os papéis da terceira linha prestam avaliação e assessoria independentes e objetivas sobre a adequação e eficácia da governança e do gerenciamento de riscos. Ao fazê-lo, pode considerar a avaliação de outros prestadores internos e externos.

Assim, temos:

a) Primeira Linha: é exercida pelos proprietários do risco, aqueles que gerenciam os riscos e têm propriedade sobre eles. Eles também são os responsáveis por implementar as ações corretivas para resolver deficiências em processos e controles;

B) Segunda Linha: é exercida considerando o apoio e monitoramento dos riscos e conformidade para ajudar a desenvolver e/ou monitorar os controles da primeira linha; e

C) Terceira Linha: é exercida pelos setores responsáveis pela função de auditoria interna, incluindo tanto a auditoria geral, realizada pela Controladoria-Geral do Distrito Federal (CGDF), quanto às unidades setoriais de auditoria interna presentes na Administração Indireta.

4 The IIA - The Institute of Internal Auditors (IIA). Associação profissional internacional organizada em 1941 para desenvolver a condição profissional da auditoria interna.

2.3 Do Processo de Gestão de Riscos

O Processo de Gestão de Riscos envolve a aplicação sistemática de políticas, procedimentos e práticas para as atividades de estabelecimento do escopo, contexto e critério, identificação, análise, avaliação, tratamento, monitoramento e análise, comunicação e consulta e registro e relato dos riscos.

Ressalta-se a importância de que o processo de gestão de riscos seja parte integrante da gestão e da tomada de decisão e seja integrado na estrutura, nas operações e nos processos da organização.

Na Secretaria de Estado da Economia do Distrito Federal (SEEC), o processo de gestão de riscos compreende:

a) **Estabelecimento do Escopo, Contexto e Critério:** tem com objetivo conhecer o contexto e definir os critérios de riscos, e assim, personalizar o processo de gestão de riscos do projeto e/ou ação;

b) **Identificação dos Riscos:** tem por finalidade identificar e registrar tanto os eventos de risco que comprometem o alcance do objetivo do processo, como as causas, efeitos e consequências de cada um deles. Por meio da identificação de eventos de riscos, pode-se planejar a forma de tratamento adequada e o qual o tipo de resposta a ser dada a esse risco, destacando que os eventos de risco devem ser entendidos como parte de um contexto, e não de forma isolada;

c) **Análise dos Riscos:** possui como propósito compreender a natureza do risco e as suas características, incluindo o nível do risco quanto à sua probabilidade (chance de o evento ocorrer) e consequência (impacto), assim como a elaboração de cada plano de ação e/ou estratégia de controle a ser implementada, visando corresponder adequadamente a cada risco identificado;

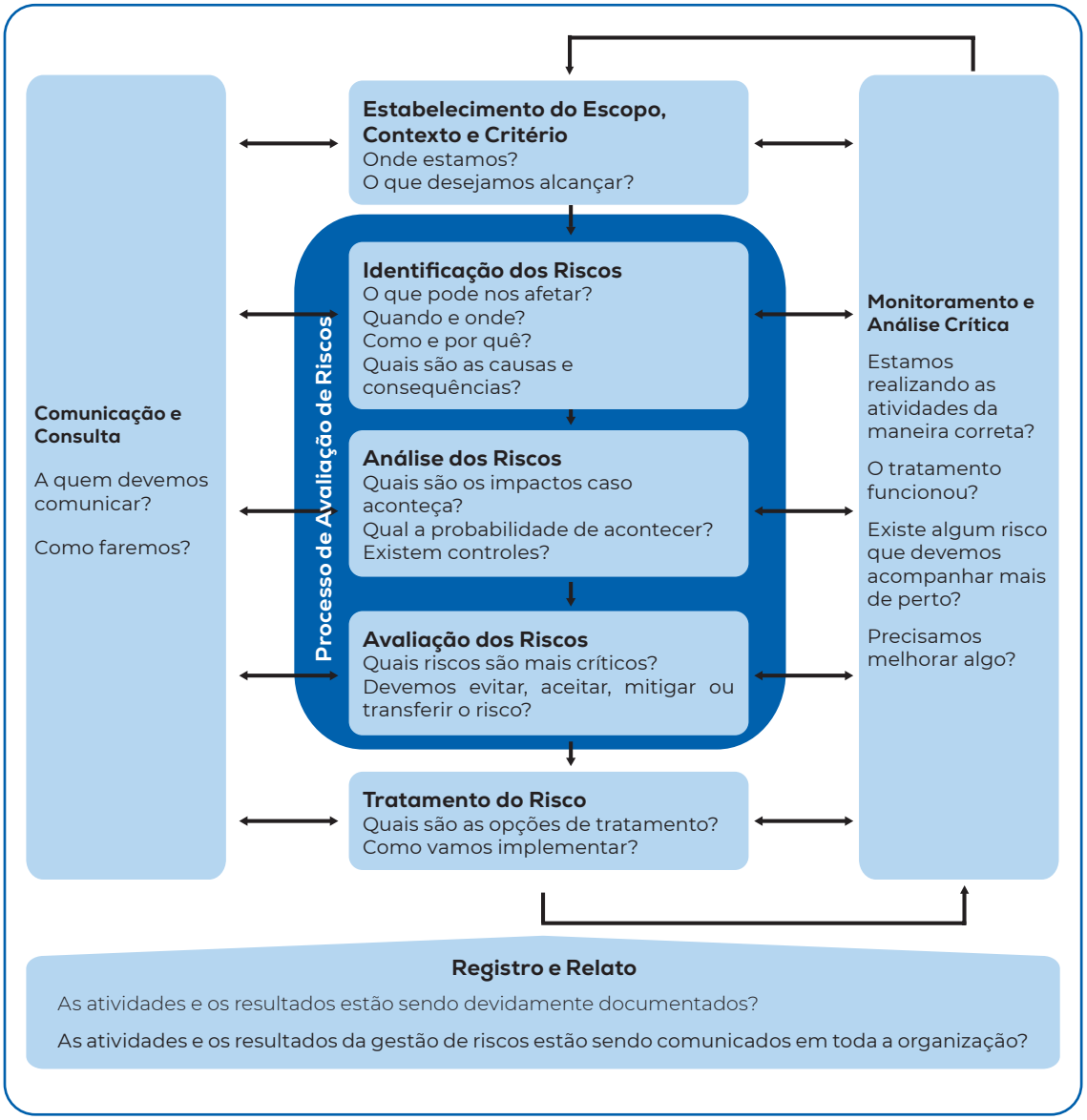
d) **Avaliação dos Riscos:** objetiva comparar os resultados da análise de riscos sob a perspectiva de probabilidade e impacto, a fim de apoiar a tomada de decisão;

e) **Tratamento dos Riscos:** tem como objetivo selecionar e implementar opções para abordar riscos, escolhendo a(s) opção(ões) mais apropriada(s) de tratamento, balanceando os benefícios potenciais derivados em relação ao alcance dos objetivos, face aos custos, esforço ou desvantagens da implementação;

f) **Monitoramento e Análise Crítica dos Riscos:** a presente atividade possui a finalidade de garantir a compreensão de todos os agentes envolvidos, no processo de tomada de decisão, de forma a reduzir riscos de respostas inadequadas aos riscos, bem como promover a eficácia dos objetos e ferramentas de controle;

g) **Comunicação e Consulta:** realizada com o propósito de auxiliar as partes interessadas na compreensão do risco, sobre as decisões que são tomadas e nas razões pelas quais eventuais ações específicas são requeridas. A comunicação busca promover a conscientização e o entendimento do risco, enquanto a consulta envolve obter retorno e informação para auxiliar na tomada de decisão; e

h) **Registro e Relato:** as atividades da gestão de riscos devem ser rastreáveis. No processo de gestão de riscos, os registros fornecem os fundamentos para a melhoria dos métodos e ferramentas, bem como de todo o processo.



Sem prejuízo das informações indicadas acima, as atividades do Processo de Gestão de Riscos da SEEC serão tratadas em seção própria.

2.3.1 Estabelecimento do Escopo, Contexto e Critério

O processo de gestão de riscos inicia-se pelo estabelecimento do escopo, contexto e critério de riscos do objeto a ser tratado.

Nesta atividade, há o entendimento do histórico da organização e de seus riscos, a definição do escopo das atividades de gestão de riscos que estão sendo realizadas e o desenvolvimento de uma estrutura para as tarefas de gestão de riscos subsequentes.

O propósito aqui é personalizar o processo de gestão de riscos, permitindo um processo de avaliação de riscos eficaz e um tratamento de riscos apropriado.

Como o processo de gestão de riscos pode ser aplicado em diferentes níveis (por exemplo, estratégico, tático, operacional, iniciativas, projetos e ações ou outras atividades), o escopo precisa ser claro, considerando os objetivos do processo e o seu alinhamento aos objetivos organizacionais.

Para o estabelecimento do contexto, deve-se realizar uma avaliação do ambiente específico da atividade ao qual o processo de gestão de riscos será aplicado. Portanto, é importante entender o histórico e identificar os fatores relacionados ao ambiente (interno e externo), de modo a alcançar uma visão abrangente de todos os fatores que possam influenciar a capacidade da organização de atingir os resultados esperados.

No contexto interno, deve-se levar em consideração políticas e normativos correlacionados, objetivos, recursos (humanos, materiais e financeiros), conhecimento, sistemas de informação, processo decisório, partes interessadas, modelos e diretrizes da organização responsável e quaisquer outras informações internas relevantes.

No contexto externo, considera-se o ambiente no qual a organização busca atingir seus objetivos, incluindo interdependências com outras organizações, dentro ou fora do governo, e macro ambiente externo (economia, política, legislação - nacional ou internacional).

O correto estabelecimento do contexto permite compreender as principais características internas e o momento em que a organização se encontra, como, por exemplo: a sua posição estratégica no Distrito Federal; o seu relacionamento com os servidores e demais colaboradores e indícios acerca do futuro e da continuidade de seus serviços esperados pelos seus principais usuários.

O estabelecimento de critérios de risco, por sua vez, deve considerar a natureza e o tipo de incertezas que podem afetar os resultados e objetivos, como as consequências e probabilidades serão definidas e medidas, como o nível de risco será determinado, entre outros aspectos.

Os critérios de risco, apesar de estabelecidos no início do processo, são dinâmicos. Logo, devem ser continuamente analisados de forma crítica e alterados, se necessário.

Para esta atividade, recomenda-se a utilização da Matriz Swot. Trata-se de uma ferramenta de gestão. A sigla provém do inglês e busca identificar Strengths (Forças/Pontos Fortes), Weaknesses (Fraquezas/Pontos Fracos), Opportunities (Oportunidades) e Threats (Ameaças) de um projeto ou de plano de negócios geral.

As características indicadas no item acima podem ser lidas da seguinte maneira:

Forças/Pontos Fortes: vantagens internas;

Fraquezas/Pontos Fracos: desvantagens internas;

Oportunidades: aspectos externos positivos que podem potencializar as atividades pertinentes ao projeto; e

Ameaças: aspectos externos negativos que podem pôr em risco as atividades pertinentes ao projeto.

A fim de facilitar o estabelecimento do escopo, contexto e critério abordados, é disponibilizada uma sugestão de documento a ser utilizado no Anexo I - Estabelecimento de Escopo, Contexto e Critério, arquivo anexo a este manual.

2.3.2 Identificação dos Riscos

A atividade de identificação de riscos pode ser caracterizada por meio das atividades de levantamento, identificação e descrição dos riscos, tendo por base as informações obtidas na atividade de estabelecimento do contexto.

A finalidade da atividade de identificação dos riscos é elaborar um registro abrangente dos eventos de riscos. Eventos de risco são situações em potencial – que ainda não ocorreram – que podem causar impacto na consecução dos objetivos da organização, caso venham a ocorrer.

Os componentes do evento de risco são as causas, os seus eventuais riscos e a consequências e podem ser descritos como indicado a seguir:

Causas são as condições que dão origem à possibilidade de um evento ocorrer, e podem ter origem no ambiente interno e externo;

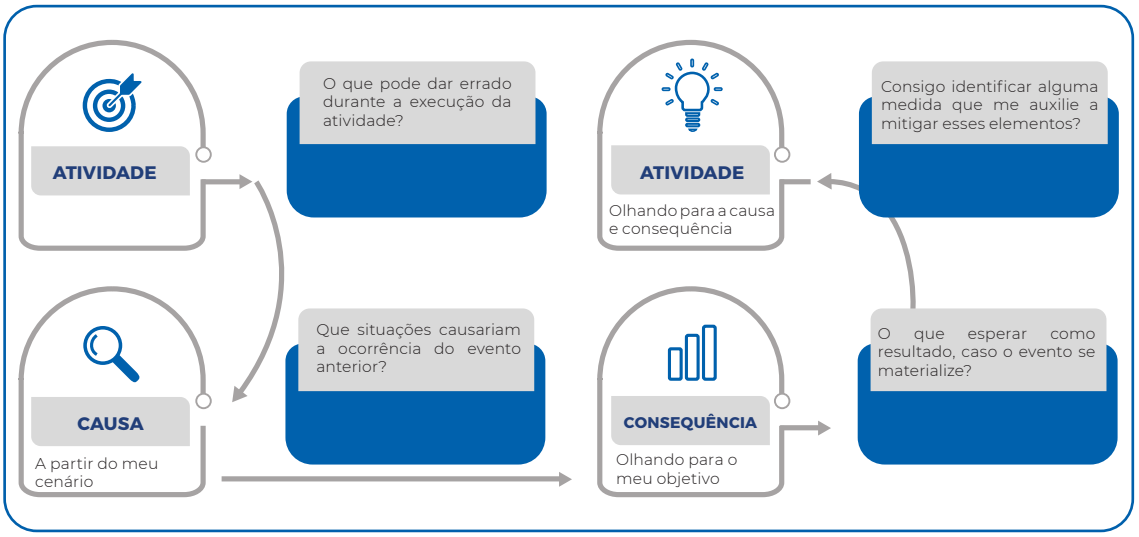
Risco é o efeito da incerteza nos objetivos; e

Consequência é o resultado de um evento que afeta os objetivos.

Esta atividade requer a participação de servidores com conhecimento do processo e visão abrangente da organização e/ou unidade. A técnica a ser utilizada na identificação de eventos de risco deve ser a que melhor se adapta ao caso, como

exemplo, mas não se limitando: questionários e formulários de checagem e/ou lista de controle (check-list); debates e/ou discussões (brainstorming), fluxogramas, diagramas de causa e efeito, entre outros.

Para facilitar a identificação dos eventos de risco, recomenda-se que a abordagem seja aplicada considerando um direcionamento geral para o específico. Isto é, inicialmente podem ser identificados os riscos que permeiam os processos mais críticos e estratégicos em um nível mais amplo, servindo como ponto inicial para, posteriormente, analisar os riscos de forma minuciosa, replicando esse método para os demais processos e/ou atividades julgados necessários.



Após identificado os eventos, recomenda-se, também, a utilização de uma estrutura em formato de planilha – podendo ser no Excel ou similar - a ser denominada "Matriz de Riscos". Assim, a primeira coluna poderá conter os eventos de riscos identificados, a segunda coluna apresentará as causas e a terceira coluna as consequências, conforme modelo indicado a seguir:

PROJETO		
IDENTIFICAÇÃO DOS RISCOS		
RISCOS	**CAUSAS**	**CONSEQUÊNCIAS**
R1		
R2		
R3		
R4		
R5		

A partir da escolha do formato para ser realizada a identificação, sugere-se a sua utilização durante todo o processo de gestão de riscos, adequando-a conforme a necessidade, por meio da inclusão de novas colunas, a depender da atividade a que se refere.

2.3.3 Análise dos Riscos

Nesta atividade por meio da análise de cada risco, além de compreender a natureza do risco e quais são as suas características, é possível determinar o nível de risco quanto à sua probabilidade de ocorrência e os potenciais impactos (negativos e/ou positivos) nos objetivos organizacionais.

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).

Nesse sentido, para o processo de gestão de riscos, considera-se probabilidade as chances reais do risco identificado ocorrer, sendo fundamentada na análise de dados históricos do processo, devidamente observada na atividade de estabelecimento do contexto.

Já o impacto de um risco pode ser caracterizado como qualquer repercussão que se manifeste após a ocorrência do risco, como exemplo, mas não se limitando: financeira, operacional, de imagem, dentre outras.

Com base nestas informações, é possível realizar a classificação dos riscos de maneira mais efetiva e precisa, assim como a elaboração de cada plano de ação e/ou estratégia de controle a ser implementada, visando corresponder adequadamente a cada risco identificado.

Considerando as metodologias disponíveis e, ainda, os instrumentos de boas práticas técnicas e gerenciais recomenda-se que a classificação dos riscos, seja realizada da seguinte maneira:

g) Quanto à probabilidade: em até 5 (cinco) níveis, sendo: 1 (um) para improvável; 2 (dois) para raro; 3 (três) possí-vel; 4 (quatro) provável) e 5 (cinco) quase certo, conforme a imagem indicada a seguir:

ESCALA SIMPLES DE PROBABILIDADES

NÍVEL	DESCRIÇÃO	DEFINIÇÃO
5	**QUASE CERTO**	De forma **inequívoca**, o evento ocorrerá, salvo exceções
4	**PROVÁVEL**	O evento é **esperado**, mas pode não ocorrer
3	**POSSÍVEL**	O evento **tem chance** de ocorrer
2	**RARO**	O evento tem **pequena chance** de ocorrer
1	**IMPROVÁVEL**	O evento tem **mínimas chances** de ocorrer

b) Quanto ao impacto: também em até 5 (cinco) níveis, conforme indicado a seguir:

b1) Risco negativos (desvantagem) - 1 (um) para desprezível; 2 (dois) menor; 3 (três) moderada; 4 (quatro) maior e 5 (catastrófica), conforme a imagem indicada a seguir:

ESCALA SIMPLES DE CONSEQUÊNCIAS (IMPACTOS) - RISCOS NEGATIVOS

NÍVEL	DESCRIÇÃO	DEFINIÇÃO
5	**CATASTRÓFICA**	Impacto **muito alto**, de **forma irreversível**
4	**MAIOR**	Impacto **significativo (alto)**, de **difícil reversão**
3	**MODERADA**	Impacto **médio**, porém **recuperável**
2	**MENOR**	Impacto **pequeno**
1	**DESPREZÍVEL**	Impacto **insignificante**

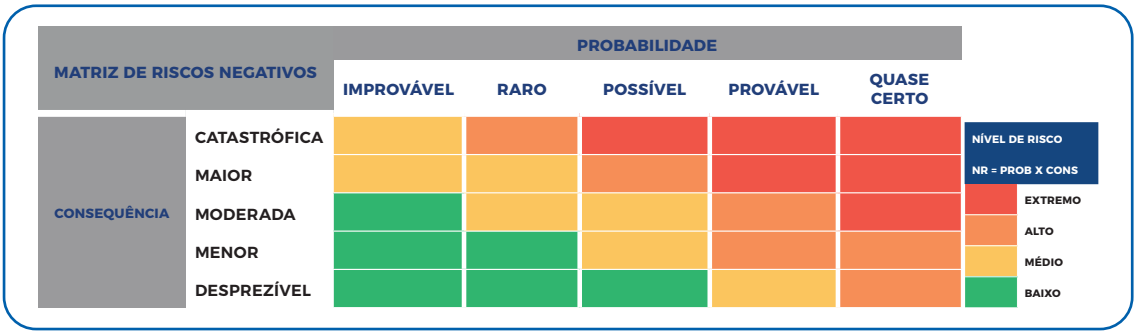
b2) Riscos positivos - 1 (um) para leve; 2 (dois) para sensível; 3 (três) para moderada; 4 (quatro) para substancial e 5 (cinco) extraordinária, conforme imagem indicada a seguir:

4 ABNT NBR ISO 31000: Gestão de Riscos – Diretrizes.

ESCALA SIMPLES DE CONSEQUÊNCIAS (IMPACTOS) RISCOS POSITIVOS		
NÍVEL	**DESCRIÇÃO**	**DEFINIÇÃO**
5	**EXTRAORDINÁRIA**	Contribuição **excelente**
4	**SUBSTANCIAL**	Contribuição **grande**
3	**MODERADA**	Contribuição **moderada**
2	**SENSÍVEL**	Contribuição **pequena**
1	**LEVE**	Contribuição **mínima**

A partir da análise conjunta dessas informações e à luz do risco analisado, é possível determinar a classificação final do risco, dando origem à Matriz de Riscos. Para a elaboração da Matriz de Risco4, é necessário dispor de dois valores: o primeiro - o peso da probabilidade do risco, enquanto o segundo peso se refere ao impacto, também, do risco em questão.

No exemplo apresentado anteriormente a combinação dos parâmetros acima descritos resulta em 4 (quatro) níveis de riscos categorizados como: baixo, médio, alto e extremos, conforme imagem indicada a seguir:



Por fim, será possível adicionar uma coluna referente às informações obtidas quanto à análise dos riscos na Matriz de Riscos, conforme imagem indicada a seguir:

PROJETO					
IDENTIFICAÇÃO DOS RISCOS			CLASSIFICAÇÃO DOS RISCOS	ANÁLISE DOS RISCOS	
RISCOS	**CAUSAS**	**CONSEQUÊNCIAS**		**PROBABILIDADE**	**IMPACTO**
R1	CA1	CO1	Ex: Operacional	Possível	Menor
	CA2	CO2		Provável	Catastrófico
R2	CA1	CO1	Ex: Legal	Raro	Desprezível
R3	CA1	CO1	Ex: Financeiro	Possível	Moderado
R4	CA1	CO1	Ex: Estratégico	Improvável	Menor
	CA2	CO2		Quase Certo	Maior
R5	CA1	CO1	Ex: Conformidade	Raro	Desprezível

2.3.4 Avaliação dos Riscos

O propósito da atividade de avaliação dos riscos é auxiliar no processo de tomada de decisões, com base nos resultados das atividades anteriores.

Nesta atividade, devem ser comparados os resultados obtidos na atividade de análise dos riscos com os critérios de riscos ora estabelecidos para determinar se é necessária realizar ação adicional, resultando em uma das seguintes decisões:

a) Fazer mais nada;
b) Considerar as opções de tratamento de riscos;
c) Realizar análises adicionais para melhor compreender os riscos;

4 A etapa de avaliação de riscos definida na norma ABNT NBR ISO 31000:2018 é composta por três atividades: identificação, análise e avaliação de riscos. O modelo de classificação indicado acima é apresentado no Portal de Gestão de Riscos do Distrito Federal apresentado pela Controladoria Geral do Distrito Federal. Endereço eletrônico: https://www.gestaoderiscos.cg.df.gov.br/index.php/implantandogr/avaliacao-de-riscos/

d) Manter os controles existentes; e

e) Reconsiderar os objetivos.

Convém destacar que as decisões levam em consideração o contexto mais amplo e as consequências reais e percebidas para as partes interessadas externas e internas, bem como que o resultado da avaliação de riscos seja registrado, comunicado e então validado nos níveis apropriados da organização.

Ressalta-se que para apoiar o processo de avaliação de riscos é necessário estabelecer critérios para a priorização e o tratamento associados aos níveis de risco (nível recomendado de atenção, tempo de resposta requerido, quem deve ser comunicado, entre outros parâmetros). A imagem a seguir apresenta sugestão de critérios para avaliação de riscos:

NÍVEL DE RISCO	CRITÉRIOS PARA AVALIAÇÃO DE RISCOS
RISCO EXTREMO	Riscos cujos responsáveis devem adotar medidas imediatas de redução ou erradicação.
RISCO ALTO	Riscos cujos responsáveis devem adotar medidas programadas de redução ou erradicação desse risco.
RISCO MÉDIO	Riscos que devem ser mitigados, mas podem ser tolerados se houver um equilíbrio entre as consequências potencialmente adversas e os benefícios que possam ser obtidos.
RISCO BAIXO	Riscos que estão dentro do apetite a risco, pois as consequências de sua materialização representam relevância tão insignficante que não há necessidade de adoção de alguma medida de tratamento, devendo o risco ser aceito pelo proprietário.

Considerando as informações das atividades anteriores e a Matriz de Riscos até então elaborada, é possível adicionar uma coluna observando os critérios para avaliação de riscos adotados, conforme imagem indicada a seguir:

PROJETO						
IDENTIFICAÇÃO DOS RISCOS			CLASSIFICAÇÃO DOS RISCOS	ANÁLISE DOS RISCOS		ANÁLISE DOS RISCOS
RISCOS	CAUSAS	CONSEQUÊNCIAS		PROBABILIDADE	IMPACTO	NÍVEL DE RISCO
R1	CA1	CO1	Ex: Operacional	Possível	Menor	Médio
	CA2	CO2		Provável	Catastrófico	Extremo
R2	CA1	CO1	Ex: Legal	Raro	Desprezível	Baixo
R3	CA1	CO1	Ex: Financeiro	Possível	Moderado	Médio
R4	CA1	CO1	Ex: Estratégico	Improvável	Menor	Baixo
	CA2	CO2		Quase Certo	Maior	Extremo
R5	CA1	CO1	Ex: Conformidade	Raro	Desprezível	Baixo

Nesta atividade, é possível, ainda, identificar e avaliar os controles internos que incidam sobre os riscos observados.

Os controles são medidas que mantêm e/ou modificam o risco, incluindo, mas não estão limitados a qualquer processo, política, dispositivo, prática ou outras condições e/ou ações. Após a listagem e/ou o mapeamento dos controles existentes, faz-se necessária a consideração de seu funcionamento em relação aos riscos que o afetam.

Nesse sentido, destaca-se que um risco pode ter mais de um controle e os controles podem afetar mais de um risco. Convém que os seguintes aspectos dos controles sejam considerados:

Em referência à listagem e/ou ao mapeamento dos controles existentes e a consideração de seu funcionamento em relação aos riscos que o afetam, conforme identificado nas atividades anteriores, é possível realizar a análise quanto à proposição de novos controles em razão aos controles existentes a fim de orientar o tratamento dos riscos. Para tanto, podem ser incluídas colunas referentes aos controles existentes e novos controles na Matriz de Riscos, conforme imagem indicada a seguir:

PROJETO								
IDENTIFICAÇÃO DOS RISCOS			CLASSIFICAÇÃO DOS RISCOS	ANÁLISE DOS RISCOS		ANÁLISE DOS RISCOS	CONTROLES EXISTENTES	NOVOS CONTROLES
RISCOS	CAUSAS	CONSEQUÊNCIAS		PROBABILIDADE	IMPACTO	NÍVEL DE RISCO		
R1	CA1	CO1	Ex: Operacional	Possível	Menor	Médio		
	CA2	CO2		Provável	Catastrófico	Extremo		
R2	CA1	CO1	Ex: Legal	Raro	Desprezível	Baixo		
R3	CA1	CO1	Ex: Financeiro	Possível	Moderado	Médio		
R4	CA1	CO1	Ex: Estratégico	Improvável	Menor	Baixo		
	CA2	CO2		Quase Certo	Maior	Extremo		
R5	CA1	CO1	Ex: Conformidade	Raro	Desprezível	Baixo		

2.3.5 Tratamento dos Riscos

O tratamento de riscos envolve a seleção de uma ou mais opções para abordar riscos, envolvendo um processo iterativo de:

a) Formular e selecionar opções para tratamento do risco;
b) Planejar e implementar o tratamento do risco;
c) Avaliar a eficácia deste tratamento;
d) Decidir se o risco remanescente é aceitável;
e) Se não for aceitável, realizar tratamento adicional.

Ao selecionar opções de tratamento de riscos, convém que a organização considere os valores, percepções e potencial envolvimento das partes interessadas, e as formas mais apropriadas para com elas se comunicar e consultar. Convém ressaltar que, embora igualmente eficazes, alguns tratamentos de riscos podem ser mais aceitáveis para algumas partes interessadas do que para outras.

As opções de tratamento de riscos não são necessariamente mutuamente exclusivas ou apropriadas em todas as circunstâncias. Dessa forma, as opções de tratamento de riscos incluem:

a) Evitar o risco: consiste em não iniciar ou de descontinuar a atividade, ou ainda desfazer-se do objeto sujeito ao risco;
b) Reduzir ou mitigar o risco: consiste em adotar medidas para reduzir a probabilidade e/ou a consequência dos riscos ou até mesmo ambos;
c) Compartilhar ou transferir o risco: consiste na ação de transferir a responsabilidade ou a parte das consequências de um risco para outra parte, o que pode ser feito por meio de contratos, seguros, terceirização, entre outros métodos; e
d) Aceitar ou tolerar o risco: consiste em não tomar, deliberadamente, nenhuma medida para alterar a probabilidade e/ou a consequência do risco. Pode ocorrer quando o risco está dentro do nível de tolerância e/ou apetite da organização, a capacidade para tomar qualquer ação sobre o risco é limitada e/ou, ainda, o custo de tomar qualquer medida é desproporcional em relação ao benefício potencial.

Adicionalmente, convém que os tomadores de decisão e outras partes interessadas estejam conscientes da natureza e da extensão do risco remanescente após o tratamento de riscos. Convém que o risco remanescente seja documentado e submetido a monitoramento, análise crítica e, onde apropriado, tratamento adicional.

É importante ressaltar que, mesmo para os riscos classificados como baixos e/ou médios, deve ser realizada avaliação quanto à aceitação do risco. Esse controle deve ser tomado em virtude de que sempre existirão oportunidades de melhorias para os processos da organização, observado entre outros fatores, o esforço e eventual custo-benefício.

Quanto à documentação desta atividade, recomenda-se a elaboração de Plano de Tratamento dos Riscos, indicando as atividades, os prazos e as responsabilidades de todos os envolvidos.

2.3.6 Monitoramento e Análise Crítica dos Riscos

O monitoramento e análise crítica é uma atividade essencial da gestão de riscos e tem por finalidade assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados do processo. Como consequência, ela deve ser contínua, ocorrer em todas as atividades e envolver a estrutura de Gestão de Riscos.

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

Com base nesse monitoramento e, ainda, nos artefatos julgados necessários, devem ser elaborados os Relatórios de Acompanhamento de Gestão de Riscos e demais relatórios institucionais que possuam a finalidade de avaliar e monitorar a operacionalização da gestão de riscos e o Plano de Gestão de Riscos da Secretaria de Estado de Economia do Distrito Federal (SEEC).

2.3.7 Comunicação e Consulta

O acesso a informações confiáveis, íntegras e tempestivas é essencial no processo de gestão de riscos e tem por finalidade assegurar que a gestão desenvolvida seja adequada às atividades e aos controles realizados e eficaz no alcance de seus objetivos.

A comunicação envolve compartilhar informação com os públicos-alvo. Deve acontecer entre os servidores e/ou equipes, precisando ser ágil e oportuna como, por exemplo, por meio de envio de e-mails.

Além disso, o fluxo das comunicações deve permitir que as informações sejam compartilhadas em todas as direções, e que os direcionamentos estratégicos, vindos do Comitê Interno de Governança e da Alta Administração alcancem toda a organização, sem prejuízo de respeitar o comando hierárquico da organização, o nível de acesso das informações e o seu caráter formal.

2.3.8 Registro e Relato

O processo de gestão de riscos e os seus resultados devem ser documentados e relatados por meio de mecanismos apropriados.

Nesse sentido, o registro e relato visam:

a) Comunicar atividades e resultados de gestão de riscos em toda a organização;

b) Fornecer informações para a tomada de decisão;

c) Melhorar as atividades de gestão de riscos; e

d) Auxiliar a interação com as partes interessadas, incluindo aquelas com responsabilidade e com responsabilização por atividades da gestão de riscos.

O relato é parte integrante da governança da organização e convém que melhore a qualidade da comunicação com as partes interessadas e apoie a alta gestão e os órgãos de supervisão a cumprirem suas responsabilidades.

Assim, é importante destacar que as decisões relativas à criação, à retenção e ao manuseio de informação documentada levem em consideração, mas não se limitem aos aspectos financeiros, técnicos e em relação à sensibilidade da informação.

3. Anexos

Anexo I - Estabelecimento de Escopo, Contexto e Critério

Clique aqui para baixar o anexo editavel

4. Glossário

Para fins deste manual entende-se por:

Consequência: resultado de um evento que afeta os objetivos;

Estrutura de Gestão de Riscos: conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria da gestão de riscos através de toda a organização;

Evento: ocorrência ou mudança em um conjunto específico de circunstâncias;

Gestão de riscos: atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos;

Governança Pública: conjunto de mecanismos de liderança, estratégia e controle voltadas para avaliar, direcionar e monitorar a gestão, com vistas à condução e geração de resultados nas políticas públicas e à prestação de serviços de interesse da sociedade;

Matriz de Riscos: ferramenta para classificar e apresentar riscos definindo faixas para consequência e probabilidade;

Nível de risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades;

Plano de Tratamento de Riscos: documento que consiste em selecionar e implementar opções para abordar os riscos identificados, analisados e avaliados;

Probabilidade: chance de algo acontecer;

Proprietário do risco: são os gerentes de projeto e os donos de processos responsáveis pelos processos de trabalho, projetos e ações desenvolvidos na Secretaria de Estado de Economia do Distrito Federal (SEEC);

Risco: efeito da incerteza nos objetivos;

Tolerância ao risco: disposição da organização ou parte interessada em suportar o risco residual, a fim de atingir seus objetivos.

5. Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. NBR ISO 31000: Gestão de Riscos - Princípios e Diretrizes. Rio de Janeiro, 2018.

_____. NBR ISO 19011: Diretrizes para Auditoria de Sistemas de Gestão. Rio de Janeiro, 2011.

BRASIL. Controladoria-Geral da União - CGU. Metodologia de Gestão de Riscos. Brasília: CGU, 2023.

_____. Tribunal de Contas da União. Referencial Básico de Gestão de Riscos. Brasília: TCU, Secretaria Geral de Controle Externo (Segecex), 2018.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION - COSO. Controle Interno: Estrutura Integrada: Sumário Executivo e Estrutura. Tradução: PriceWatherhouseCoopers e Instituto dos Auditores Internos do Brasil, São Paulo, 2013.

DISTRITO FEDERAL. Controladoria-Geral do Distrito Federal. Guia Gestão de Riscos nas Contratações. Brasília: CGDF, 2023.

_____. Controladoria-Geral do Distrito Federal. Guia prático de Gerenciamento de Riscos Corporativos. Brasília: CGDF, 2023.

_____. Decreto nº 37.302, de 29 de abril de 2016. Estabelece os modelos de boas práticas gerenciais em Gestão de Riscos e Controle Interno a serem adotados no âmbito da Administração Pública do Distrito Federal.

_____. Decreto nº 39.736, de 28 de março de 2019. Dispõe sobre a Política de Governança Pública e Compliance no âmbito da Administração Direta, Autárquica e Fundacional do Poder Executivo do Distrito Federal.

_____. Decreto nº 45.933, de 20 de junho de 2024. Dispõe sobre a composição e as competências das Unidades de Controle Interno do Poder Executivo do Distrito Federal, e dá outras providências.

_____. Portaria nº 356, de 17 de maio de 2023. Dispõe sobre a Política de Integridade Pública no âmbito da Secretaria de Estado de Planejamento, Orçamento e Administração do Distrito Federal.

Secretaria
de Economia

GDF