MANUAL DE GESTÃO DE RISCOS

METODOLOGIA EM CONFORMIDADE COM A IMPLEMENTAÇÃO DO PROGRAMA DE INTEGRIDADE ESTADUAL (LEI Nº 10.993/2019)

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

1 OBJETIVOS E ESCOPO DA GESTÃO DE RISCOS

Este Manual é elaborado em atenção ao disposto no art. 8º da Lei nº 10.993/2019, que institui o Programa de Integridade da Administração Pública Estadual Direta e Indireta, excetuadas as empresas públicas e sociedades de economia mista.

A gestão de riscos tem como objetivo auxiliar a tomada de decisão, com vistas a prover razoável segurança no cumprimento da missão e no alcance dos objetivos Institucionais, por meio do alinhamento do apetite ao risco com a estratégia, fortalecimento das decisões em respostas aos riscos, redução de surpresas e prejuízos operacionais e aproveitamento de oportunidades.

Não considerar explicitamente os riscos na tomada de decisões pode acarretar o não alcance dos objetivos ou resultados que poderiam ser atingidos. Para efeito deste Manual os seguintes conceitos, extraídos integralmente da ISO 31000:2009, devem ser considerados (*verbis*):

Risco ⇢ **Efeito da incerteza nos objetivos. Um efeito é um desvio em relação ao esperado – positivo e/ou negativo.**

Gestão de riscos ⇢ **Atividades coordenadas para dirigir e controlar uma organização no que se refere ao risco.**

Estrutura da gestão de riscos ⇢ **Conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos através de toda a organização.**

Atitude perante o risco	**Abordagem da organização para avaliar e eventualmente buscar, manter, assumir ou afastar-se do risco.**
Apetite pelo risco	**Quantidade de riscos que uma organização está preparada para buscar, manter ou assumir.**
Plano de gestão de riscos	**Esquema dentro da estrutura de gestão de riscos, especificando a abordagem, os componentes de gestão e os recursos a serem aplicados para gerenciar riscos.**
Proprietário do risco	**Pessoa ou entidade com responsabilidade e a autoridade para gerenciar o risco.**
Parte interessada	**Pessoa ou organização que pode afetar, ser afetada ou perceber afetada por uma decisão ou atividade.**

A gestão de riscos abrange qualquer processo de trabalho, atividade, projeto, iniciativa ou ação de plano institucional, assim como os recursos que dão suporte à realização dos objetivos Institucionais.

2 PRINCÍPIOS DA GESTÃO DE RISCOS NA SECONT

A gestão de riscos é uma responsabilidade de todos os colaboradores, que devem assegurar controles internos adequados para o monitoramento dos riscos dos processos e comunicar, sistemática e formalmente, fatos que possam afetar negativamente os resultados da Secretaria.

Os princípios para uma gestão de riscos eficaz estabelecidos na Seção 3 da ISO 31000:2009 e que passamos a adotar neste Manual são os seguintes (*verbis*):

- A gestão de riscos **protege e cria valor**
- A gestão de riscos **é parte integrante de todos os processos organizacionais**
- A gestão de riscos **é parte da tomada de decisões**
- A gestão de riscos **aborda explicitamente a incerteza**
- A gestão de riscos **é sistemática, estruturada e oportuna**
- A gestão de riscos **baseia-se nas melhores informações disponíveis**
- A gestão de riscos **é feita sob medida**
- A gestão de riscos **considera fatores humanos e culturais**
- A gestão de riscos **é transparente e inclusiva**
- A gestão de riscos **é dinâmica, interativa e capaz de reagir a mudanças**
- A gestão de riscos **facilita a melhoria contínua da organização**

3 PROCESSO DE GESTÃO DE RISCOS

O processo de gestão de riscos compreende as atividades coordenadas para dirigir e controlar uma organização no que se refere ao risco.[1] Para realizar a gestão de riscos de quaisquer objetos deve ser estabelecida uma aplicação sistemática de políticas, procedimentos e práticas de gestão para atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos.[2]

O processo de gestão de riscos pode ser visualizado na figura:

[1] ISO 31000:2009, Seção 2.1

[2] ISO 31000:2009, Seção 2.10

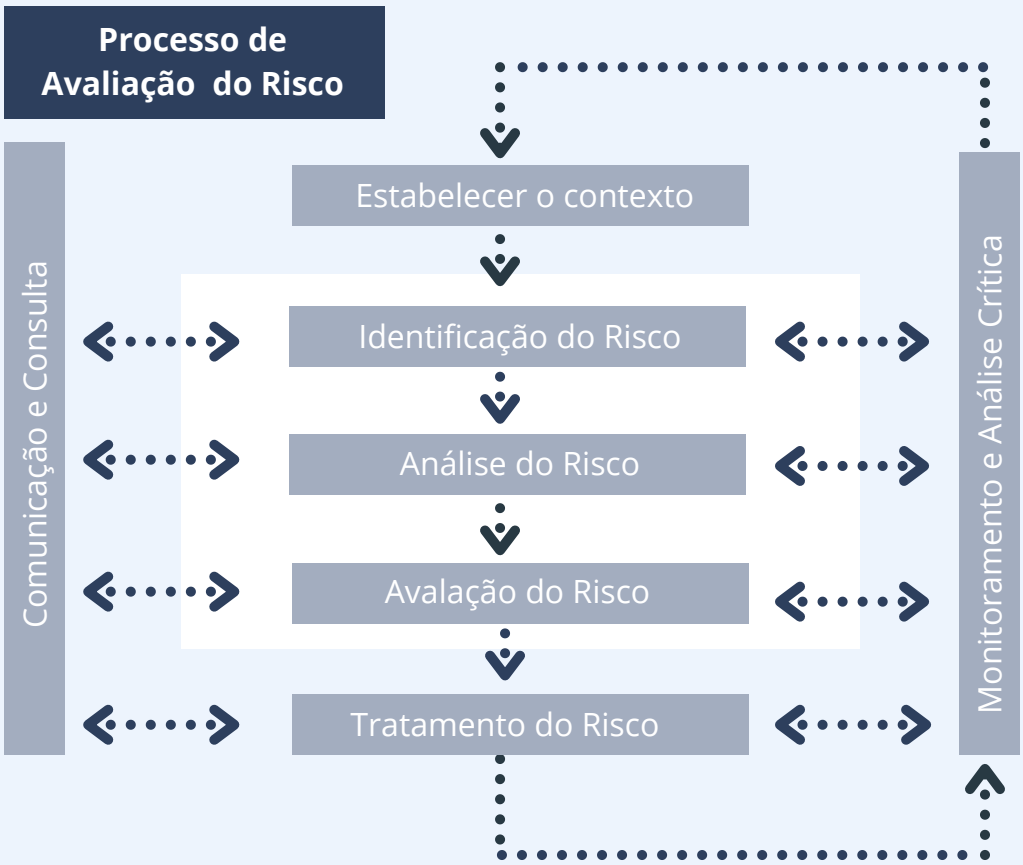


Fig. 1: Processo de Gestão de Riscos (ISO 31000:2009)

Dada a natureza multidisciplinar da gestão de riscos, o processo deve ser conduzido, preferencialmente, de forma coletiva, em oficinas de trabalho, por pessoas que conhecem aquele processo, projeto etc.

3.1. Comunicação e Consulta

A gestão de riscos envolve um conjunto de ações e decisões que acontecem em um contexto organizacional. A comunicação e a consulta são partes integrantes do processo e devem ser consideradas sempre de maneira explícita, o que permitirá o aprimoramento da gestão de riscos através do entendimento das perspectivas de cada uma das partes interessadas.

A comunicação e a consulta devem facilitar a troca de informações verdadeiras, pertinentes, exatas e compreensíveis, levando em consideração os aspectos de confidencialidade e integridade das pessoas.

A comunicação dos riscos é um processo interativo de troca de informações e opiniões, envolvendo múltiplas mensagens sobre a natureza e a gestão dos riscos, permitindo identificar e registrar as experiências, necessidades e preocupações das partes interessadas, possibilitando uma melhor percepção do nível de risco.

A consulta a comunicação informativa entre a organização e as partes interessadas, antes de ser tomada uma decisão ou de se definir um posicionamento em relação a uma questão específica.

A comunicação e a consulta devem atender os seguintes objetivos:

- Auxiliar a **estabelecer o contexto** apropriadamente
- Assegurar que os **interesses das partes interessadas** sejam compreendidos e considerados
- Auxiliar a assegurar que o**s riscos sejam identificados** adequadamente
- **Reunir diferentes áreas** de especialização em conjunto para análise dos riscos
- Assegurar que **diferentes pontos de vista sejam devidamente considerados** quando da definição dos critérios de risco e na avaliação dos riscos
- **Garantir o aval e o apoio** para um plano de tratamento
- **Aprimorar** a gestão de mudanças

Convém que a comunicação e a consulta às partes interessadas internas e externas aconteçam durante todas as fases do processo de gestão de riscos.[3]

3.2. Estabelecimento do Contexto

Devem ser estabelecidos os objetivos, as estratégias, o escopo e os parâmetros das atividades da organização, ou daquelas partes da organização em que o processo de gestão de riscos está sendo aplicado.

A gestão de riscos deve ser realizada com plena consciência da necessidade de se justificar os recursos utilizados na gestão de riscos. Os recursos requeridos, as responsabilidades e autoridades, além dos registros a serem mantidos também devem ser especificados.

Segundo determina a ISO 31000:2009 o contexto da gestão de riscos pode envolver, mas não está limitado à (*verbis*):

[3] ISO 31000:2009, Seção 3

- Definição das **metas e objetivos** das atividades de gestão de riscos
- Definição das **responsabilidades pelo processo** e dentro da gestão de riscos
- **Definição do escopo,** bem como da profundidade e da amplitude das atividades da gestão de riscos a serem realizadas, englobando inclusões e exclusões específicas
- **Definição da atividade,** processo, função, projeto, produto ou serviço ou ativo em termos de tempo e localização
- **Definição das relações** entre um projeto, processo ou atividade específicos e outros projetos, processos ou atividades da organização
- **Definição das metodologias** de avaliação de riscos
- Definição da forma como são avaliados **desempenho e a eficácia** na gestão dos riscos
- **Identificação e especificação** das decisões que têm que ser tomadas
- **Identificação, definição ou elaboração** dos estudos necessários, de sua extensão e objetivos, e dos recursos requeridos para tais estudos

Podem ser consultados nesta etapa os documentos mais importantes, como o planejamento estratégico, orçamentos, relatórios e análises e qualquer outra documentação pertinente à organização e suas finalidades.

Também pode ser necessária a consulta a documentos externos, com a legislação pertinente, assim como documentos de análise estratégica, como a análise SWOT, ajudam a manter o foco nos aspectos pertinentes dos ambientes interno e externo.

Pontos Fortes	Pontos Fracos	
Explorar	**Buscar**	**Oportunidades**
Confrontar	**Evitar**	**Ameaças**

3.3. Identificação dos Riscos

De acordo com a ISO 31000:2009, a identificação de riscos é o processo da busca, reconhecimento e descrição dos riscos; envolvendo a identificação das fontes de risco, eventos, causas e consequências potenciais.

A finalidade da etapa de identificação de risco é gerar uma lista abrangente de riscos baseada em eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos.

Os responsáveis pela identificação dos riscos podem e devem utilizar-se de ferramentas e técnicas de identificação de riscos que sejam adequadas aos seus objetivos e capacidades e aos riscos enfrentados. Por esse motivo é importante que as pessoas envolvidas nesse processo tenham um conhecimento adequado sobre o negócio, bem como sejam incentivadas a não se restringirem aos acontecimentos do passado.

A identificação dos riscos deve envolver as respostas às seguintes questões:

a) Qual é a fonte de cada risco?
b) O que poderia acontecer que provocasse:
- Aumentar ou diminuir a consecução eficaz dos objetivos?
- Tornar a consecução dos objetivos mais ou menos eficiente?
- Fazer com que as partes interessadas tomem atitudes que possam influenciar a consecução dos objetivos?
- Gerar benefícios adicionais?

c) Qual seria o efeito nos objetivos?
d) Quando, onde e por que, qual a probabilidade desses riscos acontecerem?
e) Quem poderia estar envolvido ou sofrer o impacto?
f) Que controles existem atualmente para tratar esse risco?
g) O que poderia fazer com que o controle não tivesse o efeito desejado sobre o risco?

A abordagem usada para a identificação de riscos depende do contexto da gestão de riscos, sendo comum envolver sessões de *brainstorming* em equipe, assumindo o formato de *workshop* com uso de facilitadores, que motiva o comprometimento e considera diferentes perspectivas e incorpora experiências variadas; essa técnica permite, principalmente, a identificação de riscos que não se materializaram no passado, aqueles com baixa probabilidade de ocorrência, mas de significativos impactos, chamados de “Cisne Negro”.

O risco identificado nesse processo é denominado risco inerente, que é o "risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto".[4]

Em seguida. durante a análise de riscos, serão levantados e avaliados os controles já estabelecidos em relação aos riscos para que seja obtido o risco residual, que é risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco".[5]

Nesta fase inicial de implementação da gestão de riscos, nossos esforços estarão concentrados no risco de integridade,[6] em atendimento ao art. 8º da Lei nº 10.993/2019. Esta etapa envolve ainda a identificação dos controles internos[7] para tratamento dos riscos, destacados os controles preventivos, que atuam sobre as possíveis causas do risco, com o objetivo de prevenir a sua ocorrência.

Exemplos de controles preventivos: requisitos/checklist definidos para o processo e capacitação dos servidores envolvidos no processo; e controles de atenuação e recuperação, que são 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. A documentação desta etapa será feita na "Matriz de Riscos e Controles" (CLIQUE para acessar a Matriz).

4 inc. XIV do art. 2º da Instrução Normativa Conjunta/MPOG e CGU nº 1, de 10/05/2016

5 inc. XV do art. 2º da Instrução Normativa Conjunta/MPOG e CGU nº 1, de 10/05/2016

6 Vulnerabilidade institucional que pode favorecer ou facilitar práticas de corrupção, fraudes, subornos, irregularidades e quaisquer outros desvios éticos ou de conduta (inc. V do art. 2º da Lei nº 10.993/2019)

7 Medida que está modificando o risco e incluem qualquer processo, política, dispositivo, prática ou outras ações que modificam o risco. (ISO 31000:2009)

3.4. Análise e Avaliação dos Riscos

Esta etapa compreende o desenvolvimento da compreensão sobre o risco e à determinação do nível do risco e para as decisões sobre a necessidade de os riscos serem tratados, e sobre as estratégias e métodos mais adequados de tratamento de riscos. Envolve a apreciação das causas e fontes de risco, seus impactos – positivos ou negativos – e a probabilidade de que essas consequências possam ocorrer.

Os seguintes passos devem ser observados:

- **Avaliar o impacto** do risco sobre o objetivo/resultado – o impacto mede o potencial comprometimento do objetivo/resultado (p.ex.: um risco com potencial para comprometer um objetivo na sua totalidade ou na sua quase totalidade é considerado um risco de alto impacto)
- **Avaliar a probabilidade** de ocorrência do risco (p.ex.: um evento cuja ocorrência seja quase certa de acontecer é um evento de alta probabilidade)
- **Definir o nível do risco** com base na matriz probabilidade x impacto

A matriz define o nível de riscos a partir da combinação das escalas de probabilidade e de impacto. A probabilidade é a chance de o evento[8] ocorrer dentro do prazo previsto para se alcançar o objetivo/resultado; e o impacto é o resultado de um evento que afeta o objetivo/resultado.[9]

Este Manual define a realização de uma análise qualitativa em quatro níveis e que poderá ser aprimorada ou evoluir para uma análise qualitativa/quantitativa, de acordo com a evolução do nível de maturidade da Instituição na gestão de riscos e com as revisões do próprio manual.

As escalas adotadas neste Manual[10] são as seguintes:

[8] Ocorrência ou alteração em um conjunto específico de circunstâncias (ISO 31.000:2009)

[9] ABNT ISO GUIA 73:2009, definição 3.6.1.3

[10] Adaptado do Guia Prático de Gestão de Riscos para a Integridade: CGU. https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/manual-gestao-de-riscos.pdf (consultado em 25/06/2020)

1. Probabilidade

Raro	**Baixíssima possibilidade de o evento ocorrer**
Pouco Provável	**O evento ocorre raramente**
Provável	**O evento já ocorreu algumas vezes e pode voltar a ocorrer**
Muito Provável	**O evento já ocorreu repetidas vezes e provavelmente voltará a ocorrer muitas vezes**

2. Impacto

Baixo	**Consequências insignificantes caso o evento ocorra**
Moderado	**Consequências menores em processos e atividades secundários**
Alto	**Consequências relevantes em processos e atividades secundárias ou menores em processos e atividades prioritários**
Muito Alto	**Consequências relevantes em processos e atividades prioritários**

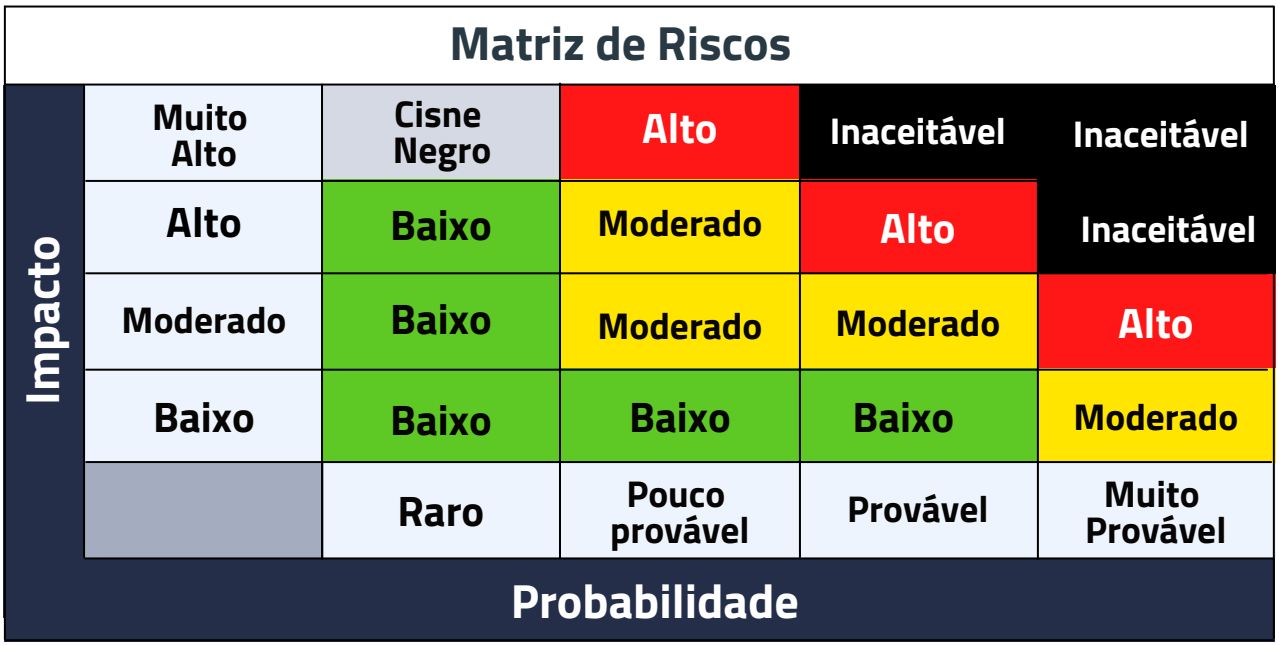
A comparação dos resultados da análise de riscos com os critérios definidos para probabilidade e impacto permitem determinar se o nível de risco e/ou sua magnitude é aceitável ou tolerável, auxiliando na decisão sobre quais riscos necessitam de tratamento e a prioridade para implementação do tratamento.[11]

Então:

NRI = P x I; onde

NR = Nível de Risco Inerente
P = Probabilidade
I = Impacto

[11] Avaliação de riscos (ABNT ISO GUIA 73:2009, definição 3.7.1)|ISO 31000:2009, Seção 5.4.4



A avaliação dos riscos estará completa após a avaliação dos controles internos em funcionamento sobre os riscos atuais e identificados, possibilitando a determinação do nível de risco residual, que definirá a necessidade e prioridade de tratamento.

O efeito dos controles na mitigação de riscos consiste em determinar o fator obtido a partir da análise do grau de efetividade da implementação dos controles, conforme apresentado na tabela a seguir:[12]

Nível	Descrição	Fator de avaliação
Inexistente	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais	1
Fraco	Controles têm abordagens ad hoc, tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo alto grau de confiança no conhecimento das pessoas	0,8
Mediano	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes devido a deficiências no desenho ou nas ferramentas utilizadas	0,6
Satisfatório	Controles implementados e sustentados por ferramentas adequadas. E, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente	0,4
Forte	Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco	0,2

[12]Adaptado do Manual de Gestão de Riscos do TCU: 2018

O risco residual será apurado mediante a multiplicação do valor do risco inerente apurado na fase de identificação de riscos e na fase inicial de análise pelo fator de avaliação do controle interno.

RR = NRI x FA; onde

RR = Risco Residual
NRI = Nível de Risco Inerente
FA = Fator de Avaliação dos Controles Internos

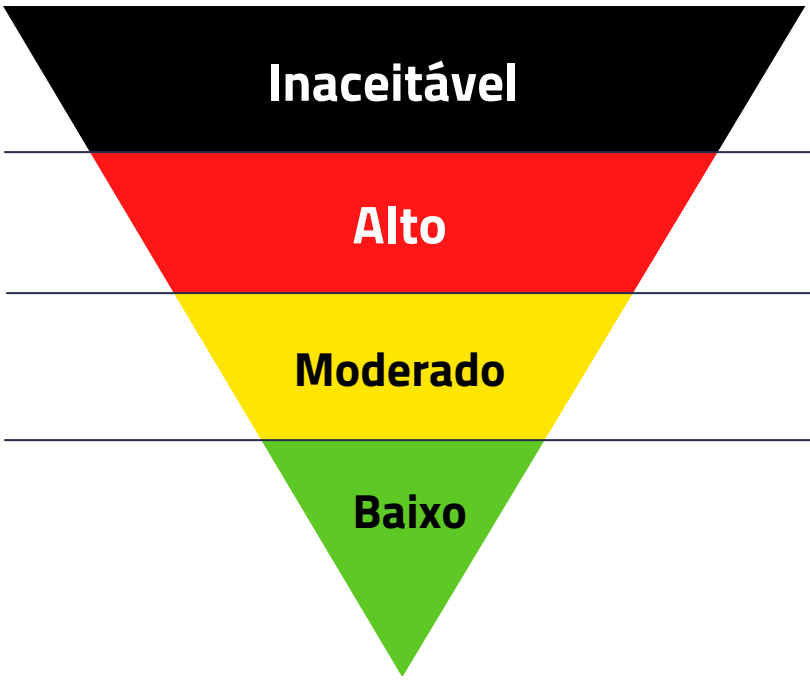
A avaliação do risco envolve a comparação do seu nível com o limite de exposição a riscos, a fim de determinar se o risco é aceitável.

A avaliação dos riscos fornece subsídios para a tomada de decisão, não se constituindo em fator determinante para eventual tratamento do risco. Ou seja, cabe ao gestor, diante da lista de riscos ordenados por nível de risco, decidir quais merecerão ações mitigadoras.

3.5. Priorização e Tratamento dos Riscos

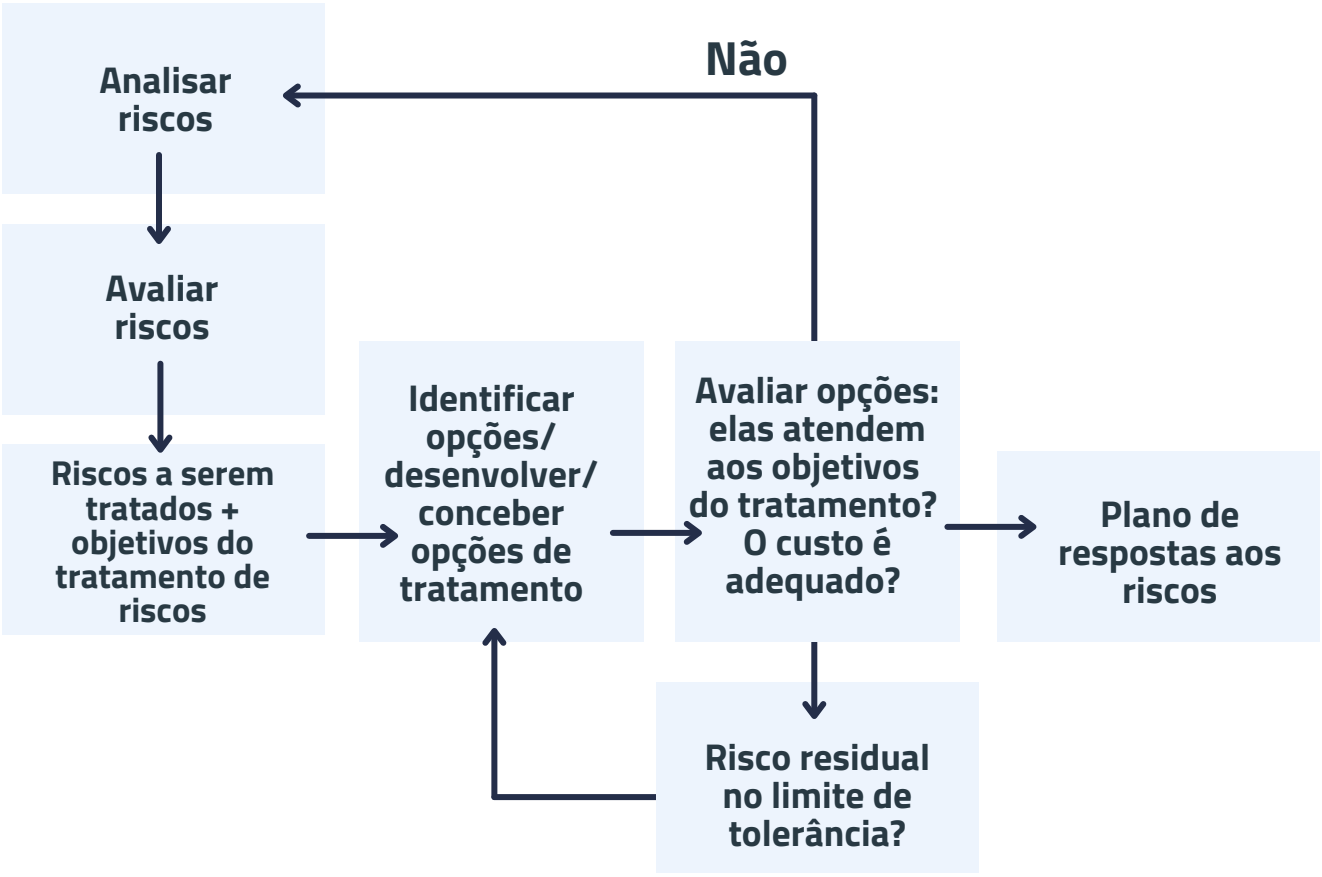
Compreende o planejamento e a realização de ações para modificar o nível do risco, considerando o resultado da avaliação do risco residual realizada na etapa anterior. O limite de exposição a riscos representa o nível de risco acima do qual é desejável o tratamento do risco. Espera-se que, com os resultados do tratamento, o nível de risco residual fique abaixo do limite de exposição.

Matriz Simples de Risco e Tolerância ao Risco



Inaceitável	Requer ação para evitar o risco. Pode envolver a interrupção do processo organizacional
Alto	Requer ação para manejar o risco. Pode envolver mitigação ou transferência
Moderado	A ação é desejável se os recursos estiverem disponíveis
Baixo	Nenhuma ação é necessária

O nível do risco pode ser modificado por meio de medidas de resposta ao risco que mitiguem, transfiram ou evitem esses riscos. O processo de tratamento de riscos pressupõe atividade iterativa para o desenvolvimento dos planos de respostas aos riscos.



O tratamento dos riscos deve seguir os seguintes passos:

- **Identificar** medidas de resposta ao risco.
- **Avaliar** a viabilidade da implantação dessas medidas (custo-benefício, viabilidade técnica, tempestividade, efeitos colaterais do tratamento etc.).
- **Decidir** quais serão implementadas.
- **Reavaliar** o risco residual após as medidas de tratamento e a necessidades de medidas de contingência.
- **Elaborar** plano de respostas aos riscos.

São dicas que facilitam a identificação de medidas de resposta ao risco:

Responder às seguintes perguntas-chave:

- Que medidas poderiam ser adotadas para reduzir a probabilidade de ocorrência do risco?
- Que medidas poderiam ser adotadas para reduzir o impacto do risco no objetivo/resultado?
- É possível adotar medidas para transferir o risco?

Considerar as fontes e causas dos riscos:

- A princípio, as medidas devem atacar as causas do risco, de modo a reduzir a probabilidade de ocorrência, ou também podem consistir em planos de contingência que amenizem os impactos, caso o risco se concretize, ou uma combinação das duas abordagens;

Na decisão quanto à implantação das medidas de resposta ao risco, considerar:

- A quantidade e o nível dos riscos mitigados por cada medida, bem como o grau de redução do nível do risco gerado pela medida

As respostas aos riscos possuem opções de tratamento, que seriam definidas após a avaliação e priorização dos riscos e podem envolver:

TRATAMENTO	DESCRIÇÃO
Mitigar	Um risco normalmente é mitigado quando é classificado como "Alto" ou "Moderado". A implementação de controles, neste caso, apresenta um custo-benefício adequado. Mitigar o risco significa implementar controles que possam diminuir as causas ou as consequências dos riscos, identificadas na etapa de Identificação e Análise de Riscos.
Compartilhar	Um risco normalmente é compartilhado quando é classificado como "Alto" ou "Extremo", mas 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.

TRATAMENTO	DESCRIÇÃO
Evitar	Um risco normalmente é evitado quando é classificado como "Inaceitável", e/ou a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco. Evitar o risco pode significar encerrar o processo organizacional. Nesse caso, essa opção deve ser aprovada em conjunto pela alta administração.
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

3.6. Monitoramento

Compreende o acompanhamento e a verificação do desempenho ou da situação de elementos da gestão de riscos, podendo abranger a política, as atividades, os riscos, os planos de tratamento de riscos, os controles e outros assuntos de interesse.

O monitoramento tem três dimensões:

1. A implementação;
2. Os resultados do tratamento de riscos;
3. A evolução do nível dos riscos que não mereceram tratamento por parte do gestor.

O monitoramento das ações de tratamento de riscos envolve a verificação contínua ou periódica do funcionamento da implementação e dos resultados das medidas mitigadoras. O monitoramento deve considerar o tempo necessário para que as medidas mitigadoras produzam seus efeitos.

O monitoramento é parte integrante do processo de gestão e de tomada de decisão e deve acompanhar o ciclo de planejamento institucional. O monitoramento deve ser efetivo sem onerar demasiadamente o processo.

O monitoramento consistirá na atualização da análise e avaliação do risco, assim como do estágio de execução das medidas de tratamento do risco e dos resultados dessas medidas. O monitoramento dos riscos de processos, unidades e projetos será realizado pelo respectivo proprietário do risco.

3.7. Melhoria Contínua

Compreende o aperfeiçoamento ou ajuste de aspectos da gestão de riscos avaliados no monitoramento. A melhoria contínua pode ser entendida em duas dimensões: uma relativa ao próprio Sistema de Gestão de Riscos; e outra relacionada aos resultados do monitoramento sobre a efetividade do tratamento do risco, a cargo dos gestores de risco.

Secretaria de Controle e Transparência - SECONT

Secretário de Estado de Controle e Transparência
Edmar Moreira Camata

Subsecretário de Integridade Governamental e Empresarial
Alexandre Del'Santo Falcão

Coordenadores do Programa de Integridade
Guilherme A. Machado Jr.
Suzanne Barcellos Damazio

subint@secont.es.gov.br

(27) 3636-5385

Av. João Batista Parra, nº 600, Ed. Aureliano Hoffman,10º andar
Enseada do Suá
CEP: 29050-375
Vitória / ES