GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle
e Transparência

GUIA ORIENTATIVO PARA IMPLEMENTAÇÃO DA GESTÃO DE RISCOS NO PODER EXECUTIVO ESTADUAL

Secretaria de Estado de Controle e Transparência
2026

BEM-VINDO!

Este guia foi desenvolvido para ajudar você a navegar pelo SIAC Gestão de Riscos — sistema criado pela Secretaria de Controle e Transparência (SECONT) para auxiliar órgãos e entidades do poder executivo estadual a gerenciar riscos de forma sistemática, estruturada e integrada.

Se você não tem experiência anterior com gestão de riscos, não se preocupe. Este guia foi pensado especificamente para você, explicando o quê, por quê e como fazer cada coisa, sempre de forma clara e prática.

EDMAR MOREIRA CAMATA
Secretário de Estado de Controle e Transparência

ARTUR ANTONIO MORAES MARQUES
Subsecretário de Estado de Controle

Equipe Técnica

Magaly Guimarães Lucas
Coordenadora de Consultoria em Governança, Gestão de Riscos e Controles Internos - CGRC

Vania Cristina Ramos
Auditora do Estado

José Mário Bispo Sant'Anna
Auditor do Estado

Lucas do Nascimento Meirelles - CACI
Coordenador de Ações de Controle Informatizados

Eduardo Luiz Santos Lehubach
Assessor Técnico - Subsecretaria de Estado de Controle

SUMÁRIO

1. Introdução

A crescente complexidade da administração pública impõe aos órgãos e entidades estatais o desafio permanente de aprimorar seus processos decisórios e operacionais, de modo a assegurar o cumprimento de seus objetivos institucionais com eficiência, eficácia, economicidade e integridade. Em um ambiente marcado por demandas sociais crescentes, restrições orçamentárias, avanços tecnológicos acelerados e maior escrutínio da sociedade, a gestão de riscos se consolida como instrumento estratégico para fortalecer a governança, elevar a maturidade da gestão e promover a entrega de valor público de forma sustentável.

A publicação deste Guia tem por finalidade oferecer orientações práticas e padronizadas para a implementação do processo de gestão de riscos nas diversas unidades organizacionais. A metodologia apresentada fundamenta-se nas boas práticas internacionais, especialmente na ABNT NBR ISO 31000:2018 – Gestão de Riscos – Diretrizes.

O projeto reafirma o compromisso do Estado com a melhoria contínua da gestão pública, com o fortalecimento dos controles internos, da integridade e da transparência, e com a criação de um ambiente institucional mais eficiente, confiável e orientado à prevenção de falhas e desperdícios.

A estrutura do Guia foi organizada para apoiar tecnicamente gestores, servidores e equipes envolvidas na execução de processos organizacionais, em especial nas áreas de planejamento, gestão, controle, integridade e compliance. O conteúdo abrange os objetivos, princípios e diretrizes da gestão de riscos, as instâncias e responsabilidades envolvidas, as categorias de riscos e o processo metodológico de gestão, incluindo ferramentas de apoio, modelos práticos e fluxos que orientam sua aplicação. Ao final, são apresentados glossário, referências e apêndices com instrumentos que facilitam a aplicação prática.

Espera-se, com isso, promover a consolidação de uma cultura organizacional orientada à gestão por riscos, contribuindo para o alcance dos objetivos estratégicos do Estado, para o fortalecimento da confiança da sociedade nas

instituições públicas e para a geração de valor público sustentável.

Este Guia apresenta os elementos essenciais para a adoção de boas práticas em gestão de riscos, fundamentados em princípios, diretrizes, objetivos, estrutura e processos — componentes indispensáveis para uma gestão integrada e coerente, conforme estabelecido na NBR ISO 31000:2018. São detalhados três componentes centrais — princípios, estrutura e processos — integralmente incorporados ao Guia e organizados de forma a servir como um "mapa orientativo" para a condução de uma gestão de riscos eficiente, eficaz e consistente.

O que este Guia traz?

- As categorias e tipos de riscos
- As etapas do processo de gestão de riscos
- Fluxos e modelos práticos para aplicar no dia a dia
- Um metódo simples para integrar à estratégia da organização

A aplicação eficiente deste processo exige engajamento, atualização constante e integração com a estratégia organizacional.

Nesse Guia os procedimentos operacionais para o processo de gestão de riscos e suas etapas foram definidos com base na literatura existente e abrange as categorias de riscos e suas definições, bem como etapas a serem apresentadas na metodologia desenvolvida.

A metodologia ainda abrange fluxos desenhados para facilitação do processo de gestão de riscos do órgão ou entidade.

2. Para que Gestão de Riscos?

A Administração Pública enfrenta, diariamente, o desafio de transformar recursos limitados em resultados concretos para a sociedade. A complexidade crescente das políticas públicas, a necessidade de respostas rápidas a demandas sociais e a pressão por maior transparência tornam indispensável a adoção de práticas que fortaleçam a capacidade do Estado de planejar, executar e entregar serviços com qualidade. Nesse contexto, a gestão de riscos se apresenta como um componente essencial para aprimorar a atuação governamental.

A gestão de riscos permite que órgãos e entidades identifiquem, compreendam e tratem, de forma estruturada, os fatores que podem comprometer seus objetivos. Em vez de reagir apenas quando problemas já ocorreram, a Administração passa a atuar de maneira preventiva, antecipando cenários adversos e reduzindo a probabilidade de falhas que impactem a continuidade dos serviços públicos. Essa mudança de postura contribui diretamente para a eficiência administrativa, para a proteção do interesse público e para o uso responsável dos recursos do Estado.

Além de apoiar decisões mais informadas, a gestão de riscos fortalece a governança ao promover maior clareza sobre responsabilidades, prioridades e vulnerabilidades institucionais. Quando os riscos são mapeados e monitorados, gestores e equipes conseguem alinhar esforços, priorizar ações estratégicas e direcionar recursos para áreas mais sensíveis, aumentando a capacidade de resposta da organização. Isso resulta em processos mais robustos, maior confiabilidade das informações e melhoria contínua da gestão.

Outro benefício relevante é o fortalecimento da integridade e da transparência. A identificação de riscos relacionados a fraudes, irregularidades, conflitos de interesse ou fragilidades de controle contribui para a construção de um ambiente institucional mais íntegro e seguro. Ao tornar visíveis os pontos de atenção e as medidas adotadas para mitigá-los, a gestão de riscos reforça a prestação de contas e amplia a confiança da sociedade nas instituições públicas.

A adoção dessa prática também estimula a inovação e o aprendizado organizacional. Ao compreender melhor seus riscos, as equipes ganham segurança para testar novas soluções, aprimorar processos e buscar alternativas mais eficientes para a entrega de políticas públicas. A gestão de riscos, portanto, não é um obstáculo à inovação, mas um instrumento que permite inovar com responsabilidade.

Implementar a gestão de riscos significa, em última análise, fortalecer a capacidade do Estado de cumprir sua missão. É garantir que políticas, programas e serviços sejam executados com maior previsibilidade, qualidade e continuidade. É criar condições para que gestores e servidores atuem com mais segurança, clareza e foco. E, sobretudo, é assegurar que a sociedade

receba serviços públicos mais confiáveis, eficientes e alinhados às suas necessidades.

Em resumo, a gestão de riscos tem um propósito claro: **proteger e gerar valor para a organização**. Ela ajuda a tomar decisões melhores, evita surpresas negativas e apoia o alcance dos objetivos.

3. Conceitos

São conceitos que devem ser apreendidos para a compreensão da Gestão de Riscos:

Nº	Conceitos	
I	Alta Administração	Secretários de Estado, Procurador-Geral do Estado, Diretores-Presidentes de autarquias, Subsecretários, Diretores e equivalentes
II	Apetite a Riscos	nível de risco que o órgão ou entidade se dispõe a admitir na realização de suas atividades e objetivos
III	Controles Internos	conjunto do plano de organização e de todos os métodos e procedimentos utilizados pela Administração, conduzidos por todos os seus agentes, para salvaguardar ativos, desenvolver a eficiência das operações, avaliar o cumprimento de programas, objetivos, metas e orçamentos, verificar a exatidão e a fidelidade das informações e assegurar o cumprimento da lei
III	Gerenciamento de riscos	processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações e fornecer segurança razoável no alcance dos objetivos organizacionais

V	Gestão de Riscos	processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, para dirigir e controlar o órgão ou entidade relativamente aos riscos
VI	Governança Pública	conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade
VII	Nível de Risco	medida da importância ou significância do risco, considerando a probabilidade de ocorrência do evento e o seu impacto nos objetivos, podendo ser classificado como baixo, médio, alto ou extremo
VIII	Objetivo Institucional	situação que se deseja alcançar, evidenciando o êxito no cumprimento da finalidade dos órgãos ou entidades
IX	Partes Interessadas	pessoa ou organização que possa afetar, ser afetada ou perceber-se afetada por uma decisão ou atividade
X	Política de Gestão de Riscos	declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos
XI	Proprietário do Risco	pessoa ou entidade com responsabilidade e autoridade para gerenciar o risco
XII	Risco	possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos da entidade
XIII	Tratamento do Risco	execução de medidas de controle com a finalidade de modificar um risco identificado, aumentando a probabilidade de que os objetivos institucionais sejam alcançados

XIV	Valor Público	produtos e resultados gerados, preservados ou entregues pelas atividades de uma organização, que representem respostas efetivas e úteis às necessidades ou às demandas de interesse público e modifiquem aspectos do conjunto da sociedade ou de grupos específicos reconhecidos como destinatários legítimos de bens e serviços públicos

4. Objetivos da Gestão de Riscos

A gestão de riscos constitui um instrumento essencial para o fortalecimento da governança, da eficiência administrativa e da integridade no setor público. Sua finalidade é apoiar a tomada de decisão em todos os níveis da organização, contribuindo para que os objetivos institucionais sejam atingidos de forma segura, sustentável e transparente.

No âmbito dos órgãos e entidades da administração pública, a gestão de riscos busca, de forma geral, alcançar os seguintes objetivos:

Quadro II – Objetivos da Gestão de Riscos

Nº	Objetivo	Exemplo
I	Proteger e criar valor para a organização, contribuindo para o alcance de seus objetivos institucionais por meio de práticas estruturadas, sistemáticas e contínuas de gestão de riscos.	Alinhar riscos à estratégia e à missão institucional, promovendo valor público e segurança nos resultados.
II	Apoiar a tomada de decisões, por meio da identificação, avaliação e tratamento dos riscos que possam impactar a consecução dos objetivos institucionais.	Garantir decisões mais informadas, conscientes e baseadas em evidências.

III	Fortalecer os controles internos da gestão, por meio da identificação de fragilidades e da implementação de mecanismos adequados de mitigação dos riscos.	Reforçar os mecanismos preventivos e corretivos da gestão, aumentando a confiabilidade dos processos.
IV	Promover o uso eficiente, eficaz e efetivo dos recursos públicos, mediante a antecipação de eventos adversos e a melhor alocação de esforços e investimentos.	Evitar desperdícios e prejuízos, otimizando a gestão orçamentária e operacional.
V	Reforçar a confiança das partes interessadas, demonstrando o comprometimento da organização com a boa governança, a integridade e a responsabilidade na gestão pública.	Aumentar a credibilidade institucional perante cidadãos, órgãos de controle e demais públicos.
VI	Aumentar a resiliência institucional, preparando a organização para responder de forma proativa a mudanças, incertezas e oportunidades.	Elevar a capacidade de adaptação e reação diante de cenários críticos ou imprevistos.
VII	Assegurar a conformidade com leis, regulamentos, normas e diretrizes aplicáveis à gestão pública.	Reduzir riscos legais e normativos, promovendo integridade e conformidade institucional.

Sob essa ótica, a gestão de riscos se apresenta como ferramenta estratégica que vai além da obrigação normativa, contribuindo para melhores resultados na Administração Pública.

Os objetivos da gestão de riscos, conforme a ISO 31000:2018, ajudam os órgãos governamentais a lidarem de forma organizada com incertezas que podem afetar suas atividades e resultados. Eles permitem prevenir falhas, melhorar processos, proteger recursos públicos e apoiar decisões mais seguras e transparentes. Assim, utilizar esses objetivos no dia a dia é fundamental para

fortalecer a confiança da sociedade, garantir maior eficiência e assegurar que as ações do governo gerem valor público de forma sustentável.

5. PRINCÍPIOS DA GESTÃO DE RISCOS

É preciso que a gestão de riscos esteja fundamentada em princípios que assegurem sua eficácia e integração à governança, à estratégia e à operação da organização. Tais princípios orientam a forma como o processo de gestão de riscos deve ser concebido, implementado, conduzido e continuamente aprimorado, de modo a agregar valor à tomada de decisão e ao alcance dos objetivos organizacionais.

A ABNT NBR ISO 31000:2018 estabelece os seguintes princípios que norteiam a gestão de riscos:

Quadro III – Princípios da Gestão de Riscos

Nº	Princípio	Descrição	Exemplo
I	Integrada	A gestão de riscos deve ser parte integrante de todas as atividades da organização, incorporando-se à governança e à tomada de decisões.	Antes da aprovação de um novo programa governamental ou da abertura de uma licitação relevante, a alta administração exige a análise prévia dos riscos (orçamentários, legais, operacionais e de integridade). Essas informações são consideradas nas decisões do gestor, influenciando a escolha do modelo de contratação, a definição de controles e até a viabilidade da política pública.
II	Estruturada, Abrangente e Sistêmica	A abordagem estruturada abrangente e sistêmica garante consistência, padronização e confiabilidade no tratamento dos riscos.	Órgão e entidades adotam uma metodologia única de gestão de riscos (matriz de riscos, critérios padronizados), permitindo comparação e consolidação das informações pela alta gestão.

III	Personalizada	Deve ser customizada conforme missão, objetivos, cultura, estrutura e ambiente regulatório de cada organização.	Uma autarquia reguladora trata com maior profundidade riscos regulatórios e de captura, enquanto um hospital público prioriza riscos assistenciais e de desabastecimento de insumos.
IV	Inclusiva	Implica no envolvimento e participação ativa das partes interessadas, de forma a contribuir para o melhor entendimento do contexto e na identificação eficaz dos riscos.	Na elaboração de uma política pública ou de um grande contrato administrativo, o órgão promove consultas internas, audiências públicas e diálogos com órgãos de controle e usuários do serviço. As contribuições recebidas são utilizadas para identificar riscos sociais, operacionais e de integridade, aumentando a qualidade das decisões e a legitimidade das ações administrativas.
V	Dinâmica	A gestão de riscos deve ser dinâmica e iterativa, adaptando-se permanentemente às mudanças no ambiente interno e externo da organização.	Durante a execução de um contrato de serviços públicos, o órgão monitora regularmente os riscos identificados e, diante de alterações legais, orçamentárias ou de contexto social, revisa a matriz de riscos e os controles adotados, ajustando decisões administrativas para garantir a continuidade e a eficiência do serviço.
VI	Melhoria Contínua	O processo deve ser continuamente aperfeiçoado por meio de lições aprendidas, análises críticas e auditorias.	Após auditorias, fiscalizações dos tribunais de contas ou a ocorrência de falhas em programas públicos, o órgão revê seus processos de gestão de riscos, atualiza procedimentos e capacita servidores, incorporando os aprendizados para prevenir reincidências e melhorar a eficiência administrativa.

VII	Baseada nas Melhores Informações Disponíveis	As decisões devem se basear em dados históricos, atuais e prospectivos, reconhecendo limitações e incertezas.	Na elaboração do planejamento orçamentário, o órgão utiliza dados históricos de execução, informações atuais de arrecadação e cenários econômicos prospectivos. Essas informações são analisadas quanto às incertezas e divulgadas de forma transparente aos gestores e órgãos de controle, subsidiando decisões mais responsáveis e alinhadas à realidade fiscal.
VIII	Considera os Fatores Humanos e Culturais	A gestão de riscos deve considerar comportamentos, valores, percepções e cultura organizacional.	O órgão promove capacitações e ações de integridade para reduzir riscos decorrentes de falhas humanas, resistência a controles ou normalização de desvios.

Em consonância com a ISO 31000:2018, os princípios da gestão de riscos no setor público devem ser entendidos como um conjunto integrado e interdependente, que somente alcança sua plena efetividade quando aplicado de forma simultânea. A governança, a transparência, a integração ao contexto organizacional, a personalização, a inclusão das partes interessadas, a dinamicidade, a melhoria contínua e a criação e proteção de valor não podem ser tratados de maneira isolada, pois a ausência ou fragilidade de um princípio compromete a efetividade dos demais. Assim, a implementação equilibrada e conjunta desses fundamentos fortalece a capacidade institucional de antecipar, avaliar e responder aos riscos, promovendo maior confiança social, eficiência administrativa e sustentabilidade das políticas públicas.

6. DIRETRIZES PARA A GESTÃO DE RISCOS

As diretrizes da gestão de riscos representam as orientações práticas que guiam como a gestão de riscos deve ser implementada, organizada e mantida dentro de uma instituição. Enquanto os princípios expressam a filosofia e os fundamentos que sustentam a gestão de riscos, as diretrizes traduzem essa filosofia em orientações concretas para a prática.

A norma ISO 31000.2018 assinala as diretrizes para a Gestão de Riscos, quais sejam:

Quadro IV - Diretrizes da Gestão de Riscos Previstas na ISO 31000:2018

Nº	Diretriz	Descrição
I	Comprometimento da alta administração e engajamento dos servidores na consolidação da cultura de gestão de riscos	É preciso que haja o comprometimento da alta administração na implementação da Gestão de Riscos. Secretários de Estado, Procurador-Geral do Estado, Diretores-Presidentes de autarquias, Subsecretários, Diretores e equivalentes devem envidar esforços para isso, valendo para tanto do engajamento de todos os servidores. A partir dessa sinergia, espera-se que haja a efetiva incorporação da gestão de riscos aos processos decisórios e à rotina institucional, consolidando uma cultura organizacional voltada à prevenção, à melhoria contínua e à entrega de valor público.
II	Integração aos modelos de gestão e processos de planejamento estratégico, tático e operacional, à cadeia de valor e à cultura organizacional do órgão ou entidade.	A gestão de riscos deve estar articulada aos instrumentos de gestão institucional, de forma a influenciar diretamente o planejamento, os processos finalísticos e a cultura organizacional.

III	Estabelecimento de níveis adequados de exposição a riscos	Devem ser definidos e formalizados o apetite e a tolerância ao risco, orientando decisões e priorizações de acordo com os limites aceitáveis pela organização.
IV	Adoção de práticas de efetividade reconhecidas, adaptadas à realidade e às necessidades do órgão ou entidade.	Devem-se aplicar metodologias e abordagens consagradas na gestão de riscos, customizadas ao contexto e à maturidade institucional do órgão ou entidade.
V	Estímulo à uniformização e padronização técnica das metodologias, instrumentos, atividades e procedimentos	As práticas de gestão de riscos devem ser normatizadas e harmonizadas em toda a organização, promovendo consistência, comparabilidade e eficiência.
VI	Fornecimento de informações relevantes à tomada de decisão nos níveis estratégico, tático e operacional	Os produtos da gestão de riscos devem subsidiar decisões em todos os níveis institucionais, com base em dados estruturados, contextualizados e tempestivos.

VII	Garantia que as partes interessadas e os responsáveis pela tomada de decisão, em todos os níveis organizacionais, tenham acesso tempestivo a informações suficientes, íntegras e confiáveis sobre os riscos aos quais a organização está exposta	A organização deve assegurar a comunicação efetiva e acessível dos riscos identificados e avaliados, permitindo ações tempestivas e baseadas em evidências.
VIII	Gerenciamento dos riscos por meio de ciclos de revisão e melhoria contínua, com periodicidade compatível à criticidade e à relevância dos riscos	A periodicidade de revisão da matriz de riscos deve estar vinculada à natureza e gravidade dos riscos, com ciclos definidos e ações de melhoria contínua implementadas.
IX	Monitoramento dos riscos e da efetividade dos controles por meio de avaliações contínuas, autoavaliações e/ou indicadores	O acompanhamento da gestão de riscos deve utilizar instrumentos sistemáticos de verificação e mensuração, promovendo ajustes necessários nos controles.
X	Aderência dos processos organizacionais às determinações legais, regulamentares e normativas internas e externas	Os processos internos devem ser periodicamente avaliados quanto à conformidade com normas vigentes, mitigando riscos legais e institucionais.

XI	Promoção do uso eficiente e integrado dos recursos disponíveis, sejam financeiros, humanos, materiais ou tecnológicos	A gestão de riscos deve contribuir para o uso racional dos recursos, favorecendo a eficiência e eliminando desperdícios ou sobreposições.
XII	Utilização de soluções tecnológicas adequadas, integradas e eficientes que sejam aderentes às metodologias e às atividades executadas	Sistemas e ferramentas tecnológicas devem apoiar a execução da gestão de riscos, integrando dados, automatizando etapas e fortalecendo o controle institucional.
XIII	Capacitação continuada da gestão e dos agentes públicos em gestão de riscos, controles e conformidade, por meio de soluções educacionais adequadas a cada nível organizacional	Devem ser ofertadas ações formativas específicas e contínuas, desenvolvendo competências adequadas a cada perfil funcional e fortalecendo a cultura institucional.
XIV	Fortalecimento e disseminação da cultura de gestão de riscos, controles e conformidade em toda a organização	A organização deve promover ações de sensibilização, comunicação interna e valorização de práticas preventivas, consolidando uma cultura orientada à integridade e ao controle.

As diretrizes de gestão de riscos da ISO 31000:2018 constituem um referencial indispensável para que os órgãos públicos integrem o gerenciamento de riscos de forma estruturada, transparente e alinhada à sua missão institucional. Sua adoção fortalece a governança, aprimora a tomada de decisão, otimiza o uso dos recursos e amplia a confiança da sociedade nas instituições. Assim, utilizar essas diretrizes de maneira consistente é essencial para consolidar uma cultura organizacional voltada à prevenção, à resiliência e à criação de valor público sustentável.

7. ESTRUTURA, INSTÂNCIAS E RESPONSABILIDADES DA GESTÃO DE RISCO

A gestão de riscos, no âmbito dos órgãos e entidades, está estruturada conforme:

Essa estrutura busca fortalecer a governança, a integridade, a transparência e a eficiência da administração pública, em conformidade com os arts. 70 e 74 da CF/88 e arts. 70 e 76 da CE/ES.

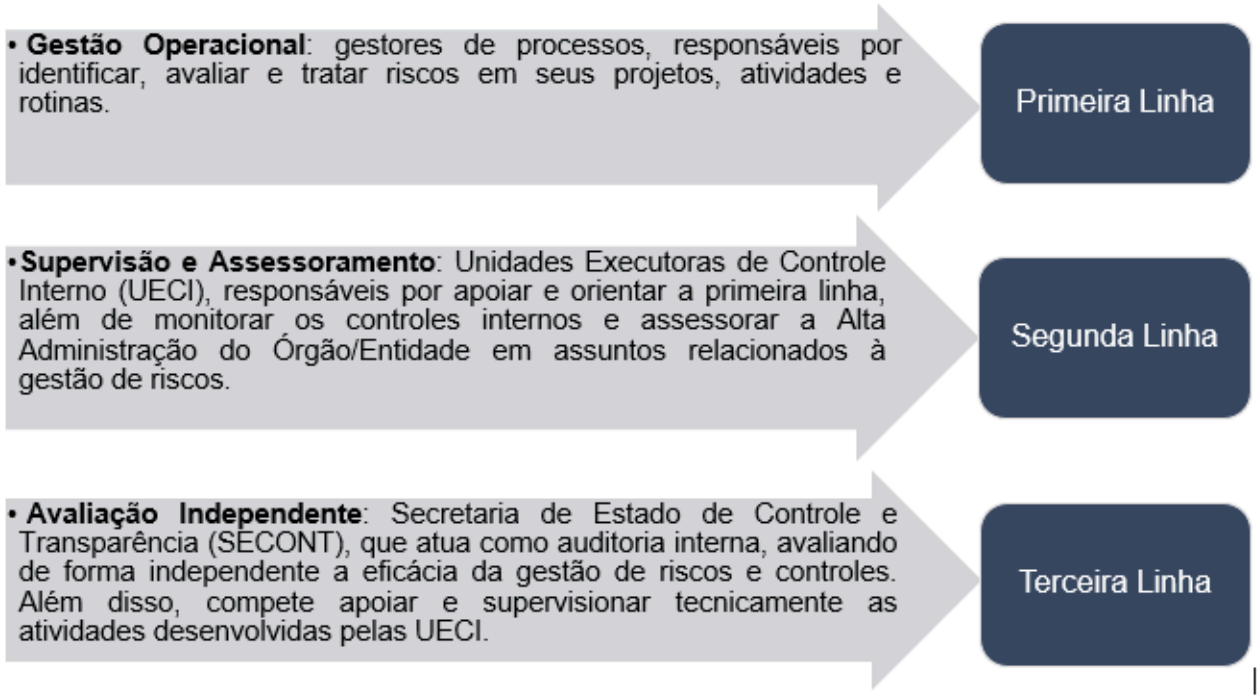
O Modelo das Três Linhas, revisado em 2020 pelo Instituto dos Auditores Internos (IIA), é uma estrutura de governança, aplicável a qualquer tipo de organização pública ou privada, cujos princípios foram adaptados à realidade estadual pela Lei Complementar nº 856/2017.

No Poder Executivo do Estado do Espírito Santo, esse modelo organiza as res-

-ponsabilidades da gestão de riscos em três níveis, fortalecendo a integração entre gestão, controle e governança. Ele define papéis e responsabilidades de forma clara, melhora a comunicação e garante melhor coordenação entre as funções envolvidas.

Portanto, a gestão de riscos deve ser elaborada sobre o Modelo das Três Linhas, que define papéis e responsabilidades de forma integrada:

Linhas de Responsabilidade*



Observa-se, ainda, que, no contexto da Administração Pública, a aplicação do modelo das três linhas implica a instituição de estruturas de governança voltadas às funções de liderança, estratégia e controle, distintas das atividades operacionais de gestão.

No âmbito federal, por exemplo, a Instrução Normativa Conjunta CGU/MPOG nº 01/2016 estabelece que os órgãos e entidades do Poder Executivo federal devem instituir, por ato de seus dirigentes máximos, o Comitê de Governança, Riscos e Controles.

Tal arranjo é necessário para assegurar a clara definição dos papéis exercidos pela Alta Administração, no exercício da governança, bem como daqueles desempenhados pela primeira linha — responsável pela condução das atividades e pela gestão de riscos e controles no âmbito dos processos

organizacionais — e pela segunda linha, cujas atribuições concentram-se, primordialmente, no assessoramento, orientação e monitoramento da gestão de riscos e dos controles internos.

Exemplo

Como são estruturadas as instâncias de governança e gestão de riscos no âmbito da SECONT?

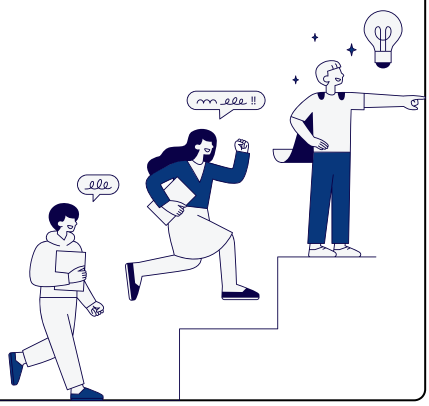
A estrutura de gestão de riscos, no âmbito da Secont, é composta pelas seguintes instâncias:

- a Autoridade Máxima do Órgão, representada pelo Secretário de Estado de Controle e Transparência;
- o Comitê de Gestão de Riscos;
- a Unidade Executora de Controle Interno – UECI; e
- os servidores responsáveis por processos, projetos, atividades e ações

Na prática, como isso funciona:

Ao **Secretário de Estado de Controle e Transparência**, Autoridade Máxima do Órgão, compete:

- **Estabelecer a política de gestão de riscos da Secont e revisá-la, quando necessário;**
- Definir e revisar o apetite a riscos da instituição;
- Instituir o Comitê de Gestão de Riscos (CGR).



Ao **Comitê de Gestão de Riscos**, órgão colegiado, deliberativo e permanente, composto pelo Secretário, subsecretários, corregedor geral e outros servidores, conforme a natureza e complexidade das matérias tratadas.
Suas principais atribuições são:

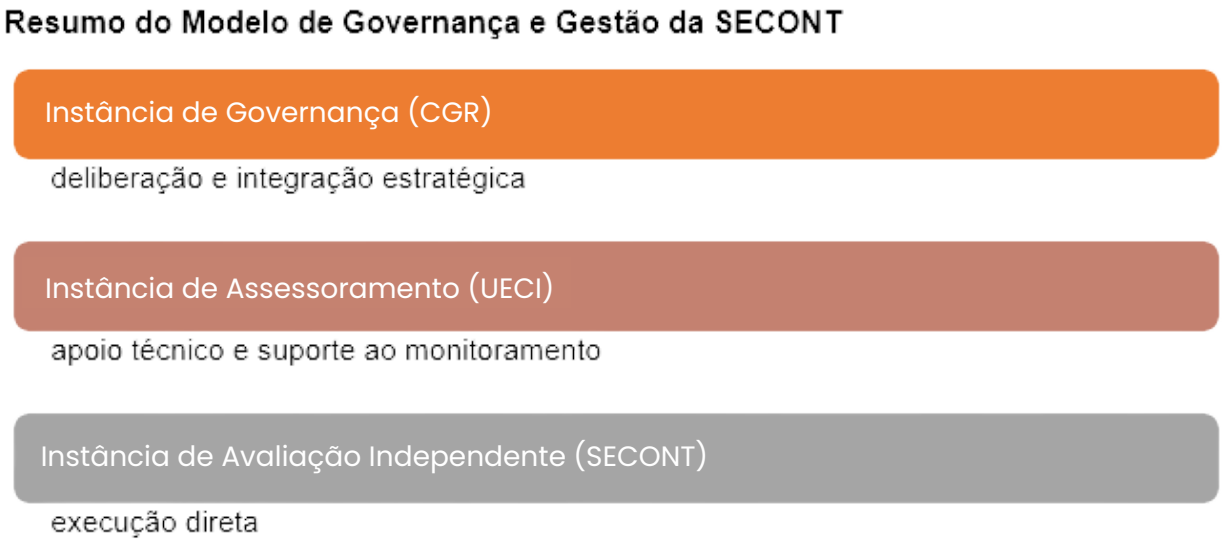
- Deliberar sobre níveis de exposição a riscos.
- Garantir a disponibilidade de informações relevantes para decisões.
- Promover comunicação clara e transparente.
- Disseminar a cultura de gestão de riscos e incentivar a capacitação dos servidores.
- Assegurar recursos para a implementação da gestão de riscos.
- Monitorar, com apoio da Unidade Executora de Controle Interno (UECI), os processos de gestão de riscos que impactam a consecução dos objetivos institucionais
- Aprovar e acompanhar planos de tratamento de riscos.
- Avaliar os resultados da implementação da gestão de riscos.
- Avaliar a adequação, suficiência e eficácia do processo de gestão de riscos.

À **Unidade Executora de Controle Interno** da SECONT, compete:

- Apoiar os gestores de riscos da Primeira Linha.
- Assessorar o CGR em temas técnicos.
- Assessorar o monitoramento da execução dos planos de tratamento de riscos.

Aos **Gestores de Processos (Primeira Linha)**, no contexto da gestão de riscos, compete :

- Mapear processos e identificar riscos.
- Propor respostas e implementar controles.
- Monitorar riscos e reportar periodicamente aspectos relevantes.
- Comunicar mudanças relevantes ao CGR e à UECI.
- Garantir mitigação de riscos e efetividade dos controles.
- Orientar e engajar servidores na gestão de riscos.



8. CATEGORIAS DE RISCOS

Após estabelecida a missão, a alta administração planeja os objetivos, seleciona as estratégias e estabelece planos a serem adotados por todo o órgão/entidade. Estes objetivos, estratégias e planos para seu cumprimento devem observar as categorias de riscos conforme tabela a seguir:

Quadro V - Categorias de Risco

Nº	Categoria de Risco	Descrição	Exemplo
I	Estratégicos	Riscos que afetam a definição ou execução dos objetivos estratégicos e da estratégia institucional.	Mudança repentina de diretrizes governamentais que afeta o plano plurianual da organização.
II	Conformidade	Riscos decorrentes do descumprimento de normas, leis, regulamentos e diretrizes.	Descumprimento da Lei de Acesso à Informação ou da Lei de Responsabilidade Fiscal.

III	Orçamentários e Financeiros	Riscos que afetam a definição ou execução dos objetivos estratégicos e da estratégia institucional.	Mudança repentina de diretrizes governamentais que afeta o plano plurianual da organização.
IV	Conformidade	Riscos associados à gestão inadequada de recursos, caixa, investimentos e obrigações.	Superestimativa da arrecadação, levando à insuficiência de recursos para ações essenciais.
V	Ambientais	Riscos que causam ou podem causar degradação ao meio ambiente ou ao ecossistema.	Vazamento de produtos químicos no descarte de resíduos de laboratórios.
VI	Tecnologia da Informação	Riscos ligados à indisponibilidade, falhas, segurança ou obsolescência de sistemas, dados e equipamentos.	Pane no sistema de gestão de contratos que impede o andamento de processos administrativos.
VII	Recursos Humanos	Riscos originados da gestão inadequada de pessoas, competências, saúde ocupacional, clima organizacional ou estrutura funcional.	Alta rotatividade de servidores em área crítica, comprometendo a continuidade das atividades.
VIII	Integridade	Riscos relacionados à fraude, corrupção, conflito de interesse ou violação de padrões éticos.	Manipulação indevida de licitações para favorecer empresas específicas.

9. PROCESSO DE GESTÃO DE RISCOS

Visão Geral do Processo de Gestão de Riscos

O processo de gestão de riscos é composto por oito etapas interligadas, que devem ser aplicadas de forma contínua e dinâmica:

Etapas do Processo de Gestão de Riscos

Etapa	Descrição	Objetivo Principal
Estabelecimento do Contexto	Consiste na compreensão dos objetivos institucionais e os processos a eles vinculados, além de identificar e definir os contextos internos e externos que devem ser considerados na gestão dos riscos, assegurando que todos os fatores relevantes sejam adequadamente analisados para a tomada de decisões informada e eficiente.	Alinhar o processo de risco ao contexto organizacional
Identificação de Riscos	Compreende a identificação sistemática de eventos que possam afetar o alcance dos objetivos institucionais, com a descrição dos riscos em termos de suas causas e possíveis consequências, considerando fontes internas e externas.	Identificar ameaças e oportunidades
Análise de Riscos	Visa compreender a natureza dos riscos e determinar seus níveis, com base na avaliação da probabilidade de ocorrência e do impacto das consequências, devendo ser considerada a eficácia dos controles existentes para fins de determinacão do risco residual.	Compreender a significância dos riscos identificados
Avaliação de Riscos	Consiste na comparação entre os níveis de risco identificados e o apetite a riscos previamente estabelecido, com vistas à definição da aceitabilidade dos riscos e à priorização daqueles que demandam tratamento.	Subsidiar a tomada de decisões
Tratamento de Riscos	Abrange a definição e implementação de medidas adequadas para modificar os riscos, podendo envolver sua mitigação, transferência, aceitação ou eliminação, devendo ser formalizado plano de ação com indicação de responsáveis, prazos e recursos necessários.	Reduzir a exposição a níveis aceitáveis
Comunicação e Consulta	Compreende o intercâmbio contínuo de informações com as partes interessadas, internas e externas, a fim de promover o entendimento mútuo acerca dos riscos e garantir a consideração de diferentes perspectivas no processo decisório.	Assegurar a eficácia e atualidade da gestão
Monitoramento e Análise Crítica	Refere-se ao acompanhamento contínuo dos riscos, dos controles e dos planos de tratamento implementados, com vistas à verificação de sua eficácia, à detecção de alterações no contexto e à promoção da melhoria contínua do processo de gestão de riscos.	Promover colaboração e compartilhamento de informação
Registro e Relato	Consiste na documentação sistemática e no relato estruturado das atividades e resultados da gestão de riscos, com vistas a assegurar a rastreabilidade das decisões e subsidiar a tomada de decisão em todos os níveis da organização.	Documentação para transparência e suporte decisório

Exemplos Práticos por Etapa do Processo

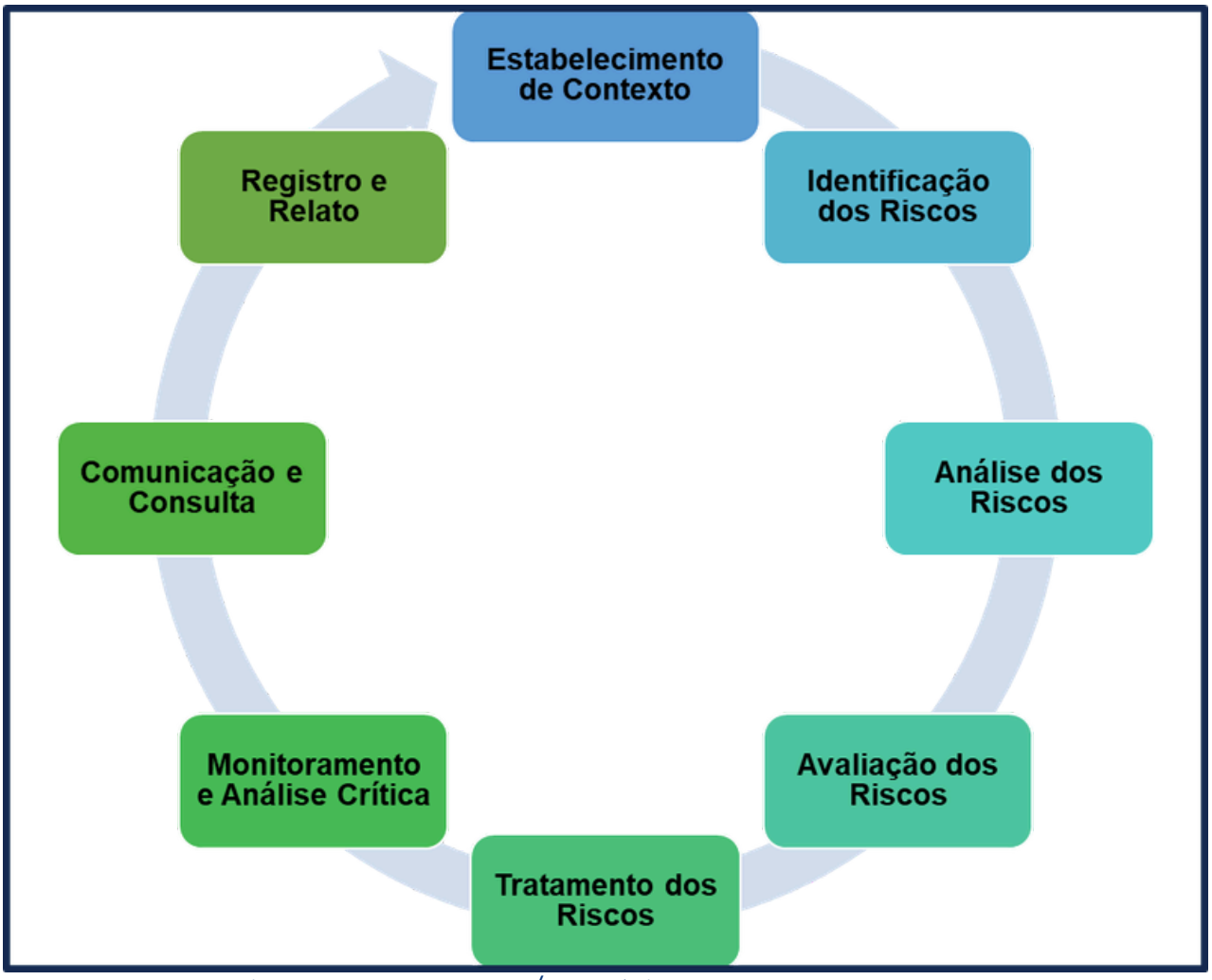
Para melhor entendimento do tema, este guia exemplifica as etapas do processo:

Quadro VI – Etapas do Processo

Etapas do Processo		
Etapa	**Exemplo Prático**	**Ferramentas/Métodos**
1. Estabelecimento do Contexto	**Caso:** Secretaria estadual de administração pública vai implementar um novo sistema de protocolo digital. Ela define: **Escopo:** riscos relacionados à implementação do sistema, desde a fase de planejamento até a implantação e monitoramento. **Contexto:** estrutura organizacional da secretaria e ambiente tecnológico e regulatório atual. **Critérios:** apetite a riscos e matriz de risco utilizadas.	Análise de documentos, reuniões com partes interessadas, estudo do ambiente interno e externo.
2. Identificação dos Riscos	**Exemplo:** riscos levantados em reuniões de alinhamento com gestores e consultas a especialistas. **Riscos identificados, com causas e consequências:** • Falha de integração com sistemas legados (antigos); • Resistência dos servidores à mudança; • Possível vazamento de dados sensíveis.	Brainstorm, análise de processos, entrevistas, consulta a projetos similares, checklists de riscos.
3. Análise dos Riscos	Exemplo: Falha de integração com sistemas legados. Probabilidade: Provável (devido à tecnologia obsoleta utilizada atualmente). Impacto: Alto (interrupção de serviços essenciais).	

	Controles existentes: equipe de TI capacitada, documentação técnica disponível. **Resultado:** risco classificado como Alto.	Análise qualitativa, análise de causa e efeito, matriz de risco (probabilidade x impacto).
5. Tratamento dos Riscos	Risco – Falha na integração com sistemas legados **Medidas de tratamento:** • Testes de integração progressivos. • Protótipos de prova de conceito. • Equipes de sobreaviso. **Justificativa:** ações visam reduzir probabilidade e/ou impacto dos riscos, alinhadas aos objetivos institucionais.	Plano de ação, políticas de segurança da informação, plano de comunicação interna.
6. Monitoramento e Análise Crítica	**Exemplo:** • Acompanhamento mensal dos indicadores-chave (número de chamados abertos, número de incidentes de falha) • Após 6 meses, nova análise de riscos para reavaliar cenários e controles. Objetivo: garantir que as medidas adotadas continuem eficazes e identificar novos riscos.	Dashboards de indicadores, reuniões periódicas do comitê de riscos, auditorias internas, relatórios de desempenho.
7. Comunicação e Consulta	**Exemplo:** • Divulgação de boletins informativos mensais com a evolução do projeto e principais riscos monitorados. • Realização de reuniões participativas com setores usuários. • Disponibilização de canal direto para sugestão e dúvidas dos servidores.	Boletins eletrônicos, reuniões presenciais e virtuais, canais de comunicação internos.
8. Registro e Relato	**Exemplo:** • Documentação completa registrada nos sistemas informatizados. • Elaboração de relatórios periódicos de acompanhamento.	Sistemas informatizados, reuniões periódicas com o comitê de riscos, relatórios de acompanhamento.

Ciclo do Processo de Gestão de Riscos



Fonte: Adaptado da Figura 4 da NBR ISO 31000/2018 página 9

O processo de gestão de riscos deverá ser aplicado sistematicamente, compreendendo cada etapa.

9.1 Estabelecimento do Contexto

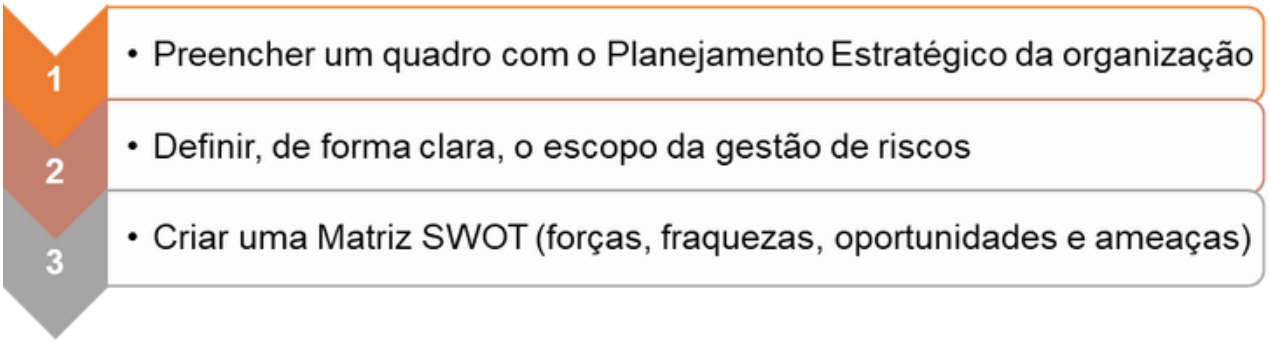
A etapa de estabelecimento do contexto consiste em compreender os objetivos organizacionais e processos essenciais, com identificação sistemática dos fatores internos (estrutura, recursos, cultura) e externos (legislação, mercado, tecnologia) que influenciam a gestão de riscos. Essa etapa inclui, também, a definição precisa do escopo e dos critérios de avaliação, garantindo que todos os elementos relevantes sejam considerados para decisões seguras, eficazes e alinhadas à estratégia institucional.

Quadro VII - Estabelecimento do Contexto

Dimensão	Aspectos a Considerar
Escopo	• Delimitação precisa do objeto da gestão de riscos (processos, projetos, atividades específicas). • Inclusões e exclusões explícitas. • Período temporal e localização geográfica. • Níveis de detalhamento e granularidade adequados. • Alinhamento aos objetivos estratégicos da organização.
Contexto do Processo de Gestão de Riscos	• Definição de papéis e limites de responsabilidade e autoridade. • Decisões e ações necessárias. • Recursos necessários (humanos, financeiros, tecnológicos). • Interfaces com outros processos organizacionais. • Forma de avaliação do desempenho da gestão de riscos.
Contexto Externo	• Ambiente cultural, político, legal, regulatório, financeiro, econômico e ambiental (nível internacional, nacional, regional ou local). • Fatores-chave e tendências que impactam os objetivos da organização. • Percepções e valores das partes interessadas externas.
Contexto Interno	• Capacidades da organização (recursos e conhecimento). • Fluxos de informação e processos de decisão. • Partes interessadas internas. • Objetivos e estratégias existentes. • Percepções, valores e cultura. • Políticas, processos, normas e modelos adotados. • Estruturas de governança, papéis e responsabilidades.
Critérios de Risco	• Natureza e tipos de consequências e como serão medidos. • Forma de expressar probabilidades. • Metodologias para avaliação de riscos. • Critérios para aceitar ou tolerar riscos. • Critérios para definir necessidade de tratamento.

É essencial entender que fatores internos da organização podem ser fontes de risco, e que os objetivos finais devem estar claros.

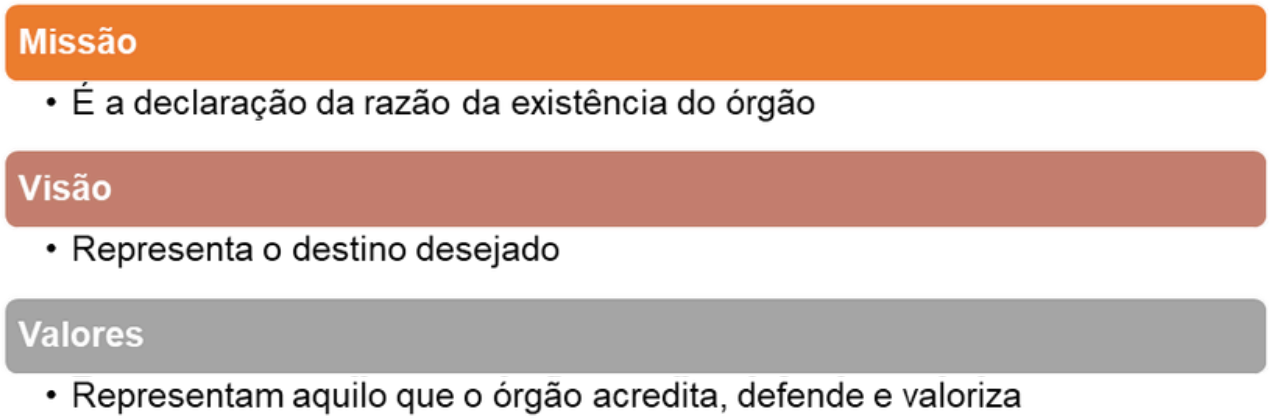
Para facilitar o aprendizado e aplicação prática dessa etapa, sugerem-se três ações:



Esses documentos podem ser solicitados pela Auditoria Interna ou pelos supervisores de riscos, por isso devem ser registrados corretamente.

9.1.1 Planejamento Estratégico

A primeira ação requerida é o preenchimento de quadro com informações sobre o Planejamento Estratégico da organização, com sua declaração de Missão, Visão e Valores.



Esse exercício sugere que toda organização já tenha feito essa declaração. Algumas, no entanto, não declararam ou a fazem de forma parcial não refletindo seu objetivo de existência. Como um dos objetivos da gestão de risco é agregar valor ao negócio, o Planejamento Estratégico deve ser declarado. Outro motivo positivo da revisão do Planejamento Estratégico em forma de quadro é que muitos servidores, apesar de anos de dedicação naquela estrutura, desconhecem essa declaração feita pela organização.

Quadro VIII - Exemplo de quadro de informações do Planejamento Estratégico da Organização

Planjamento Estratégico	
Órgão / Entidade	Secretaria de Estado de Controle e Transparência - Secont
Missão	Contribuir para o aperfeiçoamento das políticas públicas da gestão pública e contribuir para a evolução da qualidade na aplicação dos recursos em benefício da sociedade.
Visão	Ser uma instituição reconhecida pela qualidade no controle interno da Administração Pública.
Valores	Integridade: I. Agir com ética, honestidade, imparcialidade, moralidade e legalidade. II. Autonomia Técnica: Refere-se a autonomia e liberdade técnica que a equipe de auditoria interna tem para realizar seu trabalho de forma independente e objetiva III. Zelo Profissional: Trabalhar com excelência, produtividade, comprometimento, eficiência, agregação de valor e resultado na preservação dos bens e interesses da sociedade. IV. Melhoria Contínua: Refere-se ao esforço contínuo na promoção da melhoria das atividades desenvolvidas de maneira a agregar valor nos serviços prestados à população.

9.1.2 Definição do escopo

A definição do escopo é a segunda ação no estabelecimento do contexto e consiste em conhecer bem o objeto da gestão de riscos. Isso inclui identificar:

- Título: nome do objeto, que pode ser um programa, processo, atividade ou projeto, por exemplo, "Gestão de Riscos no processo de Contratação de Serviços".
- Objetivo: o que se pretende alcançar com o objeto da gestão de riscos, tanto objetivos específicos quanto estratégicos. Pergunte-se: “Quais os propósitos desse objeto?”

- Partes Interessadas: pessoas ou organizações que podem influenciar, ser influenciadas ou perceber impacto nas decisões ou atividades. É importante mapear suas necessidades, expectativas e envolver essas partes para uma gestão de riscos mais eficaz.
- Normativos, sistemas, unidade Responsável e início do trabalho: listar as normas aplicáveis, sistemas de informação envolvidos, indicar a unidade responsável pela gestão de riscos e registrar quando o trabalho começa.

Esses pontos ajudam a ter clareza sobre o que será gerido e facilitam o controle do processo.

O Quadro a seguir ilustra o registro hipotético da definição de escopo de gestão de riscos:

Quadro IX - Exemplo de Definição de Escopo

Definição de Escopo	
Título	Gestão de Riscos no Programa de Integridade do Governo do Estado do Espírito Santo
Objetivos Diretos	Identificar, avaliar, tratar e monitorar riscos que possam comprometer a implementação e efetividade do Programa de Integridade.
Objetivo(s) Estratégico(s) Associado(s)	Fortalecer a cultura da integridade e da transparência na Administração Pública Estadual; Promover a confiança da sociedade na gestão pública.
Partes Interessadas	Servidores e gestores da SECONT, órgãos e entidades do Poder Executivo Estadual, cidadãos, sociedade civil organizada, órgãos de controle externo (TCE-ES, CGU), fornecedores e parceiros institucionais.

Leis e Regulamentos Relacionados	Lei Federal nº 12.846/2013 (Lei Anticorrupção); Lei de Acesso à Informação (Lei nº 12.527/2011);
Sistemas	e-SIC (Sistema Eletrônico do Serviço de Informação ao Cidadão), SEI-ES (Sistema Eletrônico de Informação), e-Social, sistemas de auditoria eletrônica e sistemas de monitoramento de integridade da SECONT.
Unidade Responsável	Subsecretaria de Integridade Governamental.
Início do Trabalho	01/10/2025 (data hipotética para início do processo de gestão de riscos do Programa de Integridade).

9.1.3 Matriz SWOT

Para entendimento do contexto interno e externo as organizações utilizam a ferramenta "Matriz SWOT". Essa ferramenta, se bem aplicada, ajuda na análise dos elementos que impactam a organização, internamente e externamente. Com as iniciais dos termos em inglês - Strengths, Weaknesses, Opportunities and Threats - ou FOFA – Força, Oportunidades, Fraqueza e Ameaças – busca demonstrar o impacto sobre o objeto de gestão de riscos em análise, afetando o resultado almejado.

Na análise do ambiente externo são identificadas as oportunidade e ameaças, representadas por um contexto favorável ou desfavorável e sobre os quais a organização não tem poder de decisão ou influência. Aqui são relacionados aspectos como fatores sociais, culturais, políticos, jurídicos, regulatórios, financeiros, tecnológicos, econômicos e ambientais.

Para a análise do ambiente interno são avaliadas as forças e fraquezas da organização. Sobre esses fatores a organização possui algum controle ou

gerência, como visão, missão, valores, objetivos estratégicos, estrutura organizacional, governança, pessoas, sistemas, políticas, processos, cultura organizacional, entre outros.

O resultado apresentado desse instrumental é que as forças e oportunidades são fatores positivos a serem considerados e com as fraquezas e ameaças identificadas representam os fatores negativos a serem conhecidos e devem ser evitados pela organização.

A Matriz SWOT é uma ferramenta simples e super útil para entender o que está acontecendo dentro e fora da organização. Ela ajuda a identificar os pontos fortes e fracos que a organização tem controle, além das oportunidades e ameaças que vêm do ambiente externo, onde a organização não pode mexer.

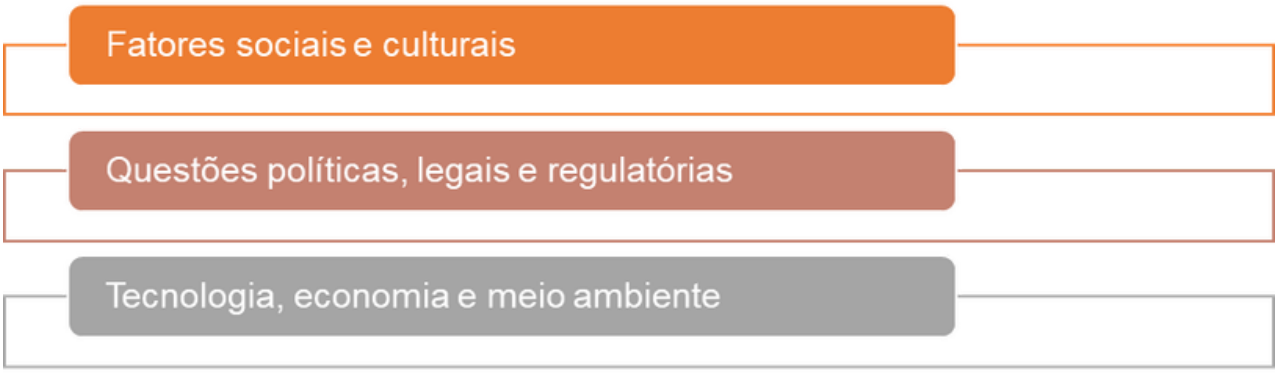
• **Ambiente interno**

Nesta parte, identificamos o que a organização pode controlar, como:

Esses são os pontos fortes (forças) que ajudam, ou os pontos fracos (fraquezas) que precisam melhorar.

• Ambiente externo

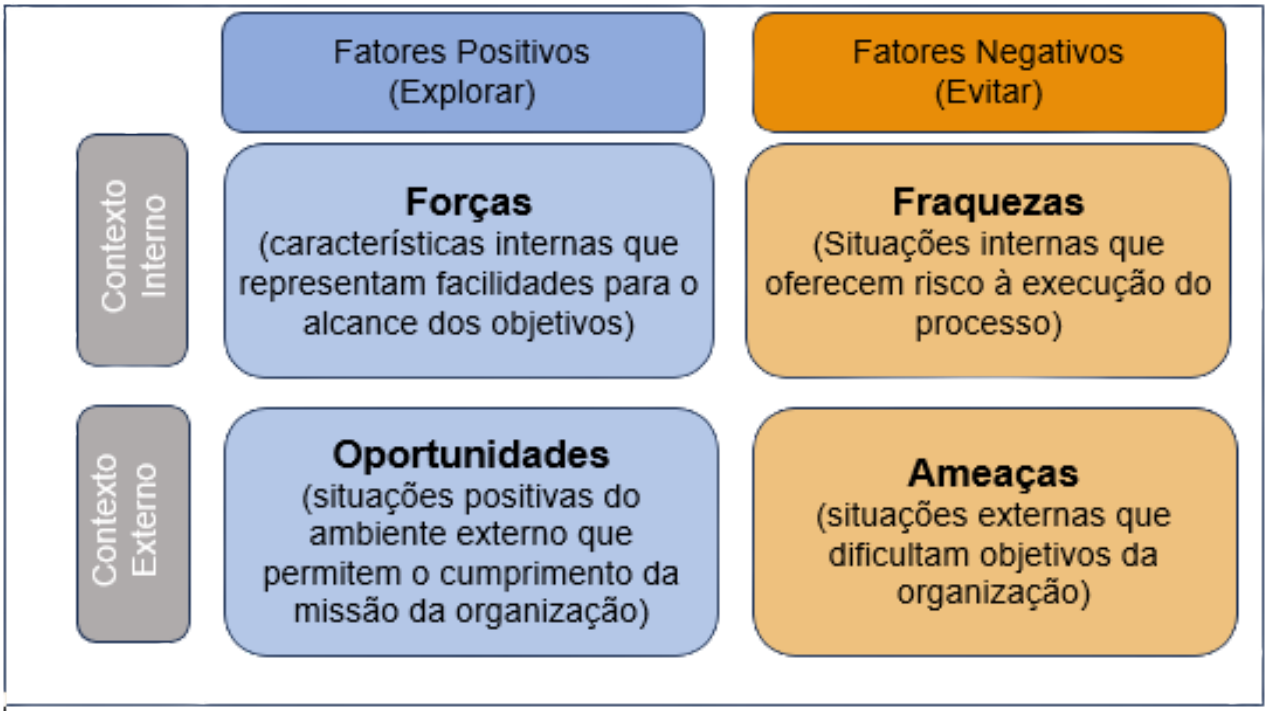
Nesta parte, identificamos oportunidades e ameaças que vêm de fora e sobre as quais a organização não tem controle. Exemplo:



Forças e oportunidades são coisas boas que a organização pode usar a seu favor. Já as fraquezas e ameaças são desafios que é importante conhecer para evitar problemas e ajudar na gestão dos riscos.

Assim, aplicando a Matriz SWOT, a organização entende melhor seu contexto e fica mais preparada para tomar decisões estratégicas.

Representação gráfica de uma Matriz SWOT



Fatores Internos	Fatores Externos
Forças (Strengths)	**Oportunidades (Opportunities)**
• Existência de normativa institucional de gestão de riscos (ex: portarias, decretos); • Comprometimento da alta direção com o tema; • Equipe capacitada em governança e gestão de riscos; • Estrutura de controles internos já estabelecida; • Ferramentas e sistemas de apoio à gestão de riscos.	• Apoio dos órgãos de controle e regulamentações que incentivam a gestão de riscos; • Maior valorização da transparência e da integridade pública; • Parcerias com outras instituições para troca de boas práticas; • Oferta de capacitações por instituições de renome (ex: ENAP, CGU); • Evolução tecnológica para monitoramento e tratamento de riscos.
Fraquezas (Weaknesses)	**Ameaças (Threats)**
• Cultura organizacional ainda resistente a mudanças; • Falta de integração da gestão de riscos com o planejamento estratégico e a execução orçamentária; • Escassez de recursos humanos e financeiros; • Alta rotatividade de servidores nas áreas responsáveis; • Dificuldade na comunicação entre áreas.	• Mudanças políticas que afetem o comprometimento com a governança; • Riscos emergentes (ex: cibersegurança, mudanças climáticas); • Exigências crescentes dos órgãos de • controle sem aumento de recursos; • Falta de uniformidade na aplicação da metodologia entre unidades; • Possibilidade de judicialização por falhas na prevenção de riscos.

9.1.4 Definindo os Critérios de Risco

- Definir os critérios de risco inclui decidir:
- Quais tipos de consequências serão consideradas e como serão medidas;
- Como expressar as probabilidades;
- Como determinar o nível de risco;
- Critérios para aceitar ou tolerar riscos;
- Critérios para definir necessidade de tratamento;

Este guia orienta os usuários na definição completa desses critérios, funcionando como referência prática para toda a gestão de riscos.

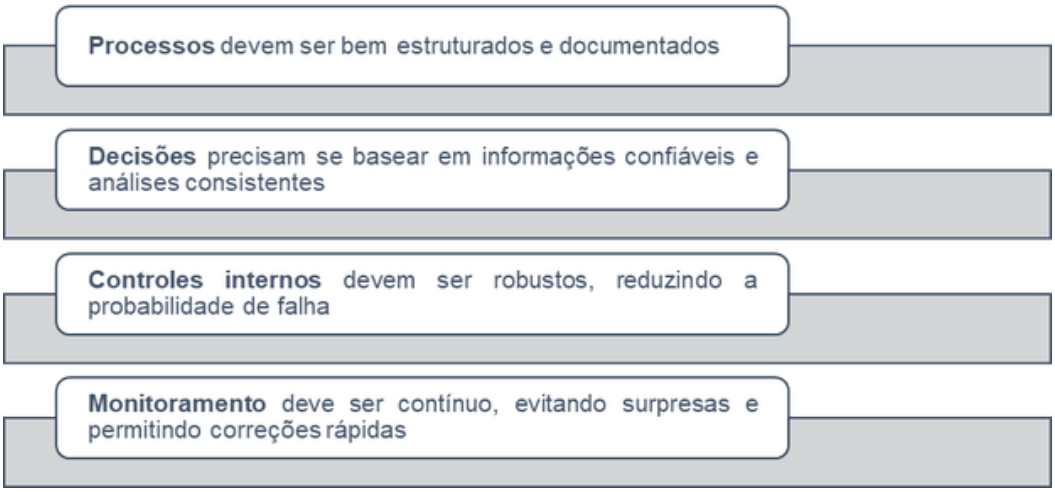
9.1.4.1 Apetite a riscos

O apetite a riscos representa o nível de risco que uma organização está disposta a admitir na realização de suas atividades e objetivos. Em termos simples, trata-se do quanto o órgão ou entidade admite "encarar" incertezas para cumprir sua missão institucional.

Por que isso importa na Administração Pública?
A definição do apetite ao risco é essencial para orientar decisões, priorizar recursos e fortalecer a governança. No setor público, isso significa garantir que a busca por resultados — como políticas públicas, serviços essenciais e entregas à sociedade — ocorra de forma **responsável, transparente e segura**.

- **Exemplo prático**

Imagine uma secretaria que define seu apetite ao risco como baixo. Isso implica que:



Em outras palavras, a organização aceita pouca variação ou incerteza e exige maior rigor na gestão.

- **Nem todas as áreas têm o mesmo nível de risco**

É importante reconhecer que cada área possui características próprias. Órgãos com processos mais complexos ou com impacto direto na vida da população — como Saúde, Educação, Segurança Pública e Justiça — naturalmente enfrentam maior exposição a riscos.

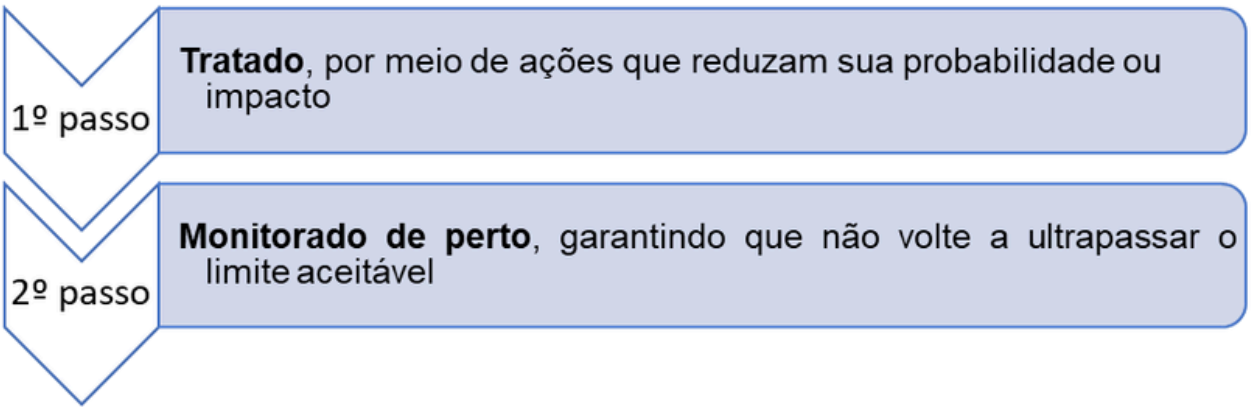
Por isso, antes de definir o apetite ao risco, é indispensável realizar uma análise detalhada dos riscos intrínsecos à área. Sem essa etapa, corre-se o risco de estabelecer um apetite incompatível com a realidade, como exigir "tolerância zero" para riscos em atividades que, por natureza, envolvem

incertezas (ex.: atendimento emergencial, operações policiais, gestão hospitalar).

Apetites irreais acabam se tornando apenas documentos formais, sem utilidade prática.

- **O que fazer com riscos que ultrapassam o apetite?**

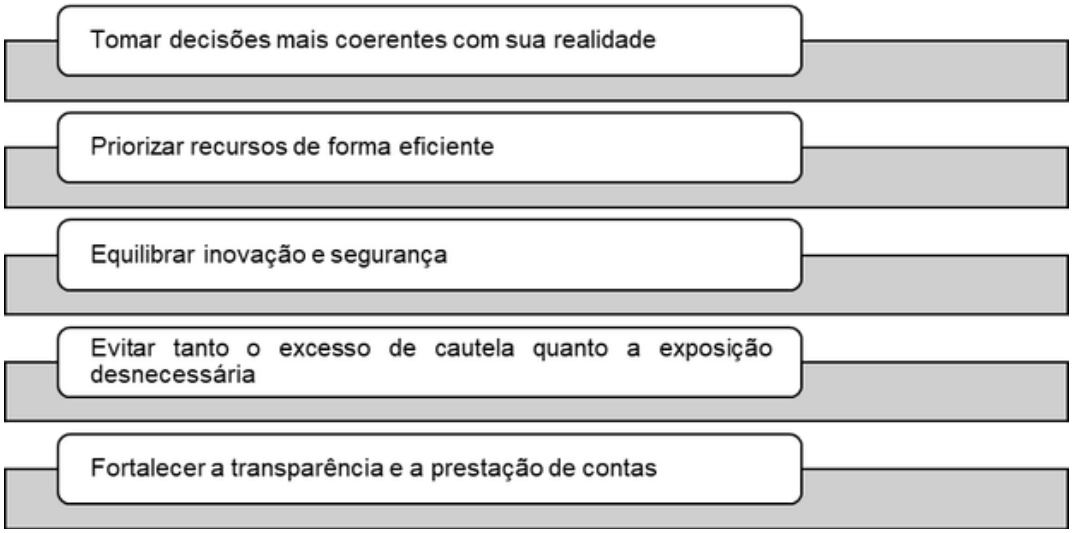
Quando um risco identificado ultrapassa o apetite definido, ele deve ser:



Caso a unidade decida não tratar determinado risco, essa decisão deve ser justificada, demonstrando que foi tomada de forma consciente e alinhada à governança.

- **Como o apetite ao risco contribui para a gestão pública?**

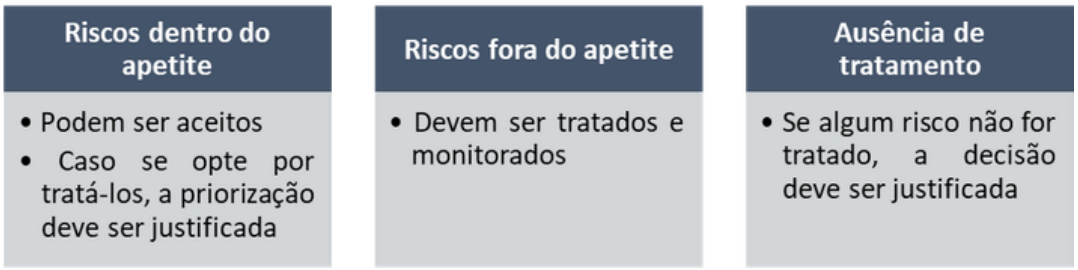
O apetite ao risco ajuda a organização a:



Em síntese, ele orienta até onde a organização pode "arriscar" para cumprir sua missão com segurança, eficiência e responsabilidade.

- **Diretrizes gerais**

A declaração de apetite ao risco da unidade organizacional deve estabelecer, de forma clara:



Quadro XI – Exemplo de tratamento riscos de uma organização com apetite baixo

Nível de risco	Situação	Diretriz principal
Extremo	Acima do apetite a riscos	Requer ação imediata para tratamento do risco e pode envolver a interrupção do processo organizacional ou adoção de medidas emergenciais de contenção até a eliminação completa da causa raiz.
Alto	Acima do apetite a riscos	Requer a implementação de medidas de tratamento que reduzam o risco a níveis toleráveis, com monitoramento intensivo dos controles.
Médio	Acima do apetite a riscos	Não se faz necessário adotar medidas sofisticadas de tratamento, mas aprimorar os controles já existentes ou implementar ações complementares que reduzam o risco.
Baixo	Dentro do apetite a riscos	Não se faz necessário adotar qualquer medida adicional de tratamento, exceto monitorar continuamente oscontroles já existentes e indicadores de desempenho.

Saúde

A área da Saúde lida com atividades críticas, alta complexidade e impacto direto na vida das pessoas. Por isso, costuma ter apetite ao risco baixo para riscos que afetem a segurança do paciente, mas pode aceitar níveis maiores em temas administrativos ou de inovação.

Tipo de risco	Situação	Apetite provável	Justificativa
Estratégico Operacional	Falha na administração de medicamentos	Baixo	Impacto direto na vida e integridade do paciente
Operacional	Adoção de novo sistema eletrônico de prontuário	Médio	Inovação necessária, riscos controláveis com testes e capacitação
Financeiro	Atraso na entrega de insumos de baixo impacto	Médio a alto	Possível de mitigar com estoques mínimos e fornecedores alternativos
Estratégico	Implantação de telemedicina	Médio	Envolve incertezas, mas traz ganhos relevantes de acesso e eficiência

Como isso se traduz na prática

- Um hospital público **não pode aceitar** risco elevado em protocolos de segurança do paciente.
- Mas pode aceitar algum risco ao testar um novo fluxo de atendimento que promete reduzir filas.

Educação

A Educação envolve atividades contínuas, com impacto social relevante, mas com riscos menos imediatos à integridade física do cidadão. Assim, o apetite ao risco tende a ser **moderado**, variando conforme o tipo de risco.

Tipo de risco	Situação	Apetite provável	Justificativa
Estratégico Operacional	Adoção de nova metodologia de ensino	Médio a alto	Inovação pedagógica é desejável e riscos são controláveis
Operacional	Falhas pontuais no transporte escolar	Baixo	Impacta a segurança e acesso dos estudantes
Tecnológico	Implantação de plataforma digital de aprendizagem	Médio	Riscos de adoção podem ser mitigados com capacitação
Financeiro	Variação no custo de manutenção predial das escolas	Médio	Impacto gerenciável com planejamento e priorização

Na prática

- Uma secretaria pode aceitar riscos maiores ao testar um novo modelo de avaliação escolar.
- Mas deve ter **apetite baixo** para riscos que comprometam a segurança de alunos no transporte ou na infraestrutura física.

Segurança Pública

A Segurança Pública opera em ambiente de alta incerteza, com riscos inerentes e inevitáveis. O apetite ao risco costuma ser baixo para riscos que afetem vidas, mas médio ou alto para riscos estratégicos e operacionais que fazem parte da atividade policial.

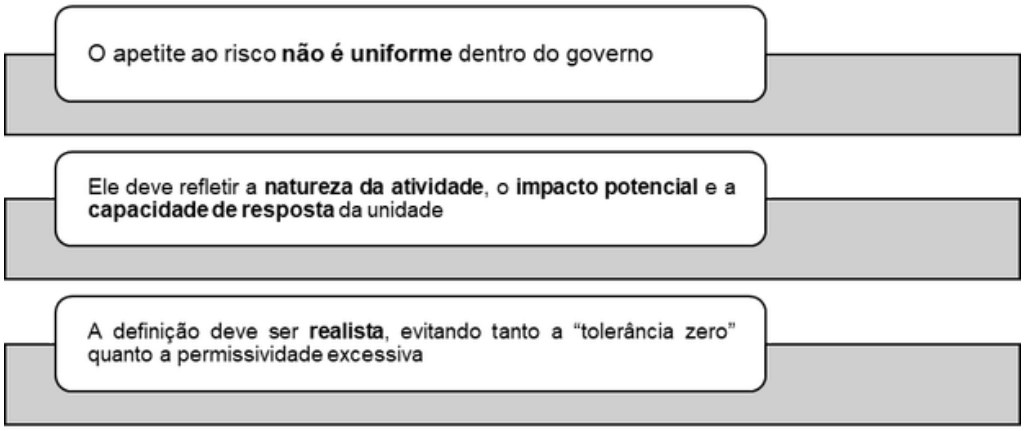
Tipo de risco	Situação	Apetite provável	Justificativa
Operacional	Operações policiais em área de risco	Baixo	Necessidade de preservar vidas de agentes e cidadãos
Tecnológico	Implantação de sistema de reconhecimento de placas	Médio	Inovação com riscos controláveis
Estratégico	Reestruturação de batalhões ou delegacias	Médio a alto	Mudanças estruturais envolvem incertezas, mas podem gerar ganhos significativos
Operacional	Comunicação inadequada de operações	Baixo	Impacta na confiança pública e integridade institucional

Na prática

- A corporação **não pode aceitar** riscos elevados em protocolos de uso progressivo da força.
- Mas pode aceitar riscos moderados ao testar novas tecnologias de monitoramento ou reorganizar unidades.

Como esses exemplos ajudam na definição do apetite ao risco

Esses cenários mostram que:



9.2 Identificação e Análise dos Riscos

A identificação dos riscos é o processo de encontrar e registrar possíveis eventos que possam afetar os objetivos da organização, destacando as fragilidades nos processos.

A análise dos riscos, por sua vez, tem como objetivo entender esses riscos, avaliando a probabilidade de ocorrência e os impactos, para definir o nível de risco e a necessidade de ações.

Identificação dos riscos	• Compreende a identificação sistemática de eventos que possam afetar o alcance dos objetivos institucionais, com a descrição dos riscos em termos de suas causas e possíveis consequências, considerando fontes internas e externas.
Análise dos riscos	• Visa compreender a natureza dos riscos e determinar seus níveis, com base na avaliação da probabilidade de ocorrência e do impacto das consequências, devendo ser considerada a eficácia dos controles existentes para fins de determinação do risco residual.

Dessa forma, a identificação dos riscos é o processo de encontrar, reconhecer e registrar os riscos, para uma ação preventiva da organização. Após o risco identificado, a organização passa a analisar esse risco, identificando a existência de controles sobre o item avaliado, como funcionalidades projetadas, pessoas, processos e sistemas.

Um evento de risco pode ter múltiplas causas e consequências e pode afetar

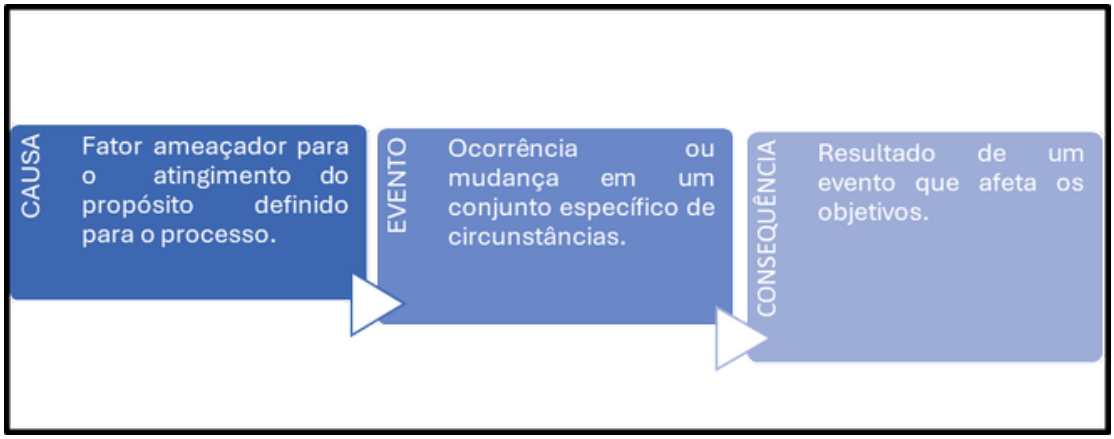
múltiplos objetivos. Apresentamos um exemplo hipotético de identificação dos riscos no contexto do Estado do Espírito Santo:

Quadro XII - Exemplo de Identificação dos Riscos

Área	Evento de Risco	Possíveis Causas	Possíveis Consequências	Objetivos Estratégicos Afetados	Categoria de Risco
Saúde	Indisponibilidade de medicamentos em hospitais estaduais	• Falhas no processo de aquisição • Atrasos na entrega por fornecedores	Comprometimento da assistência à população	• Promoção da saúde • Redução da mortalidade	Estratégico /Operacional
Educação	Evasão escolar no ensino médio	• Fatores socioeconômicos • Baixa atratividade da grade curricular • Dificuldade de acesso às escolas em regiões rurais	• Redução da taxa de conclusão escolar; • Impacto na qualificação da força de trabalho	• Desenvolvimento social e econômico	Estratégico
Infraestrutura	Deterioração precoce de rodovias estaduais	• Má qualidade dos materiais • Falhas na fiscalização contratual • Excesso de carga nos veículos	• Maior risco de acidentes; • Elevação dos custos de manutenção	• Segurança viária Integração logística • Escoamento da produção	Operacional/ Orçamentário e financeiro
Meio Ambiente	Rompimento de barragens de rejeitos	• Falhas estruturais • Ausência de monitoramento contínuo • Eventos climáticos extremos	• Danos ambientais severos • Impactos sociais e econômicos duradouros	• Sustentabilidade Proteção da biodiversidade	Ambiental
Segurança Pública	Aumento repentino da criminalidade em determinada região	• Crise econômica • Disputas entre facções • Ausência de policiamento ostensivo	• Prejuízo à sensação de segurança do cidadão	• Redução da violência • Garantia da ordem pública	Estratégico /Operacional

Uma forma simples de diferenciar os componentes causa, risco e consequência é raciocinar como demonstrado a seguir:

Trinômio Causa – Evento – Consequência



Ainda para ajudar a identificar riscos, é essencial considerar os fatores de risco: eventos ou condições com potencial de afetar negativamente os objetivos organizacionais. São exemplos de fatores de risco:

Quadro XIII - Exemplos de Fatores de Risco

Fator de Risco	O que significa	Exemplo
Fontes tangíveis e intangíveis	Coisas que podem ser medidas (máquinas, prédios) ou que são mais abstratas (reputação, clima, desastres).	Uma enchente que danifica escolas (tangível) e A imagem negativa do governo pela demora na resposta (intangível)
Causas e eventos	O que gera o risco e o que de fato pode acontecer.	Causa: chuva forte. Evento: enchente em Cariacica.
Ameaças e oportunidades	O risco pode ser ruim (ameaça) ou bom (oportunidade).	Ameaça: queda de pontes. Oportunidade: modernizar infraestrutura com verbas federais.

Vulnerabilidades e capacidades	Fraquezas e forças que influenciam o risco.	Vulnerabilidade: drenagem urbana precária. Capacidade: Defesa Civil bem treinada.
Mudanças nos contextos externo e interno	Transformações fora ou dentro do governo que afetam riscos.	Externo: mudança climática aumenta chuvas. Interno: corte de verbas de manutenção.
Indicadores de riscos emergentes	Sinais de alerta que apontam risco futuro.	Aumento do nível dos rios medido por sensores.
Natureza e valor dos ativos e recursos	Importância do que pode ser afetado.	Hospital estadual localizado em área de alagamento.
Consequências e impactos nos objetivos	O que acontece e como afeta metas do governo.	Interrupção de aulas (afeta objetivo de garantir educação contínua).
Limitações de conhecimento e informação	O que não se sabe ou é incerto.	Falta de dados atualizados sobre áreas de risco.
Fatores temporais	Quando o risco pode acontecer.	Enchentes mais prováveis no verão.
Vieses, hipóteses e crenças	Percepções ou crenças dos envolvidos.	População acredita que enchente “só acontece no centro”, ignorando áreas periféricas.

Convém que a organização identifique os riscos, independentemente de suas fontes estarem ou não sob seu controle.

Após a identificação de riscos, avança-se para a etapa de análise. De acordo com a NBR ISO 31010:2012, para a análise de riscos podem ser utilizados métodos qualitativos, semiquantitativos ou quantitativos. A escolha decorrerá principalmente da relação do grau de detalhe requerido, da disponibilidade de dados confiáveis e, principalmente, das necessidades de tomada de decisão da organização.

Quadro XIV - Tipos de análise de riscos

Tipo de Análise	Características Principais	Observações e Aplicações Práticas
Qualitativa	Define consequência, probabilidade e nível de risco com base em níveis de significância, como alto, médio e baixo. Pode combinar consequência e probabilidade, e avalia o nível de risco resultante em comparação com os critérios qualitativos.	Requer explicitação clara dos termos utilizados e registro da base conceitual dos critérios. Deve-se seguir o grau de detalhamento eventualmente exigido por norma ou legislação.
Semiquantitativa	Utiliza escalas numéricas para consequência e probabilidade. Os níveis de risco são calculados por fórmulas, que podem envolver escalas lineares, logarítmicas ou outras relações.	Pode ser útil quando se deseja maior rigor que a análise qualitativa, mas não há dados suficientes para uma abordagem totalmente quantitativa.
Quantitativa	Estima valores numéricos específicos para consequências e probabilidades. Produz níveis de risco expressos em unidades previamente definidas no contexto da análise.	Nem sempre é viável, especialmente em razão da falta de dados, da influência de fatores humanos ou da não justificativa do esforço analítico. Pode ser substituída por análises comparativas.

Adotaremos, neste guia, o método semiquantitativo como abordagem balanceada para priorizar riscos, por meio de matriz 4x4 (probabilidade × impacto) que confere objetividade numérica, reduz subjetividade e assegura consistência nas avaliações, conforme ISO 31000. A seguir, os elementos dessa análise:

9.2.1 Apuração do indicador Probabilidade

A probabilidade é a chance de ocorrência do risco no percurso para atingir os objetivos, podendo ser medida de forma qualitativa ou quantitativa.

A probabilidade é um elemento chave dentro do processo de avaliação de riscos. É componente importante para a definição e medição do nível de risco que a organização está suscetível.

O quadro a seguir demonstra os níveis de probabilidade, com suas descrições e a frequência de ocorrência como balizador para avaliação.

Quadro XV - Níveis de probabilidade

Probabilidade	Descrição da probabilidade	Peso
Raro	O evento ocorre raramente	1
Pouco Provável	A possibilidade de o evento ocorrer é baixa.	2
Provável	O evento já ocorreu algumas vezes e pode voltar a ocorrer	3
Muito Provável	O evento já ocorreu repetidas vezes e provavelmente voltará a ocorrer muitas vezes	4

9.2.2 Apuração do indicador Impacto

O impacto do risco mede o quanto ele pode afetar a organização, considerando a gravidade e a natureza desse efeito. Ele será classificado em quatro níveis: baixo, moderado, alto e muito alto.

O quadro, a seguir, demonstra os níveis de impacto, sua descrição e o impacto de sua ocorrência como balizador para avaliação.

Quadro XVI - Níveis de impacto

Impacto	Descrição do Impacto	Peso
Baixo	Consequências insignificantes caso o evento ocorra	1
Moderado	Consequências menores em processos e atividades secundários	2
Alto	Consequências relevantes em processos e atividades secundárias ou menores em processos e atividades prioritários	3
Muito Alto	Consequências relevantes em processos e atividades prioritários.	4

9.2.3 Cálculo do Nível de Risco

Após definir os indicadores de probabilidade e impacto, utiliza-se a Matriz de Risco para calcular o Nível de Risco Inerente (NRI).

A classificação do NRI é apurada a partir da aplicação da função de risco. A função risco é fundamentalmente um produto das variáveis probabilidade e impacto. A fórmula aplicada é:

Quadro XVII – Matriz de Risco

$$fNRE\ (Nível\ de\ Risco\ Inerente) = Probabilidade\ x\ Impacto$$

IMPACTO					
	MUITO ALTO (4)	4 RM	8 RA	12 RE	16 RE
	ALTO (3)	3 RB	6 RM	9 RA	12 RE
	MODERADO (2)	2 RB	4 RM	6 RM	8 RA
	BAIXO (1)	1 RB	2 RB	3 RB	4 RM
		RARO (1)	POUCO PROVÁVEL (2)	PROVÁVEL (3)	MUITO PROVÁVEL (4)
		PROBABILIDADE			

A Matriz de Risco gera 16 níveis possíveis de risco, variando de 1: impacto baixo e probabilidade rara, até 16: impacto muito alto e probabilidade muito provável.

Assim, cada célula da matriz indica o nível de risco resultante da combinação entre probabilidade e impacto.

Com a aplicação dos indicadores previstos para a Matriz de Risco os valores deverão oscilar dentre das seguintes faixas:

Quadro XX - Classificação do Nível de Risco

Nível de Risco	Risco Baixo (RB)	Risco Médio (RM)	Risco Alto (RA)	Risco Extremo (RE)
Pontuação	0 a 2,99	3,00 a 7,99	8,00 a 11,99	12,00 a 16

Quanto ao tipo de classificação de risco, o risco pode ser observado sob duas formas principais: risco inerente e risco residual ou real.

Risco Inerente

- É aquele presente em qualquer atividade ou processo, considerando a sua execução sem controles

Risco Residual (ou real)

- Corresponde ao risco que permanece mesmo após a implementação de controles existentes ou adicionais para o seu tratamento

Na prática, é improvável que nos dias atuais processos sejam conduzidos sem nenhum controle, especialmente no setor público, em qualquer esfera de governo. Assim, a avaliação de riscos deve contemplar tanto a identificação do risco inerente quanto a análise do risco residual, de modo a verificar até que ponto os controles aplicados reduzem o risco a um nível aceitável. Risco residual é aquele que permanece mesmo com a ação e resposta da administração.

Esse aprofundamento é essencial para o refinamento da gestão de riscos, permitindo definir qual é o nível de risco que a organização está disposta a assumir. O modelo internacional de gestão de riscos (GRC Capability Model – versão 3.5) orienta que a organização adote medidas e controles para transformar o risco inerente em um risco residual compatível com sua capacidade de gestão.

Nesse sentido para o refinamento do processo de gestão de riscos se faz necessário não apenas a avaliação do risco inerente, mas seu aprofundamento para um nível mais sensível de riscos a que a organização está disposta a assumir.

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

Segue abaixo o quadro exemplificativo da definição dos níveis e dos fatores de avaliação do efeito dos controles na mitigação de riscos, determinando o fator obtido a partir da análise do grau de efetividade da implementação/existência dos controles:

Quadro XVIII - Escala de avaliação dos controles

Nível	Descrição	Fator de Avaliação dos Controles (FAC)	Nível de Confiança (NC)
Inexistente	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais	1,0	0
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	20%
Mediano	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes devido a deficiências no desenho ou nas ferramentas utilizadas	0,7	30%
Satisfatório	Controles implementados e sustentados por ferramentas adequadas e embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente	0,5	50%
Forte	Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco	0,3	70%

A função para apurar o risco residual é o produto do nível de risco inerente sobre o fator de avaliação dos controles internos.

$$f(Nível\ de\ Risco\ Residual) = Nível\ Risco\ Inerente\ x\ Fator\ de\ Avaliação\ dos\ Controles$$

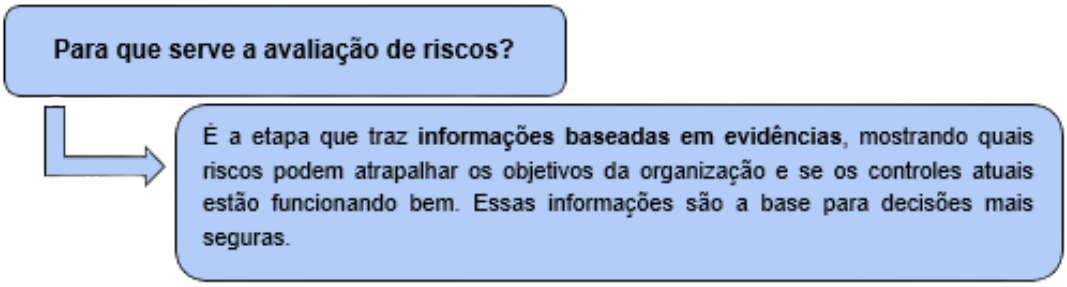
O risco residual será apurado mediante a multiplicação do valor do risco inerente apurado na fase de identificação de riscos e na fase inicial de análise pelo fator de avaliação do controle interno.

NRR = NRI x FAC; onde:
NRR = Nível de Risco Residual
NRI = Nível de Risco Inerente
FAC = Fator de Avaliação dos Controles

Quadro XXII - Exemplo de Cálculo do Risco Residual

Evento de Risco	Nível de Risco Inerente (NRI)	Nível dos Controles	Fator de Avaliação dos Controles	Cálculo	Risco Residual	Classificação
Falha na atualização do sistema de gestão orçamentária	12 (Risco Extremo)	Forte	0,3	12 × 0,3 = 3,6	3,6	Médio

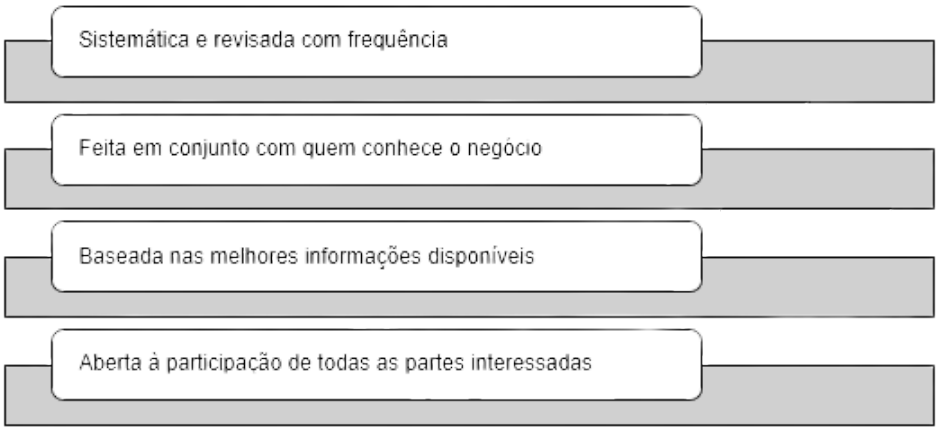
9.3 Avaliação dos Riscos



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.

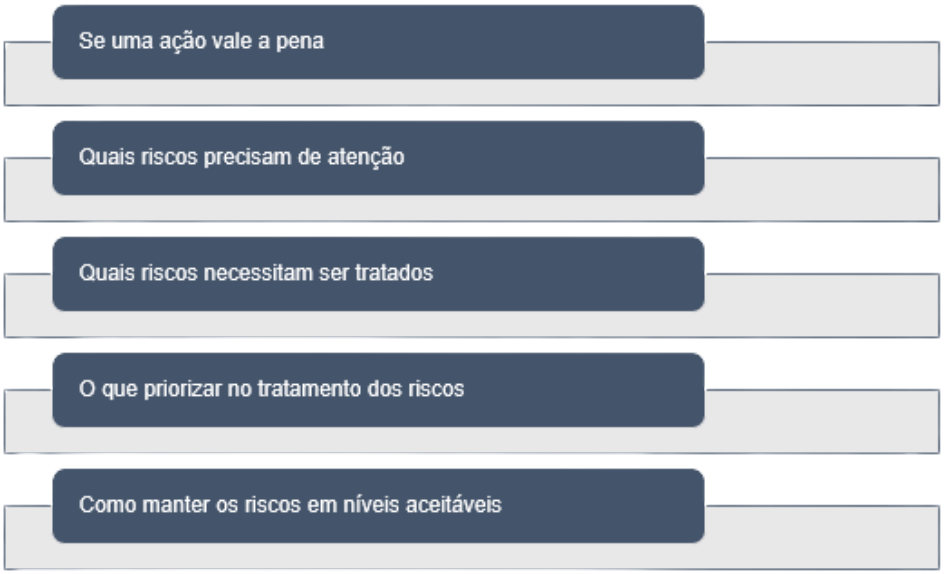
- **Como deve ser feita?**

Segundo a ISO 31000, a avaliação de riscos deve ser:



- **O que a avaliação ajuda a decidir?**

Com uma boa avaliação, a organização pode saber:



9.4 Tratamento dos riscos

Após as etapas de definição do contexto interno e externos da organização, a definição do apetite a risco, a identificação e análise dos riscos durante a execução e avaliação desses riscos quanto aos critérios de impacto e probabilidade, dá-se início à etapa de tratamento dos riscos.

O tratamento do risco envolve aplicar medidas de controle para modificar o risco identificado e aumentar as chances de alcançar os objetivos da organização. O foco principal é agir nos riscos que estejam acima do apetite a

riscos da organização, definindo respostas e elaborando planos de ação para trazer os riscos a níveis aceitáveis.

Cada risco deve estar vinculado a (pelo menos) uma ação de tratamento, escolhida com base no nível de risco, contexto e custo do controle. Durante a definição dos tratamentos, é importante avaliar se o custo das ações propostas não excede os benefícios gerados.

As ações de tratamento podem mitigar, compartilhar ou evitar riscos, e devem ser planejadas e executadas para modificar efetivamente o nível do risco:

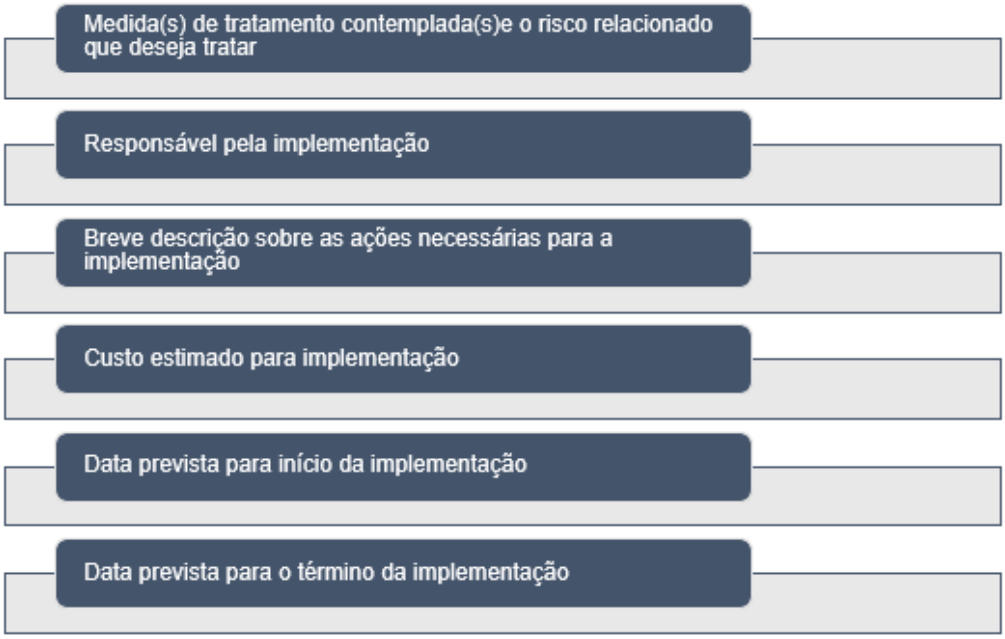
Quadro XIX - Tipos de tratamento

Tratamento	Descrição	Observações e Aplicações Práticas	Exemplos
Mitigar	Implementar ações para reduzir a probabilidade ou o impacto do risco	Um risco normalmente é mitigado quando é classificado como "Alto" ou "Médio". A implementação de controles, neste caso, deve apresentar um custo-benefício adequado. Mitigar o risco significa implementar controles que possam diminuir as causas ou as consequências dos riscos.	Realizar treinamentos periódicos sobre legislação aplicável, sistema utilizado e procedimentos internos
Compartilhar	Transferir total ou parcialmente a responsabilidade e os efeitos do risco para terceiros	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.	Exigir, em contrato, apólice de seguro para determinados eventos
Evitar	Alterar ou descontinuar atividades para eliminar completamente o risco	Um risco normalmente é evitado quando é classificado como "Extremo", 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.	Substituir atendimento presencial em área de risco por atendimento remoto
Aceitar	Reconhecer o risco mas não adotar tratamentos adicionais	Um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco. Nessa situação, nenhum novo controle precisa ser implementado para reduzir o risco.	Não propor tratamento adicional para o risco de pequenas inconsistências formais em documentos internos

O objetivo na etapa do tratamento de riscos converge para a atenção que deve ser dada aos riscos priorizados como o resultado do processo de gestão de riscos. O propósito é definir respostas aos riscos apurados, com a elaboração de planos de ação para modificar o nível dos riscos, trazendo-os para patamares aceitáveis pela gestão. É importante nessa fase relacionar os benefícios da ação com o custo da implementação de controles.

Os tratamentos propostos para os riscos subsidiarão a elaboração do Plano de Tratamento de Riscos. Esse plano é essencial para assegurar que os níveis de risco permaneçam compatíveis com a Declaração de Apetite a Riscos do órgão ou entidade, por meio da definição de respostas específicas e de planos de ação para cada risco identificado. Sua relevância decorre da possibilidade de mitigar exposições por meio de estratégias como evitar, aceitar, transferir ou reduzir o risco, sempre considerando o nível de risco, o contexto organizacional e o custo dos controles.

O Plano de Tratamento de Riscos deverá conter, no mínimo, as seguintes informações:



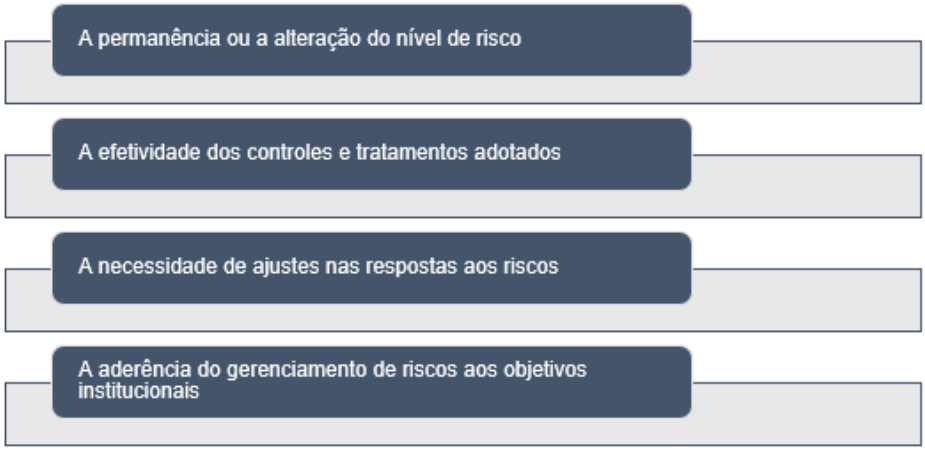
A validação dos resultados do processo de gerenciamento de riscos e o Plano de Tratamento de Riscos proposto devem ser aprovados pela Alta Administração do órgão/entidade.

9.5 Monitoramento e Análise Crítica

O monitoramento tem por objeto acompanhar os riscos e avaliar o desempenho e a evolução da maturidade do Sistema de Gestão de Riscos e

Controle Interno do órgão ou entidade.

Seu foco consiste em verificar:



Além disso, o monitoramento deverá observar os seguintes princípios:

Quadro XXIV – Princípios do monitoramento

Princípio	Conceito	Desafio prático
Contínuo	Realizado de forma permanente, e não apenas em momentos pontuais	É preciso que seja definida previamente uma periodicidade para a realização do monitoramento, adequada à natureza do risco enfrentado
Proporcional	Compatível com a relevância e o nível dos riscos	Quanto maior os riscos envolvidos, maiores serão os esforços para o seu monitoramento
Integrado	Articulado com planejamento, execução orçamentária, gestão de processos e controles internos	Planejamento e execução orçamentária: Cada risco monitorado deve estar associado a um objetivo estratégico, tático ou operacional ou a um programa, ação ou projeto institucional Gestão de processos: O monitoramento deve ocorrer nos pontos críticos do fluxo do processo, nas atividades mais sensíveis a falha Controles internos: cada risco deve ter controles preventivos e/ou detectivos associados, responsáveis definidos e evidências de execução.
Documentado	Devidamente registrado, assegurando rastreabilidade e transparência	O registro histórico das informações
Baseado em evidências	Sustentado por informações, indicadores e dados confiáveis	Para que os dados sejam considerados confiáveis, devem atender aos critérios de exatidão, completude, tempestividade, consistência e rastreabilidade

São etapas do monitoramento de riscos:

Definição do Plano de Monitoramento

- **O monitoramento deve ser previamento planejado, definindo-se:**
- Riscos a serem monitorados
- Periodicidade das análises
- Responsáveis pelas informações
- Indicadores e critérios de acompanhamento
- Forma de reporte ao Comitê de Gestão de Riscos

Acompanhamento dos Riscos Identificados

- **O acompanhamento deve verificar, entre outros aspectos**
- Se houve alteração na probabilidade ou impacto dos riscos
- Se surgiram novos riscos ou se riscos deixaram de exisitir
- Se os pressupososotos utilizados na avaliação permanecem válidos

Avaliação da Efetividade dos Controles e Tratamento

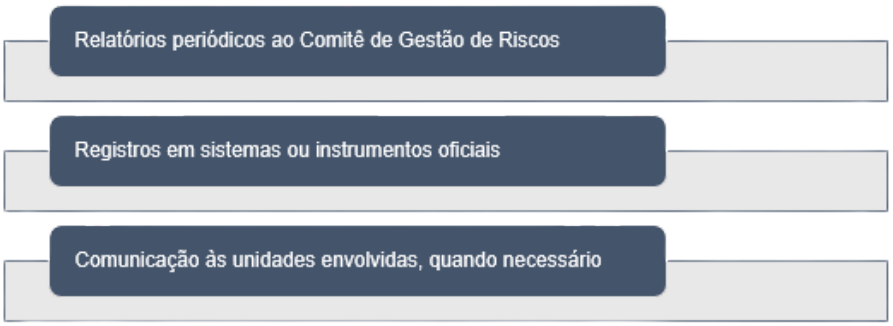
- **Deve-se analisar se:**
- Os controles estão sendo executados conforme previsto
- Os tratamentos de risco reduziram o nível de risco esperado
- Existem falhas, desvios ou fragilidades nos controles
- Os custos dos tratamentos são compatíveis com os benefícios esperados

9.7 Comunicação e Consulta

A etapa de comunicação e consulta deve fornecer e compartilhar informações sobre a gestão de riscos e controles internos com as partes interessadas, respeitada a classificação de sigilo das informações.

Esse intercâmbio deve ocorrer em todas as fases do processo, entre as instâncias de gestão de riscos, viabilizando a melhoria contínua e a evolução da maturidade organizacional.

Os resultados do monitoramento serão comunicados de forma clara e tempestiva, por meio de:



A título de exemplo, na estrutura de gestão de riscos da Secont, o fluxo de informações ocorre da seguinte forma:

Gestores de Processos	UECI	Comitê de Gestão de Riscos
•Comunicam informações primárias sobre execução dos controles e tratamentos; •Reportam falhas, desvios e dificuldades.	•Consolidam, analisam criticamente e estruturam a informação; •Traduzem dados operacionais em informações gerenciais; •Elaboram relatórios e notas técnicas.	•Recebem a comunicação estruturada; •Analisam, deliberam e definem encaminhamentos; •Determinam ajustes, reforços ou mudança de estratégia.

O que exatamente deve ser comunicado

A comunicação dos riscos deve responder, de forma objetiva, às seguintes questões:

Execução dos controles
Os controles estão sendo executados conforme previsto?

- **Devem ser comunicadas informações como:**
- Controles implementados x planejados
- Frequência de execução
- Responsáveis
- Evidências de funcionamento

Efetividade dos tratamentos
Os tratamentos de riscos reduziram o nível de risco esperado?

- **Aqui, a comunicação deve demonstrar:**
- Nível de risco antes e depois do tratamento;
- Se houve redução de probabilidade e/ou impacto
- Riscos residuais acima do apetite ao risco

Falhas, desvios ou fragilidades
Existem falhas, desvios ou fragilidades nos controles?

- Devem ser comunicados:
- Falhas operacionais
- Controles ineficazes
- Riscos de não conformidade
- Eventos ou quase eventos ocorridos

Relação custo-benefício
Os custos dos tratamentos são compatíveis com os benefícios esperados?

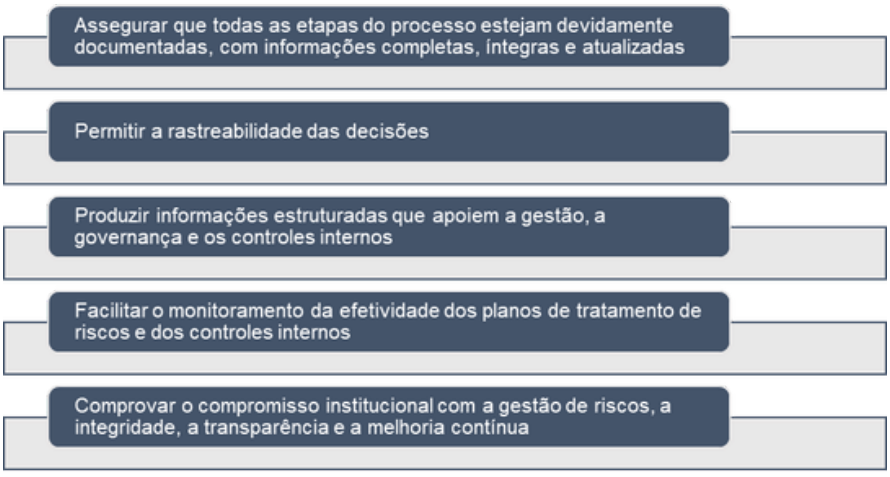
- A comunicação deve permitir ao Comitê avaliar:
- Custo financeiro, operacional ou administrativo dos tratamentos
- Benefícios efetivos na redução do risco
- Alternativas mais eficientes

9.8 Registro e Relato

O registro e o relato constituem a base documental da gestão de riscos, garantindo a rastreabilidade das decisões, a transparência dos procedimentos adotados e a disponibilidade de informações confiáveis para subsidiar a tomada de decisão em todos os níveis da organização.

Mais do que um mero cumprimento formal, o adequado registro e relato dos riscos permite consolidar evidências, demonstrar a coerência entre os riscos identificados, os controles implementados e os resultados obtidos, além de facilitar o acompanhamento por instâncias de governança, órgãos de controle e demais partes interessadas.

São objetivos desta etapa:



O registro da gestão de riscos deve observar, no mínimo, os seguintes princípios:

Quadro XXV – Princípios do registro

Princípio	Conceito
Sistematicidade	Os registros devem ser realizados de forma padronizada, contínua e tempestiva, utilizando formatos e campos definidos na metodologia institucional (planilhas, formulários eletrônicos, sistemas informatizados etc.).
Integralidade	As informações registradas devem contemplar, de forma clara e objetiva, o contexto, o evento de risco, suas causas e consequências, os critérios de probabilidade e impacto adotados, o nível de risco inerente e residual, os controles existentes e os planos de tratamento.
Rastreabilidade	Cada informação registrada deve possibilitar a identificação de sua origem (responsáveis, datas, versão do documento ou da matriz de riscos, deliberações do CGR), de modo a permitir reconstruir o histórico de decisões.
Atualização	Os registros devem ser revisados sempre que houver alteração relevante no contexto, nos riscos, nos controles ou nos resultados dos planos de tratamento, evitando descompasso entre a realidade e os documentos de gestão.
Segurança e confidencialidade	Os registros devem observar as normas de segurança da informação, classificação de documentos e proteção de dados pessoais, garantindo acesso adequado às diferentes partes interessadas.

O relato da gestão de riscos, por sua vez, consiste na apresentação estruturada das informações registradas, em linguagem acessível e orientada às necessidades de cada nível decisório.

Deve, preferencialmente, seguir as diretrizes a seguir:

Quadro XXVI – Diretrizes do relato

Diretriz	Conceito
Adequação ao público-alvo	Relatórios destinados à Alta Administração e ao CGR devem enfatizar riscos estratégicos, tendências, prioridades e decisões necessárias, enquanto relatórios operacionais podem detalhar planos de ação, cronogramas e responsáveis.
Foco em riscos relevantes	Os relatos devem destacar riscos acima do apetite definido, riscos críticos para a continuidade dos serviços, riscos de integridade, bem como a situação dos planos de tratamento e eventuais atrasos ou obstáculos à sua implementação.
Linguagem clara e objetiva	Recomenda-se evitar excessos de jargões técnicos, apresentando os riscos de forma compreensível, com síntese executiva e, quando pertinente, uso de gráficos, painéis e indicadores e periodicidade definida.

Para potencializar a utilidade dos registros e relatos, recomenda-se adotar, sempre que possível, as seguintes boas práticas:

a) Utilização de modelos padronizados (templates) para análise e mapeamento de riscos, planos de tratamento de riscos e relatórios, facilitando a comparação entre unidades e a consolidação das informações.
b) Integração dos registros de riscos com outros sistemas corporativos (planejamento estratégico, gestão de contratos, orçamento, integridade, ouvidoria), evitando retrabalho e fragmentação de dados.
c) Manutenção de histórico de versões das matrizes de riscos e dos relatórios, permitindo acompanhar a evolução dos riscos, dos controles e da maturidade da gestão.

d) Registro explícito das lições aprendidas, recomendações de auditoria, determinações de órgãos de controle e decisões da Alta Administração, indicando como foram incorporadas aos processos e controles.
e) Divulgação interna, em linguagem acessível, de sínteses executivas dos principais riscos e resultados da gestão, contribuindo para o engajamento das equipes e para a consolidação da cultura de gestão de riscos.

10. APRIMORAMENTO CONTÍNUO

O aprimoramento representa o compromisso permanente da organização com a melhoria contínua da gestão de riscos, dos controles internos e da governança, a partir das evidências produzidas pelas etapas de monitoramento, comunicação, registro e relato.

Trata-se de reconhecer que a gestão de riscos não é um projeto pontual, mas um processo cíclico, dinâmico e evolutivo, que deve ser ajustado à medida que o contexto muda, que novos riscos emergem e que a maturidade institucional se desenvolve.

Seus objetivos principais incluem:

a) Incorporar lições aprendidas de eventos de risco, falhas, quase falhas, sucessos e boas práticas, de modo a evitar reincidências e potencializar resultados positivos.
b) Ajustar metodologias, critérios, ferramentas, indicadores e rotinas de trabalho, alinhando-os às necessidades reais da organização e às melhores práticas nacionais e internacionais.
c) Fortalecer a cultura organizacional orientada à prevenção, à integridade, à transparência e à geração de valor público.
Integrar recomendações de órgãos de controle externo, auditoria interna, avaliações de governança e resultados de autoavaliações de riscos e controles.
d) Integrar recomendações de órgãos de controle externo, auditoria interna, avaliações de governança e resultados de autoavaliações de riscos e controles.

O aprimoramento deve ser entendido como um ciclo contínuo, em que as informações provenientes do monitoramento, da comunicação, do registro e do relato retroalimentam o processo de gestão de riscos.

11. CONSIDERAÇÕES FINAIS

A gestão de riscos integrada a processos é um instrumento estratégico para fortalecer a governança, elevar a eficiência administrativa e proteger o valor público.

A adoção consistente da metodologia aqui apresentada – desde o estabelecimento do contexto, passando pela identificação, análise, avaliação, tratamento, monitoramento, comunicação, registro e relato dos riscos – depende do comprometimento da Alta Administração, do engajamento das equipes e da atuação coordenada das três linhas do controle interno.

Ao incorporar a gestão de riscos como prática permanente, o Poder Executivo Estadual consolida uma postura proativa, capaz de antecipar cenários adversos, responder com agilidade a mudanças e aproveitar oportunidades de inovação e melhoria na prestação de serviços à sociedade.

Este Guia não se encerra em si mesmo: ele deve ser utilizado como referência viva, sujeita a revisões, atualizações e aperfeiçoamentos periódicos, à medida que a experiência acumulada, as lições aprendidas e a evolução das boas práticas de governança e gestão de riscos apontarem novos caminhos.

Espera-se, assim, que a gestão de riscos integrada a processos se consolide como parte indissociável da cultura organizacional, contribuindo para decisões mais responsáveis, transparentes e efetivas, e para a construção de um Estado cada vez mais íntegro, resiliente e orientado à geração de valor público sustentável.

GOVERNO DO ESTADO
DO ESPÍRITO SANTO

Secretaria de Controle
e Transparência