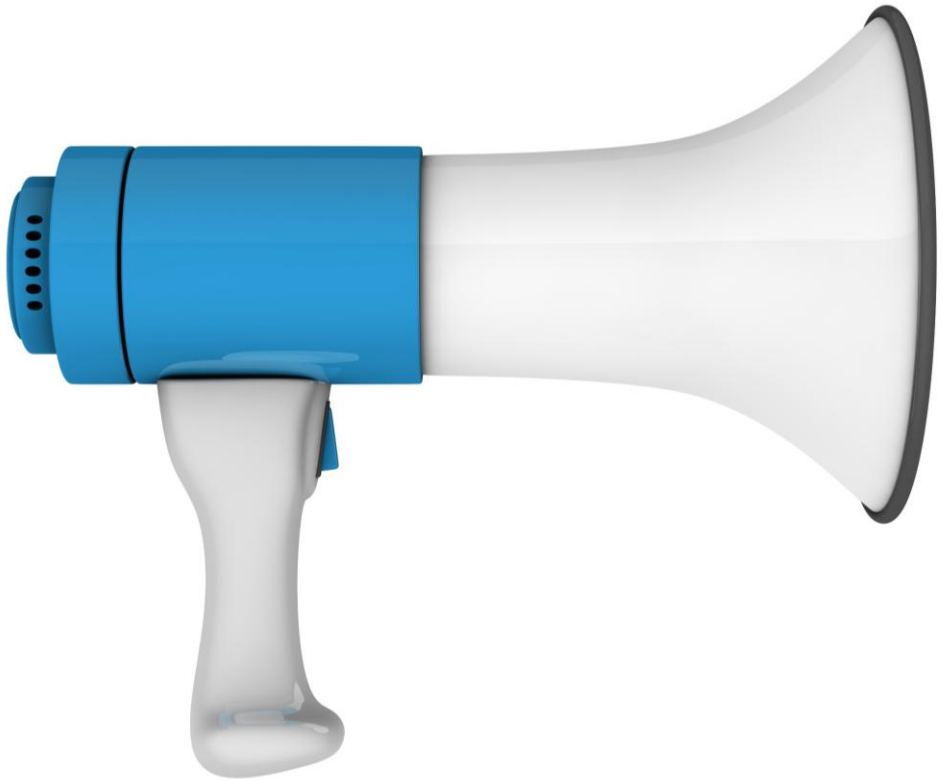
Secretaria de Estado de Controle e Transparência
Subsecretaria de Integridade Governamental e Empresarial

Gestão de riscos à integridade

Por: Guilherme A. Machado Jr.



Este treinamento e o material a ele relacionado não substitui Normas Regulamentadoras, Decretos, Resoluções, Procedimentos, Políticas, Instruções ou Leis específicas relativas ao gerenciamento de riscos em vigor ou em processo de introdução.

Disclaimer

Agenda

- Conceitos
  - Risco
  - Categorias de Risco
  - Controles Internos
  - Gestão de Riscos
  - Estruturas para Gestão de Riscos
  - O Modelo de Três Linhas
- ABNT/ISO 31000
- O Processo de Gestão de Riscos da ISO 31000
- Gestão de riscos à integridade
- Estudo de Caso

Agenda

Conceitos

- Risco
  - Categorias de Risco
  - Controles Internos
  - Gestão de Riscos
  - Estruturas para Gestão de Riscos
  - O Modelo de Três Linhas

ABNT/ISO 31000

O Processo de Gestão de Riscos da ISO 31000

Gestão de riscos à integridade

Estudo de Caso

Perigo, risco e problema

Afinal, o que é risco?

O risco é simplesmente a possibilidade de algo dar errado (ou até certo!) durante uma jornada, e saber disso nos ajuda estar preparado para aproveitar o melhor e evitar imprevistos.

> Risco é o efeito da incerteza sobre os objetivos de uma organização.

ISO 31000

- Um efeito é um desvio em relação ao esperado. Pode ser positivo, negativo ou ambos, e pode abordar, criar ou resultar em oportunidades e ameaças.
- Objetivos podem possuir diferentes aspectos e categorias, e podem ser aplicados em diferentes níveis.
- Risco é normalmente expresso em termos de fontes de risco, eventos potenciais, suas consequências e suas probabilidades.

Agenda

Conceitos

- Risco
- Categorias de Risco
- Controles Internos
- Gestão de Riscos
- Estruturas para Gestão de Riscos
- O Modelo de Três Linhas

ABNT/ISO 31000

O Processo de Gestão de Riscos da ISO 31000

Gestão de riscos à integridade

Estudo de Caso

Categorização dos riscos

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Estratégicos	Operacionais	Financeiros	Cibernéticos
Associados à direção e aos objetivos da organização e que, com frequência, passam pelas decisões de alto nível	Inerentes às operações do dia a dia e podem resultar em perdas financeiras, danos à reputação e interrupções nas atividades empresariais	Aqueles que podem comprometer a saúde econômica e financeira de uma organização.	Ameaças que exploram vulnerabilidades em sistemas e redes digitais.

Conformidade	Integridade	Reputacionais
Referem-se ao não cumprimento de leis, de regulamentação, de normas internas ou de padrões éticos aplicáveis às suas atividades.	Envolvem situações que podem comprometer a credibilidade e a imagem de uma empresa perante seus stakeholders	Ameaças à imagem e à reputação da organização

Exemplos de riscos por categorias

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Qual é a estratégia da Airbnb para mudar o mercado de hotelaria e hospedagem

Reforma Tributária: estados e municípios vão perder?

Unificação deve acabar com 'guerra fiscal'. Governadores e prefeitos temem perder arrecadação

Estratégico

Seis anos após o crime da Vale em Brumadinho (MG), ninguém foi punido; entenda os processos

Com muitos atrasos, o processo voltou a correr e as famílias esperam que os depoimentos aconteçam ainda em 2025

24-JAN-2025 ÀS 15H08 · BELO HORIZONTE (MG) · FLORA VILLELA

Operacional / Reputacional

Como essa empresa brasileira perdeu R$ 2,1 bilhões tentando se proteger do dólar

Em 2008, a Aracruz Celulose sofreu um colapso bilionário com derivativos. Entenda onde a empresa errou, o que são esses instrumentos financeiros e como usá-los com segurança

Financeiro

Fraude no INSS: 30% dos aposentados aptos não aderiram a acordo; veja como pedir reembolso

Integridade/Reputacional

Portais do STJ e do CNJ são alvo de tentativas de ataque hacker

Páginas, no entanto, funcionam normalmente. Equipes da área de tecnologia da informação dos respectivos órgãos tentam evitar comprometimento no funcionamento das plataformas.

Por Márcio Falcão, g1 e TV Globo
05/03/2025 14h23 · Atualizado há 6 meses

STJ SUPERIOR TRIBUNAL DE JUSTIÇA

oops!
Você excedeu a taxa limite de tentativas de acesso ao site.

SEGURANÇA CIBERNÉTICA

"Roubo do século"? Entenda o ataque hacker que pode ter desviado até R$ 1 bilhão do Banco Central

Estimativas apontam que, no mínimo, R$ 400 milhões foram movimentados ilegalmente em dois dias. Ataque afetou apenas contas entre bancos; dinheiro de pessoas físicas não foi mexido

Jornal: Embraer pagou US$ 10 mi para encerrar disputa com a Microsoft

A Microsoft acusava a fabricante brasileira de aviões de uso de softwares sem licença

Conformidade

Cibernético/Operacional

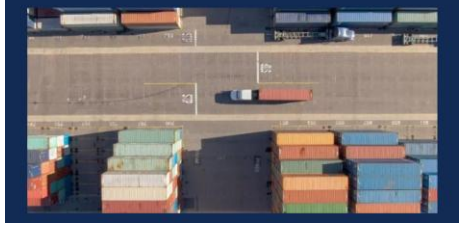
Barômetro de Risco da Allianz

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Os 10 principais riscos empresariais globais para 2025

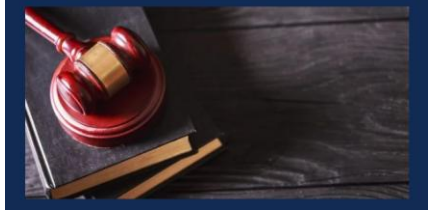
Classificação 1: Incidentes cibernéticos

Classificação 2: Interrupção de negócios



Rank 3: Catástrofes naturais

Classificação 4: Mudanças na legislação e regulamentação



Classificação 5: Mudanças climáticas

Rank 6: Fogo, explosão

Classificação 7: Desenvolvimentos macroeconômicos

Rank 8:
Desenvolvimentos de mercado

Classificação 9: Riscos políticos e violência

Classificação 10: Novas tecnologias

Fonte: https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

Agenda

Conceitos

- Risco
- Categorias de Risco
- Controles Internos
- Gestão de Riscos
- Estruturas para Gestão de Riscos
- O Modelo de Três Linhas

ABNT/ISO 31000

O Processo de Gestão de Riscos da ISO 31000

Gestão de riscos à integridade

Estudo de Caso

Controles internos

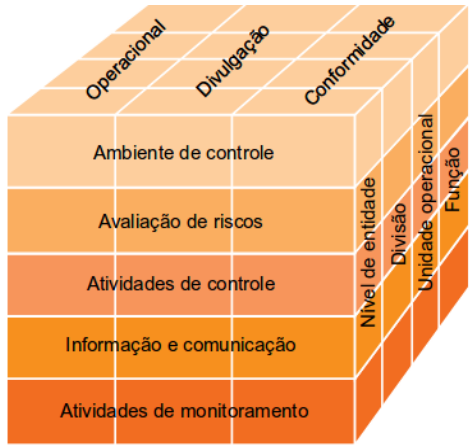
GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

São as políticas e procedimentos adotados pela administração de uma entidade para ajudá-la a atingir o objetivo de assegurar, tanto quanto for praticável, um modo ordenado e eficiente de conduzir seus negócios, incluindo o cumprimento de políticas administrativas, a salvaguarda de ativos, a prevenção e detecção de fraude e erro, a precisão e integridade dos registros contábeis, e a preparação oportuna de informações financeiras confiáveis.

Preventivos: evitam a ocorrência dos fatores de riscos.

Detectivos: identificam desvios ou falhas após ocorrerem.

Corretivos: corrigem as falhas e ajustam os processos.



Componente	Considerar
Ambiente de Controle	• Integridade, ética e comportamento dos executivos principais • Conscientização de controle e estilo de funcionamento • Compromisso com a competência • Governança e supervisão da Diretoria/Comitê de Auditoria • Estrutura, autoridade e responsabilidade organizacional • Políticas e procedimentos de RH
Avaliação de Risco	• Processo de avaliação de risco • Mecanismos para a antecipação, identificação e reação a eventos significativos
Informação & Comunicação	• Produção de relatórios adequados de desempenho • Relacionamento com a estratégia do negócio • Compromisso de RH e finanças com o desenvolvimento, teste e monitoramento de sistemas e programas de TI • Canais estabelecidos de comunicação para que os funcionários desempenhem suas responsabilidades
Atividades de Controle	• Existência de políticas e procedimentos necessários • Objetivos claros com monitoramento ativo • Segregação lógica de funções • Comparações periódicas entre valor contábil e valor real • Salvaguarda adequada de documentos, registros e ativos • Controles de acesso em funcionamento
Monitoramento	• Avaliações periódicas de controles internos • Implementação de recomendações para melhoria • Função de auditoria interna estabelecida para monitorar atividades

O ***Committee of Sponsoring Organizations of the Treadway Commission*** (COSO) publicou a obra *Internal Control – Integrated Framework* para ajudar empresas e outras organizações a avaliar e aperfeiçoar seus sistemas de controle interno, com a missão de prover liderança de pensamento através do desenvolvimento de um modelo de referência gerais e orientações sobre gestão dos riscos empresariais, controle interno e intimidação da fraude para melhorar o desempenho organizacional e de governança e reduzir a dimensão da fraude nas organizações

Dimensões dos controles internos

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Controles	Preventivos	Detectivos	Corretivos
Nível Entidade: formam a base e o tom do ambiente de controle. Eles garantem que a cultura, a estrutura e a estratégia da organização estejam alinhadas com os princípios de controle e ética. Pense neles como o "telhado" e a "estrutura" da casa de controles internos.	Código de conduta e treinamento sistemático / Políticas institucionais / Recrutamento, seleção e sucessão / Estrutura e hierarquia / Comissão de Ética	Auditoria interna / Auditoria externa / Canal de Denúncias / Ouvidoria / Transparência	Medidas disciplinares / PAD / PAR / Comissão de Ética
Nível de Processo: são os controles detalhados aplicados às atividades do dia a dia. Eles são os "muros" e "portas" dentro da casa, projetados para gerenciar riscos específicos de transações e operações.	Alçadas de aprovação / Segregação de Funções / Controles de acesso / Rotação de pessoal / Listas de verificações	Testes de conformidade / Monitoramento de controles / Revisões e reconciliações / Relatórios de exceção / Monitoramento por indicadores	Revisão e reprocessamento / Ajustes de processos e procedimentos / Treinamento e reciclagem / Ajustes em sistemas

Agenda

Conceitos

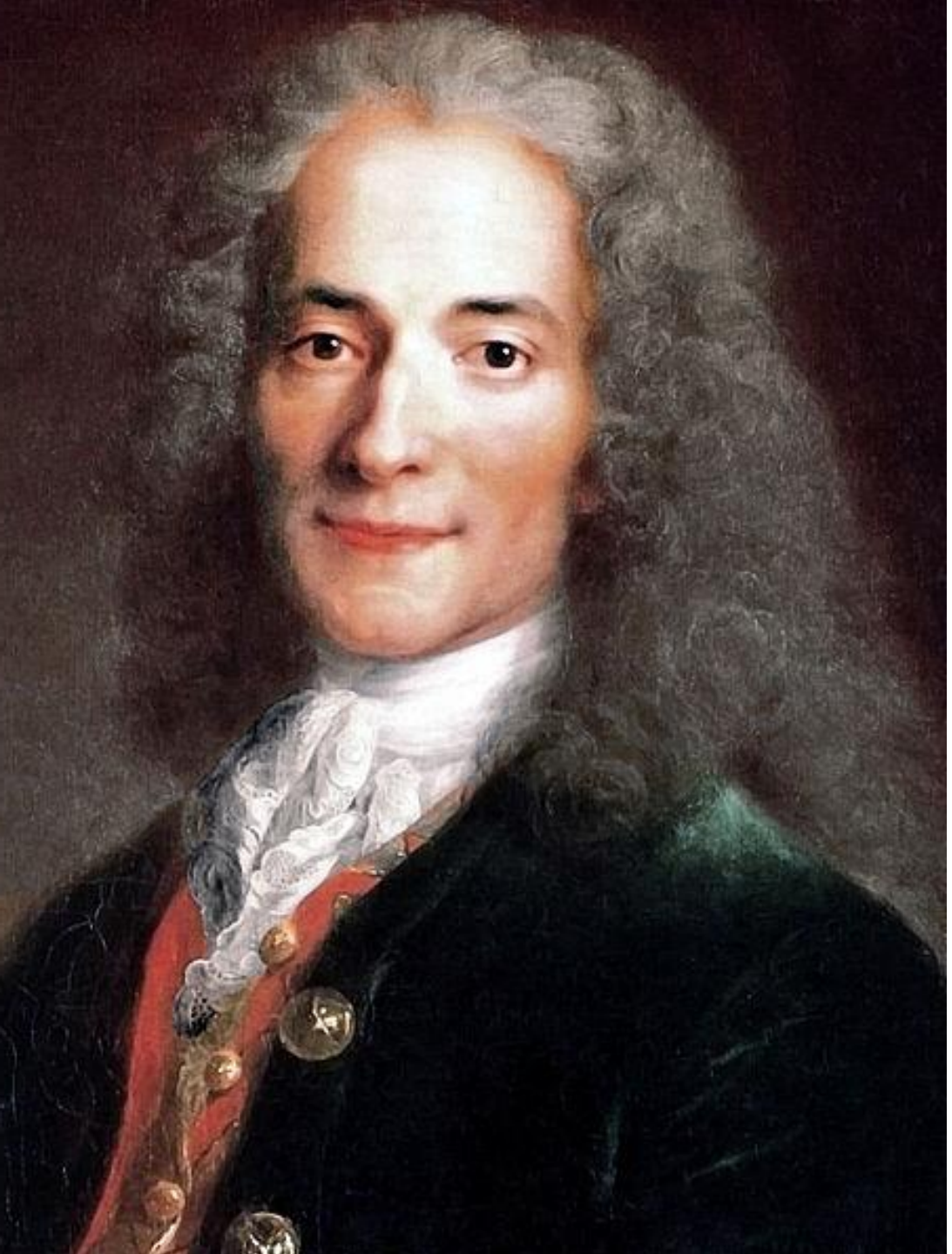
- Risco
- Categorias de Risco
- Controles Internos
- Gestão de Riscos
- Estruturas para Gestão de Riscos
- O Modelo de Três Linhas

ABNT/ISO 31000

O Processo de Gestão de Riscos da ISO 31000

Gestão de riscos à integridade

Estudo de Caso



Por que gerir riscos?

"Aquilo a que chamamos acaso não é – não pode deixar de ser – senão a causa ignorada de um efeito conhecido."

(Voltaire, 1694-1778)

Conceituando a Gestão de riscos

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

A gestão de riscos é uma disciplina essencial para organizações – sejam elas públicas ou privadas – que buscam alcançar seus objetivos de forma eficaz e eficiente. Ela envolve a identificação, avaliação e mitigação de eventos que possam impactar os objetivos de uma organização. A gestão de riscos é um processo que lida com **as incertezas que afetam a criação, destruição ou preservação de valor nas organizações** (Vieira; Barreto, 2019).

A doutrina moderna de risco preconiza que a Gestão de Riscos é a **capacidade de uma organização de tomar decisões proativas sob incerteza**, ponderando a probabilidade de eventos e seus impactos (sejam eles adversos ou favoráveis) para proteger seus ativos e impulsionar seus resultados. Em um cenário de rápidas mudanças, essa prática é crucial para **evitar surpresas negativas e aproveitar as oportunidades**, permitindo que a organização prospere de forma consistente.

Gestão de riscos na prática

Agenda

Conceitos

- Risco
- Categorias de Risco
- Controles Internos
- Gestão de Riscos
- Estruturas para Gestão de Riscos
- O Modelo de Três Linhas

ABNT/ISO 31000

O Processo de Gestão de Riscos da ISO 31000

Gestão de riscos à integridade

Estudo de Caso

Estruturas para Gestão de Riscos

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Conceito/Framework	Descrição Resumida	Entidade/Autor de Referência	Principais Características	Aplicação Prática
ISO 31000	Princípios e diretrizes para estabelecer, implementar e melhorar a gestão de riscos.	ISO (International Organization for Standardization)	Princípios; Estrutura (Framework); Processo	Aplicável a qualquer organização; base para políticas, apetite e integração com decisões.
COSO ERM (2017+)	Integra riscos à estratégia e performance, com foco em valor e cultura.	COSO	Componentes e Princípios; Apetite a Risco; Integração à Estratégia	Mapeamento de objetivos, avaliação de riscos e controles conectados ao desempenho.
NIST SP 800-37 (RMF)	Risk Management Framework para sistemas de TI com ciclo Prepare–Categorize–Authorize–Monitor.	NIST	Controles (NIST 800-53); Autorização; Monitoramento Contínuo	Órgãos públicos e setores críticos; avaliação técnica, compliance e segurança cibernética.
TCU — Gestão de Riscos	Diretrizes e boas práticas para riscos no setor público, integrando governança e controles.	Tribunal de Contas da União (TCU)	Governança; Transparência; Accountability	Aplicação em políticas, planos de integridade e auditorias com foco em riscos.
CGU — Gestão de Riscos/Integridade	Orientações para gestão de riscos e programas de integridade na administração pública.	Controladoria-Geral da União (CGU)	Mapeamento de Riscos; Integridade; Controles Preventivos	Planos de integridade, compras públicas e gestão de terceiros com matriz de risco.
Kaplan & Mikes (tipos de risco)	Classificação em riscos preventáveis, estratégicos e externos para respostas diferenciadas.	Robert S. Kaplan; Anette Mikes	Tipologias; Apetite Diferenciado; Respostas Adaptadas	Separar riscos operacionais de estratégicos e externos para priorização e governança.

Agenda

Conceitos

- Risco
- Categorias de Risco
- Controles Internos
- Gestão de Riscos
- Estruturas para Gestão de Riscos
- O Modelo de Três Linhas

ABNT/ISO 31000

O Processo de Gestão de Riscos da ISO 31000

Gestão de riscos à integridade

Estudo de Caso

O Modelo de Três Linhas

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Funções que gerenciam e são proprietárias dos riscos

Funções que supervisionam os riscos/Facilitadores

Funções que fornecem avaliações independentes

A abordagem das Três Linhas de Defesa, embora não seja um modelo de gestão de riscos, é uma forma simples e eficaz para melhorar a comunicação e a conscientização sobre os papéis e as responsabilidades essenciais de gestão de riscos e controles, aplicável a qualquer organização

1ª) Funções que gerenciam e são proprietárias dos riscos: nível se identificam, avaliam e mitigam riscos por meio do desenvolvimento e da implementação de políticas e procedimentos internos

2ª) Funções que supervisionam os riscos/Facilitadores constituída por funções – unidades, comitês ou outras estruturas organizacionais – estabelecidas para garantir que a primeira linha funcione como pretendido no que diz respeito à gestão de riscos e controles.

3ª) Funções que fornecem avaliações independentes: eficiência e eficácia das operações; salvaguarda de ativos; confiabilidade e integridade dos processos de reporte; conformidade com leis e regulamentos e o processo de gestão de riscos

Agenda

- Conceitos
  - Risco
  - Categorias de Risco
  - Controles Internos
  - Gestão de Riscos
  - Estruturas para Gestão de Riscos
  - O Modelo de Três Linhas
- ABNT/ISO 31000
- O Processo de Gestão de Riscos da ISO 31000
- Gestão de riscos à integridade
- Estudo de Caso

ABNT/ISO 31000

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Norma de referência adotada para a metodologia de gestão de riscos da administração pública estadual

Justificativa

A aplicabilidade da ISO 31000 é universal, estendendo-se a organizações de qualquer tipo, tamanho, atividade ou setor. Ao fornecer uma estrutura flexível e não prescritiva, a norma permite que empresas e instituições de diversos segmentos integrem a gestão de riscos em suas decisões estratégicas e operacionais, aprimorando a tomada de decisões, protegendo ativos e otimizando o desempenho em um cenário de incertezas.

Pontos chave

Natureza da Norma: A ISO 31000 é uma norma de diretrizes, não uma norma de requisitos.

Objetivo: Seu propósito é fornecer uma abordagem comum e coerente para gerenciar qualquer tipo de risco.

Conformidade, não Certificação: Embora não seja certificável, uma organização pode declarar que seu sistema de gestão de riscos está em conformidade com os princípios e diretrizes da ISO 31000.

Benefícios da Implementação:

- Melhora na tomada de decisões.
- Aumento da resiliência organizacional.
- Otimização do desempenho.
- Melhor aproveitamento de oportunidades e redução de perdas.
- Maior confiança das partes interessadas

ISO 31000: Princípios, estrutura e processo

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Criar e proteger valor

Princípios

1. Integrado: Parte integrante de todas as atividades organizacionais
2. Estruturado e abrangente: contribui para resultados consistentes e comparáveis
3. Customizado: Proporcional ao contexto e objetivos da organização
4. Inclusivo: Envolve as partes interessadas de maneira apropriada e oportuna
5. Dinâmico: Antecipa, detecta e responde às mudanças
6. Melhor Informação Disponível - Baseado em informações históricas, atuais e futuras
7. Fatores Humanos e Culturais - Considera comportamento humano e cultura
8. Melhoria Contínua - Aprimorado através do aprendizado e experiência

Processo

Estrutura

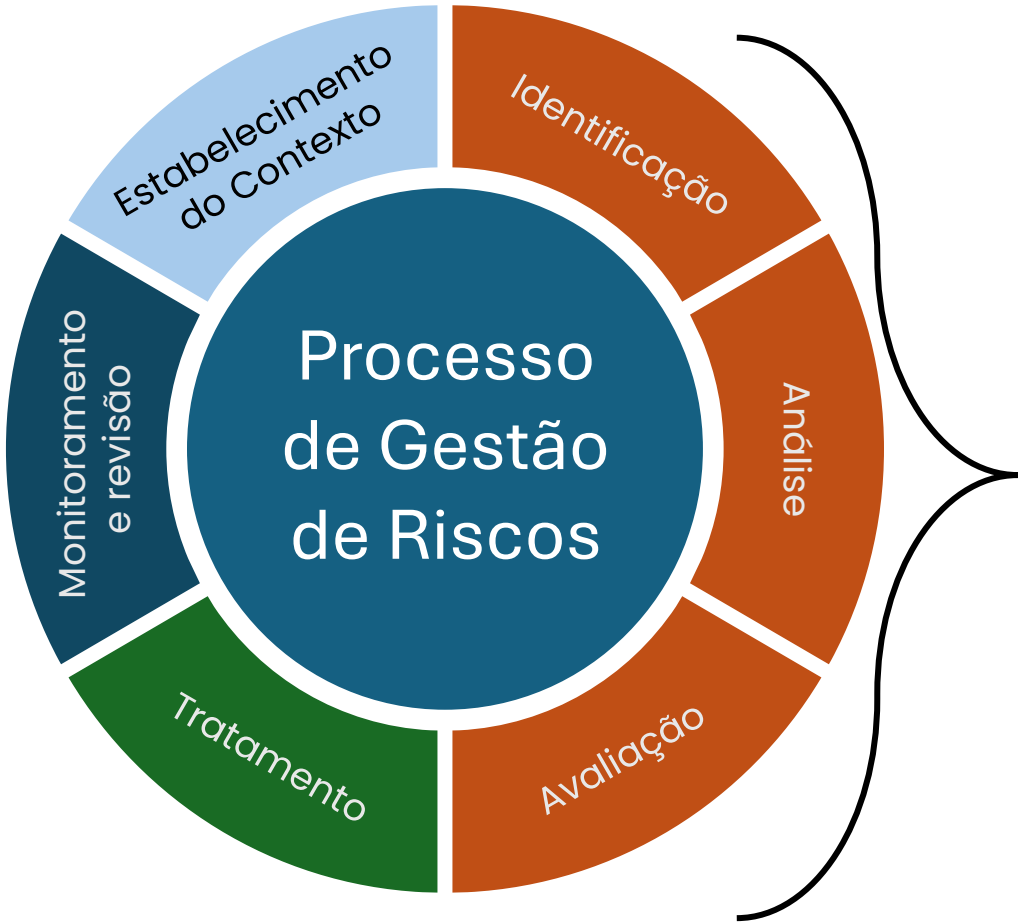
1. Liderança e Comprometimento: apoio contínuo e integração à governança e à cultura
2. Integração: todos devem responder por riscos
3. Design: abordagem adaptada ao contexto e objetivos
4. Implementação: operacionalização da estrutura e aplicação aos processos
5. Avaliação: verificação periódica da adequação e da eficácia
6. Melhoria: otimização contínua da estrutura, corrigindo deficiências

Agenda

- Conceitos
  - Risco
  - Categorias de Risco
  - Controles Internos
  - Gestão de Riscos
  - Estruturas para Gestão de Riscos
  - O Modelo de Três Linhas
- ABNT/ISO 31000
- **O Processo de Gestão de Riscos da ISO 31000**
- Gestão de riscos à integridade
- Estudo de Caso

Visão geral do processo de gestão de riscos da ABNT/ISO 31000

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência



A V A L I A R

1. Comunicação e consulta: envolvimento das partes interessadas em todas as etapas
2. Estabelecimento do contexto: definição do escopo e critérios de risco
3. Avaliação de riscos: identificação, análise e avaliação de riscos
4. Tratamento de riscos: Seleção e implementação de opções de tratamento
5. Monitoramento e Revisão: Acompanhamento contínuo e melhoria
6. Registro e Relato: Documentação e comunicação dos resultados

Comunicação e consulta:

A gestão de riscos deve ser transparente e envolver todas as partes interessadas relevantes, desde a Alta Administração até os funcionários, fornecedores e até mesmo o público em geral, quando necessário.

- Auxilia no estabelecimento do contexto
- Interesses dos stakeholders
- Correta identificação dos riscos (multidisciplinariedade Diferentes pontos de vista)
- Aval e apoio aos planos de tratamento
- Gestão de mudanças

Estabelecendo o contexto

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

O estabelecimento do contexto é a etapa fundamental da gestão de riscos, onde se definem os parâmetros internos e externos da organização, os objetivos a serem alcançados e os critérios de risco.

Ambiente Interno: Compreende os elementos sob controle direto da organização que impactam sua capacidade de gerenciar riscos.

Comprometimento da alta administração:

- Política de gestão de riscos
- Alinhamento com cultura e valores organizacionais
- Estrutura e processos, normas e procedimentos
- Objetivos, estratégias e metas
- Recursos disponíveis (humanos, financeiros, tecnológicos, informacionais, tangíveis e intangíveis)
- Capacidades e competências da equipe
- Papéis e responsabilidades
- Comunicação dos benefícios da gestão de riscos

Ambiente Externo: Engloba as forças e tendências externas que podem influenciar os objetivos e a tomada de decisão da organização.

- Condições econômicas, de mercado e competitivas
- Ambiente político, legal e regulatório
- Fatores sociais, culturais e demográficos
- Avanços tecnológicos e inovações disruptivas
- Expectativas de concorrentes e partes interessadas

Variáveis para gestão de riscos

- Objetivos e escopo
- Taxonomia de riscos
- Critérios de risco
- Apetite e tolerância

Taxonomia de riscos (1)

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Estabelece uma linguagem comum para todos os envolvidos no processo de gestão de riscos. Isso evita ambiguidades e garante que, ao discutir um determinado risco, todos entendam a mesma coisa.

Estratégico

Governança corporativa:
- Performance da administração
- Responsabilidade social
- Ambiente de Controles (*entity level*)

Planejamento e alocação de recursos:
- Estrutura organizacional
- Planejamento estratégico
- Planejamento orçamentário
- Alianças e parcerias

Iniciativa estratégicas:
- Execução
- Monitoramento
- Implantação de tecnologias
- *Change management*

Fusões e aquisições:
- Avaliação e precificação
- *Due Diligence*
- Aprovações regulatórias
- Execução e integração

Dinâmica de mercado:
- Incerteza regulatória
- Competição
- Fatores macroeconômicos
- Fatores sóciopolíticos

Comunicação e relação com partes interessadas:
- Execução
- Monitoramento

Operacional

Vendas e marketing:
- Marketing
- Pesquisa
- Relacionamento com cliente

Fornecimento e entrega:
- Previsão de oferta e demanda
- Gestão de recursos
- Fornecimento

Comercialização:
- Preço
- Crédito
- Liquidez
- Operacional

Ativos físicos:
- Imobilizado
- Inventário
- Outros tangíveis

Pessoas:
- Cultura
- Reconhecimento e performance
- Plano de sucessão
- Plano de remuneração e benefícios

Operacional

Tecnologia da Informação:
- Acesso e segurança de TI
- Disponibilidade e continuidade
- Integridade
- Infra–estrutura

Ameaças:
- Eventos naturais
- Desastres
- Terrorismo e vandalismo

Conformidade

Ética e Conduta:
- Ética
- Fraude

Legal:
- Contratos
- Contencioso
- Propriedade intelectual
- Relações trabalhistas
- Corrupção
- Tributário

Regulatório:
- Direitos de clientes
- Meio–ambiente
- Saúde e segurança
- Concessões e autorizações

Financeiro

Mercado:
- Taxa de juros
- Moeda estrangeira
- *Commodities*
- Derivativos

Crédito e liquidez:
- Fluxo de caixa
- *Hedge*
- Credito e cobrança
- Seguros

Relatórios contábeis/ financeiros:
- Elaboração
- Divulgação

Legal/ tributário:
- Planejamento tributário
- Preço de transferência

Estrutura de capital:
- Dívida
- Patrimônio líquido
- Fundos de pensão
- Opções de ações

CONTEXTO EXTERNO		CONTEXTO INTERNO	
RISCOS ECONÔMICOS		**RISCOS FINANCEIROS**	
· Disponibilidade de capital · Emissões de crédito, inadimplência · Concentração · Liquidez	· Mercados financeiros · Desemprego · Concorrência · Fusões / aquisições	· Falta de liquidez · Disponibilidade de bens · Acesso ao capital	
RISCOS SOCIOAMBIENTAIS		**RISCOS DE PESSOAL**	
· Emissões e dejetos · Energia · Desenvolvimento sustentável		· Capacidade dos empregados · Atividade fraudulenta · Saúde e segurança	
RISCOS SOCIAIS		**RISCOS OPERACIONAIS**	
· Características demográficas · Comportamento do consumidor	· Cidadania corporativa · Privacidade · Terrorismo	· Capacidade · Design · Execução	· Dependências / fornecedores
RISCOS TECNOLÓGICOS		**RISCOS TECNOLÓGICOS**	
· Interrupções · Comércio eletrônico	· Dados externos · Tecnologias emergentes	· Integridade de dados · Disponibilidade de dados e sistemas · Seleção de sistemas	· Desenvolvimento · Alocação · Manutenção
RISCOS NATURAIS		**RISCOS DE IMAGEM**	
· Desastres naturais		· Exposição negativa em meios de comunicação	· Perda de confiança de partes interessadas
RISCOS LEGAIS/REGULATÓRIOS		**RISCOS LEGAIS/REGULATÓRIOS**	
· Multas, sanções aplicadas por órgãos reguladores		· Suspensão de licenças de funcionamento · Legislação	· Política pública · Regulamentos

Taxonomia de riscos (2)

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Estratégico	Descrição	Exemplos
Mudanças políticas	Alterações no governo ou políticas que afetam a instituição	Eleições, mudanças de governo, novas políticas públicas
Desalinhamento estratégico	Falta de alinhamento entre objetivos institucionais e estratégias	Objetivos mal definidos, estratégias inadequadas
Concorrência	Concorrência de outras instituições ou entidades	Privatização de serviços públicos, competição por recursos
Mudanças demográficas	Alterações na demografia da população atendida	Envelhecimento da população, mudanças nos padrões de migração
Crise econômica	Crises econômicas que afetam a instituição	Recessão econômica, cortes orçamentários

Financeiros	Descrição	Exemplos
Orçamento insuficiente	Falta de recursos financeiros para realizar objetivos	Cortes orçamentários, falta de aprovação de orçamento
Problemas de arrecadação	Problemas com a arrecadação de receitas	Dívida ativa, problemas de cobrança
Despesas não planejadas	Despesas não previstas que afetam o orçamento	Emergências, despesas não orçadas
Risco de crédito	Risco de crédito associado a empréstimos ou financiamentos	Inadimplência de devedores, problemas de crédito
Flutuações cambiais	Flutuações cambiais que afetam a instituição	Variações cambiais, problemas de hedge

Integridade	Descrição	Exemplos
Fraude	Fraude cometida por funcionários ou terceiros	Inserção de fucionários fantasmas na folha
Corrupção	Corrupção ou suborno de funcionários ou terceiros	Solicitação de vantagens para a execução de serviço
Conflito de interesses	Conflito de interesses entre funcionários ou terceiros	Prestação particular de serviços em que está investido
Violação de código de conduta	Violação do código de conduta da instituição	Problemas de ética, violação de políticas
Problemas de governança	Problemas de governança ou supervisão	Problemas de supervisão, falta de transparência
Nepotismo	Favorecimento a parente em contratações e/ou promoções	Contratação de pessoal terceirizado sem critérios claros de seleção
Abuso de autoridade	Uso indevido de prerrogativas do cargo para benefício próprio ou de terceiros.	Favorecimento na tramitação de processos
Vazamento de Informações Confidenciais	Quebra de sigilo funcional.	Vazamento de informações sobre processos em andamento
Assédio (Moral e Sexual)	Abuso de poder e violação da dignidade no ambiente de trabalho.	Isolamento funcional do servidor
Concussão	Exigência de dinheiro ou vantagem em função do cargo exercido	Solicitação de vantagens para liberação de licença
Peculato	Desvio de dinheiro ou bem sob responsabilidade	Utilização de bens públicos em interesse particular.
Prevaricação	Não assummir as responsabilidades do cargo público	Retardar a decisão em um processo
Improbidade administrativa	Enriquecimento ilícito em função do cargo	Venda de sentença judicial
Advocacia administrativa	Utilização do cargo para defender interesses de terceiros	Interferências em processos administrativos em andamento

Operacional	Descrição	Exemplos
Falhas de processos	Falhas nos processos internos que afetam a eficiência	Processos ineficientes, falta de treinamento
Problemas de infraestrutura	Problemas com infraestrutura física ou tecnológica	Falhas de energia, problemas de conectividade
Gestão de recursos humanos	Problemas com a gestão de pessoal	Rotatividade de funcionários, falta de habilidades
Dependência de fornecedores	Dependência de fornecedores críticos	Falhas de fornecedores, problemas de qualidade
Desastres naturais	Desastres naturais que afetam a instituição	Terremotos, furacões, enchentes

Cibernéticos	Descrição	Exemplos
Ataques cibernéticos	Ataques cibernéticos que afetam a segurança da informação	Malware, phishing, ataques de negação de serviço
Falhas de segurança	Falhas de segurança que permitem acesso não autorizado	Vulnerabilidades de software, problemas de autenticação
Perda de dados	Perda de dados críticos devido a falhas ou ataques	Perda de dados, corrupção de dados
Interrupção de serviços	Interrupção de serviços críticos devido a problemas cibernéticos	Downtime de sistemas, problemas de conectividade
Roubo de identidade	Roubo de identidade de funcionários ou cidadãos	Phishing, roubo de informações pessoais

Conformidade	Descrição	Exemplos
Não conformidade regulatória	Não conformidade com regulamentos e leis aplicáveis	Multas, penalidades, problemas de reputação
Problemas de licenciamento	Problemas com licenças ou permissões necessárias	Licenças vencidas, problemas de renovação
Falhas de auditoria	Falhas em auditorias internas ou externas	Problemas de compliance, observações de auditoria
Não conformidade com normas	Não conformidade com normas e padrões aplicáveis	Problemas de qualidade, não conformidade com normas técnicas
Risco de litígio	Risco de litígio devido a não conformidade ou outras questões	Ações judiciais, problemas de responsabilidade

Reputacional	Descrição	Exemplos
Crise de reputação	Crise de reputação devido a eventos ou ações	Crise de reputação, problemas de imagem
Problemas de comunicação	Problemas de comunicação que afetam a reputação	Comunicação inadequada, problemas de mídia
Desastre de relações públicas	Desastre de relações públicas devido a eventos ou ações	Problemas de relações públicas, crise de reputação
Problemas de responsabilidade social	Problemas de responsabilidade social ou ambiental	Problemas de responsabilidade social, questões ambientais
Perda de confiança	Perda de confiança dos stakeholders devido a eventos ou ações	Perda de confiança, problemas de reputação

Variáveis para avaliação de riscos

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Critérios de riscos

	Nível	Nome	Descrição
Probabilidade	1	Muito Baixa	Praticamente improvável de acontecer. Ocorrências conhecidas são extremamente raras ou nunca observadas no histórico da organização/indústria. Chance remota (0-10%).
	2	Baixa	Pode ocorrer em raras ocasiões. Eventos similares aconteceram poucas vezes em histórico muito longo. Pequena chance de ocorrência (11-30%).
	3	Média	Pode ocorrer ocasionalmente. Eventos similares já aconteceram e podem se repetir em certas circunstâncias. Chance moderada de ocorrência (31-60%).
	4	Alta	É provável que ocorra. Eventos similares já aconteceram e há fortes indícios de que acontecerão novamente. Alta chance de ocorrência (61-80%).
	5	Muito Alta	Quase certeza de que ocorrerá ou já ocorreu frequentemente. Eventos similares são comuns e esperados. Chance muito alta ou certa de ocorrência (81-100%).

	Nível	Nome	Descrição
Impacto	1	Insignificante	Nenhum ou impacto mínimo nas finanças (ex: < R\$1.000), operacional (pequeno ajuste), reputação (não notado), segurança (pequeno incômodo).
	2	Menor	Impacto financeiro baixo (ex: R\$1.000 - R\$10.000), pequena interrupção operacional (horas), reputação local/interna, segurança de dados pessoais não sensíveis (menor vazamento).
	3	Moderado	Impacto financeiro médio (ex: R\$10.000 - R\$100.000), interrupção operacional significativa (dias), dano à reputação com cobertura limitada, vazamento de dados de clientes não críticos.
	4	Maior	Impacto financeiro alto (ex: R\$100.000 - R\$1.000.000), interrupção operacional grave (semanas/mês), perda de clientes, dano à reputação com cobertura nacional, multa regulatória significativa, vazamento de dados críticos.
	5	Crítico	Impacto financeiro severo (ex: > R\$1.000.000 ou falência), interrupção total das operações (parada), perda massiva de clientes, dano catastrófico à reputação (irreversível), multas milionárias, ação legal coletiva, perda de licença.

Matriz de riscos

Probabilidade / Impacto	1. Insignificante	2. Menor	3. Moderado	4. Maior	5. Crítico
5. Muito Alta	**Moderado**	**Alto**	**Extremo**	**Extremo**	**Extremo**
4. Alta	**Baixo**	**Moderado**	**Alto**	**Extremo**	**Extremo**
3. Média	**Baixo**	**Baixo**	**Moderado**	**Alto**	**Extremo**
2. Baixa	**Baixo**	**Baixo**	**Baixo**	**Moderado**	**Alto**
1. Muito Baixa	**Baixo**	**Baixo**	**Baixo**	**Baixo**	**Moderado**

Apetite a riscos

Zona de Risco	Ações Recomendadas
Risco Baixo	Nível de risco geralmente aceitável. Ações de monitoramento rotineiro e revisão periódica são suficientes.
Risco Moderado	Risco aceitável com algumas condições. Requer monitoramento mais frequente e pode necessitar de controles adicionais a baixo custo.
Risco Alto	Risco que excede o apetite da organização. Requer planos de tratamento detalhados, alocação de recursos específicos e acompanhamento da alta gestão.
Risco Extremo	Risco inaceitável. Exige tratamento imediato e prioritário, podendo levar à paralisação de atividades ou mudança de estratégia.

Critérios de riscos

O processo de avaliação de riscos é o processo global de identificação de riscos, análise e avaliação de riscos. Para tanto é necessário definir os critérios de riscos, envolvendo:

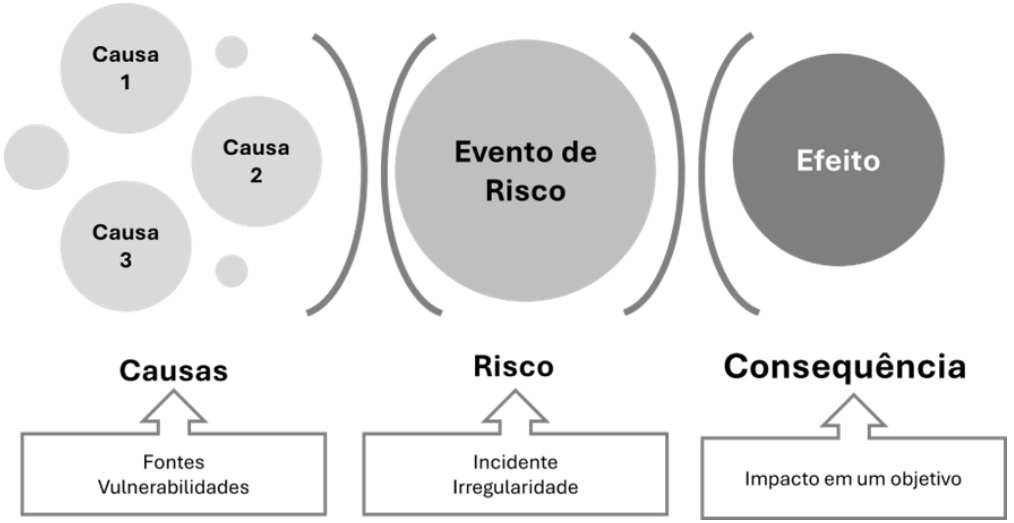
- Natureza e os tipos de consequência e como serão medidos
- Como expressar as probabilidades
- Como determinar o nível de risco
- Critério para decidir pelo tratamento do risco
- Critérios para decidir quando um risco é aceitável ou tolerável
- Combinações de riscos

Identificando riscos

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Envolve a identificação de fontes de risco, eventos, suas causas e seus efeitos potenciais. Os riscos devem estar relacionado com os objetivos da organização, do processo, do projeto, etc.

A identificação deve ser abrangente e com analises da criticidade, pois um risco não identificado pode ser um risco não tratado



Devido a <**CAUSA/FONTE**>, poderá acontecer <**DESCRIÇÃO DA INCERTEZA**>, o que poderá levar a <**DESCRIÇÃO DO IMPACTO, CONSEQUÊNCIA, EFEITO**>, impactando no/na <**DIMENSÃO DE OBETIVO IMPACTADA**>.

Fonte de Risco: elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco.

Vulnerabilidade: fonte de risco inexistente, inadequada, deficiente
Elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco.

Causa = Fonte + Vulnerabilidade
É o resultado da ocorrência do risco afetando o objetivo.

Consequência
É o resultado da ocorrência do risco afetando o objetivo.

Controles
- Preventivos
- Atenuação e recuperação
- Detectivos

Ferramentas
- *Brainstorming*
- Entrevistas
- Análise de cenários
- *Check list* de riscos
- Diagrama de *Bow-Tie*
- *Workshops*

Informações e registros
- Lista abrangente de riscos identificados, com suas descrições, causas e consequências potenciais.
- Mapa de registro de riscos

Fatores de riscos por categoria

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

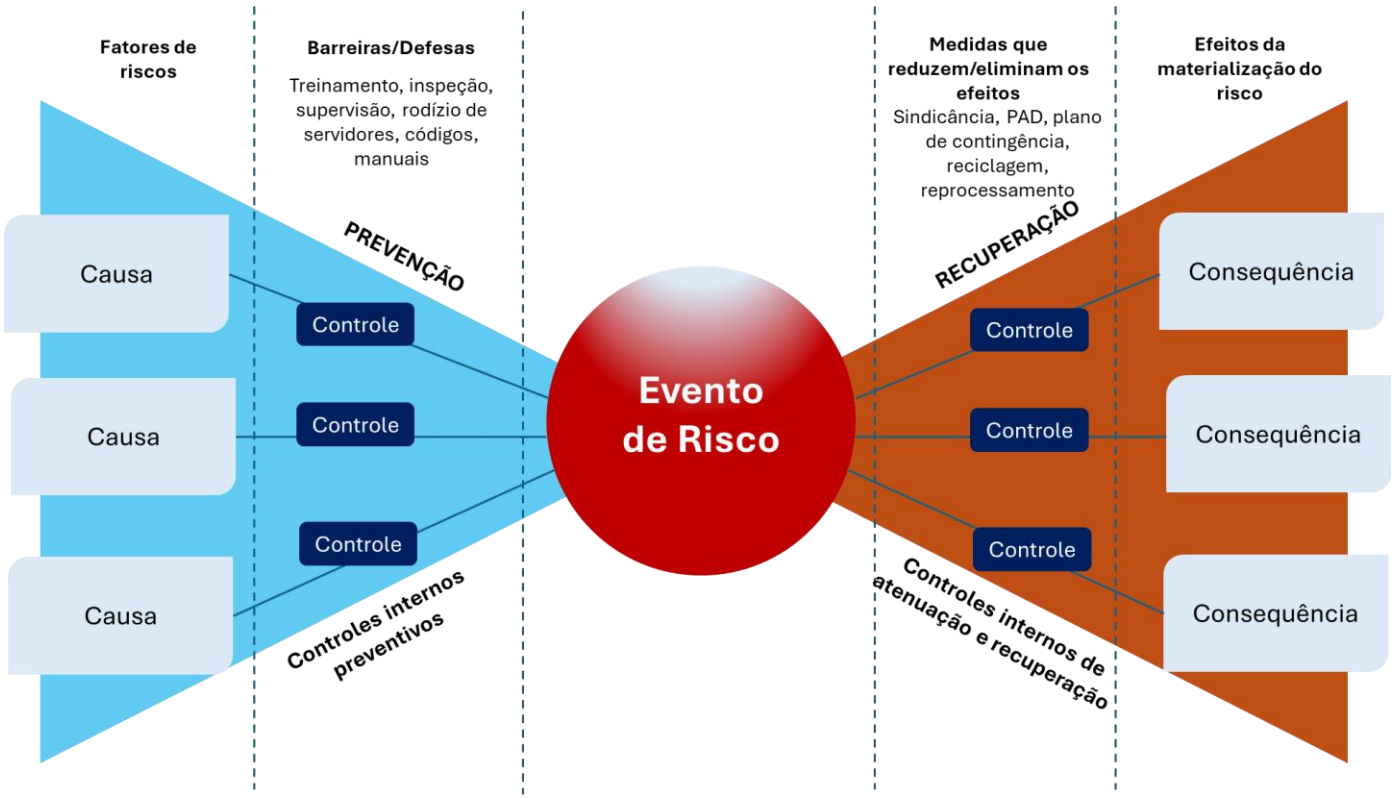


Diagrama de Bow Tie

Fonte:
- Pessoas

Vulnerabilidades:
- Em nº insuficiente
- Sem capacitação
- Perfil inadequado
- Desmotivadas

Fonte:
- Sistemas informatizados

Vulnerabilidades:
- Obsoletos
- Ausência de backups
- Indisponíveis

Fonte:
- Tecnologia

Vulnerabilidades:
- Técnica de produção ultrapassada
- Patentes não registradas
- Sigilo industrial desprotegido

Fonte:
- Estrutura organizacional

Vulnerabilidades:
- Indefinição de papéis e responsabilidades
- Centralização
- Departamentalização excessiva

Fonte:
- Infraestrutura física

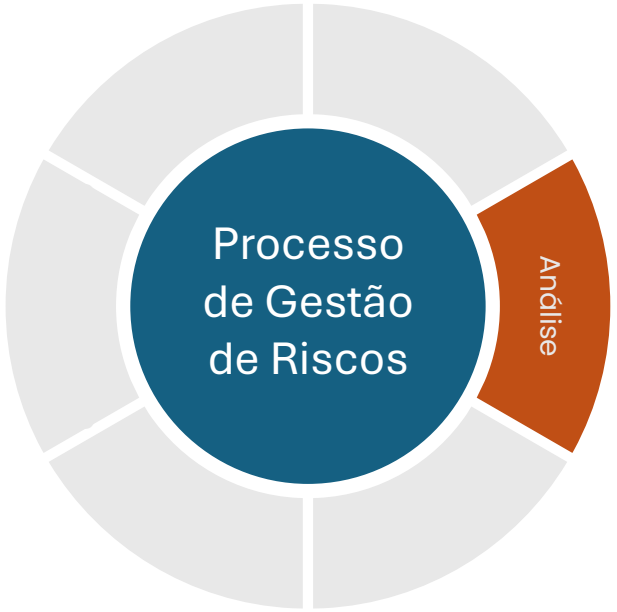
Vulnerabilidades:
- Localização
- Falta de manutenção
- Instalações obsoletas

Fonte:
- Processos

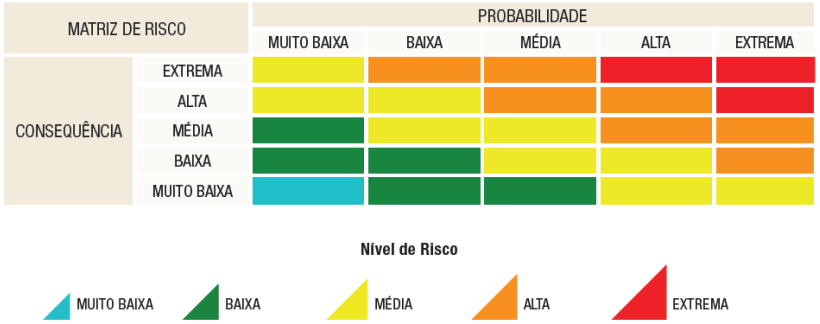
Vulnerabilidades:
- Mal concebidos
- Complexos
- Ausência de segregação de funções

Analisando riscos

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência



Compreende o desenvolvimento da compreensão sobre o risco e à determinação do nível do risco. A organização deve definir as variáveis e critérios para avaliar seus riscos.



Risco inerente: é o risco bruto sem considerar quaisquer ações que possam reduzir a sua probabilidade ou impacto.

Risco residual: é o risco remanescente após a implementação de ações de tratamento.

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

Avaliação dos controles: o nível de risco dependerá da adequação e da eficácia dos controles existentes.

- Quais são os controles existentes para um risco em particular?
- Os controles são capacidades de controlar o risco a um nível tolerável?
- Estão operando na forma pretendida e podem ser demonstrados como eficazes quando requerido?

Cálculo do Risco residual (RR)

RR = NRI x FA, onde:

NRI = Nível de Risco inerente
FA = Fator de avaliação de controles internos

Avaliando riscos

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Consiste em comparar os níveis estimados de risco com critérios de risco definidos quando o contexto foi estabelecido, a fim de determinar a significância do nível e do tipo de risco. Utiliza a compreensão do risco obtida durante a análise do risco para tomar decisões sobre ações futuras.

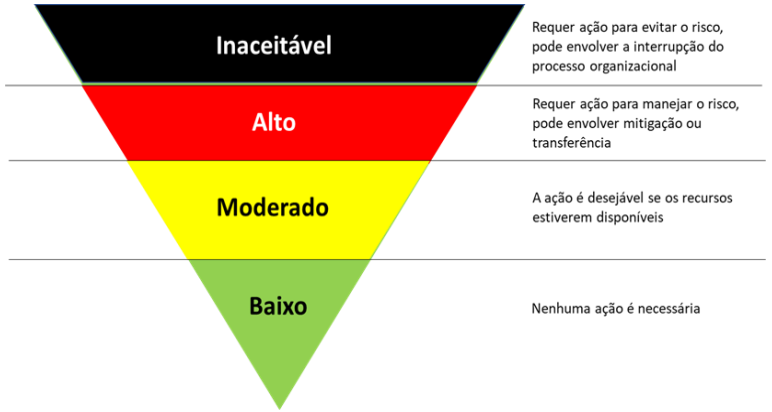
Nível de risco: medida de importância ou significância do risco, quanto à sua criticidade, obtido a partir da análise da combinação de probabilidade e impacto.

Muito alto	4	4	8	12	16
Alto	3	3	6	9	12
Moderado	2	2	4	6	8
Baixo	1	1	2	3	4
Matriz de riscos		1	2	3	4
		Raro	Pouco provável	Provável	Muito provável

Decisões de riscos podem incluir:

- Se um risco precisa de tratamento
- Prioridade para tratamento
- Se uma atividade deve ser realizada
- Qual caminho alternativo deve ser seguido

Escala de Nível de Risco	
Níveis	**Pontuação**
RC - Inaceitável	12 a 16
RA - Risco Alto	7 a 11
RM - Risco Moderado	4 a 6
RP - Risco Baixo	1 a 3



Apetite e tolerância

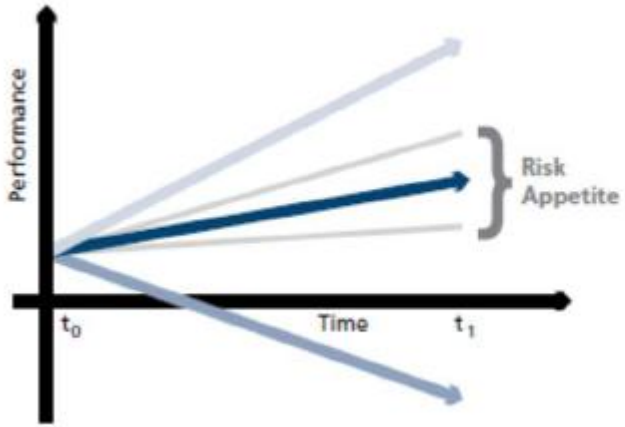
Apetite a risco: é a quantidade de risco, em um nível abrangente, que a entidade aceita em troca de valor, ou o nível de risco que uma organização está preparada a aceitar para atingir seus objetivos.

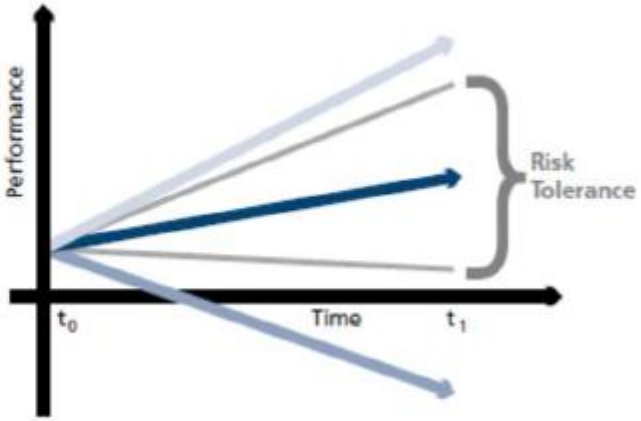
Tolerância a risco: é o limite máximo de exposição a um risco específico que a organização pode suportar sem comprometer sua capacidade de alcançar seus objetivos fundamentais.

Resiliência: é a capacidade de uma organização de antecipar, preparar-se, responder e adaptar-se a eventos disruptivos e aprender com eles.

Requisitos ao apetite a risco:

- Compatibilizar com a estratégia e objetivos organizacionais
- Ser direcionador e balizador do modelo decisório
- Considerar as habilidades, recursos e tecnologias existentes para monitorar a exposição ao risco.
- Compreendido e aprovado pela Alta Administração
- Declaração formal de apetite a risco





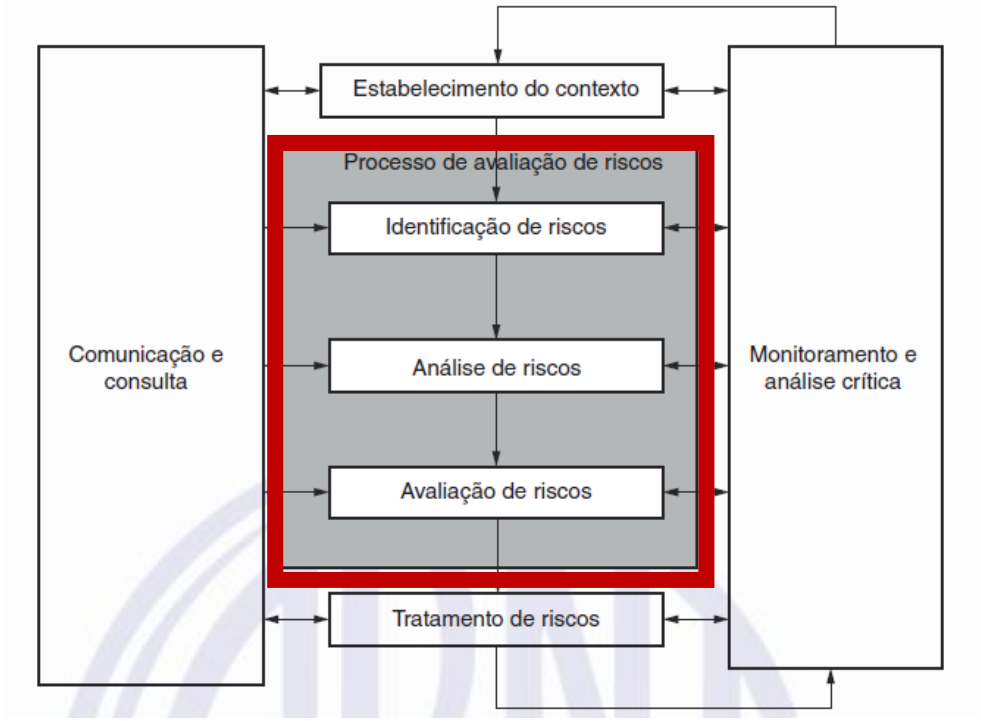
Técnicas de avaliação de riscos – ISO 31010

O processo de avaliação de riscos pode requerer uma abordagem multidisciplinar, uma vez que os riscos podem abranger uma ampla gama de causas e consequências.

Pode ser conduzido em vários graus de profundidade e detalhe e utilizando um ou muitos métodos que vão do simples ao complexo.

Em termos gerais, convém que as técnicas apropriadas apresentem as seguintes características:

- convém que sejam justificáveis e apropriadas à situação ou organização em questão;
- convém que proporcionem resultados de uma forma que amplie o entendimento da natureza do risco e de como ele pode ser tratado;
- convém que sejam capazes de utilizar uma forma que seja rastreável, repetível e verificável.



Os métodos utilizados na análise de riscos podem ser **qualitativos, semi-quantitativos ou quantitativos**. O grau de detalhe requerido dependerá da aplicação em particular, da disponibilidade de dados confiáveis e das necessidades de tomada de decisão da organização

Técnicas para o processo de avaliação de riscos:

- Brainstorming
- Entrevistas estruturadas e semi-estruturadas
- Técnica Delphi
- Listas de verificação
- Análise preliminar de perigos
- HAZOP
- Análise de perigos e pontos críticos de controle
- Técnica estruturada “What if”
- Análise de cenários
- BIA
- Análise de causa raiz (RCA)
- FMEA

Tratando riscos

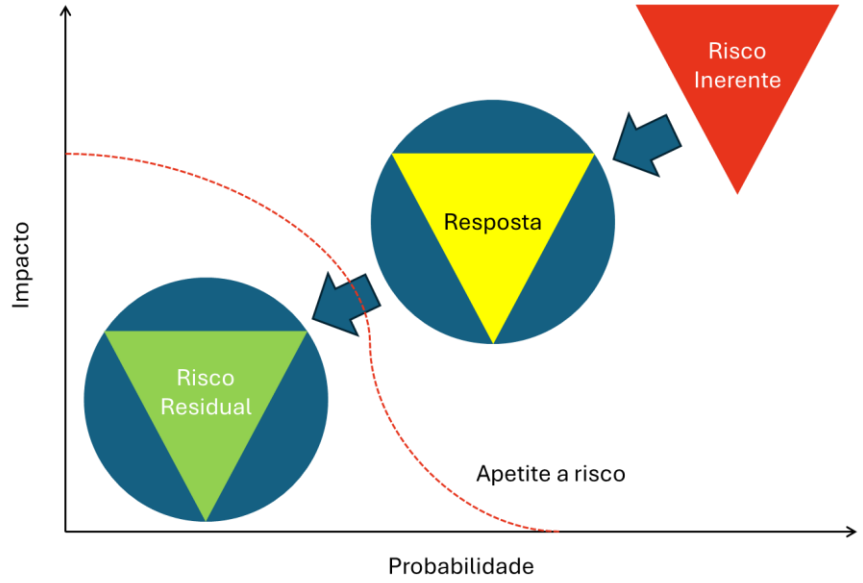
GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Consiste na seleção e implementação de opções para atuar sobre cada risco identificado.

O tratamento de riscos envolve etapas como a avaliação do tratamento já realizado, a verificação se os riscos residuais são toleráveis, a definição de tratamentos adicionais, caso necessário, e a avaliação da eficácia dessas ações.

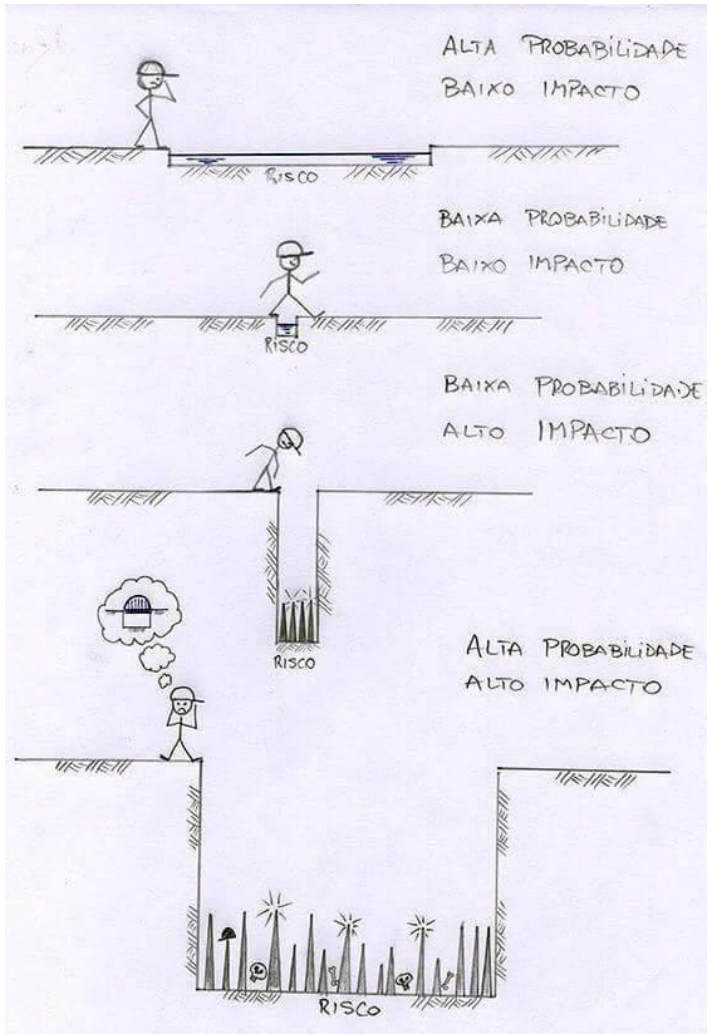
A partir de um **plano de tratamento** é definida a ordem de prioridade das ações, considerando:

- Razões para escolha do tratamento
- Benefícios esperados
- Responsáveis (aprovação e implementação)
- Recursos necessários
- Cronograma
- Medidas de monitoramento



Estratégias de tratamento de riscos

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência



Mitigar (Reduzir): Ações para diminuir a chance ou o impacto do risco. **Transferir (Compartilhar):** Passar o risco a terceiros (seguros, parcerias). **Aceitar:** Decidir não agir sobre o risco, ciente das consequências (riscos residuais). **Evitar:** Modificar o processo para eliminar o risco. **Reter:** recuperar operações/atividades.

Evitar	Negar, Proibir, Parar, Focar, Eliminar	Uma organização sem fins lucrativos identificou e avaliou os riscos de fornecer serviços médicos diretos aos seus membros e decidiu, desse modo, não aceitar os riscos associados.
Reter	Aceitar, Compensar, Rever preços, Programar	Uma empresa de varejo após registrar um índice recorde de inadimplência, criou um programa de recuperação de clientes duvidosos, incluindo a oferta de abatimentos e descontos em compras futuras.
Mitigar	Dispersar, Controlar	Uma empresa que produz microchips e componentes eletrônicos de alto valor agregado, após ter registrado um número recorde de perdas por motivos desconhecidos, decidiu implantar um sistema de segurança e um procedimento trimestral de inventário completo em seus centros de armazenamento.
Transferir	Segurar, Hedgear, Partilhar, Terceirizar	A organização sem fins lucrativos mencionada anteriormente decidiu terceirizar os serviços médicos prestados a seus membros para uma empresa especializada.
Aceitar	Alocar, Criar, Renegociar, Reorganizar, Diversificar	Uma instituição pública avaliou o risco de incêndio de suas instalações em diversas regiões e o custo de transferir o risco por meio de cobertura de seguro e considerou que o custo de substituição seria inferior ao custo do seguro pretendido.

Plano de respostas

Documento ou conjunto de diretrizes que detalha como uma organização pretende lidar com os riscos identificados em seu ambiente. Não é apenas uma lista de problemas, mas um guia prático sobre o que fazer para gerenciar esses riscos.

Monitoramento e reporte:

- KPI's para aferição da eficácia
- Frequência e formato dos relatórios
- Papéis e responsabilidades definidas (monitoramento, reporte e ação, se necessária)

Elementos essenciais

- **Riscos identificados**: Descrição detalhada de cada risco, suas causas e como podem afetar os objetivos do projeto.
- **Donos do risco**: A pessoa responsável por monitorar o risco e garantir que as respostas sejam implementadas.
- **Estratégia de resposta**: A abordagem escolhida para cada risco (evitar, mitigar, transferir, aceitar, etc.).
- **Ações específicas**: As ações concretas que precisam ser tomadas para implementar a estratégia escolhida.
- **Orçamento e cronograma**: Recursos e tempo necessários para executar as ações de resposta.
- **Planos de contingência**: Ações a serem tomadas caso a estratégia de resposta original falhe ou um risco inesperado ocorra.

Tratando riscos

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Inaceitável

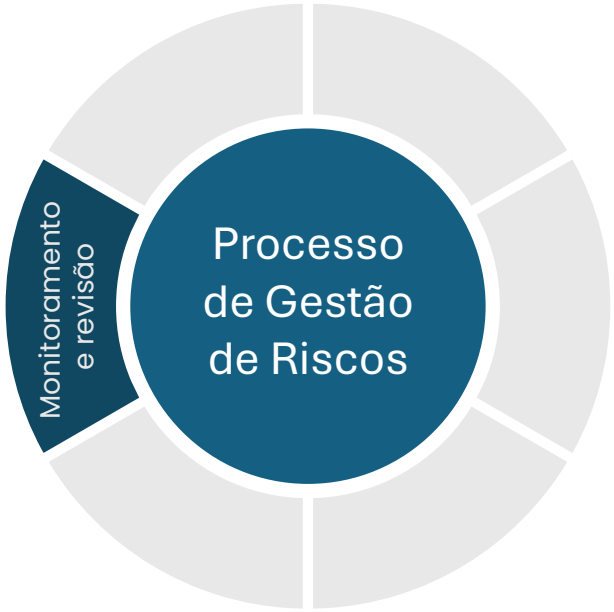
Alto

Moderado

Baixo

Monitoramento e revisão

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência



Assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados do processo

Monitoramento: Acompanhamento regular da eficácia dos controles, do desempenho dos planos de ação, e da identificação de novos riscos ou mudanças no ambiente (legislativo, político, social).

Revisão: Avaliações periódicas do processo de gestão de riscos como um todo, para garantir que ele permanece relevante e eficaz.

Frequência de monitoramento: Definir a frequência do monitoramento com base no nível de risco residual

Mecanismos de feedback e ajustes

- Canais de denúncias e Ouvidorias: detecção de riscos e irregularidades
- Auditorias interna e externa: verificação independente da eficácia de controles e processos
- Pesquisa de clima organizacional: percepção dos servidores sobre a cultura organizacional
- Lições aprendidas: análise de incidentes
- Relatórios de desempenho de indicadores (KPI's / KRI's): eficácia dos planos de ação e evolução do perfil de risco

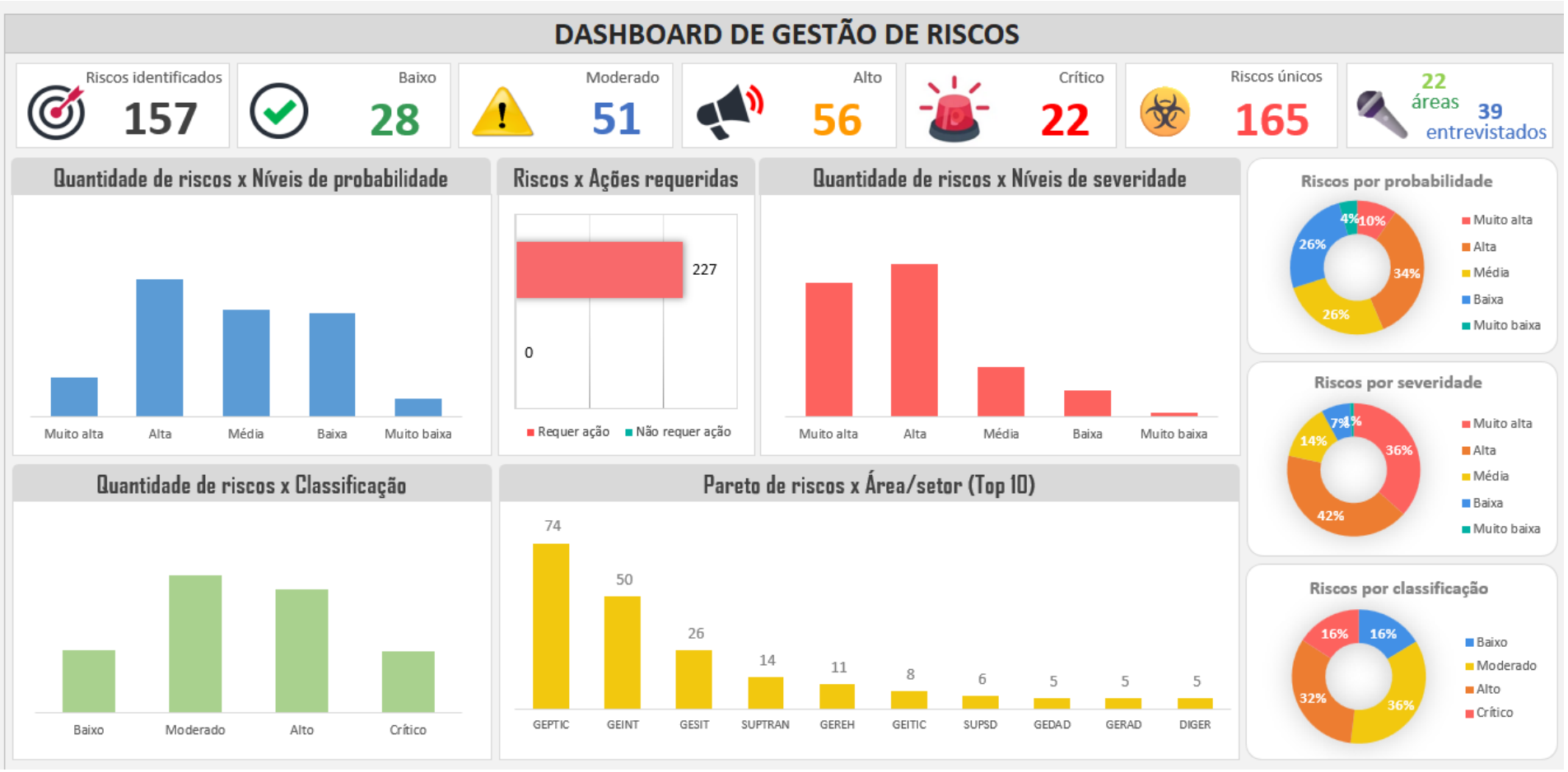
Indicadores-Chaves de Risco (KRI's)

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Categoria de Risco	KRI (Indicador-Chave de Risco)	Descrição/Exemplo de KRI
Estratégico	Taxa de Conclusão de Metas e Projetos Estratégicos	Percentual de metas do Plano Plurianual (PPA) ou Plano de Governo atingidas dentro do prazo e orçamento.
	Índice de Satisfação do Cidadão/Usuário do Serviço	Avaliação média dos serviços prestados (ex: pesquisa de satisfação, avaliação de ouvidoria).
	Variação na Reputação Institucional	Análise de menções em mídias (online/tradicional), volume e teor de manifestações em canais de ouvidoria.
Operacional	Tempo Médio de Atendimento/Conclusão de Serviços	Média de tempo para finalizar um processo ou serviço público (ex: emissão de documentos, concessão de licenças).
	Taxa de Erros/Não Conformidades em Processos Chave	Percentual de falhas em processos críticos (ex: folha de pagamento, processos licitatórios).
	Disponibilidade de Sistemas Críticos para o Cidadão	Tempo de atividade (uptime) de plataformas e sistemas de atendimento ao público.
	Taxa de Absenteísmo de Servidores	Percentual de servidores ausentes do trabalho, indicando potencial sobrecarga ou problemas de gestão de pessoal.
Conformidade	Número de Auditorias com Ressalvas ou Apontamentos Graves	Quantidade de auditorias internas ou externas que identificaram não conformidades significativas.
	Volume de Multas e Sanções Recebidas	Valor ou número de penalidades aplicadas por órgãos reguladores ou de controle (TCU, CGE, etc.).
	Aderência a Prazos Regulatórios	Percentual de cumprimento de prazos estabelecidos por leis (ex: Lei de Responsabilidade Fiscal, Lei de Acesso à Informação, Lei de Licitações).
	Número de Processos Administrativos/Judiciais por Não Conformidade	Casos abertos devido a descumprimento de normas.
Integridade	Número de Denúncias no Canal de Ética/Ouvidoria	Volume de comunicações que apontam desvios de conduta, fraude ou corrupção.
	Casos Confirmados de Assédio/Fraude/Corrupção	Número de incidentes comprovados e suas respectivas sanções.
	Resultado de Avaliações de Clima Ético	Nível de percepção dos servidores sobre a cultura de integridade e ética na instituição.
	Transparência e Competitividade em Licitações	Indicadores que monitorem a competição em processos de compra (ex: número médio de participantes por licitação, percentual de dispensas/inexigibilidades).
Tecnologia da Informação (TI)	Número de Incidentes de Segurança da Informação	Quantidade de ataques, tentativas de invasão, vazamentos de dados ou infecções por malware.
	Tempo de Inatividade de Sistemas Críticos	Horas totais de sistemas essenciais fora do ar (planejadas e não planejadas).
	Percentual de Dados Públicos Criptografados/Protegidos	Proporção de dados sensíveis ou críticos que estão devidamente protegidos.
	Conformidade com Políticas de Segurança da Informação	Avaliação do cumprimento das políticas internas (ex: % de servidores com treinamento em segurança, % de patches de segurança aplicados).
Orçamentário	Percentual de Execução Orçamentária	Comparação entre o orçamento planejado e o executado (receitas e despesas).
	Desvios Orçamentários em Projetos Chave	Percentual de variação entre o custo orçado e o custo real de projetos de investimento.
	Percentual de Gastos com Pessoal em Relação à Receita Corrente Líquida	Medida de conformidade com os limites da Lei de Responsabilidade Fiscal.
	Saldo de Caixa/Disponibilidade Financeira	Monitoramento da liquidez da instituição para honrar seus compromissos.

Dashboard

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência



As atividades de monitoramento e análise crítica devem ser registradas e reportadas interna e externamente. As informações obtidas se tornam fonte de conhecimento que precisa estar disponível a pessoas certas, na forma e no momento adequados. As informações precisam fluir para alcançar quem possa se beneficiar delas para aperfeiçoar o processo de gestão de riscos e os demais processos de tomada de decisão da agência. **Assegurar a qualidade e a relevância das informações é um aspecto essencial da gestão de riscos.**

Registro e relato

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Mapa de Riscos:

O processo de gestão de riscos e seus resultados deve ser documentado e relatado por meio de mecanismos apropriados, objetivando:

- Comunicar atividades e resultados da gestão de riscos em toda a organização
- Fornecer informações para a tomada de decisão
- Melhorar as atividades de gestão de riscos
- Auxiliar a interação com as partes interessadas

A criação, retenção e manuseio de informação devem levar em consideração a sensibilidade das informações no contexto interno e externo.

Mapeamento de Risco

Subprocesso / Atividade	Identificação de Eventos de Riscos					Avaliação do Riscos							Resposta a Risco					
						Risco Inerente			Identificação dos Controles Existentes			Risco Residual			Possível Responsável	Controles Propostos / Ações Propostas			
	Eventos de Risco	Causas	Efeitos / Consequências	Categoria do Risco	Natureza do Risco orçamentário/financeiro	I	P	NR	Descrição do Controle Atual	Avaliação quanto ao Desenho do Controle	Avaliação quanto a Operação do Controle	I	P	NR		Tipo	Descrição	Data do Início	Data da Conclusão	Status	Situação
Subprocesso / Atividade 1	Evento 1	1. 2. n.	1. 2. n.	Orçamentária	Sim	0	1	Risco Pequeno	1. 2. n.			4	4	Risco Crítico		Preventiva	a	23/02/2017	23/02/2017	Em andamento	
	Evento 2	1. 2. n.	1. 2. n.	Fiscal	Sim	5	3	Risco Crítico	1. 2. n.			0	1	Risco Pequeno		0	x	01/01/2017	05/01/2017	Não iniciada	
	Evento 3	1. 2. n.	1. 2. n.	Estratégica	Não	0	1	Risco Pequeno	1. 2. n.			0	1	Risco Pequeno		0	y	01/01/2017	22/01/2017	Não iniciada	
Subprocesso / Atividade 2	Evento 1	1. 2. n.	1. 2. n.		Não	0	1	Risco Pequeno	1. 2. n.			0	1	Risco Pequeno		0	h	00/01/1900	00/01/1900	Não iniciada	
	Evento 2	1. 2. n.	1. 2. n.		Não	0	1	Risco Pequeno	1. 2. n.			0	1	Risco Pequeno		0	j	00/01/1900	00/01/1900	Não iniciada	
	Evento 3	1. 2. n.	1. 2. n.		Não	0	1	Risco Pequeno	1. 2. n.			0	1	Risco Pequeno		0	k	00/01/1900	00/01/1900	Não iniciada	
Subprocesso / Atividade 3	Evento 1	1. 2. n.	1. 2. n.	Estratégica	Não	0	1	Risco Pequeno	1. 2. n.		(2) Controle parcialmente executado e com deficiências;	0	1	Risco Pequeno		0	q	00/01/1900	00/01/1900	Não iniciada	
	Evento 2	1. 2. n.	1. 2. n.		Não	0	1	Risco Pequeno	1. 2. n.			0	1	Risco Pequeno		0	t	00/01/1900	00/01/1900	Não iniciada	
	Evento 3	1. 2. n.	1. 2. n.		Não	0	1	Risco Pequeno	1. 2. n.			0	1	Risco Pequeno		0	v	00/01/1900	00/01/1900	Não iniciada	
Subprocesso / Atividade 4	Evento 1	1. 2. n.	1. 2. n.		Não	0	1	Risco Pequeno	1. 2. n.			0	1	Risco Pequeno		0	q	00/01/1900	00/01/1900	Não iniciada	
	Evento 2	1. 2. n.	1. 2. n.		Não	0	1	Risco Pequeno	1. 2. n.			0	1	Risco Pequeno		0	t	00/01/1900	00/01/1900	Não iniciada	
	Evento 3	1. 2. n.	1. 2. n.		Não	0	1	Risco Pequeno	1. 2. n.			0	1	Risco Pequeno		0	z	00/01/1900	00/01/1900	Não iniciada	
Subprocesso / Atividade 5	Evento 1	1. 2. n.	1. 2. n.		Não	0	1	Risco Pequeno	1. 2. n.			0	1	Risco Pequeno		0	q	00/01/1900	00/01/1900	Não iniciada	
	Evento 2	1. 2. n.	1. 2. n.		Não	0	1	Risco Pequeno	1. 2. n.			0	1	Risco Pequeno		0	t	00/01/1900	00/01/1900	Não iniciada	
	Evento 3	1. 2. n.	1. 2. n.		Não	0	1	Risco Pequeno	1. 2. n.			0	1	Risco Pequeno		0	v	00/01/1900	00/01/1900	Não iniciada	
Subprocesso / Atividade 6	Evento 1 teste	1. 2. n.	1. 2. n.		Não	0	1	Risco Pequeno	1. 2. n.			0	1	Risco Pequeno		0	q	00/01/1900	00/01/1900	Não iniciada	
	Evento 2	1. 2. n.	1. 2. n.		Não	0	1	Risco Pequeno	1. 2. n.			0	1	Risco Pequeno		0	t	00/01/1900	00/01/1900	Não iniciada	
	Evento 3	1. 2. n.	1. 2. n.		Não	0	1	Risco Pequeno	1. 2. n.			0	1	Risco Pequeno		0	v	00/01/1900	00/01/1900	Não iniciada	

SECRETARIA DE ESTADO DE CONTROLE E TRANSPARÊNCIA

Subsecretaria/Gerência/Setor	
Macroprocesso (Atividades chave)	
Processo	
Gestor responsável	
Responsável pela análise	
Período da análise	

PROCESSO/ATIVIDADE	#	Risco de Integridade (Inerente)	Causa	PROBABILIDADE	IMPACTO	NÍVEL DO RISCO (PxI)	Descrição da atividade de controle	Avaliação do controle	Risco residual	Tratam
		#N/D		#	#	0 Baixo		Satisfatório	Baixo	
		#N/D		#	#	0 Baixo			Baixo	
		#N/D		#	#	0 Baixo			Baixo	
		#N/D		#	#	0 Baixo			Baixo	
		#N/D		#	#	0 Baixo			Baixo	
		#N/D		#	#	0 Baixo			Baixo	
		#N/D		#	#	0 Baixo			Baixo	
		#N/D		#	#	0 Baixo			Baixo	
		#N/D		#	#	0 Baixo			Baixo	
		#N/D		#	#	0 Baixo			Baixo	
		#N/D		#	#	0 Baixo			Baixo	
		#N/D		#	#	0 Baixo			Baixo	
		#N/D		#	#	0 Baixo			Baixo	
		#N/D		#	#	0 Baixo			Baixo	
		#N/D		#	#	0 Baixo			Baixo	
		#N/D		#	#	0 Baixo			Baixo	
		#N/D		#	#	0 Baixo			Baixo	
		#N/D		#	#	0 Baixo			Baixo	

Etapas da Gestão de Riscos

Agenda

- Conceitos
  - Risco
  - Categorias de Risco
  - Controles Internos
  - Gestão de Riscos
  - Estruturas para Gestão de Riscos
  - O Modelo de Três Linhas
- ABNT/ISO 31000
- O Processo de Gestão de Riscos da ISO 31000
- Gestão de riscos à integridade
- Estudo de Caso

Gestão de Riscos à integridade

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Objetivos:

Assegurar a confiança da sociedade, o uso eficiente dos recursos públicos, a conformidade com a legislação e a própria missão de servir ao cidadão

A compreensão sobre a importância da gestão de riscos requer um claro entendimento dos valores e objetivos da função pública exercida.

Para que as políticas de integridade sejam relevantes, eficientes e eficazes, os riscos para a integridade necessitam ser adequadamente identificados, avaliados e minimizados.

Obstáculos

- Os gestores públicos desconhecem ou negligenciam os parâmetros, políticas ou diretrizes sobre gestão de riscos.
- Os gestores públicos não possuem um claro entendimento sobre o conceito de “risco” e sobre os processos e a utilidade da gestão de riscos.
- Os gestores públicos acreditam que a gestão de riscos é uma função a ser assumida por terceiros e não a consideram como tarefa inerente à sua própria função gerencial.

OCDE/2019

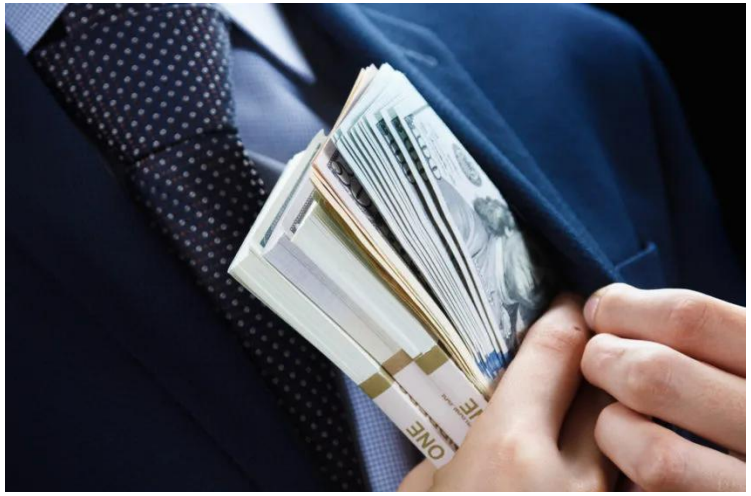
Desafios:

- Cultura Organizacional: Resistência à mudança, percepção de que é "mais burocracia", aversão à exposição de problemas.
- Recursos: Falta de pessoal qualificado, tempo e orçamento para implementar e manter o processo.
- Apoio da Liderança: Ausência de comprometimento explícito e visível da alta direção.
- Fragmentação: Ações isoladas sem uma visão integrada.
- Mensuração: Dificuldade em quantificar o "retorno sobre o investimento" em integridade.
- Interferências Externas: Pressões políticas, rotatividade de gestores.

Riscos à integridade

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

O **risco à integridade** é conceituado pela Lei nº 10.993/2019 como “a vulnerabilidade institucional que pode favorecer ou facilitar práticas de corrupção, fraudes, subornos, irregularidades e quaisquer outros desvios éticos e de conduta.”



Características

- Derivam da conduta dos colaboradores da organização (servidores, terceirizados ou estagiários, incluindo membros da alta administração);
- São praticados por meio de dolo (intenção ou má-fé) ou culpa (imperícia, imprudência ou negligência comprovada);
- Envolve uma afronta aos princípios da administração pública: legalidade, impessoalidade, moralidade, publicidade e eficiência;
- Implica alguma forma de deturpação, desvio ou negação da finalidade pública ou do serviço público a ser entregue ao cidadão.

USO INDEVIDO OU MANIPULAÇÃO DE DADOS E INFORMAÇÕES	DESVIO ÉTICO OU DE CONDUTA PROFISSIONAL INADEQUADA	NEPOTISMO	PATRONAGEM
ABUSO DE POSIÇÃO OU PODER EM FAVOR DE INTERESSES PRIVADOS	CONFLITO DE INTERESSES	PRESSÃO INTERNA OU EXTERNA ILEGAL OU ANTIÉTICA PARA INFLUENCIAR AGENTE PÚBLICO	PATROCÍNIOS, VIAGENS E DESPESAS PROMOCIONAIS
SOLICITAÇÃO OU RECEBIMENTO DE VANTAGEM INDEVIDA	UTILIZAÇÃO DE RECURSOS PÚBLICOS EM FAVOR DE INTERESSES PRIVADOS	DESVIO DE PESSOAL OU RECURSOS MATERIAIS	ASSÉDIO E/OU PRECONCEITO NO TRABALHO

Conexão dos riscos à integridade com outras categorias

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Riscos	Relação	Exemplo
Operacionais	Processos mal desenhados, falta de segregação de funções, controles internos fracos ou inexistentes criam oportunidades para desvios de integridade. A complexidade operacional ou a falta de padronização podem esconder condutas antiéticas.	Um processo de aquisição manual com poucas etapas de conferência (risco operacional) pode facilitar o sobrepreço ou o conluio (risco à integridade).
Estratégicos	A falta de integridade pode comprometer a reputação, a confiança das partes interessadas (cidadãos, órgãos de controle, parceiros), e a capacidade da organização de alcançar seus objetivos de longo prazo. Decisões estratégicas baseadas em informações falsas ou tendenciosas também são riscos à integridade que impactam a estratégia.	Escândalos de corrupção (risco à integridade) podem levar à perda de legitimidade de um governo, impactando diretamente a execução de políticas públicas e a confiança social (risco estratégico).
Financeiros	Desvios de integridade quase sempre resultam em perdas financeiras diretas (fraude, desvio de recursos) ou indiretas (multas, custos de investigação, má alocação de verbas).	Fraude em folha de pagamento (risco à integridade) impacta diretamente o orçamento (risco financeiro).
Tecnologia	Sistemas de TI vulneráveis podem ser explorados para manipular dados, desviar informações confidenciais ou cometer fraudes. A falta de controles de acesso e rastreabilidade digital pode facilitar desvios de integridade.	Um sistema de gestão de benefícios sem logs de acesso robustos (risco de tecnologia) pode permitir que um servidor altere dados de beneficiários para desviar pagamentos (risco à integridade e financeiro).

Adequações para a Gestão de Riscos à integridade

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Incluir o ambiente ético, legal e regulatório específico para a integridade no setor público (leis anticorrupção, códigos de conduta, tratados internacionais). Os critérios de risco devem refletir o baixo apetite a riscos de integridade.

Workshops de identificação devem incluir explicitamente a perspectiva de integridade. Não apenas "o que pode dar errado operacionalmente?", mas "como a integridade pode ser comprometida neste processo/decisão?". Utilizar taxonomias de riscos que contemplem a dimensão da integridade.

A comunicação sobre riscos deve ser transparente e envolver todas as partes interessadas, incluindo a alta gestão, servidores e órgãos de controle.

A Matriz Probabilidade x Impacto deve considerar impactos específicos da integridade, como dano reputacional, perda de confiança pública, implicações éticas e legais, além dos impactos financeiros e operacionais. A avaliação deve refletir o apetite ao risco de integridade.

Monitorar não apenas a ocorrência de eventos de risco, mas também a eficácia dos controles de integridade, a percepção da cultura de integridade na organização e a adesão aos códigos de conduta.

As opções de tratamento devem buscar mitigar a raiz das vulnerabilidades à integridade. Priorizar controles que fortaleçam a cultura ética.

Critérios de impacto para riscos à integridade

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Nível	Critérios para avaliação do impacto					
	Dano reputacional	Perda de Confiança Pública	Implicações Éticas	Implicações Legais	Impactos Financeiros	Impactos Operacionais
Muito Baixo	Insignificante ou nulo	Nula	Não há violação de princípios éticos	Nulas	<0,1% Orçamento anual	Nulos ou facilmente remediados
Baixo	Localizado, reversível. Pouca atenção da mídia	Limitada, rápida recuperação	Pequenas falhas internas	Pequenas não-conformidades, sem multas significativas (< R$10.000)	0,1% - 0,5% Orçamento anual	Pequenas disrupções, resolvidas com recursos existentes
Moderado	Relevante regional/setorial. Possível atenção da mídia local	Perceptível, requer plano de comunicação.	Violação de princípios éticos estabelecidos	Infrações regulatórias, multas moderadas (R$10.000 - R$100.000)	0,5% - 2% Orçamento anual	Interrupção de processos-chave por um período.
Alto	Grave, nacional/internacional, ampla cobertura de mídia, impacto duradouro	Substancial, dificuldade de recuperação a longo prazo	Violação grave de códigos de conduta	Processos, investigações, multas pesadas (> R$100.000), suspensão de licenças.	2% - 5% Orçamento anual	Paralisação de operações críticas, perda de produtividade
Muito Alto	Catastrófico e irreversível, ameaça à continuidade	Total, inviabilizando negócios essenciais	Colapso da cultura de integridade, evidência de má-fé generalizada	Ações penais, dissolução da empresa, multas bilionárias, prisões	> 5% Orçamento anual	Colapso completo das operações, encerramento de atividades

Tratando riscos à integridade

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

EVITAR → Reformular processos, descontinuar programas de alto risco, não se envolver em parcerias com histórico de falta de integridade.

REDUZIR

- **PREVENÇÃO** → Políticas claras, segregação de funções, alçadas de aprovação, automatização de processos, treinamento, *due diligence* de fornecedores, códigos de conduta.
- **DETECÇÃO** → Auditorias internas e externas, canais de denúncia (Ouvidorias), monitoramento de transações, análise de dados.
- **CORREÇÃO** → Plano de resposta a incidentes, processos disciplinares, recuperação de ativos, comunicação de crise.

CONTROLES EM NÍVEL DE ENTIDADE

COMPARTILHAR → Acordos de cooperação com órgãos de controle (CGU, MP), contratação de seguros (para perdas financeiras advindas de fraude, por exemplo), garantias contratuais.

ACEITAR → Aceitar o risco residual (aquele que permanece após o tratamento) se estiver dentro do apetite e tolerância, e se o custo de tratamento for desproporcional.

Fatores de riscos x Controles

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Fator de risco	Controle em nível de Entidade						
	Preventivo		Detectivo			Corretivo	
	Código de Ética	Normas e Políticas	Ouvidoria	Transparência	Auditoria Interna	PAD	PAR
Uso particular de bens públicos	X	X	X		X	X	
Má Gestão de Estoques e Ativos (e.g., perdas por obsolescência, vencimento)	X	X	X	X	X	X	
Medição/Pagamento de Serviços Não Executados (e.g., medições falsas)	X	X	X	X	X	X	X
Uso de Informação Privilegiada	X		X		X	X	X
Extorsão (e.g., fiscal que exige "colaboração" para não multar)	X		X		X	X	

Fator de risco	Controle em nível de Processo		
	Preventivo	Detectivo	Corretivo
Uso particular de bens públicos	Elegibilidade para uso de veículo/formulário de utilização de veículos	Relatório de consumo e quilometragem / TAG de utilização / rastreamento	Revisão das permissões para uso de veículo / Ajustes de procedimentos
Má Gestão de Estoques e Ativos (e.g., perdas por obsolescência, vencimento)	Política de estoque mínimo e ressuprimento / FIFO	Relatórios de movimentação de estoques / inventários periódicos	Ajustes nas políticas de estoques / substituição de gestor
Medição/Pagamento de Serviços Não Executados (e.g., medições falsas)	Duplo grau para aprovação de medições / sistemas informatizados de aprovação	Inspeções de campo / Acompanhamento do ritmo do desembolso contratual	Revisão de parâmetros de aprovação / reescalonamentos de cronograma
Uso de Informação Privilegiada	Perfis de acesso a informações /	Revisão de acesso por perfis / rastreio de logs	Corte de acessos não autorizados e/ou
Extorsão (e.g., fiscal que exige "colaboração" para não multar)	Sistemas automatizados de fiscalização / rotina de duplas de fiscalização	Relatórios de produtividade de fiscalização / estatísticas por segmento e/ou região	Rotação de fiscal por região segmento / Ajustes de procedimentos

Riscos à integridade x Decreto 1595/05 e LC 46/94

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

N°	RISCO DE INTEGRIDADE	DESCRIÇÃO	Decreto nº 1.595-R/2005	LC nº 46/94
R01	NEPOTISMO	Nomeação, designação, contratação ou alocação de familiar de Secretário de Estado ou de ocupante de cargo em comissão ou função de confiança para exercício de cargo em comissão ou função de confiança ou para prestação de serviços no órgão.	Art. 4º, IV	Art. 221, IV
R02	CONFLITO DE INTERESSES	Caracteriza-se pelo exercício de atividades Incompatíveis com as atribuições do cargo, intermediação indevida de interesses privados, concessão de favores e privilégios ilegais a pessoa jurídica e recebimento de presentes/vantagens.	Art. 2º, IX; Art. 4º, X; Art. 8º; Art. 9º; Art. 10; Art. 12	Art. 221, XV, XIX XXVI
R03	PRESSÃO INTERNA OU EXTERNA ILEGAL OU ANTIÉTICA PARA INFLUENCIAR AGENTE PÚBLICO A ATUAR DE MANEIRA PARCIAL OU SEM AUTONOMIA TÉCNICA.	Ser influenciado a agir de maneira parcial por pressões internas ou externas indevidas. Normalmente ocorridas entre pares, por abuso de poder, por tráfico de influência ou constrangimento ilegal.	Art. 3º; Art. 14, II, III, IV, V; Art. 2º, X, XV	Art. 221, VII, IX, X
R04	CONDUTA PROFISSIONAL INADEQUADA	Deixar de realizar as atribuições conferidas com profissionalismo, honestidade, imparcialidade, responsabilidade, seriedade, eficiência, qualidade e/ou urbanidade.	Art. 2º, II, III, IV, VI, VII, IX, XII, XIV, XVI, XVII; Art. 4º, III, IX, XII, XV; Art. 12	Art. 25, 26 e 27, 29; Art. 39, §2º; Art. 40; Art. 45; Art. 53; Art. 220; Art. 221, I, III, IV, XII, XIII, XIV, XVI, XXI
R05	USO INDEVIDO DE AUTORIDADE CONTRA O EXERCÍCIO PROFISSIONAL, O PATRIMÔNIO E A HONRA	Atentar contra a honra ou o patrimônio ou contra o exercício profissional com abuso ou desvio do poder hierárquico ou sem competência legal.	Art. 2º, X, XV	
R06	USO INDEVIDO E/OU MANIPULAÇÃO DE DADOS E INFORMAÇÕES	Caracteriza-se pela divulgação ou uso indevido de dados ou informações, alteração indevida de dados/informações ou restrição de publicidade/acesso a dados/informações.	Art. 2º, V; Art. 4º VI, XI, XIV	Art. 221, VII, XXV
R07	DESVIO DE PESSOAL E/OU RECURSOS MATERIAIS	Desviar ou utilizar, em obra ou serviço particular, veículos, máquinas, equipamentos ou material de qualquer natureza, de propriedade ou à disposição de entidades públicas, bem como o trabalho de servidores públicos, empregados ou terceiros contratados por essas entidades para fins particulares ou para desempenho de atribuição que seja de sua responsabilidade ou de seu subordinado.	Art. 2º, XI, Art. 4º, II, IX; Art. 5º; Art. 6º; Art. 7º	Art. 221, V
R08	INTERFERÊNCIAS EXTERNAS E/OU POLÍTICAS E/OU ALTERAÇÕES NO CENÁRIO POLÍTICO	Relacionados com mudanças de governo e/ou de políticas de governo que possam implicar em supressão de atribuições, esvaziamento do órgão e/ou desaparelhamento por falta de recursos.	Art. 14, II, III, IV, V	
R09	CORRUPÇÃO, FRAUDE OU EMPREGO IRREGULAR DE VERBAS PÚBLICAS	Solicitação de recebimento de vantagem indevida, abuso de posição ou poder em favor de interesses privados, ilícitos contra a administração pública, previstos no ordenamento jurídico nacional, como, por exemplo, no Código Penal ou em leis específicas.	Art. 4º, I, V, VII, VIII, XI, XII, XIII, XIV; Art. 11	Art. 221, XI, XVIII, XXI, XXII, XXIII
R10	ASSÉDIO E/OU PRECONCEITO NO TRABALHO	Representado por situações de assédio moral ou sexual e preconceito de raça, gênero, religião, origem ou orientação sexual. ·Assédio moral: expor de forma prolongada e repetitiva os servidores a situações humilhantes, constrangedoras e vexatórias que podem provocar danos psicológicos e físicos. ·Assédio sexual: constranger com conotação sexual no ambiente de trabalho, em que, como regra, o agente utiliza sua posição hierárquica superior ou sua influência para obter o que deseja.	Art. 2º III, XII, XV; Art. 3º; Art. 4º, III	Art. 221, XIII, XIV, XXVII, XXVIII

Resiliência Organizacional para a Integridade

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Significa não apenas evitar falhas, mas também a capacidade de uma instituição de se recuperar de incidentes de integridade, restaurar a confiança pública, aprender com os erros e emergir mais forte.

Pilares da resiliência.

- **Engajamento da Liderança:** Patrocínio ativo e comunicação constante do topo.
- **Comunicação Clara:** Explicar o "porquê" da gestão de riscos, não apenas o "o quê".
- **Abordagem por Fases:** Implementar gradualmente, começando por áreas de maior risco ou com maior receptividade.
- **Capacitação:** Treinamento contínuo para todos os níveis da organização.
- **Integração:** Inserir a gestão de riscos nos processos e rotinas existentes, e não como uma atividade paralela.
- **Cultura de Reconhecimento:** Celebrar as "pequenas vitórias" e o engajamento dos servidores.
- ***Benchmarking:*** Aprender com outras instituições que já implementaram.

Secretaria de Estado de Controle e Transparência
Subsecretaria de Integridade Governamental e Empresarial

Agenda

- Conceitos
  - Risco
  - Categorias de Risco
  - Controles Internos
  - Gestão de Riscos
  - Estruturas para Gestão de Riscos
  - O Modelo de Três Linhas
- ABNT/ISO 31000
- O Processo de Gestão de Riscos da ISO 31000
- Gestão de riscos à integridade
- Estudo de Caso

Cenários

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Cenário 1:

Uma Ouvidoria de um Tribunal de Justiça recebe várias denúncias anônimas sobre favorecimento em processos seletivos internos para cargos de chefia, onde há relatos de que os critérios de escolha não são claros e que determinados candidatos sempre "se destacam" mesmo com qualificações questionáveis.

Atividade:

- Identificar quais riscos à integridade estão presentes neste cenário.

Cenário 3:

O Departamento de Compras de uma grande prefeitura possui um histórico de atrasos na entrega de materiais e insatisfação de fornecedores. Recentemente, um novo chefe foi nomeado com a missão de modernizar e aumentar a transparência. Ele suspeita de possíveis vulnerabilidades à integridade no processo de aquisição.

Atividades:

- **Identificar** pelo menos 3 riscos à integridade presentes neste processo.
- **Analisar:** Para um dos riscos identificados, atribuir uma probabilidade e um impacto (usando escalas simples: Baixo/Médio/Alto para ambos) e justificar.
- **Avaliar:** Se o apetite da prefeitura para riscos à integridade for "muito baixo", como o risco analisado se posiciona em relação a isso?

Caso prático SES-ALFA (Solução)

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Secretaria Estadual de Saúde Alfa – SES-Alfa

órgão público de grande porte, responsável pela gestão da rede de saúde pública em um estado brasileiro. Sua atuação abrange desde a formulação de políticas de saúde, gestão de hospitais e unidades de saúde, até a aquisição de medicamentos, insumos e equipamentos, e a gestão de recursos humanos para uma força de trabalho de mais de 30 mil servidores. Historicamente, a SES-Alfa enfrentava desafios com processos fragmentados e uma percepção pública de baixa eficiência e vulnerabilidade a escândalos.

Uma taxonomia de riscos foi desenvolvida para categorizar os riscos identificados, incluindo uma categoria primária de "Integridade".

- Estratégicos
- Operacionais
- Financeiros
- Tecnologia
- Conformidade
- Integridade

Riscos identificados

- **Operacional:** Atraso/falha na entrega de medicamentos essenciais por fornecedor
- **Tecnologia:** Vulnerabilidade do sistema de regulação de leitos a manipulações
- **Operacional:** Contratação de pessoal terceirizado sem critérios claros de seleção

Atividade:

- Relacionar os riscos identificados com riscos à integridade
- Relacionar possíveis impactos por categoria de riscos

Risco Identificado	Categoria Principal (Primária)	Dimensão de Integridade / Relação com Outras Categorias	Impactos Potenciais (Integrados)
Atraso/falha na entrega de medicamentos essenciais por fornecedor	Operacional	**Integridade:** Possibilidade de favorecimento a fornecedor específico com atraso (conflito de interesses, fraude), ou desvio de medicamentos.	**Operacional:** Falta de medicamentos, interrupção de tratamento. **Estratégico:** Dano à reputação da SES-Alfa, perda de confiança da população. **Financeiro:** Multas por atraso, custos adicionais para compras emergenciais. **Conformidade:** Violação de contratos, regulamentos de saúde pública. **Integridade:** Corrupção, fraude na cadeia de suprimentos.
Vulnerabilidade do sistema de regulação de leitos a manipulações	Tecnologia	**Integridade:** Possibilidade de servidores alterarem a fila de pacientes para favorecimento (abuso de poder, corrupção).	**Tecnologia:** Quebra de segurança, dados inconsistentes. **Operacional:** Falha na alocação de leitos, atendimento ineficiente. **Integridade:** Favorecimento, corrupção, perda de credibilidade do sistema. **Estratégico:** Percepção de injustiça social, impactos na saúde pública. **Conformidade:** Violação da legislação de transparência e acesso à saúde.
Contratação de pessoal terceirizado sem critérios claros de seleção	Financeiro / Operacional	**Integridade:** Risco de nepotismo, favorecimento, "cabides de emprego", desvio de recursos públicos.	**Financeiro:** Desperdício de recursos, folha de pagamento inflada. **Operacional:** Ineficiência, baixa qualidade dos serviços, desmotivação da equipe. **Integridade:** Nepotismo, uso da máquina pública para fins privados. **Estratégico:** Dano à imagem da instituição, descredibilidade. **Conformidade:** Violação de princípios da administração pública (impessoalidade, moralidade).

Caso prático

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Concessão de benefícios:

O Ministério da Cidadania está prestes a lançar um novo programa de transferência de renda em larga escala. A equipe técnica está focada nos desafios operacionais (logística de pagamentos, cadastro de beneficiários), mas esqueceu de considerar os riscos relacionados à integridade.

Atividade:

- Identificar os riscos à integridade que estão presentes neste cenário.
- Indique ações para o tratamento dos riscos

Requisitos de resposta:

1. Risco:
2. Por que ocorre:
3. Impactos
4. Ações para tratamento

Caso prático – Ministério da Cidadania (Solução)

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

#	Risco	Fator de risco	Impactos	Ações de tratamento
A	**Fraud**e por meio do Cadastro indevido e "beneficiários fantasmas"	Pressão por volume/velocidade, validações frágeis, ausência de cruzamentos com bases oficiais	Desvio de recursos, baixa legitimidade pública, responsabilização dos gestores	Definir conjunto mínimo de validações cadastrais (CPF, óbito, renda, vínculos empregatícios, base de benefícios sociais) Bloqueio de pagamento em casos de inconsistência até revisão. Amostragem estratificada de 5% dos cadastros aprovados.
B	**Captura** política/local e favorecimento indevido	Intermediários informais, assimetrias de poder em municípios, comitês de elegibilidade sem transparência	Direcionamento de benefícios, fraudes em massa localizadas, dano reputacional.	Definir governança com papéis separados (quem indica não decide; quem decide não executa) Publicar critérios de elegibilidade em linguagem simples; criar canal de denúncias independente com SLAs. Canal de denúncias independente com SLA de triagem em 72 horas.
C	**Uso indevido de dados pessoais e vazamentos**	Grande volume de dados sensíveis, integrações apressadas, acessos excessivos	Violação à LGPD, danos a cidadãos, sanções administrativas	Privacy by design no fluxo: minimização de dados, segregação de ambientes, logs de acesso, DPO envolvido. Testes de segurança nas integrações (pentest, varredura de vulnerabilidades). Termo de responsabilidade e treinamento específico de proteção de dados para todos que acessam o sistema.
D	**Corrupção** em contratações de meios de pagamento e TI	Especificações direcionadas, competição limitada, pagamentos por volume sem controle	Superfaturamento, contratos ineficientes, dependência tecnológica	Matriz de riscos na fase de planejamento da contratação; triagem de integridade de fornecedores (sanções, PEPs). Comitê técnico com atas públicas de decisões. Cláusulas anticorrupção, auditorias independentes e indicadores de desempenho no contrato
E	**Conflitos de interesses e nepotismo** em pontos de atendimento	Agentes locais com vínculos familiares/comunitários, supervisão fraca	Preterição de elegíveis, inclusão indevida de aliados, erosão da confiança.	Declaração de conflito de interesses obrigatória; rodízio de funções; duplo controle para casos sensíveis. Treinamento objetivo e casos práticos; cartazes e QR Codes para denúncias no local de atendimento
F	Viés e **discriminação** nos critérios de elegibilidade	Regras ou modelos que excluem grupos vulneráveis sem justificativa técnica	Violações de princípios constitucionais, judicializações, reputação	Testes de viés nos critérios e simulações de impacto; comitê ético-técnico para revisar efeitos adversos. Pilotos controlados e ajustes iterativos antes do lançamento pleno

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

SECRETARIA DE ESTADO DE CONTROLE E TRANSPARÊNCIA – SECONT

Av. João Batista Parra, nº 600,
Ed. Aureliano Hoffman, 10º andar.
Enseada do Suá. Vitória, ES.

Tel.: (27) 3636-5352

Secretário de Estado de
Controle e Transparência
Edmar Moreira **Camata**
secretario@secont.es.gov.br

Subsecretário de Integridade
Governamental e Empresarial
Alexandre Del'Santo **Falcão**
subint@secont.es.gov.br

Coordenação de Promoção e
Avaliação da Integridade
Guilherme A. Machado Jr.
guilherme.junior@secont.es.gov.br