



# Gestão de Riscos na Administração Pública



# PROFESSOR RESPONSÁVEL

## Prof. Rodrigo Fontenelle

- Auditor Federal de Finanças e Controle da CGU, atualmente é **Controlador-Geral do Estado de MG** e Presidente do **Conselho Nacional de Controle Interno - CONACI**, biênio 2022-2023.
- Foi **Conselheiro de Administração** da Novacap, Hemobrás, INB e Casa da Moeda e **presidente do Conselho Fiscal** do BDMG.
- **Mestre em Contabilidade** (UnB). Pós-graduado em Finanças (Ibmec) e Auditoria Financeira (UnB/TCU). Bacharel em Ciências Econômicas pela UFMG.
- Professor da **Fundação Dom Cabral**, também atua como instrutor e mentor para altos executivos na ENAP.
- **Autor** dos livros *Implementando a Gestão de Riscos no Setor Público* (Ed. Fórum, 2ª edição) e *Auditoria Privada e Governamental* (Ed. Impetus, 4ª edição).
- Possui **cinco certificações internacionais**: CGAP, CIA, CCSA e CRMA, emitidas pelo *The Institute of Internal Auditors* (IIA) e ISO 37001 e 37301, pela Tradius.

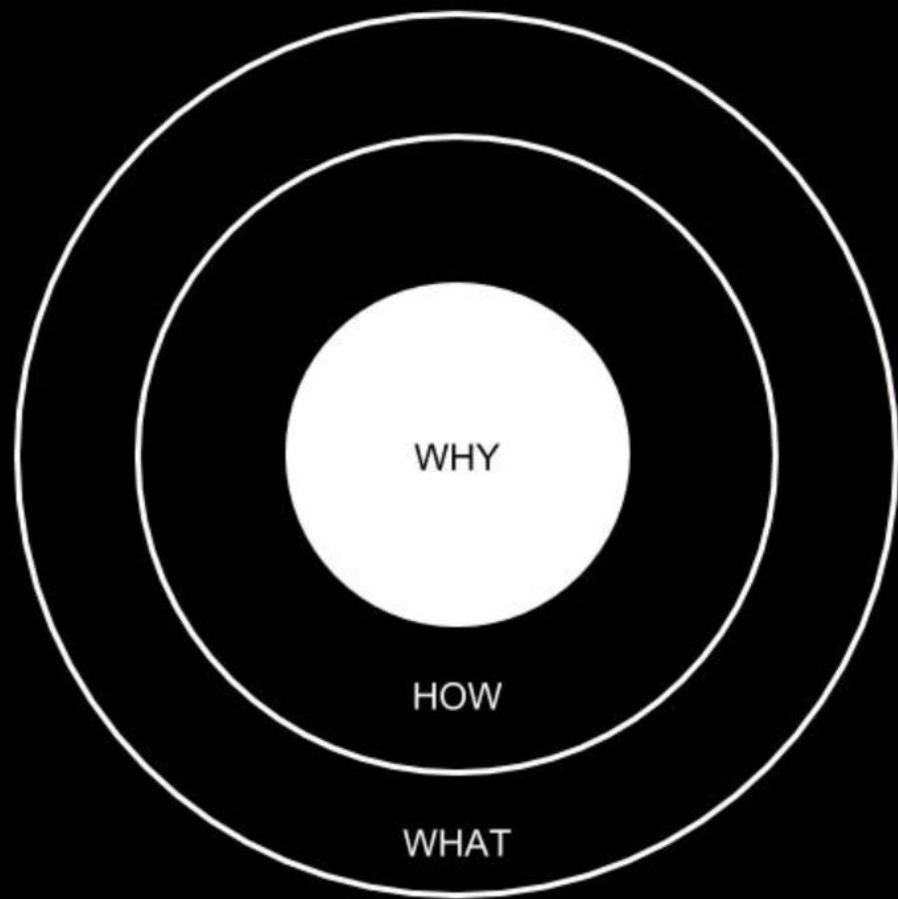
1

**Por que eu  
preciso disso?**

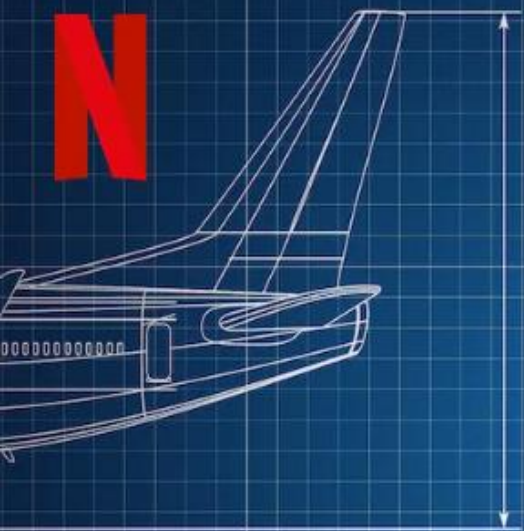


**Por que estamos aqui hoje?**

**Promover educação de excelência, sendo pública, gratuita e laica, por meio da indissociabilidade do ensino, da pesquisa e da extensão, resultando na formação de pessoas capazes de intervir de modo responsável na sociedade.**



**N**

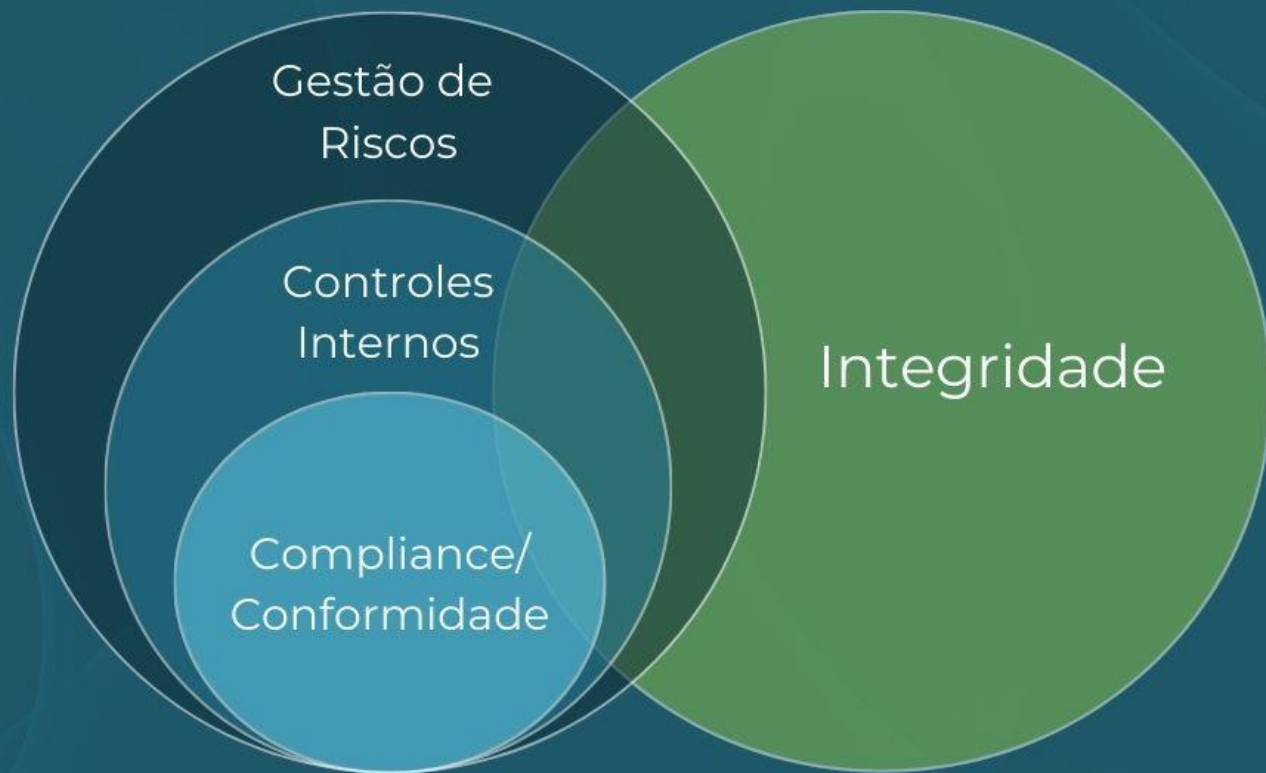


ANGLE OF  
ATTACK SENSOR  
OUTPUT 747

# DOWNFALL

THE CASE AGAINST BOEING

## Interação entre instrumentos de governança





# 2

## Principais legislações

# IN MP/CGU Nº01/16



# Decreto Nº 9.203/17

Política de Governança  
da Administração Pública



# LEI 14.133/21



A alta administração do órgão ou entidade é responsável pela governança das contratações e deve implementar processos e estruturas, **inclusive de gestão de riscos e controles internos**, para avaliar, direcionar e monitorar os processos licitatórios e os respectivos contratos, com o intuito de alcançar os objetivos estabelecidos no caput deste artigo, promover um ambiente íntegro e confiável, assegurar o alinhamento das contratações ao planejamento estratégico e às leis orçamentárias e promover eficiência, efetividade e eficácia em suas contratações.

As contratações públicas deverão submeter-se a práticas contínuas e permanentes de gestão de riscos e de controle preventivo, inclusive mediante adoção de recursos de tecnologia da informação, e, além de estar subordinadas ao controle social, sujeitar-se-ão às seguintes linhas de defesa:

I - primeira linha de defesa, integrada por servidores e empregados públicos, agentes de licitação e autoridades que atuam na estrutura de governança do órgão ou entidade;

II - segunda linha de defesa, integrada pelas unidades de assessoramento jurídico e de controle interno do próprio órgão ou entidade;

III - terceira linha de defesa, **integrada pelo órgão central de controle interno da Administração** e pelo tribunal de contas.



## Primeira Linha

Servidores e  
Empregados Públicos

Agentes de Licitação

Autoridades  
de Governança



## Segunda Linha

Unidades de  
Assessoramento  
Jurídico

Unidades de  
Controle Interno



## Terceira Linha

Órgão Central de  
Controle Interno

Tribunal de Contas

# 3

## Conceitos e fundamentos



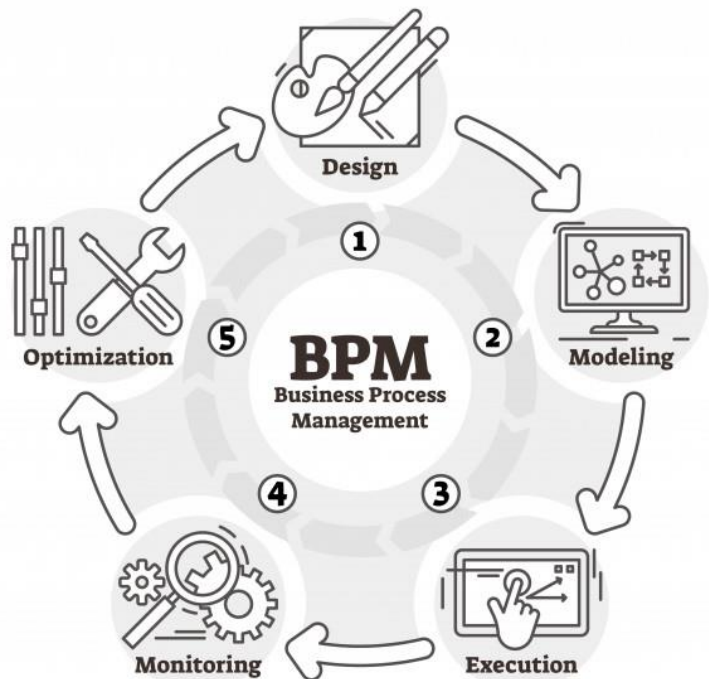
# Todos nós fazemos Gestão de Riscos



# Processo sem Gestão de Riscos



# Por que falar em Riscos?



“Vamos viver diante de mudanças imprevisíveis e instabilidade por um longo tempo – talvez para sempre. Em ambientes assim, **tem mais resultado quem mantém uma disciplina extraordinária**. As empresas que se preparam para o pior antecipadamente.”

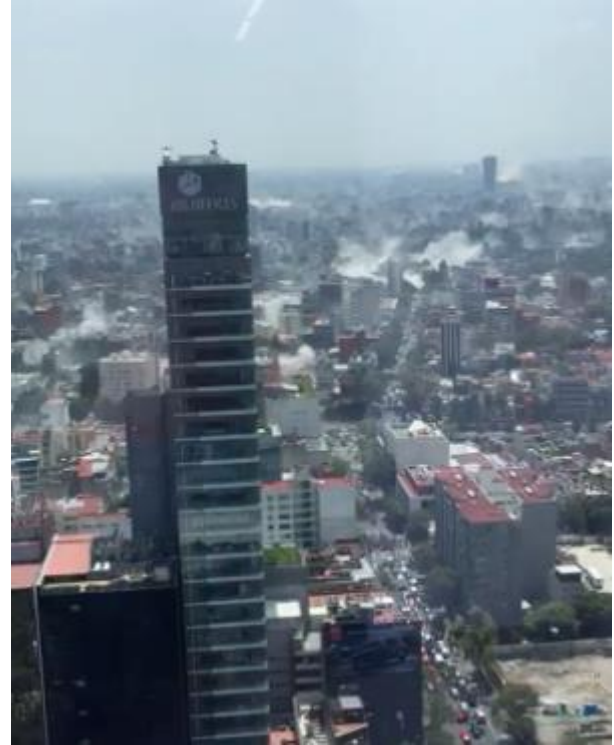
*Jim Collins*

Efeito da incerteza nos objetivos (ISO 31000).



Evento futuro e incerto que, caso ocorra, pode impactar negativamente o alcance dos objetivos da organização (COSO ERM).

# Probabilidade X Impacto



Precisamos apenas de:

A word cloud featuring the word 'Target' in various languages and scripts. The words are arranged in a cluster, with 'Target' being the largest and most prominent. Other words include 'Meta', 'Objetivo', 'Objectif', 'Doel', 'Цель', '目標', 'Ziel', 'στόχος', 'ΤΥ', and 'Propositum'. The words are in various colors, including shades of blue, green, and black. Some words have small Japanese characters next to them, such as 'ターゲット' (target) and 'トターゲット' (to target).

Propositum  
Obbiettivo  
Target  
Meta  
Objectif  
Doel  
Цель  
目標  
Ziel  
στόχος  
ΤΥ  
ターゲット  
トターゲット

# Apetite a Riscos



# Conceito

“O apetite a risco é a quantidade de riscos, no sentido mais amplo, que uma organização está disposta a aceitar em sua busca para agregar valor.” (COSO ERM)



“Expressão ampla de quanto risco uma organização está disposta a enfrentar para implementar sua estratégia, atingir seus objetivos e agregar valor para as partes interessadas , no cumprimento de sua missão.” (TCU 2018)



# Teoria

## Alto Appetite a Riscos



## Baixo Appetite a Riscos



# Prática

Matriz da CGU

IMPACTO	Muito Alto 10	10 RM	20 RM	50 RA	80 RE	100 RE
	Alto 8	8 RB	16 RM	40 RA	64 RA	80 RE
	Médio 5	5 RB	10 RM	25 RM	40 RA	50 RA
	Baixo 2	2 RB	4 RB	10 RM	16 RM	20 RM
	Muito Baixo 1	1 RB	2 RB	5 RB	8 RB	10 RM
		Muito Baixa 1	Baixa 2	Média 5	Alta 8	Muito Alta 10
		PROBABILIDADE				

Matriz do MPDG

IMPACTO	Catastrófico 5	Risco Moderado	Risco Alto	Risco Crítico	Risco Crítico	Risco Crítico
	Grande 4	Risco Moderado	Risco Alto	Risco Alto	Risco Crítico	Risco Crítico
	Moderado 3	Risco Pequeno	Risco Moderado	Risco Alto	Risco Alto	Risco Crítico
	Pequeno 2	Risco Pequeno	Risco Moderado	Risco Moderado	Risco Alto	Risco Alto
	Insignificante 1	Risco Pequeno	Risco Pequeno	Risco Pequeno	Risco Moderado	Risco Moderado
		1	2	3	4	5
		Muito baixa	Baixa	Possível	Alta	Muito alta
		PROBABILIDADE				

# 4

## Mitos e verdades

# FAKENEWS

## Mitos e Verdades

- Modismo **FAKE**
- Exterminador de Corrupção **FAKE**
- “Coisa” de Órgãos de Controle **FAKE**
- + Trabalho **FAKE**

Fonte: Miranda (2021)

# PERCEPÇÃO SOBRE GESTÃO DE RISCOS

“Mesmo que por vezes não apareça,  
a **Gestão de Riscos** pertence ao processo”.



## Processo com Gestão de Riscos



5

# Modelo de 3 linhas

**“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 GERENCIAMENTO DE RISCOS E CONTROLES, APLICÁVEL A QUALQUER ORGANIZAÇÃO – NÃO IMPORTANDO O SEU TAMANHO OU A SUA COMPLEXIDADE – AINDA QUE NÃO EXISTA UMA ESTRUTURA OU SISTEMA FORMAL DE GESTÃO DE RISCOS” (TCU, 2017).**



## O Modelo das Três Linhas do The IIA



LEGENDA

↑ Prestação de contas, reporte

↓ Delegar, orientar, recursos, supervisão

↔ Alinhamento, comunicação, coordenação, colaboração

**Papéis do corpo administrativo**

O corpo administrativo garante estruturas e processos adequados, objetivos e atividades alinhados aos interesses, delega responsabilidades e recursos a gestão, estabelece e supervisiona função de auditoria interna.

**Papéis da terceira linha**

A auditoria interna presta avaliação e assessoria independentes e objetivas sobre a adequação e eficácia da governança e do gerenciamento de riscos.

**Criando e protegendo valor**

Todos os papéis que trabalham juntos contribuem coletivamente para a criação e proteção de valor quando estão alinhados entre si e com os interesses prioritizados dos stakeholders.

1

**Governança**

A governança de uma organização requer estruturas e processos apropriados que permitam prestação de contas por parte de um corpo administrativo, ações da gestão, avaliação e assessoria por uma função de auditoria interna independente.

2

**Gestão e os papéis da primeira e segunda linhas**

A responsabilidade da gestão de atingir os objetivos organizacionais compreende os papéis da primeira e segunda linhas.

3

4

**A independência da terceira linha**

A independência da auditoria interna em relação a responsabilidades da gestão é fundamental para sua objetividade, autoridade e credibilidade.

5

6



## GESTÃO

## AUDITORIA INTERNA

## Papéis de primeira linha



**Liderar e dirigir ações** (incluindo gerenciamento de riscos) e aplicação de recursos para atingir os objetivos da organização.



**Manter um diálogo contínuo** com o corpo administrativo e **reportar resultados** planejados, reais e esperados, vinculados aos objetivos da organização; e riscos.



**Estabelecer e manter estruturas e processos** apropriados para o gerenciamento de operações e riscos (incluindo controle interno).



**Garantir a conformidade** com as expectativas legais, regulatórias e éticas.

**Fornecer expertise complementar**, apoio, monitoramento e questionamento quanto ao gerenciamento de riscos, incluindo: 1) desenvolvimento, implantação e melhoria contínua das práticas de gerenciamento de riscos nos níveis de processo, sistemas e entidade; 2) o atingimento dos objetivos de gerenciamento de riscos como: conformidade; controle interno e outros.



**Fornecer análises e reportar** sobre a adequação e eficácia do gerenciamento de riscos (incluindo controle interno).



## Papéis de segunda linha



@somosauditores



**Mantém a prestação de contas primária** perante o corpo administrativo e a **independência** das responsabilidades da gestão.

**Comunica avaliação e assessoria independentes e objetivas** à gestão e ao corpo administrativo sobre a adequação e eficácia da governança e do gerenciamento de riscos, para apoiar o atingimento dos objetivos organizacionais e promover e facilitar a melhoria contínua.



**Reporta** ao corpo administrativo **prejuízos à independência e objetividade** e implanta salvaguardas conforme necessário.



@somosauditores

PRESTADORES EXTERNOS DE AVALIAÇÃO



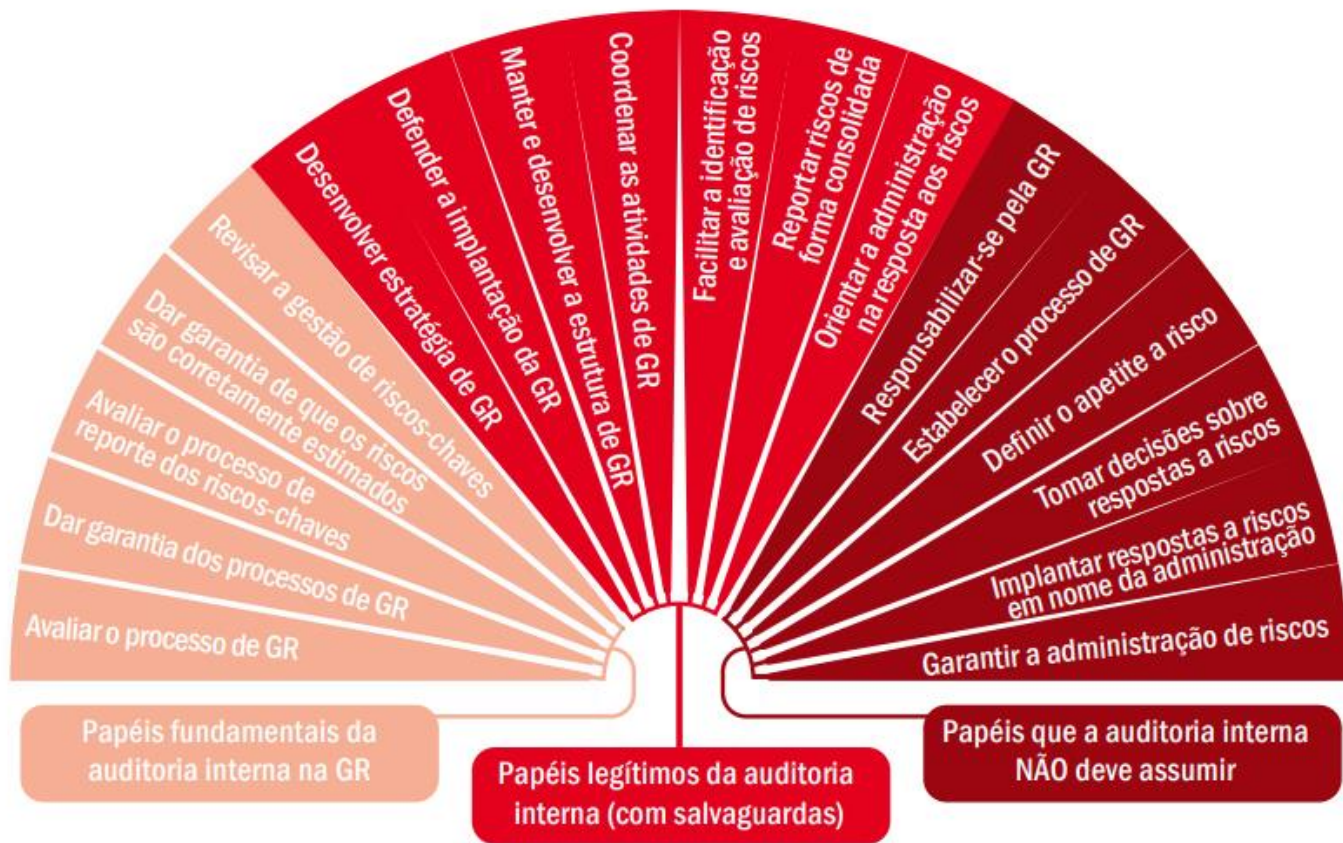
**Prestam avaliação adicional para:**

<p>Cumprir com as expectativas legislativas e regulatórias que servem para proteger os interesses dos stakeholders.</p>	<p>Atender aos pedidos da gestão e do corpo administrativo para complementar as fontes internas de avaliação.</p>
---	---

@somasauditores



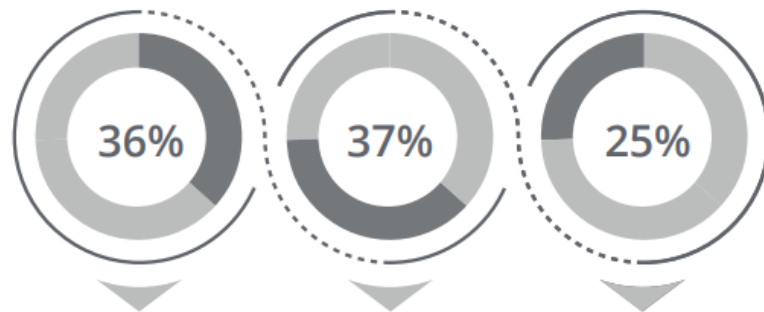
@somasauditores



TCU (2018), adaptado de IIA (2009)

# Modelo de Três Linhas – Maturidade

Maturidade do modelo das três linhas



Em implementação

Estabelecido

Amadurecido

<p><b>1ª linha</b> Média e alta gestão das áreas de apoio e de negócios</p>	<p>Excesso de confiança nas gerências</p>	<p>Gerências carecem de propriedade para riscos e controles</p>	<p>Tem responsabilidade ativa na gestão de riscos e inicia o monitoramento de controles</p>
<p><b>2ª linha</b> Gestão de riscos, canal de denúncias, controles internos e conformidade</p>	<p>Imaturidade em atividades de supervisão</p>	<p>Não possuem um monitoramento de conformidade eficaz</p>	<p>Visão holística e expandida na identificação de riscos emergentes</p>
<p><b>3ª linha</b> Auditoria interna</p>	<p>Independente e objetiva, mas com asseguarção insuficiente</p>	<p>Esta é a principal fonte de asseguarção</p>	<p>Esforços de asseguarção duplicados</p>



Se você é de primeira linha de defesa, **não transfira sua responsabilidade primária sobre um risco**, ouça com atenção os pareceres do colega de segunda linha e tome decisões que otimizem o valor da empresa em longo prazo; se você atua na segunda linha, respeite a responsabilidade do colega e suas decisões, mas **faça sua voz ser ouvida e nunca se omita**.

Nutini, Marco Antonio. Risco não é um número: Como evitar a banalização e a burocratização do processo de gestão de riscos (p. 94). Edição do Kindle.



# O PAPEL DO LÍDER



# Cultura de Riscos: o legado de Paul O’neill, zerar o risco operacional

“Pensei no básico: Todos merecem sair do trabalho tão ilesos como chegaram, certo? Foi nisso que eu me concentrei, propor que os indivíduos desta empresa concordem em se tornar parte de algo importante: **dedicar-se a criar um hábito de excelência.**”

(Em visita a uma fábrica do grupo)

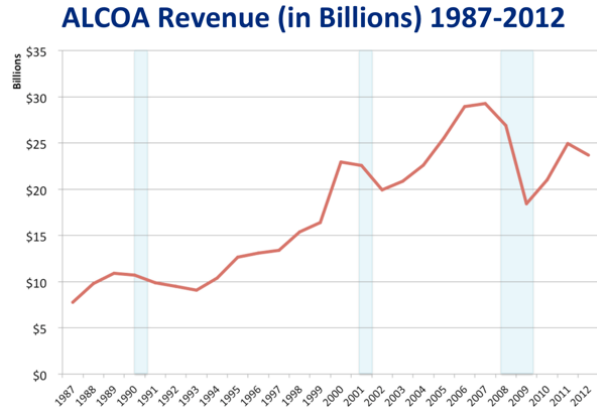
Créditos: Prof. Dr. Oliviero Roggi



# Cultura de Riscos: o legado de Paul O'neill

*"I intend to make Alcoa the safest Company in America. I intend to go for **ZERO INJURIES**"*

**Speech at Wall Street shareholders in 1987**



Créditos: Prof. Dr. Oliviero Roggi



# Cultura de Riscos: o legado de Paul O'Neill

Em suas ações, O'Neill disponibilizou seu contato direto para estar integralmente disponível às pessoas.

## REFLEXÃO:

- Estamos deixando os canais abertos e claros para ouvir a respeito de riscos?
- Estamos dispostos a ouvir, falar e ser exemplo em gestão de riscos para os demais?

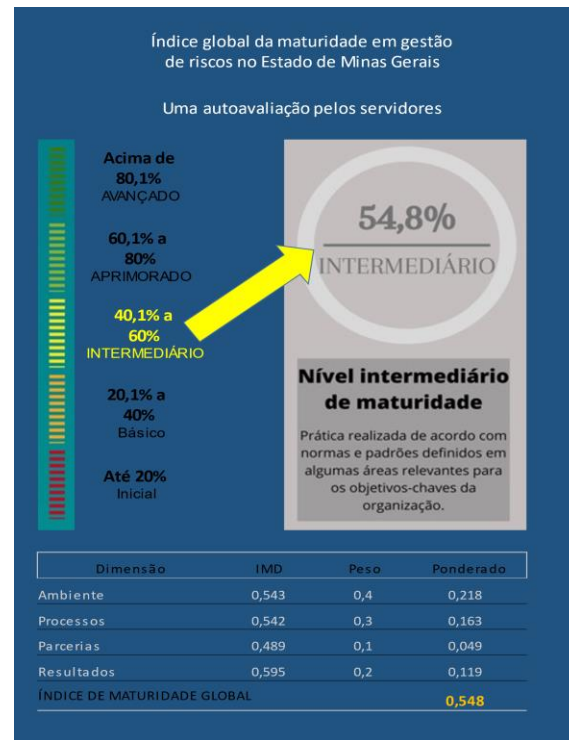
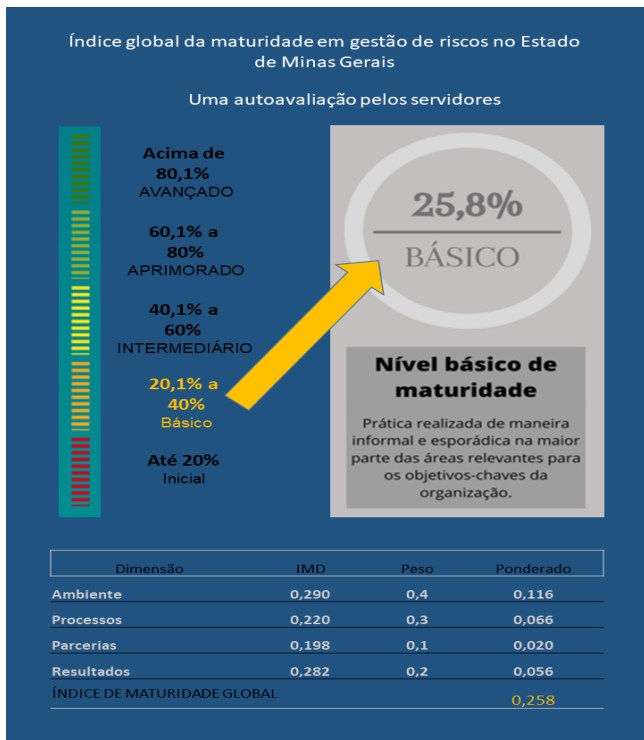
Créditos: Prof. Dr. Oliviero Roggi



# 6

## Casos de sucesso

# Caso Minas Gerais



# Minas Consciente



# Minas Consciente

**MINAS  CONSCIENTE**  
RETOMANDO A ECONOMIA DO JEITO CERTO



**Onda vermelha**  
serviços essenciais



**Onda amarela**  
serviços não  
essenciais



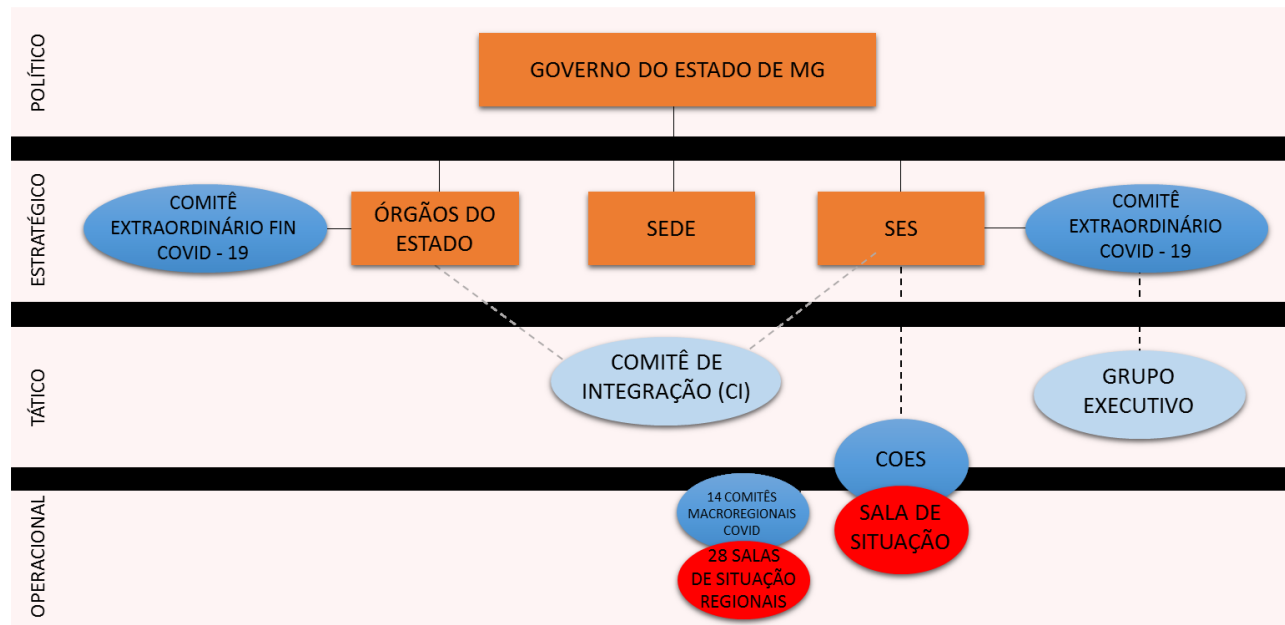
**Onda verde**  
serviços não  
essenciais com alto  
risco de contágio





# Minas Consciente

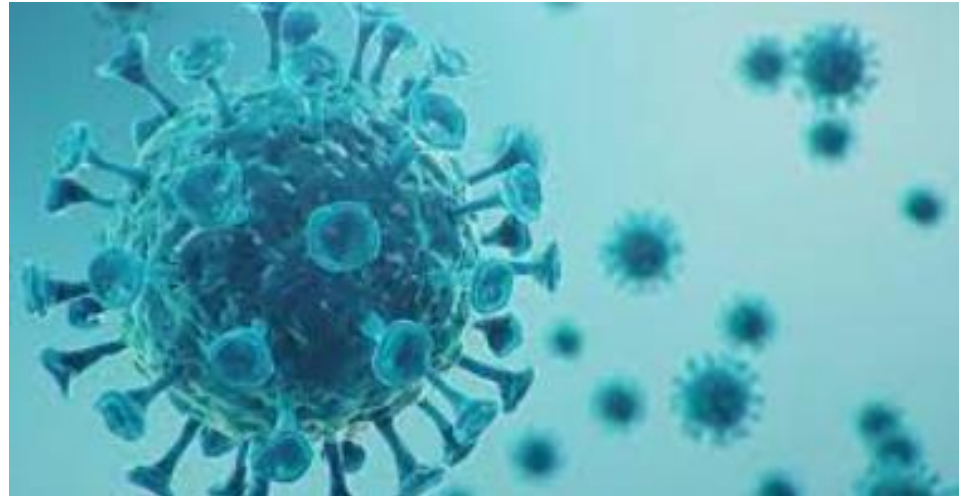
## Estrutura de Governança do Plano Minas Consciente



# Gestão de Riscos COVID 19



# Gestão de Riscos Covid-19



## Duas frentes principais de atuação



**Força Tarefa**

Novos dados sobre a **COVID-19** em MG disponibilizados em **formato aberto**



## Auxílio ao Gestor

**CGE-MG disponibiliza  
Roteiro de Consultoria  
sobre Riscos em  
Contratações**



**BOAS PRÁTICAS EM  
COMPRAS PÚBLICAS  
EMERGENCIAIS NO  
CONTEXTO DA  
PANDEMIA DE  
COVID-19**



CONTROLADORIA-GERAL  
DO ESTADO



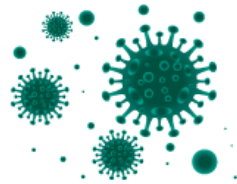
**MINAS  
GERAIS**

GOVERNO  
DIRETENTE  
SÉRIOSO  
EFICIENTE

**PERGUNTAS E  
RESPOSTAS  
SOBRE  
CONTRATAÇÕES  
EMERGENCIAIS**

CONTROLADORIA  
GERAL DO ESTADO  
DE MINAS GERAIS





**ARCCO realiza  
pente fino em  
recursos para  
combate à  
pandemia**



## Força-tarefa

- Criada em 23/03/2020.
- **Coordenação:** AUGE.
- **Membros:** Controladorias Setoriais: Saúde; Planejamento e Gestão; Desenvolvimento Social; e Segurança Pública. Controladorias Seccionais: FHEMIG; Hemominas; FUNED; IPSEMG; IPSM; UNIMONTES; CBMMG e PMMG.
- **Objetivo:** auxiliar a Alta Administração na mitigação dos riscos das aquisições de bens e serviços para o combate à pandemia do Covid-19 e integrar as atividades de auditoria interna dos órgãos e entidades envolvidos diretamente com as contratações emergenciais.
- **Periodicidade das reuniões:** semanais (alinhamento das ações, integração dos membros e compartilhamento de experiências e de documentos de auditoria).

- Elaboração de Matriz Consolidada dos Riscos envolvidos nos processos de contratação por emergência: classificação dos riscos identificados pela Força Tarefa;

Consequência	Avaliação do Risco			
Muito Relevante	Médio	Alto	Extremo	Extremo
Relevante	Baixo	Médio	Alto	Extremo
Pouco relevante	Insignificante	Baixo	Médio	Alto
Irrelevante	Insignificante	Insignificante	Baixo	Médio
	Raríssima	Rara	Eventual	Frequente
	Probabilidade			



## Força-tarefa

**GT de Levantamentos  
de Empresas/ Contratos/ Licitações  
(80 municípios)**



**GT de Investigação  
de Empresas/ Contratos/ Licitações  
da administração pública federal,  
estadual e municipal no  
Estado de Minas Gerais**



**14 trilhas de auditoria  
(tipologias)**

**Estratificação das  
empresas/fornecedores:**

100 Mil Reais

1 Milhão de Reais

Acima de 1 milhão de Reais



**Identificação/Divisão das contratações**

- Estaduais (CGE-MG e PCMG)
- Municipais (TCE-MG; MPE-MG; MPC-MG)
  - Do Município de BH: CGTM-BH
- Federais (CGU-MG; TCU; MPF; RFB)

**Investigação e  
Compartilhamento de  
Informações**



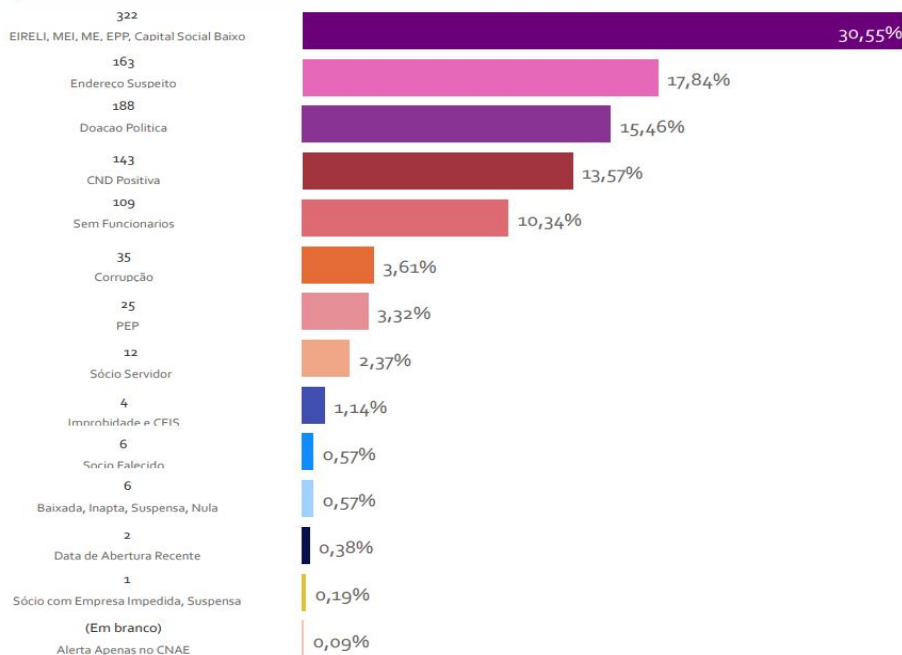


# Força-tarefa

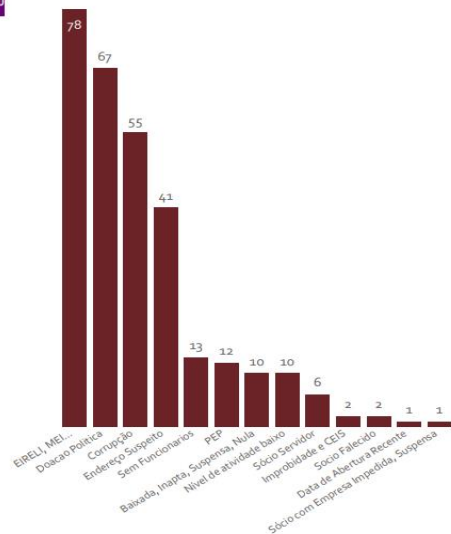


## PAINEL - ARCCO

INDÍCIOS



Nº de Índícios contratos acima de R\$1.000.0000,00



# Gerenciamento de Riscos

[www.rodrifontenelle.com.br](http://www.rodrifontenelle.com.br)

# 1

# Analizando o ambiente



1ª - Análise de Ambiente  
Interno/Externo e Fixação dos Objetivos



2ª - Identificação de Eventos de Riscos



3ª - Avaliação de Riscos e Controles



4ª - Resposta a Riscos e Plano de Ação



5ª - Informação, Comunicação  
e Monitoramento

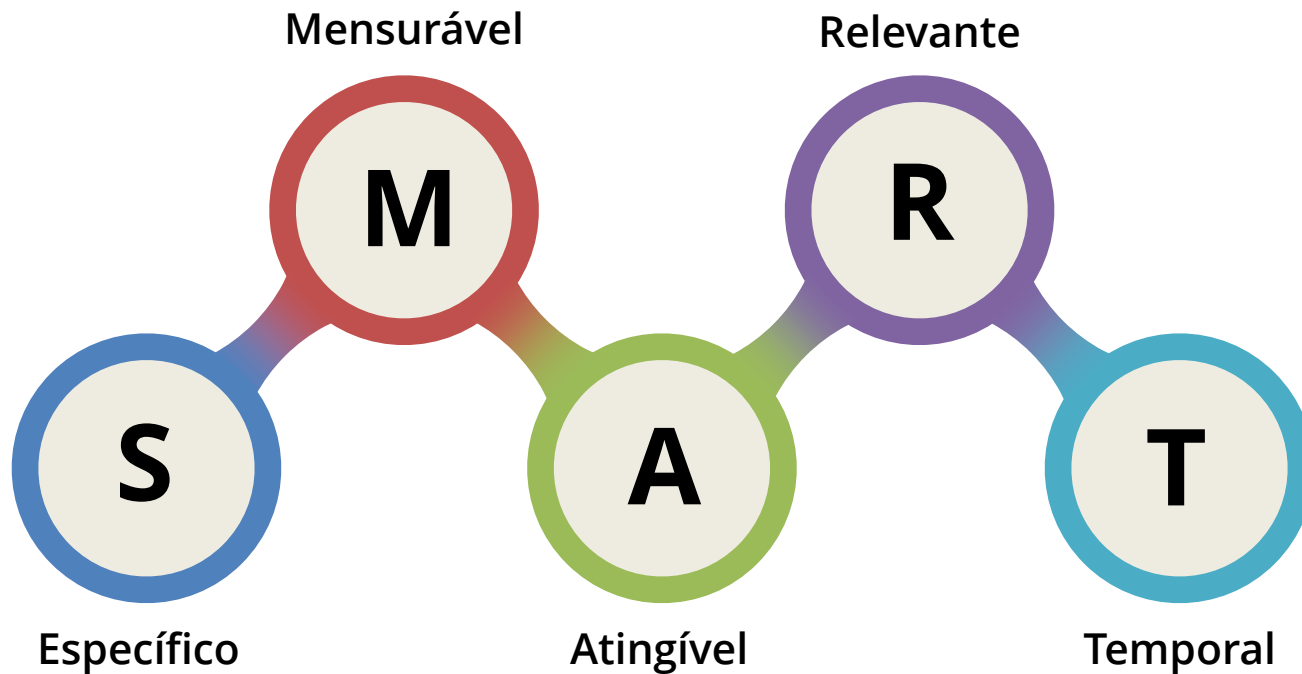
# Objetivos

## • 1ª Etapa – Fixação dos objetivos

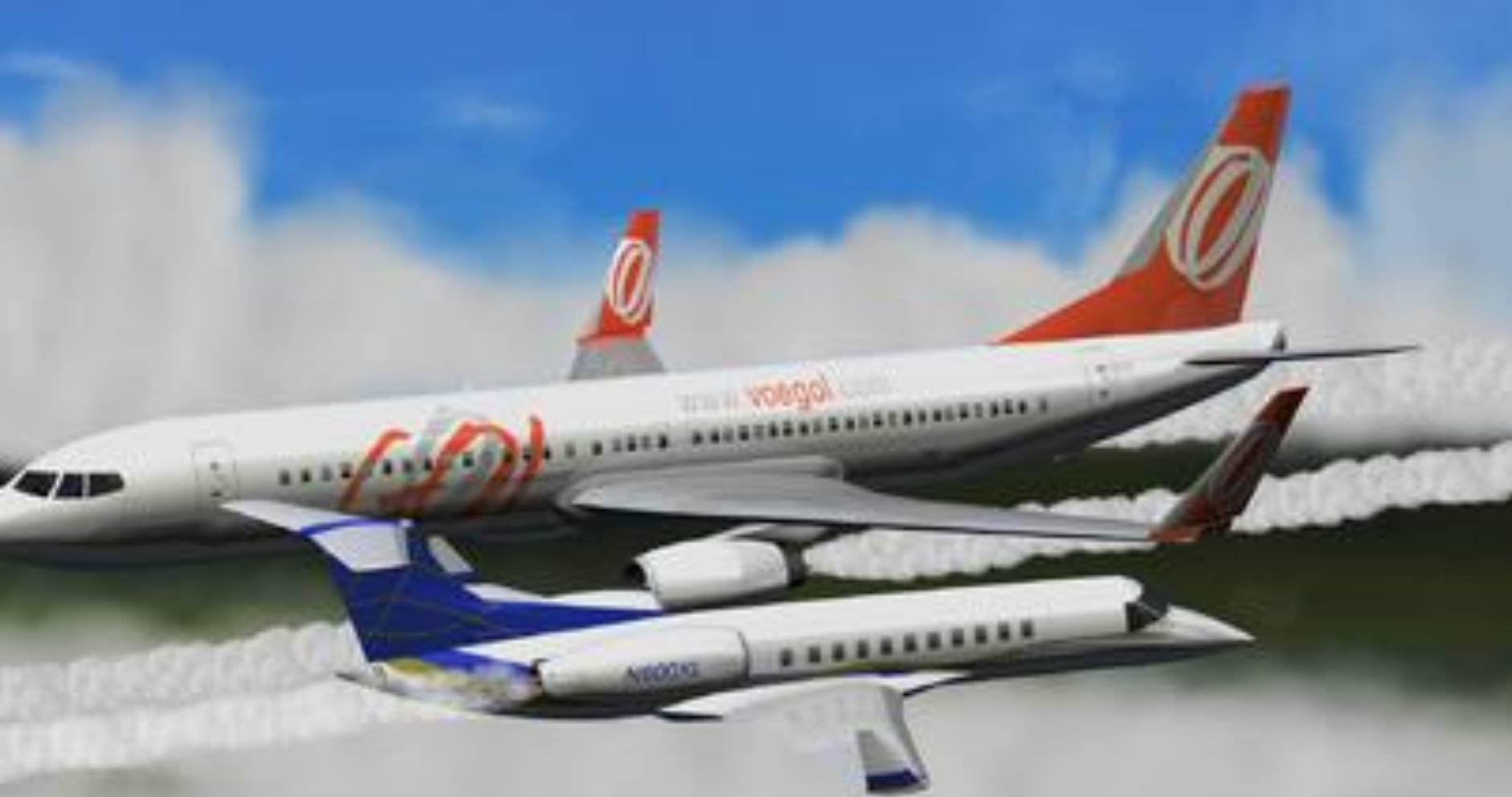
Fixação de Objetivos: todos os níveis da organização devem ter **objetivos fixados e comunicados**. Inclui a verificação da existência de **missão, visão e objetivos**. Essa verificação é necessária para permitir a identificação de eventos que potencialmente impeçam sua consecução.

**O que queremos atingir?**

# SMART





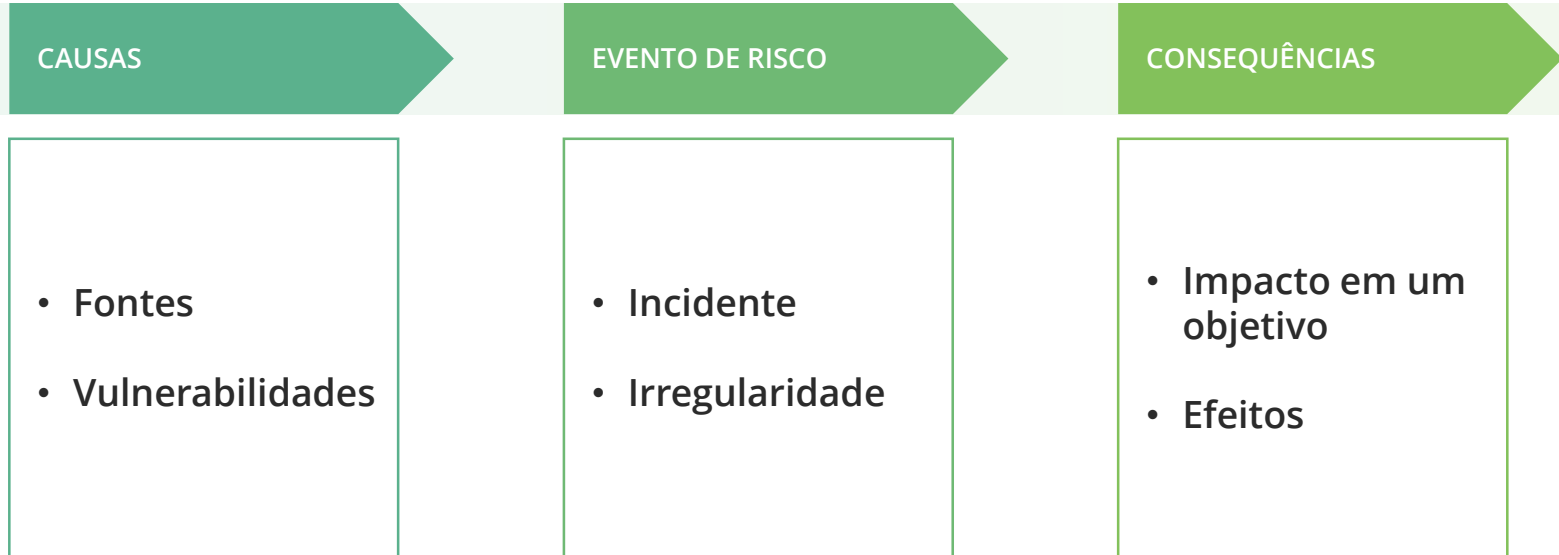


	Fatores positivos	Fatores negativos
Fatores internos	<b>S</b> Strengths (força)	<b>W</b> Weaknesses (fraquezas)
Fatores externos	<b>O</b> Opportunities (oportunidades)	<b>T</b> Threats (ameaças)

# 2

## Identificando os riscos

# O que pode nos impedir de alcançar nossos objetivos



# Sintaxe

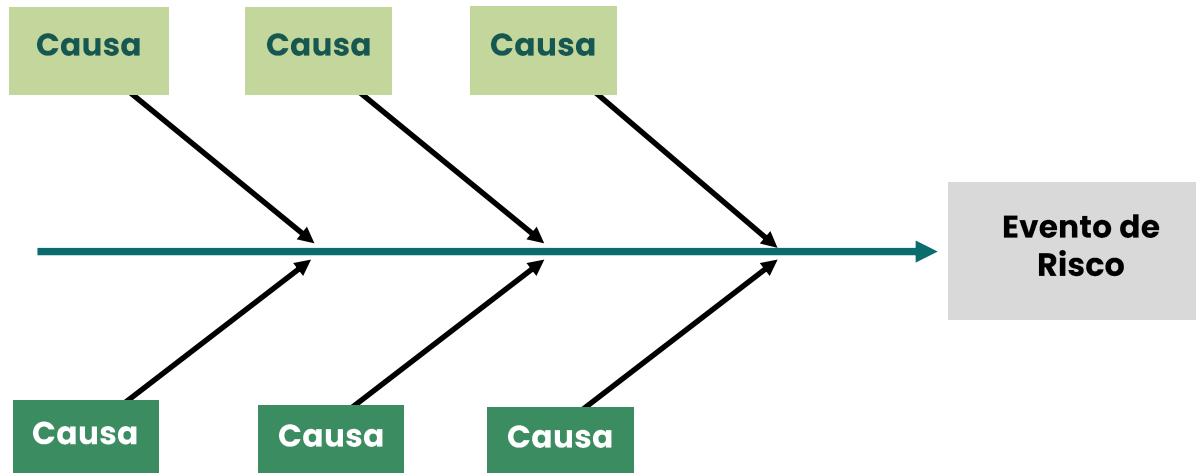
Devido à <CAUSA>, poderá acontecer <RISCO>, o que poderá levar à <CONSEQUÊNCIA> impactando no/na <OBJETIVO>.

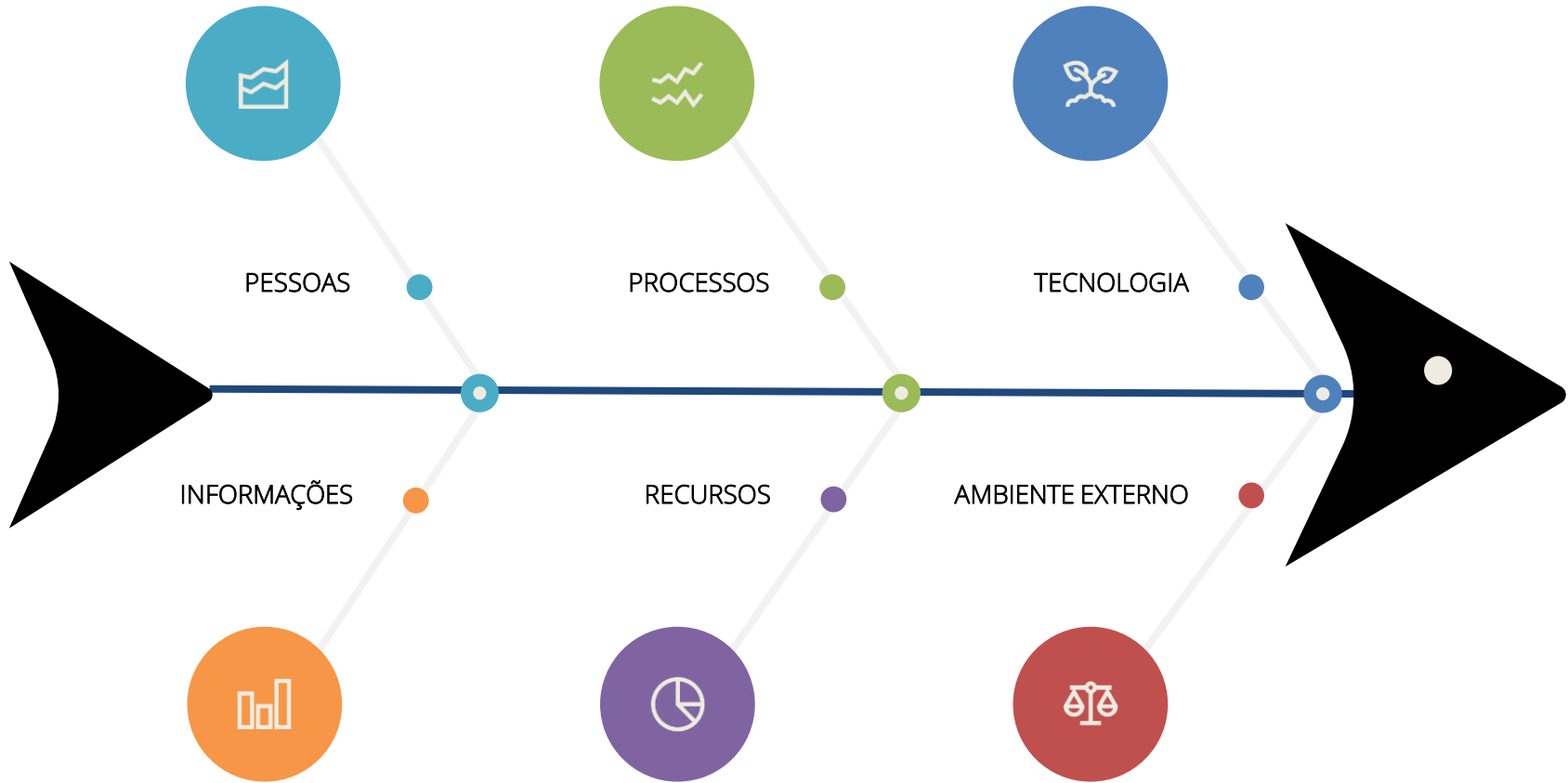
# Exemplificando

Devido ao contato direto dos empregados da área de licitações com fornecedores, poderá acontecer o oferecimento ou solicitação de pagamento indevido, o que poderá levar à corrupção dos empregados impactando na entrega de bens à população.

# Técnicas

## Diagrama de *Ishikawa* (Espinha de Peixe)







Falta de capacitação

Processo mal elaborado

Preço de referência  
acima do mercado

Definição imprecisa  
do objeto

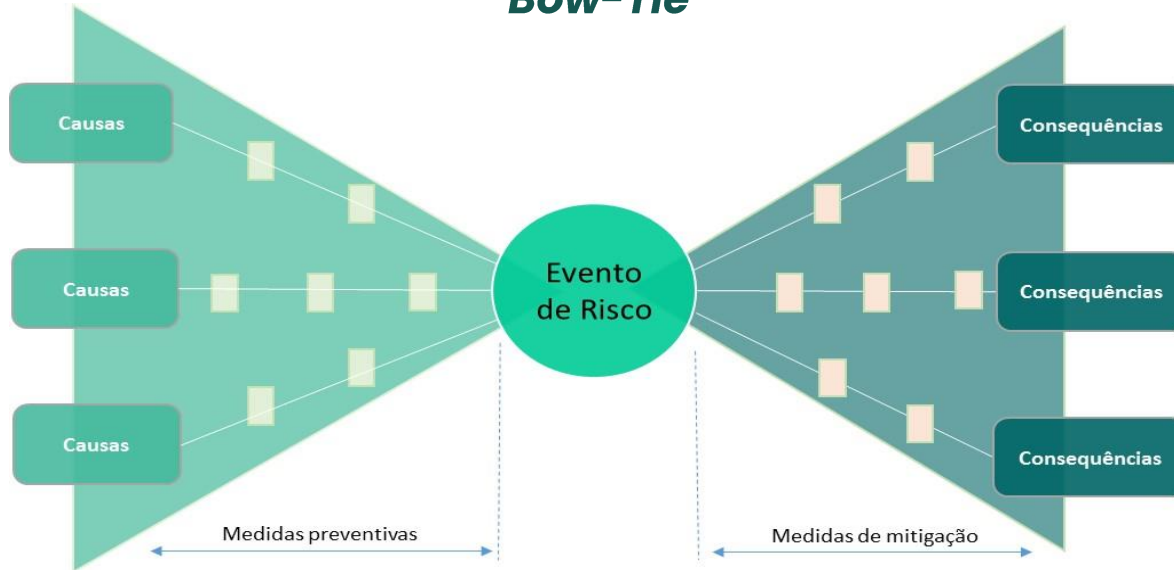
Falta de publicidade

Conluio

**Licitação  
Irregular**

# Técnicas

## Bow-Tie



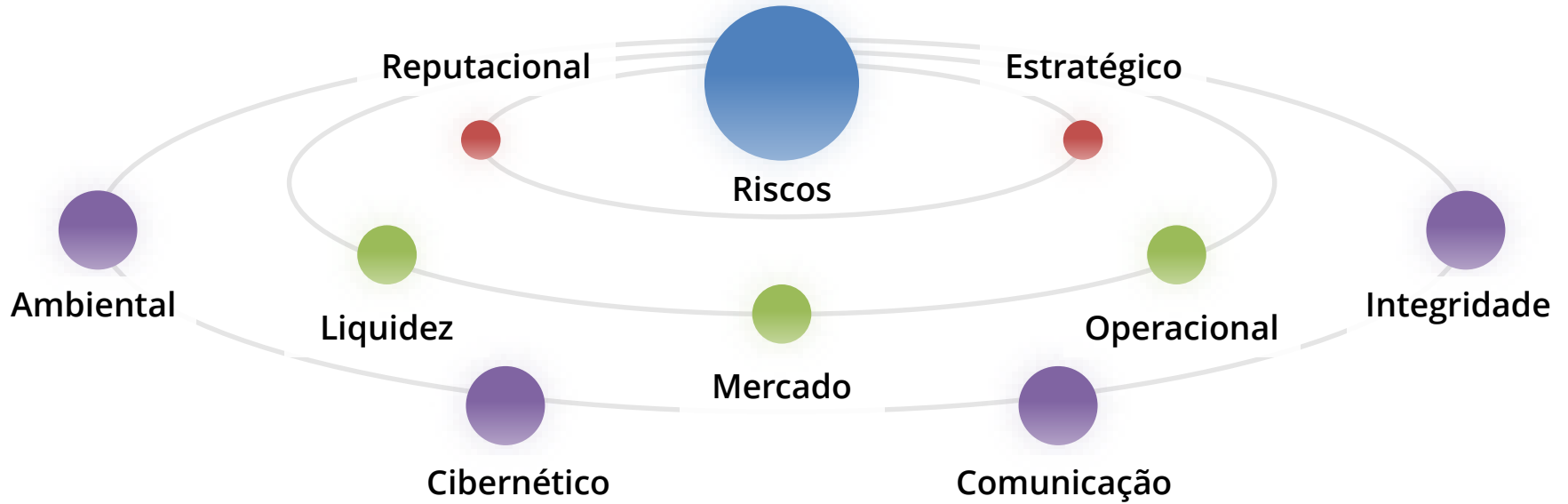
# Técnicas



# 3

## Tipos de riscos

# Tipos de Riscos



# Principais Categorias

1

## Estratégico

Decisões que podem afetar negativamente o alcance dos objetivos da organização.

3

## Integridade

Possibilidade de ocorrência de evento de corrupção, fraude, irregularidade ou desvio ético ou de conduta que venha a impactar o cumprimento dos objetivos institucionais.

2

## Operacional

Perdas resultantes de falhas, deficiências ou inadequação de processos internos, estrutura, pessoas, sistemas, tecnologia, assim como de eventos externos.

4

## Reputacional

Comprometimento da confiança da sociedade em relação à capacidade da organização em cumprir sua missão institucional e interferência direta na imagem da organização.

# Principais Categorias

5

## Orçamentário/Financeiro

Comprometimento dos recursos orçamentários e financeiros necessários à realização das atividades da organização.

6

## Comunicação

Eventos que podem impedir ou dificultar a disponibilidade de informações para a tomada de decisões e para o cumprimento das obrigações de prestação de contas às instâncias controladoras e à sociedade.

7

## Conformidade

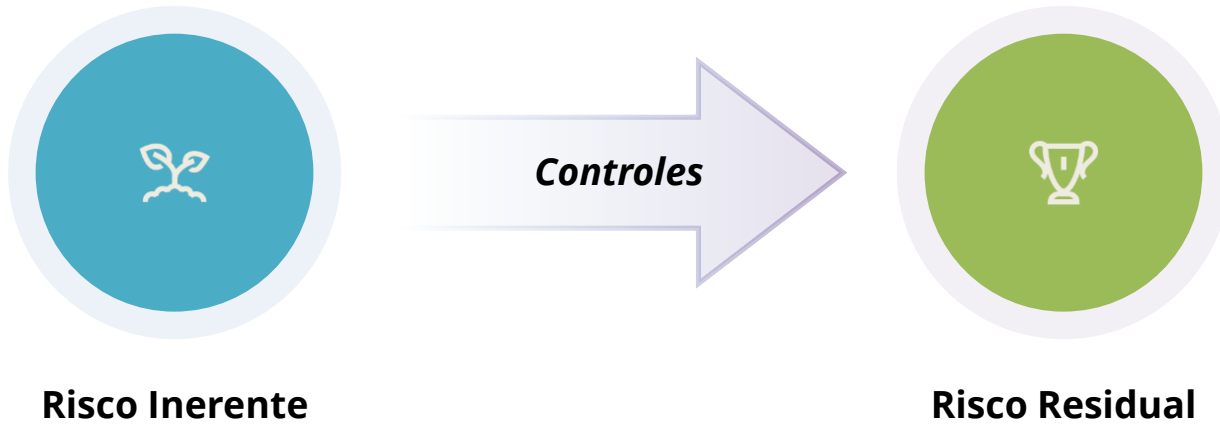
Não cumprimento de princípios constitucionais, legislações específicas ou regulamentações externas aplicáveis ao negócio, bem como de normas e procedimentos internos.

# 4

## Matriz de Riscos



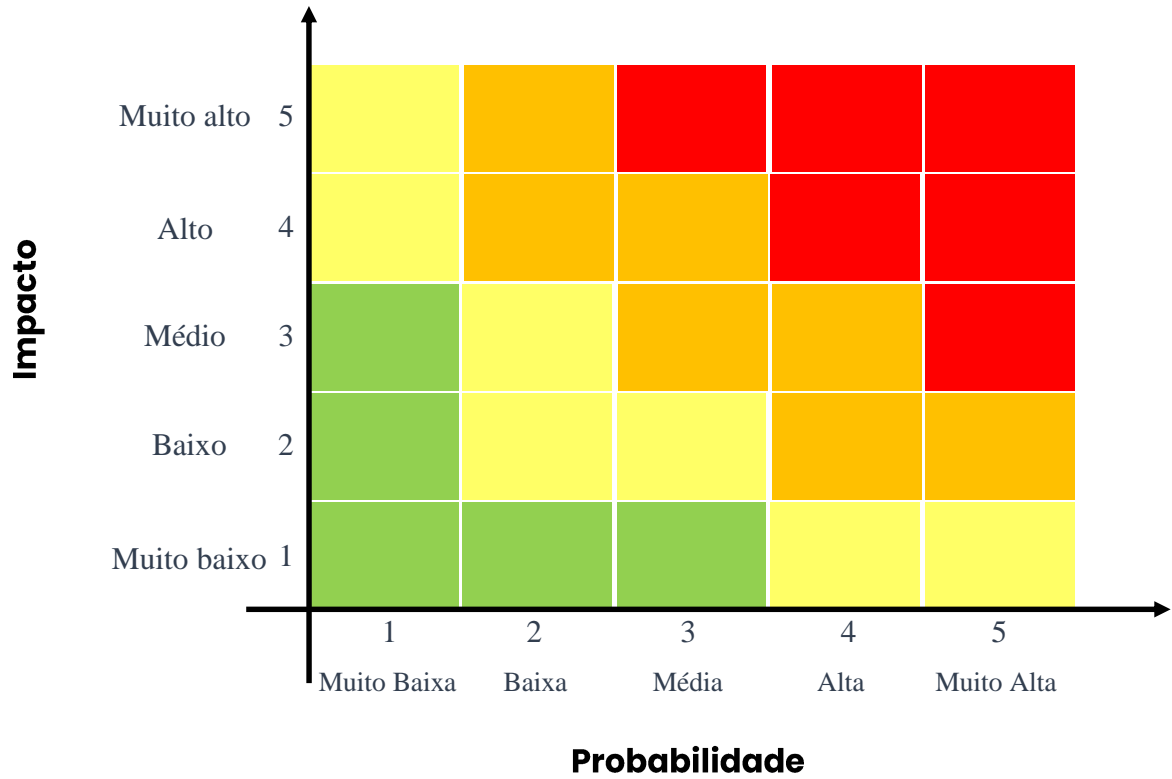
# Avaliação de Riscos



Nível de risco antes de quaisquer ações de mitigação de risco terem sido levadas em conta, como atividades de controle.

*COSO 2013*

# Matriz de Riscos



## Níveis de riscos

- Risco Crítico**
- Risco Alto**
- Risco Moderado**
- Risco Pequeno**

# Matriz de Riscos

## Escala de Probabilidade

Peso	Escala	Frequência Observada / Esperada	Descrição
5	Muito Alta	$\geq 90\%$	O evento é esperado na maioria das circunstâncias.
4	Alta	$\geq 50\% < 90\%$	O evento provavelmente ocorre na maioria das circunstâncias.
3	Média	$\geq 30\% < 50\%$	O evento deve ocorrer em algum momento.
2	Baixa	$\geq 10\% < 30\%$	O evento pode ocorrer em algum momento.
1	Muito Baixa	$< 10\%$	O evento pode ocorrer apenas em circunstâncias excepcionais.

# Matriz de Riscos

## Escala de Impacto

Peso	Escala	Descrição
5	Muito alto	O impacto ocasiona colapso às ações de gestão, a viabilidade estratégica pode ser comprometida.
4	Alto	O impacto compromete acentuadamente às ações de gestão, os objetivos estratégicos podem ser fortemente comprometidos.
3	Médio	O impacto é significativo no alcance das ações de gestão.
2	Baixo	O impacto é pouco relevante ao alcance das ações de gestão.
1	Muito baixo	O impacto é mínimo no alcance das ações de gestão.

# 5

## **Avaliando os controles**

# Controles

Estudar padrões de  
comportamento



Capacitar uma equipe



Implantar câmeras de  
movimento



Inspecionar um produto



Dupla checagem de um relatório  
financeiro



Monitorar um indicador



A close-up, low-angle shot of a car's interior floor. A person's foot is resting on the accelerator pedal, which has a black rubber tread with a wavy pattern. To the right is the brake pedal, also with a rubber tread. The background is dark, showing the underside of the car and the floor mat. The text "Controles Internos" is overlaid in white on the left side.

# Controles Internos



**Controles Internos da Gestão** são um conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de servidores das organizações, destinados a **enfrentar os riscos e fornecer segurança razoável** de que, na consecução da missão da entidade, os seguintes objetivos gerais serão alcançados:



Execução ordenada, ética, econômica, eficiente e eficaz das operações



Cumprimento das obrigações de accountability



Cumprimento das leis e regulamentos aplicáveis



Salvaguarda dos recursos para evitar perdas, mau uso e danos

## Preventivos



## Detectivos



## Corretivos




# Limitações

Nenhum controle interno é 100% infalível. O que ele deve proporcionar é uma **segurança razoável** de que os objetivos da empresa serão atingidos. Dessa forma, as principais limitações do controle interno são:



Conluio de  
Servidores



Eventos  
Externos



Servidores  
Negligentes



Custo  
x  
Benefício

# Avaliação dos Controles

## Nível de Eficácia

Eficácia do Controle	Descrição	Fator de Avaliação dos Controles
Inexistente	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	1,0
Fraco	Controle depositado no conhecimento pessoal, em geral de maneira manual, responsabilidade individual.	0,8
Mediano	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco, devido a deficiências no desenho ou nas ferramentas utilizadas.	0,6
Satisfatório	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	0,4
Forte	Controles implementados podem ser considerados a “melhor prática”, mitigando todos os aspectos relevantes do risco.	0,2

# 6

## Risco residual

Nível de risco **após** ter levado em consideração as **ações de mitigação de risco** tais como atividades de controle.

*COSO 2013*

# Apetite a Riscos

“Quantidade e tipo de riscos que uma organização está disposta a buscar ou reter.” ISO 31073/2022

A última fase da 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.

O limite de exposição a riscos representa o nível de risco acima do qual é desejável o tratamento do risco.

Espera-se que, com os resultados do tratamento, o nível de risco residual fique abaixo do limite de exposição.

# Apetite a Riscos

Matriz de Riscos						
I m p a c t o	Muito Alto	5	10	15	20	25
	Alto	4	8	12	16	20
	Médio	3	6	9	12	15
	Baixo	2	4	6	8	10
	Muito Baixo	1	2	3	4	5
		Raro	Pouco Provável	Provável	Muito Provável	Praticamente Certo
		Probabilidade				



# Apetite a Riscos

## Apetite a Riscos - Legenda

Muito Baixo	A organização não aceita nenhum risco, devendo tratar todos os eventos de risco.
Baixo	A organização aceita a possibilidade de ocorrência de eventos de riscos baixos.
Médio	A organização aceita a possibilidade de ocorrência de eventos de riscos baixo e moderados
Alto	A organização aceita a possibilidade de ocorrência de eventos de riscos baixo, moderado e altos
Muito Alto	A organização aceita a possibilidade de ocorrência de eventos de todos os níveis de risco.

# Apetite a Riscos

		Nível de Risco			
		Pequeno	Moderado	Alto	Crítico
Apetite a Riscos	Muito Baixo	Tratar	Tratar	Tratar	Tratar
	Baixo	Aceitar	Tratar	Tratar	Tratar
	Médio	Aceitar	Aceitar	Tratar	Tratar
	Alto	Aceitar	Aceitar	Aceitar	Tratar
	Muito Alto	Aceitar	Aceitar	Aceitar	Aceitar

# Apetite a Riscos

## Atitude perante o Risco Residual Exemplo: Appetite a Riscos Médio

Pequeno	<b>Nível de risco dentro do apetite a risco.</b> Podem existir oportunidades de maior retorno que possam ser exploradas. Pode ser o caso de assumir mais riscos, avaliando a relação custo x benefício e diminuindo alguns controles.
Moderado	<b>Nível de risco dentro do apetite a risco.</b> Requer atividades de monitoramento e manutenção dos controles.
Alto	<b>Nível de risco, além do apetite a risco.</b> Alguma ação deve ser tomada.
Crítico	<b>Nível de risco muito além do apetite a risco.</b> Ações devem ser tomadas tempestivamente.

# 7

## Definindo a resposta ao risco

# Resposta ao Risco

Conhecido o nível de risco residual, verifique qual estratégia a ser adotada para responder ao evento de risco. A escolha da estratégia **dependerá do nível de exposição a riscos** previamente estabelecido pela organização em confronto com a avaliação que se fez do risco.

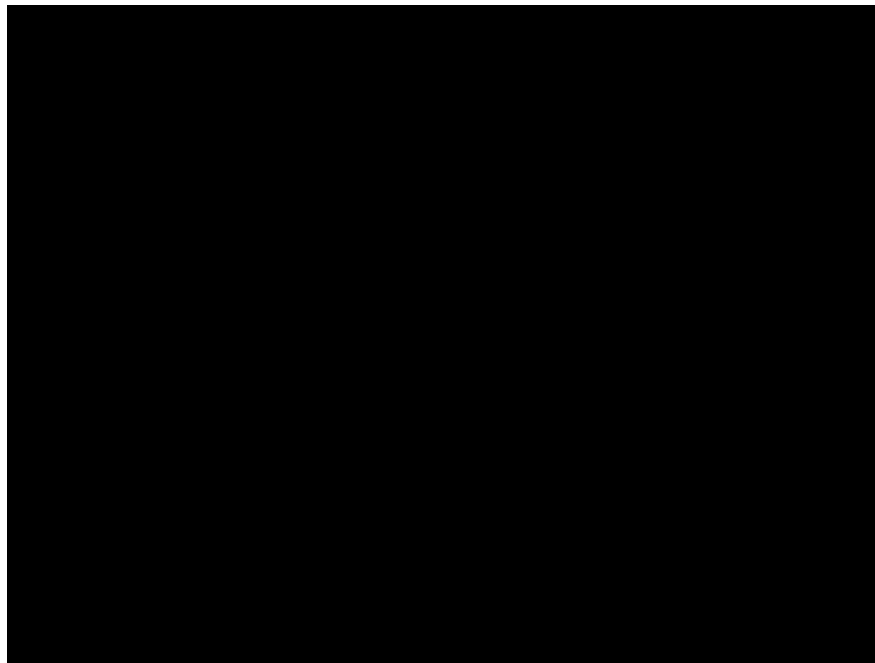
Aceitar

Mitigar

Transferir

Evitar

# Cuidado com a resposta!



# Resposta ao Risco

**O tratamento dos riscos deve seguir os seguintes passos (TCU, 2018):**



Identificar medidas de resposta ao risco.

Avaliar a viabilidade da implantação dessas medidas (custo benefício, viabilidade técnica, etc.).



Decidir quais serão implementadas

Elaborar plano de implementação das medidas para inclusão nos planos institucionais.



# Mitigação

1. As ações de mitigação tenham um custo-benefício positivo.
2. Eventual plano de ação deve ser eficaz na redução do risco.
3. Deve-se monitorar as atividades de mitigação.





# Transferência

Envolve a ação de transferir o impacto negativo de uma ameaça (e a titularidade da resposta) a um terceiro.

## Importante:

- A transferência de risco não elimina uma ameaça, simplesmente faz com que a outra parte seja responsável pelas perdas econômicas/físicas conectadas.
- As organizações transferem para terceiros (companhias de seguros, mercados de derivativos etc.), principalmente, quando o custo de transferência é menor ou igual a perda esperada.
- Não exagere com o *overhedging* dos riscos → Pode acontecer de você transferir a terceiros as oportunidades também (*upside risk*).

# Evitar



O risco deve que ser evitado quando:

- a) É inconsistente com os objetivos da organização.
- b) É maior que o *apetite* de riscos da organização.
- c) Os custos incrementais de *hedging* são maiores do que os resultados positivos de cobertura.

# Apetite a Riscos

## Apetite a Riscos - Legenda

Muito Baixo	A organização não aceita nenhum risco, devendo tratar todos os eventos de risco.
Baixo	A organização aceita a possibilidade de ocorrência de eventos de riscos baixos.
Médio	A organização aceita a possibilidade de ocorrência de eventos de riscos baixo e moderados
Alto	A organização aceita a possibilidade de ocorrência de eventos de riscos baixo, moderado e altos
Muito Alto	A organização aceita a possibilidade de ocorrência de eventos de todos os níveis de risco.

# Apetite a Riscos

		Nível de Risco			
		Pequeno	Moderado	Alto	Crítico
Apetite a Riscos	Muito Baixo	Tratar	Tratar	Tratar	Tratar
	Baixo	Aceitar	Tratar	Tratar	Tratar
	Médio	Aceitar	Aceitar	Tratar	Tratar
	Alto	Aceitar	Aceitar	Aceitar	Tratar
	Muito Alto	Aceitar	Aceitar	Aceitar	Aceitar

# Apetite a Riscos

## Atitude perante o Risco Residual Exemplo: Apetite a Riscos Médio

Pequeno	<b>Nível de risco dentro do apetite a risco.</b> Podem existir oportunidades de maior retorno que possam ser exploradas. Pode ser o caso de assumir mais riscos, avaliando a relação custo x benefício e diminuindo alguns controles.
Moderado	<b>Nível de risco dentro do apetite a risco.</b> Requer atividades de monitoramento e manutenção dos controles.
Alto	<b>Nível de risco, além do apetite a risco.</b> Alguma ação deve ser tomada.
Crítico	<b>Nível de risco muito além do apetite a risco.</b> Ações devem ser tomadas tempestivamente.

# 8

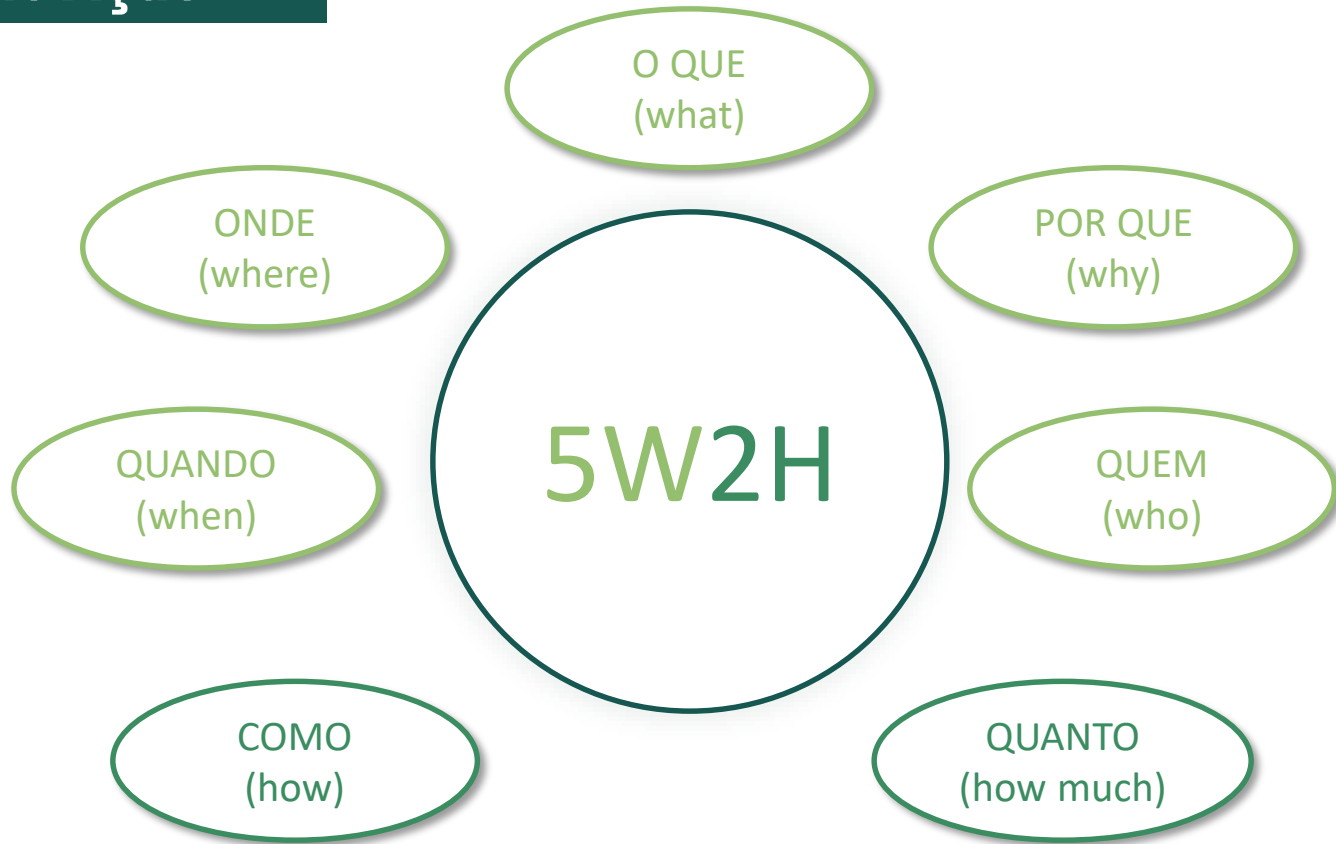
## Elaborando um plano de ação

# Plano de Ação

## Dica prática

- Uma das boas opções disponíveis para a elaboração de um plano de ação é a metodologia 5W2H, exemplificada a seguir.
- Na implementação de um plano de ação, identifique claramente a ordem de prioridade em que cada tratamento deva ser implementado.
- Ao pensar em uma atividade de controle para mitigar determinado risco avaliado, faça uma avaliação da relação benefício/custo da implementação daquele controle. Fará sentido você implementá-lo se o resultado for maior que 1.







# 9

# Monitorando os riscos

As **informações relevantes devem ser identificadas, coletadas e comunicadas**, a tempo de permitir que as pessoas cumpram suas responsabilidades, não apenas com dados produzidos internamente, mas, também, com informações sobre eventos, atividades e condições externas, que possibilitem o gerenciamento de riscos e a tomada de decisão.

## Informações

Confiáveis, íntegras e tempestivas

## Comunicação

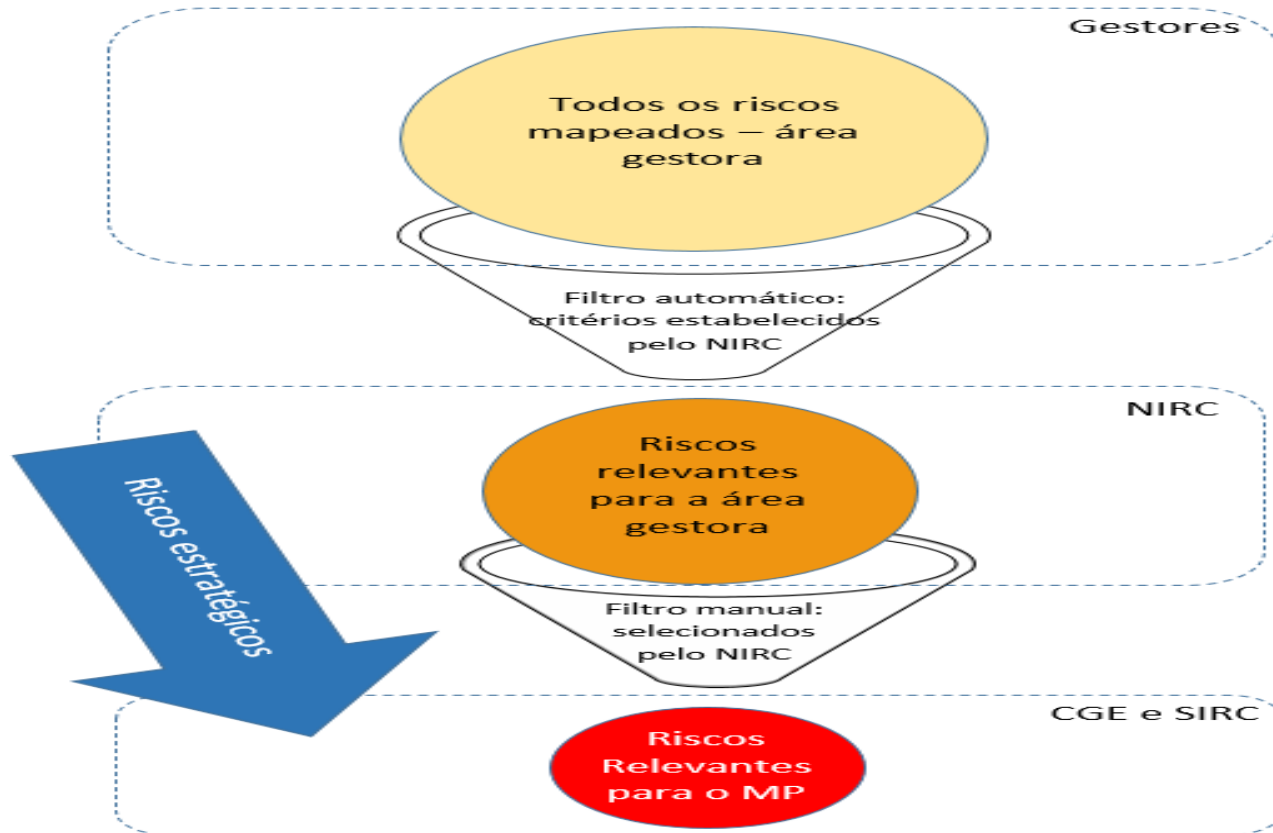
Flui em todas as direções e que alcance toda a organização

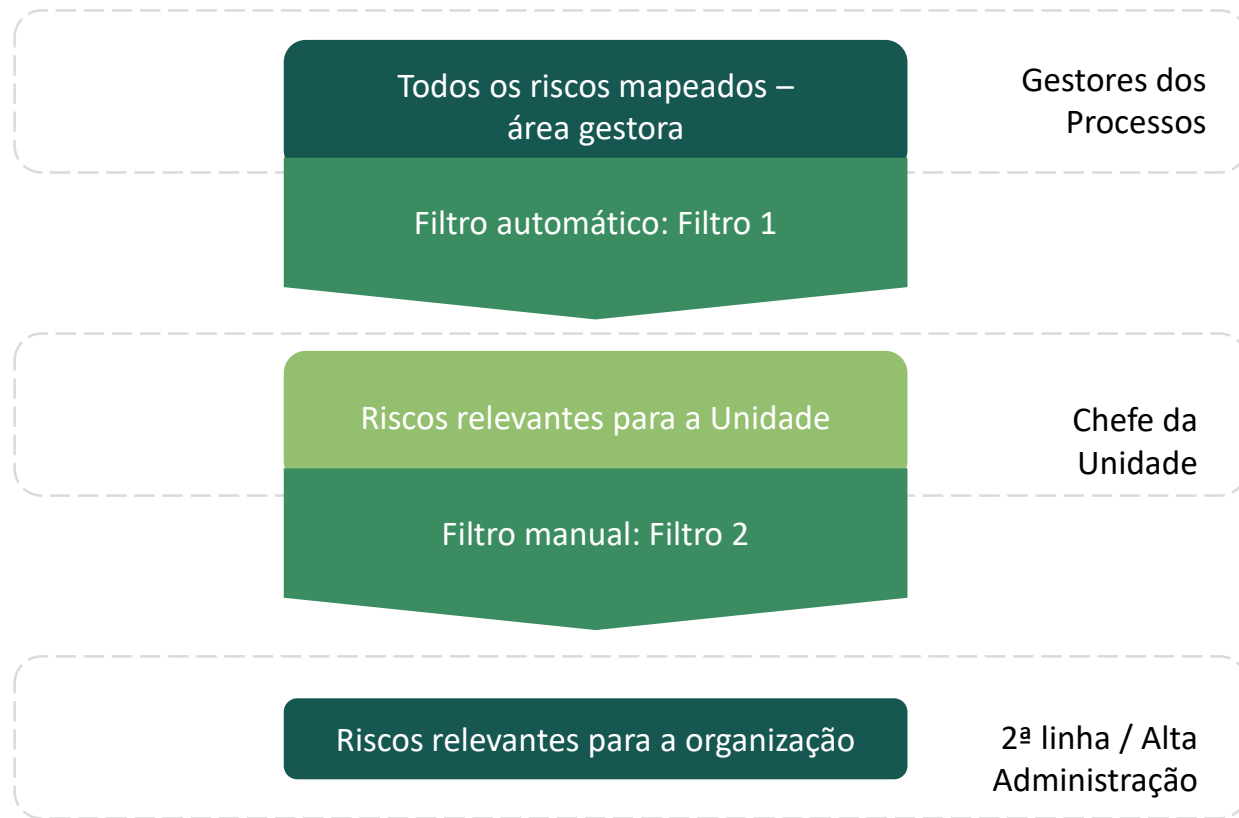
Entre instâncias de supervisão de gestão de riscos e controles internos ocorre por meio dos níveis de relacionamento delineados no Modelo de Relacionamento.

## DEFINIÇÃO DAS MEDIDAS DE CONTROLE

### ▶ Critérios de Classificação riscos-chave (SCGE/PE)







Exemplo:  
MPOG, adaptado

## Filtro 1

Serão selecionados automaticamente os riscos considerados relevantes, de acordo com a classificação abaixo:

- ✓ Riscos Estratégicos ou de Integridade.
- ✓ Riscos inerentes com Impacto 5 ou residuais com Impacto 4.
- ✓ Riscos residuais em nível “Crítico” ou “Alto”.

## Filtro 2

A 2ª linha avaliará individualmente cada risco selecionado no Filtro 1, reportando às instâncias superiores (Alta Administração) os que possuam maior relevância.

# Definição das medidas de controle

Critérios de classificação riscos-chave



Exemplo: SCGE-PE

## Orange Book

“Devem ser criados processos para verificar se os riscos continuam a existir, se surgiram novos riscos, se a probabilidade e impacto dos riscos mudaram, reportar alterações significativas que ajustem as prioridades de risco e garantir a eficácia dos controles.”

## COSO ERM

“O gerenciamento de riscos corporativos de uma organização modifica-se com o passar do tempo. As respostas a risco que se mostravam eficazes anteriormente podem tornar-se inúteis; as atividades de controle podem perder a eficácia ou deixar de ser executadas; ou os objetivos podem mudar. Essas modificações podem ser causadas pela chegada de novos profissionais, pelas mudanças na estrutura ou no direcionamento da organização ou, ainda, pela introdução de novos processos. Diante dessas mudanças, a administração necessita determinar se o funcionamento do gerenciamento de riscos corporativos permanece eficaz.”

## ISO 31073:2022

“Verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado.”



## Formas

### Contínuo

Feitas de forma rotineira e definida. Em geral são realizadas pelos administradores das áreas, sendo inseridas no processo de negócio e efetuadas em tempo real.

### Independente

Periódicas e conduzidas pela administração, auditoria interna, auditoria externa, entre outros. O que será avaliado, bem como a periodicidade são definidos pela administração do órgão avaliador. Sua periodicidade depende do ritmo de mudanças na entidade a ser avaliada.

## Indicadores-chave de Risco

- ✓ São indicadores definidos para dar maior visibilidade às principais fontes de riscos da organização.
- ✓ Ao monitorar dados associados aos eventos, as organizações identificam a existência de condições que poderiam originar um evento.
- ✓ O KRI fornece um aviso antecipado com o objetivo de identificar potenciais eventos que possam impactar um objetivo de negócio traçado.
- ✓ Habilitam a prevenção de potenciais riscos elevados.
- ✓ Ajudam a identificar fraquezas em processos e/ou controles de forma a permitir ações a serem tomadas com objetivo de fortalecer o controle e resolver casos específicos.





Mensuráveis.

Previsíveis.

Comparáveis.

Informativos.



Confira este exemplo prático:

Risco: Infarto

Fatores de Risco

Indicadores-chave

Obesidade

IMC > 35

Pressão alta

> 14 por 9

Colesterol alto

> 200 mg/dl

RF

► Objetivo: construção de uma escola por meio de convênio



## Risco: execução irregular

Fatores de Risco

KRI

Recursos parados na maior parte da execução do convênio

Demora na conclusão do processo licitatório

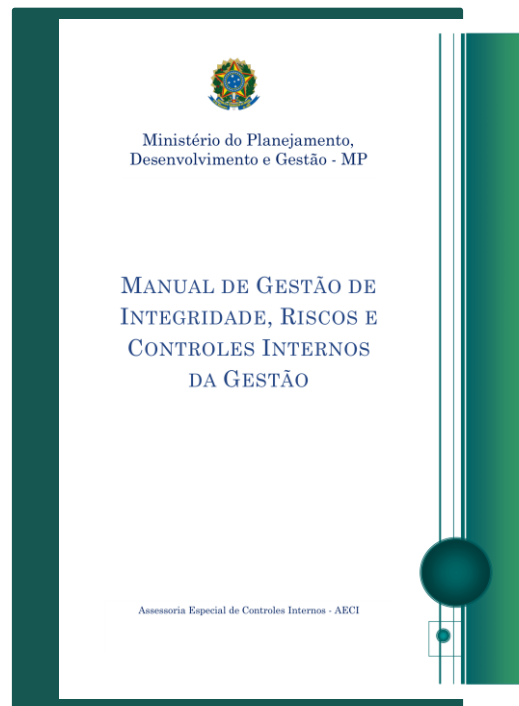
Documentação inidônea para comprovação de despesas

% de recursos executados *versus* % de recurso previsto para o período no plano de trabalho

Número de recursos de licitantes

Número de comprovações de despesas inidôneas

- **Ministério do Planejamento, Desenvolvimento e Gestão - MP**

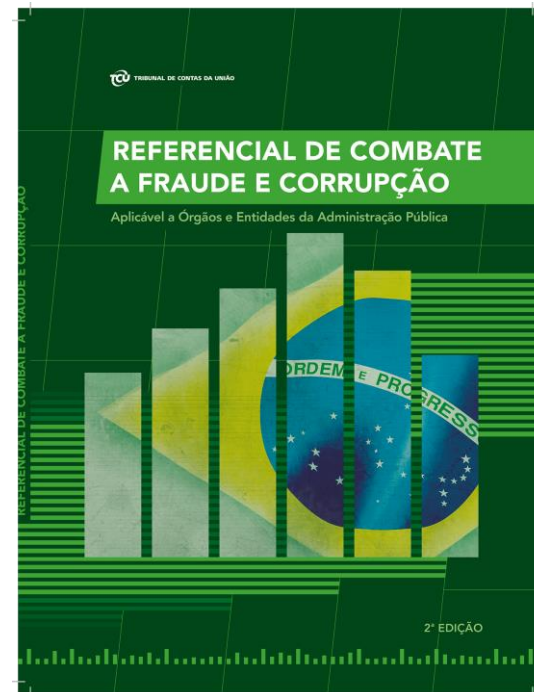




# Gestão de Riscos e Fraude

RODRIGO  
FONTENELLE

## • Tribunal de Contas da União



- **Controladoria-Geral da União**

## METODOLOGIA DE GESTÃO DE RISCOS

Ministério da Transparência e  
Controladoria-Geral da União - CGU



## GUIA PRÁTICO DE GESTÃO DE RISCOS PARA A INTEGRIDADE

*Orientações para a administração pública  
federal direta, autárquica e fundacional*

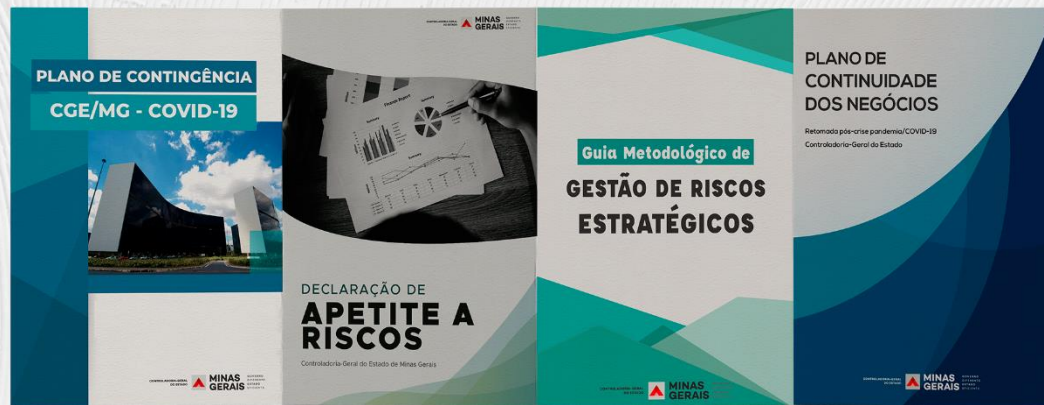
MINISTÉRIO DA TRANSPARÊNCIA E  
CONTROLADORIA-GERAL DA UNIÃO

# Gestão de Riscos

## • Controladoria-Geral do Estado de Minas Gerais

Conheça  
o portfólio  
Gestão de  
Riscos da  
CGE-MG!

Baixe gratuitamente!



# Gestão de Riscos

RODRIGO  
FONTENELLE

## • STF / TJMG / MAPA



# Gestão de Riscos





WEBINAR

# GESTÃO DE RISCOS NA PRÁTICA

com Rodrigo Fontenelle, Rodrigo Pironti,  
Marcelo Zenkner e Daniel Lança

NOVA DATA

18/09 às 19h

Evento gratuito



# Obrigado!

 @rodrigofonte

 [www.rodrigofontenelle.com.br](http://www.rodrigofontenelle.com.br)

