CGU

GESTÃO DE RISCOS E AS TRÊS LINHAS DE DEFESA

JOÃO HENRIQUE
Wetter Bernardes

MARCELA
Jacominy de Amorim Mendes

Dezembro
2020

OBJETIVO SOLICITADO

Capacitar colaboradores das áreas finalísticas, em bases teóricas e fundamentos metodológicos sobre gerenciamento de riscos, para aplicação nos processos operacionais ou como multiplicadores do tema, no âmbito do Ministério da Saúde.

OBJETIVO GERAL

Apresentar os conceitos de Gestão de Riscos necessários à implementação da estrutura de governança, gestão de riscos e controles internos prevista na IN MP/CGU 01/2016

AGENDA

1º Dia

- Contextualização:
  - Governança;
  - Modelo das 3 linhas de defesa do IIA

- Conceitos

- Evolução histórica

- Aplicações do tema no Poder Executivo Federal

AGENDA

2º Dia

- Processo de Gestão de Riscos:
  - Entendimento do contexto
  - Identificação de riscos
  - Análise
  - Avaliação
    - Nível de risco (outras visões)
  - Risco inerente e risco residual

AGENDA

3º Dia

- Tratamento;
- Controle Interno
- Comunicação e Monitoramento;
- E quando o risco se materializa?

O QUE É GESTÃO DE RISCOS?

ISSO 31000:2018: Atividades Coordenadas para dirigir e controlar uma organização no que se refere a *RISCOS.*

COSO ERM 2017: A cultura, as competências e as práticas, integradas com a definição da estratégia e com a performance, com que as organizações contam para gerenciar o risco na criação, preservação e realização de valor.

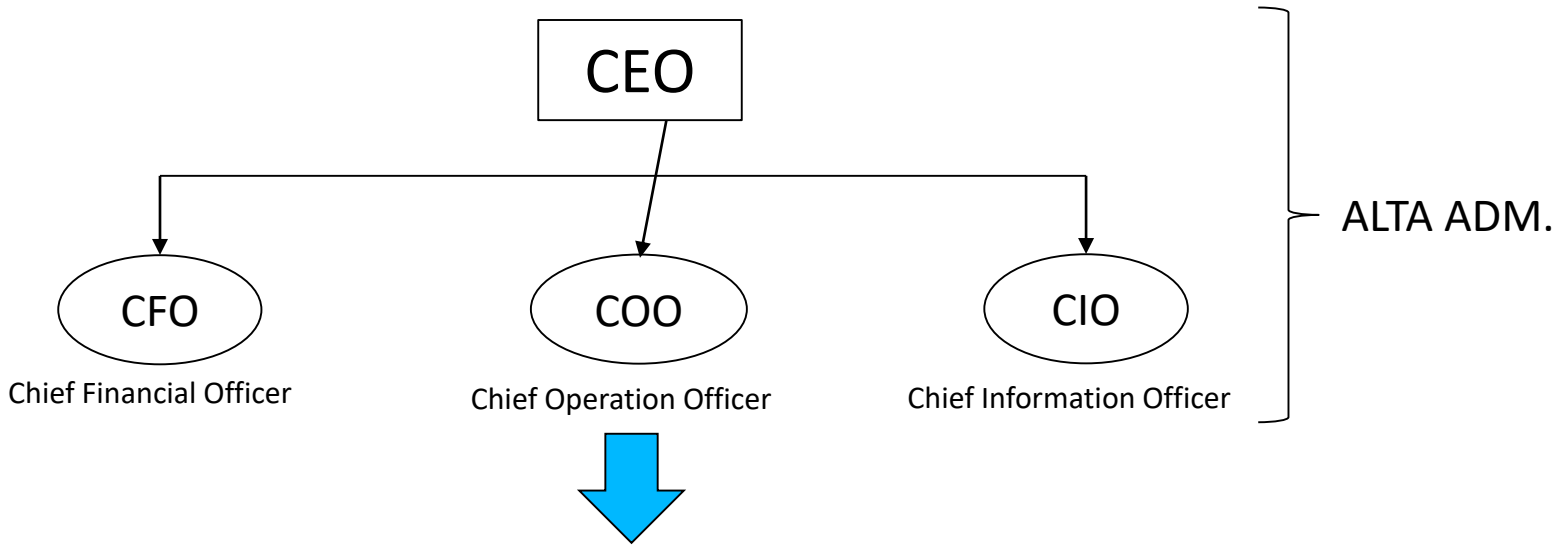
CONTEXTUALIZAÇÃO

GOVERNANÇA

- O QUE É?
- PARA QUE SERVE?
- QUEM SÃO OS ATORES?
- QUANDO SURGIU?
- TODAS AS ORGANIZAÇÕES DEVEM ADOTAR?

ACIONISTAS, SOCIEDADE, FUNCIONÁRIOS...

Interesses e necessidades



ACIONISTAS, SOCIEDADE, FUNCIONÁRIOS...

Interesses e necessidades

CONFLITO DE AGÊNCIA

CEO

CFO

Chief Financial Officer

COO

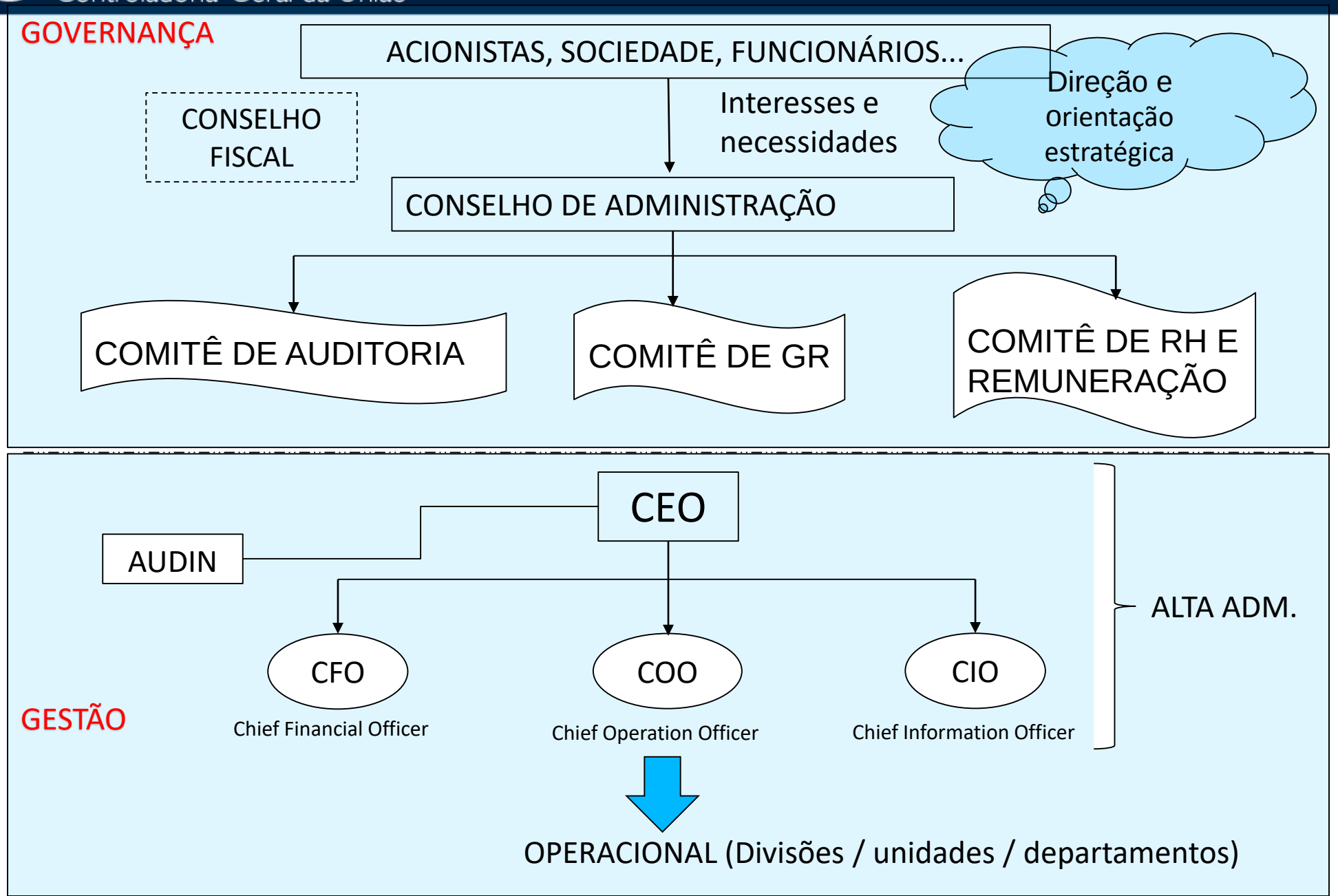
Chief Operation Officer

CIO

Chief Information Officer

ALTA ADM.

OPERACIONAL (Divisões / unidades / departamentos)


GOVERNANÇA
ACIONISTAS, SOCIEDADE, FUNCIONÁRIOS...
CONSELHO FISCAL
Interesses e necessidades
Direção e orientação estratégica
CONSELHO DE ADMINISTRAÇÃO
COMITÊ DE AUDITORIA
COMITÊ DE GR
COMITÊ DE RH E REMUNERAÇÃO
CEO
AUDIN
CFO
Chief Financial Officer
COO
Chief Operation Officer
CIO
Chief Information Officer
ALTA ADM.
GESTÃO
OPERACIONAL (Divisões / unidades / departamentos)

GOVERNANÇA

O QUE É:

forma de administração/gestão ESTRUTURADA.

Conjunto de processos, regulamentos, decisões, costumes, ideias que mostram a maneira pela qual aquela empresa ou sociedade é dirigida ou administrada.

GOVERNANÇA

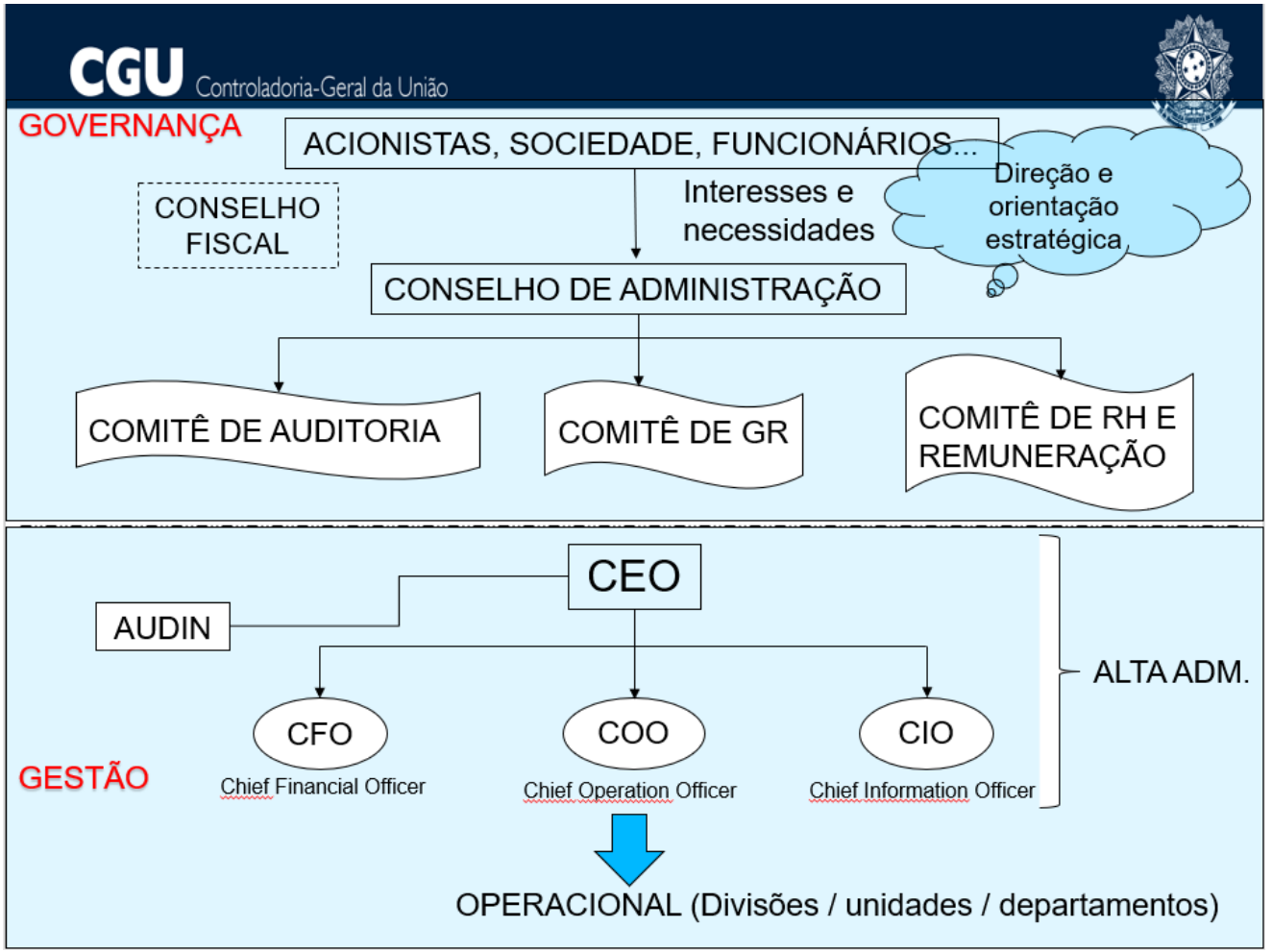
PARA QUE SERVE:

garantir que diretores e acionistas (partes interessadas) de uma empresa (organização) tenham confiança nela. Mantém os interesses dos executivos e acionistas ligados aos interesses da empresa.

ALINHAMENTO DE INTERESSES

GOVERNANÇA

ATORES:



GOVERNANÇA

QUANDO SURGIU:

- **1650: primeira “corporation” na Inglaterra – acionistas elegeram um Conselho, que nomeou um CEO;**
- **Década de 80 e 90, escândalos, modernização da governança.**

GOVERNANÇA

TODAS AS ORGANIZAÇÕES DEVEM ADOTAR?

REFLEXÃO

GOVERNANÇA PÚBLICA

CF 88, art. 70: A fiscalização contábil, financeira, orçamentária, operacional e patrimonial da União e das entidades da administração direta e indireta, quanto à legalidade, legitimidade, economicidade, aplicação das subvenções e renúncia de receitas, será exercida pelo Congresso Nacional, mediante controle externo, e pelo sistema de controle interno de cada Poder.

DECRETO 9.203/2017: governança pública - conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade;

GOVERNANÇA PÚBLICA– Decreto 9.203/2017

Conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade

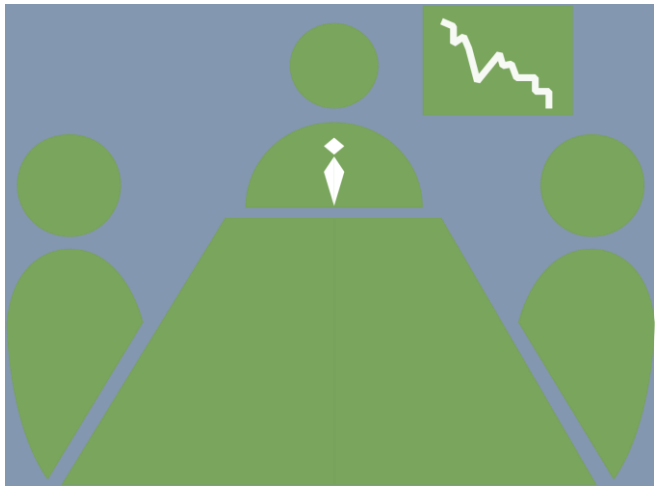
Fonte: Decreto nº 9.203/2017
TCU - Referencial Básico de Governança, 2014

GOVERNANÇA PÚBLICA

PRINCÍPIOS

Princípios de governança no setor público

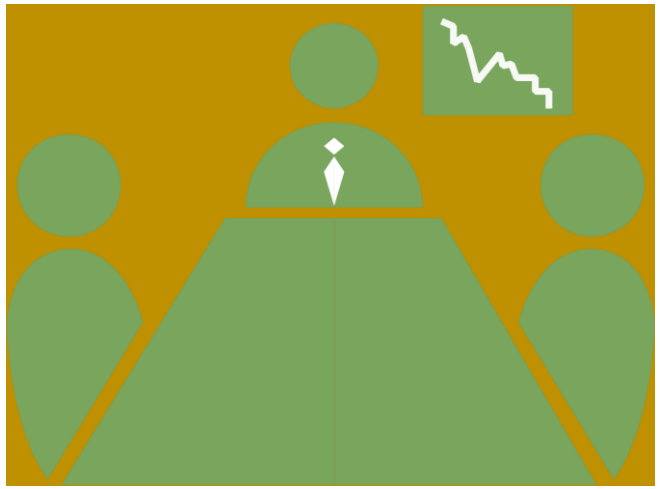
Decreto nº 9.203/2017

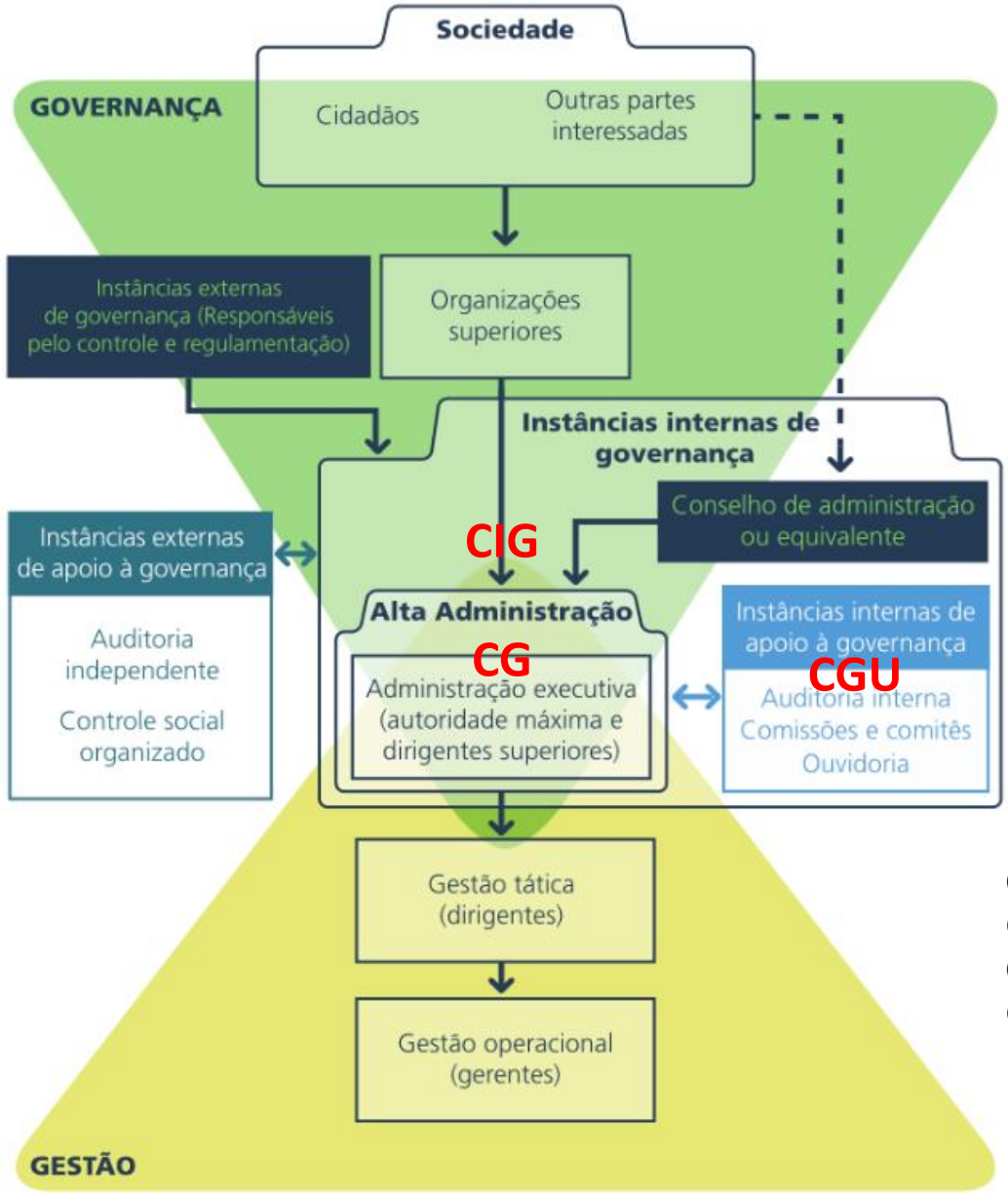


- Liderança
- Integridade
- Responsabilidade
- Corporativa
- Compromisso
- Transparência
- *Accountability*
- Equidade

Princípios básicos de Governança

IBGC





CIG – Comitê Interministerial de Governança (CC, MF, MP, CGU)
CG – Comitês Internos de Governança (constituídos em cada ministério)

Fonte:
TCU - Referencial Básico de Governança, 2014 - Adaptado

Governança Pública – Decreto 9.203/2017

Princípios da Gestão de Riscos (Art. 17):

I - implementação e aplicação de forma sistemática, estruturada, oportuna e documentada, subordinada ao interesse público;

II - integração da gestão de riscos ao processo de planejamento estratégico e [demais processos de gestão] relevantes para a execução da estratégia e o alcance dos objetivos institucionais;

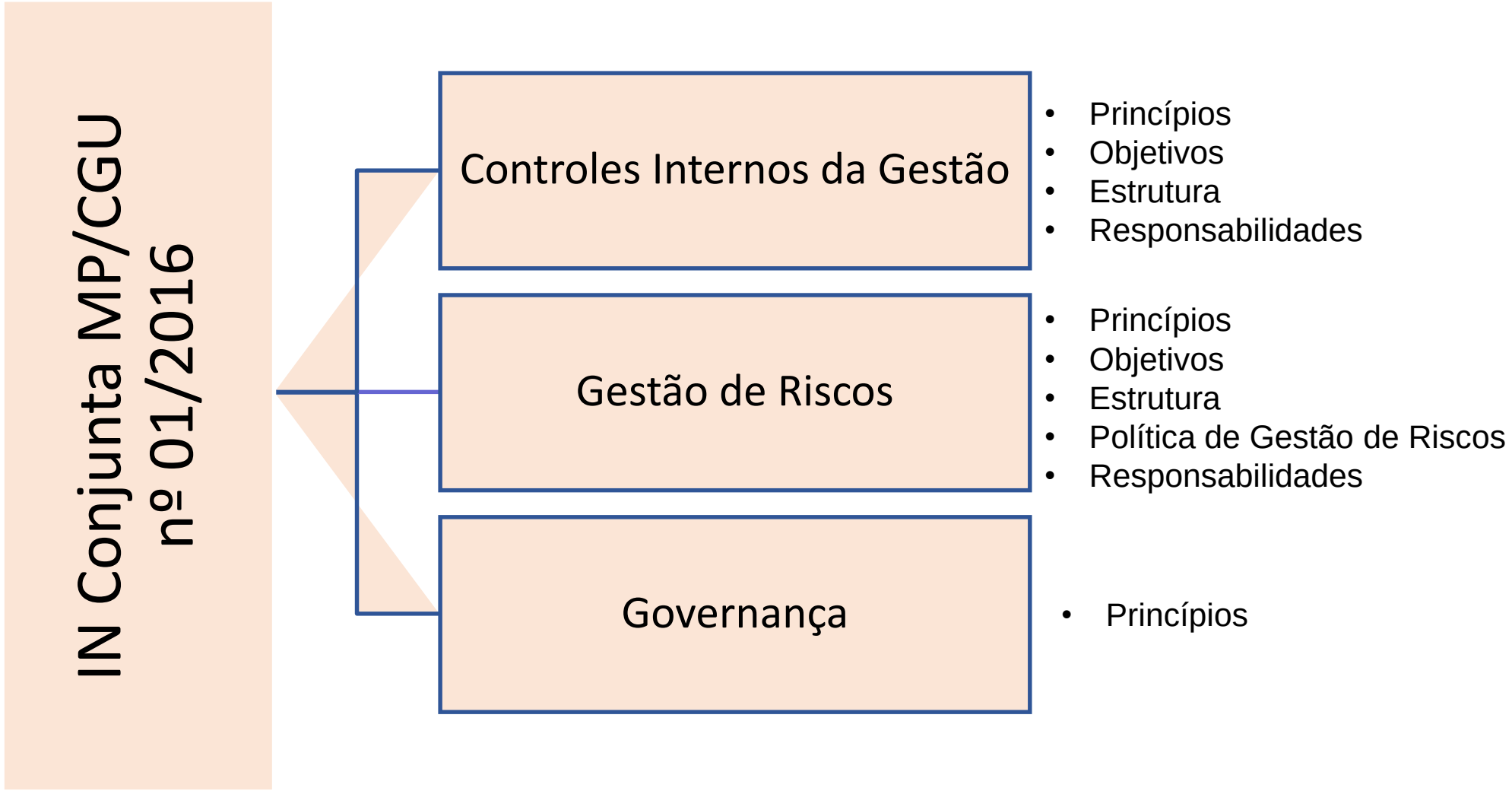
III - estabelecimento de controles internos proporcionais aos riscos...;

IV - utilização dos resultados para apoio à melhoria contínua do desempenho e dos processos de GR, controle e governança.

IN MP/CGU Nº 01, de 10/5/2016

Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal

IN CGU/MP nº 01/2016 – ESTRUTURA



IN CGU/MP nº 01/2016

Comitê de Governança, Riscos e Controles

Composição

Competências

POLÍTICA DE GESTÃO DE RISCOS

Deve abordar:

- **Propósito da organização em relação à GR**
- **Ligação entre objetivos da organização e da GR**
- **Integração da GR com a tomada de decisão**
- **Autoridade, Responsabilidade e *Accountability***
- **Tratamento de conflitos de interesse**
- **Recursos**
- **Medição e reporte do desempenho**
- **Análise crítica e melhoria contínua**

IN CGU/MP nº 01/2016 – POLÍTICA DE GESTÃO DE RISCOS

Art. 17. A política de gestão de riscos (...) deve especificar ao menos:

I – princípios e objetivos organizacionais;

II – diretrizes sobre:
a) como a gestão de riscos será integrada ao planejamento estratégico, aos processos e às políticas da organização;
b) como e com qual periodicidade serão identificados, avaliados, tratados e monitorados os riscos;
c) como será medido o desempenho da gestão de riscos;
d) como serão integradas as instâncias do órgão ou entidade responsáveis pela gestão de riscos;
e) a utilização de metodologia e ferramentas para o apoio à gestão de riscos; e
f) o desenvolvimento contínuo dos agentes públicos em gestão de riscos; e

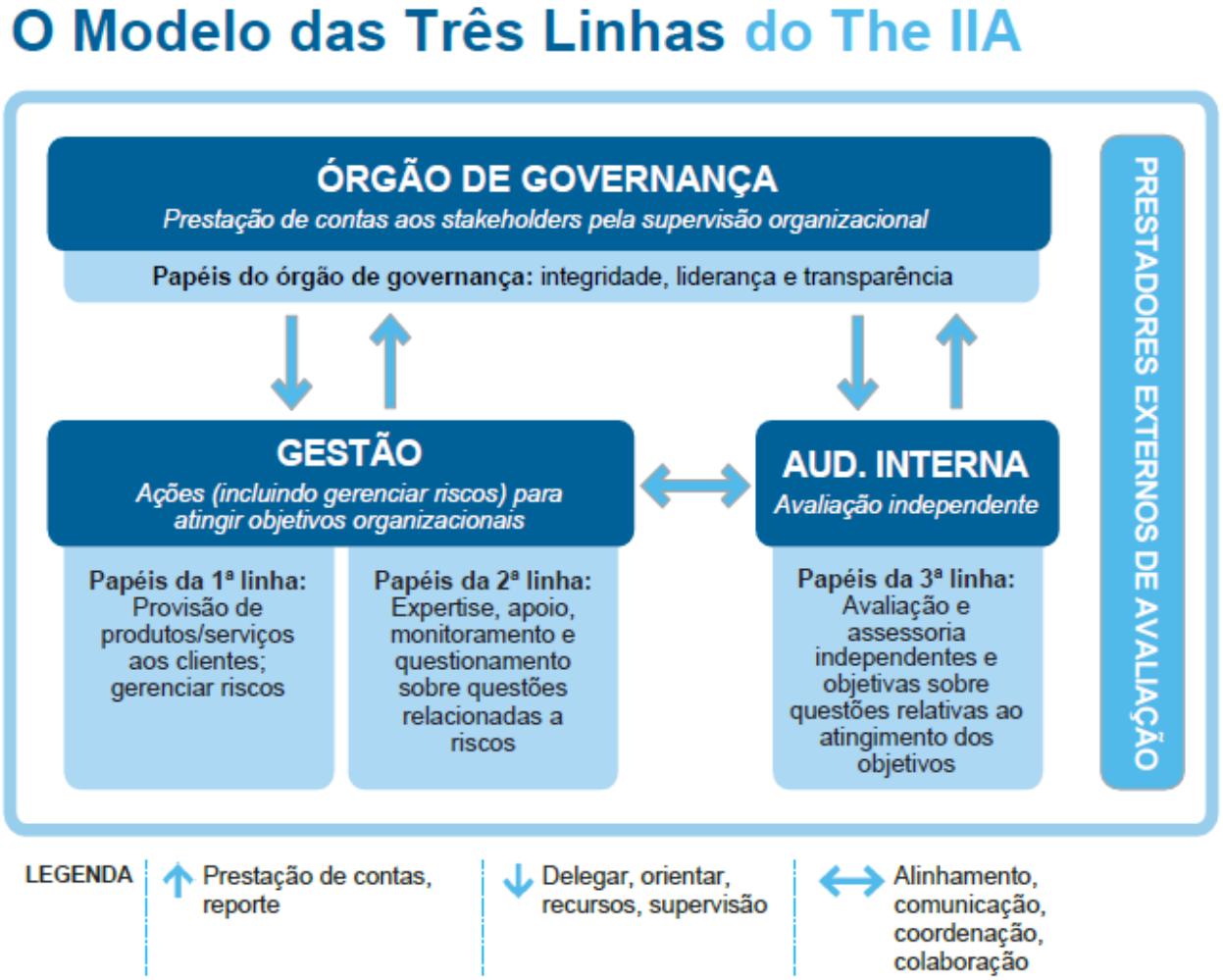
III – competências e responsabilidades para a efetivação da gestão de riscos no âmbito do órgão ou entidade.

RESPONSABILIDADES DOS GESTORES E AUDITORES

MODELO DAS TRÊS LINHAS DO IIA 2020

Uma atualização das Três Linhas de Defesa

Princípios:
1. Governança;
2. Papéis do órgão de governança (instância);
3. Gestão e os papéis da primeira e segunda linhas;
4. Papéis da terceira linha;
5. A independência da terceira linha
6. Criando e protegendo valor



AUDITORIA INTERNA

Linhas de Defesa no PEF

3 LINHAS DE DEFESA

IN MP/CGU 01/2016, Art. 2º, III

As auditorias internas no âmbito da Administração Pública se constituem na terceira linha ou camada de defesa das organizações, uma vez que são responsáveis por:

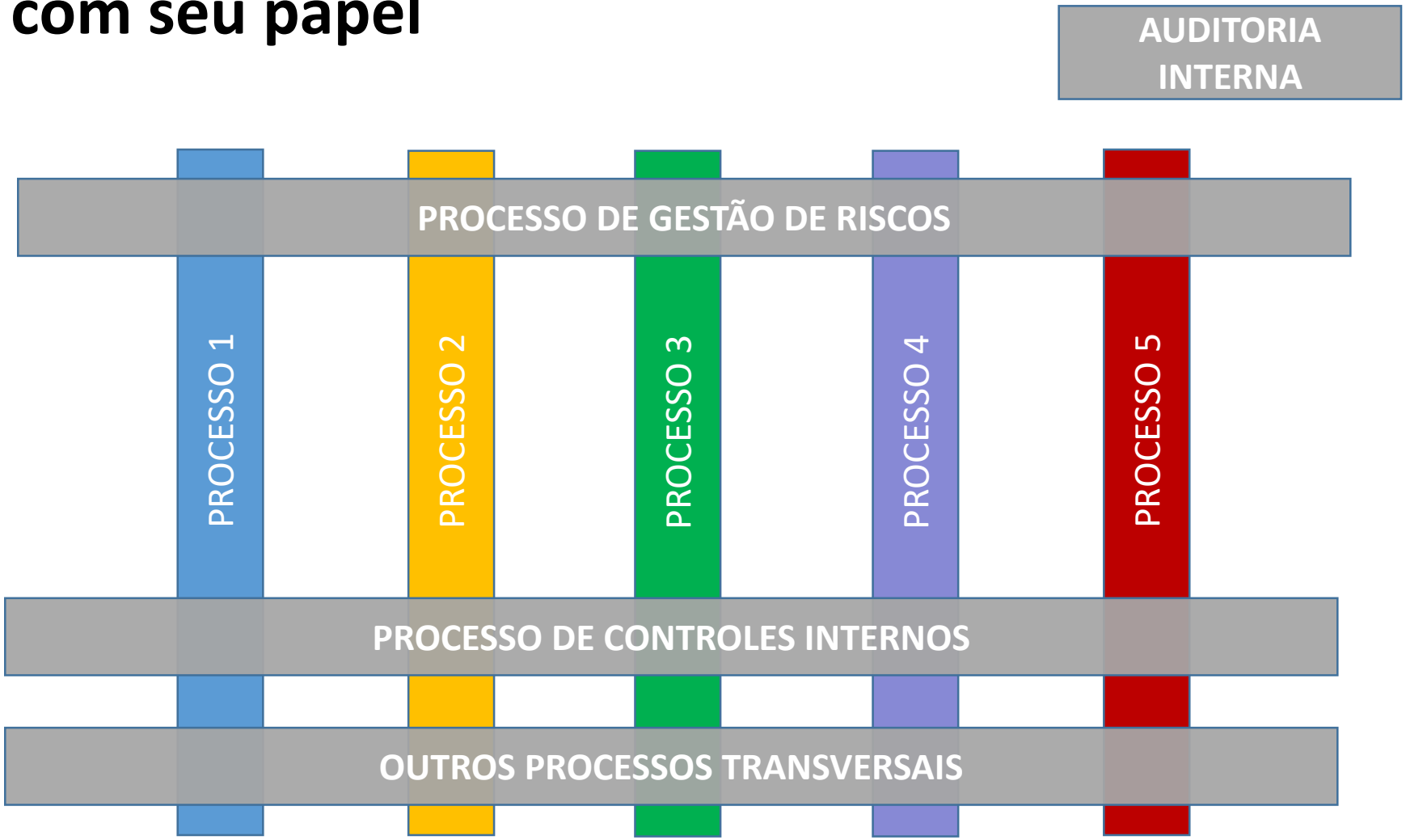
• avaliar a operacionalização dos controles internos da gestão (primeira linha de defesa, executada por todos os níveis da gestão)

• supervisionar os controles internos (segunda linha de defesa, executada por instâncias específicas)

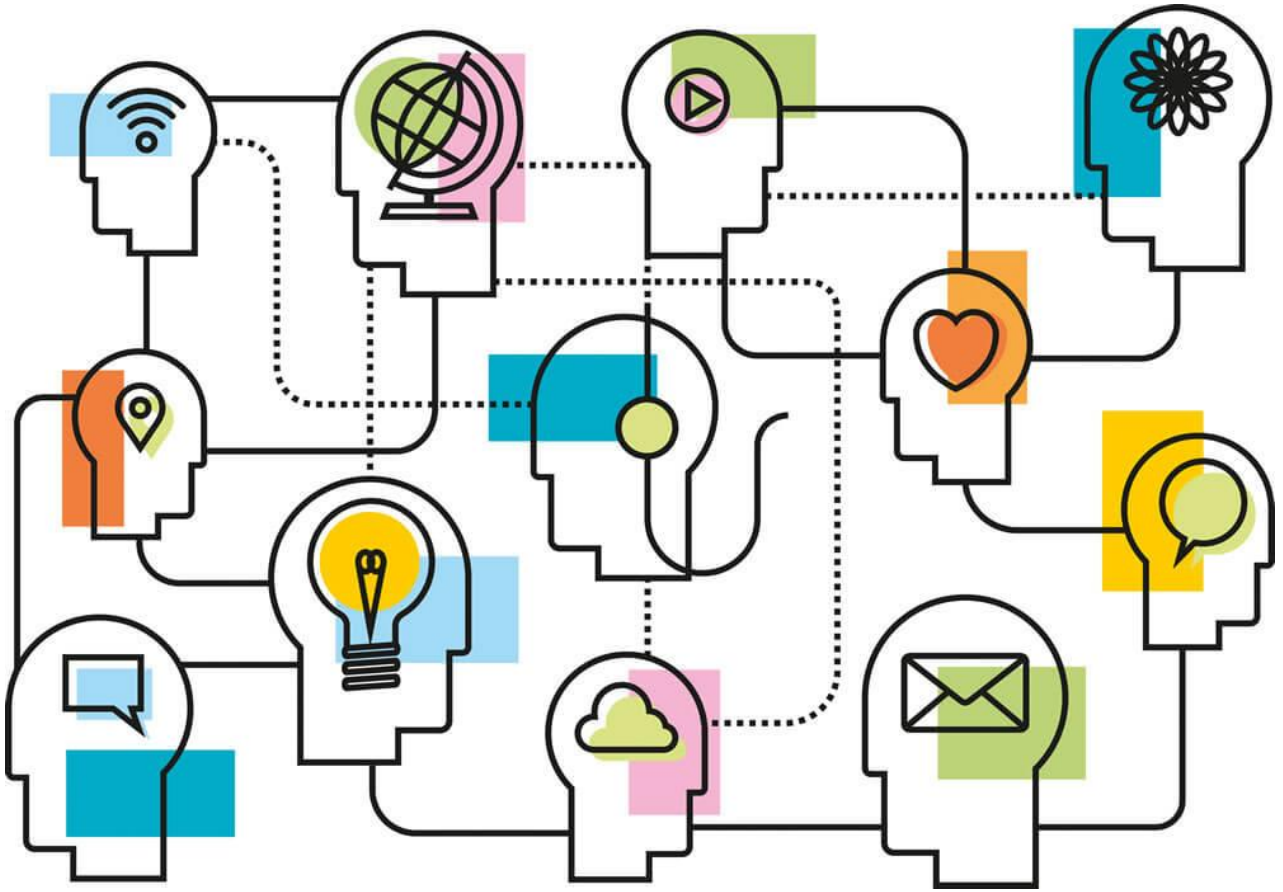
• fornecer avaliações e assessoramento destinadas ao aprimoramento dos controles internos, de forma que possam mitigar os principais riscos que ameacem o alcance dos objetivos organizacionais

AUDITORIA INTERNA

Cada um com seu papel



CONCEITOS



CONCEITOS

Objetivo

Meta ou **propósito** que se deseja **alcançar** de forma a se obter **êxito** no cumprimento da **missão** e no alcance da **visão de futuro** da organização

OBJETIVOS – DEFINIÇÃO DOS OBJETIVOS

CONCEITOS

Risco

Efeito da incerteza nos objetivos
(da organização, da unidade, do processo, etc)

ISO 31000/2018

Possibilidade de que eventos venham a ocorrer e afetem o alcance da estratégia e dos objetivos de negócio.

COSO ERM 2017

CONCEITOS

Controles

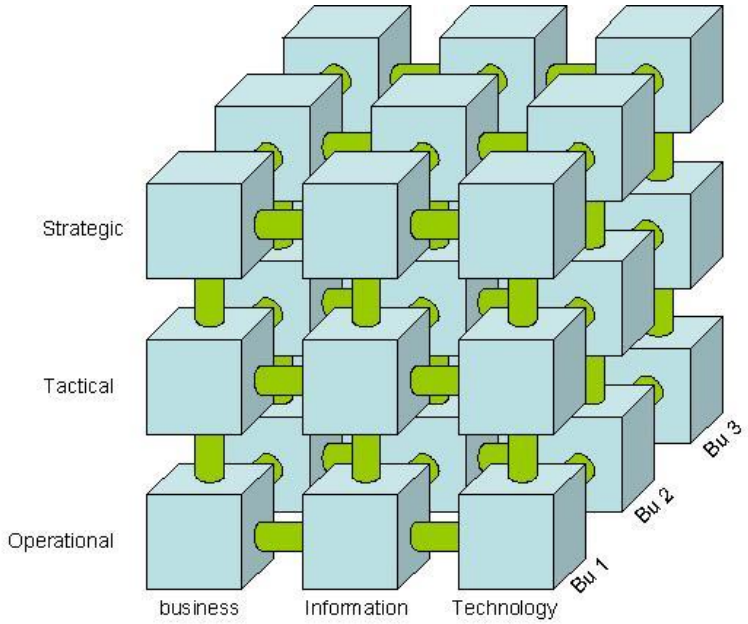
Medidas tomadas pela gestão com vistas a enfrentar os riscos e fornecer segurança razoável de que os objetivos serão alcançados.

Controles internos da gestão: 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 (...)

IN 01/2016

CONCEITOS

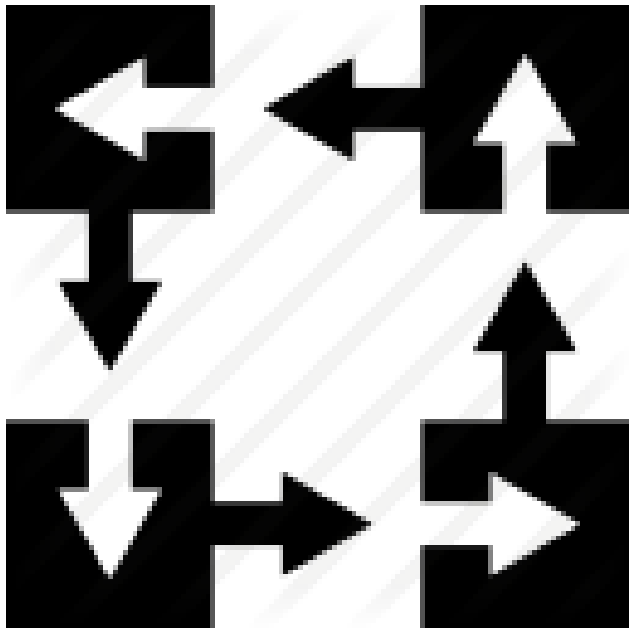
Framework



Conjunto de conceitos e boas práticas usados para orientar as atividades relacionadas a um domínio específico

CONCEITOS

Metodologia



Explicação **minuciosa**, **detalhada**, **rigorosa** e **exata** de **toda ação** desenvolvida no método (caminho) de trabalho

CONCEITOS

Política

Declaração das intenções, comprometimento e diretrizes gerais de uma organização relacionadas à gestão de riscos.

OBJETIVO DA GESTÃO DE RISCOS

Permitir o TRATAMENTO ADEQUADO dos EVENTOS (riscos e oportunidades), de forma a melhorar a capacidade de CONSTRUIR VALOR, proporcionando SERVIÇOS mais EFETIVOS, EFICIENTES E EFICAZES

PROPÓSITO (ISO 31000/2018):
Criação e proteção de valor

GESTÃO DE RISCOS – BENEFÍCIOS

- Cria e protege valor
- Melhoria da performance
- Encoraja a inovação
- Aumenta a probabilidade de alcance dos objetivos
- Melhor alocação dos recursos
- Proporciona base confiável para a tomada de decisão
- Melhora a governança
- Melhora a confiança das partes interessadas

GESTÃO DE RISCOS – MITOS

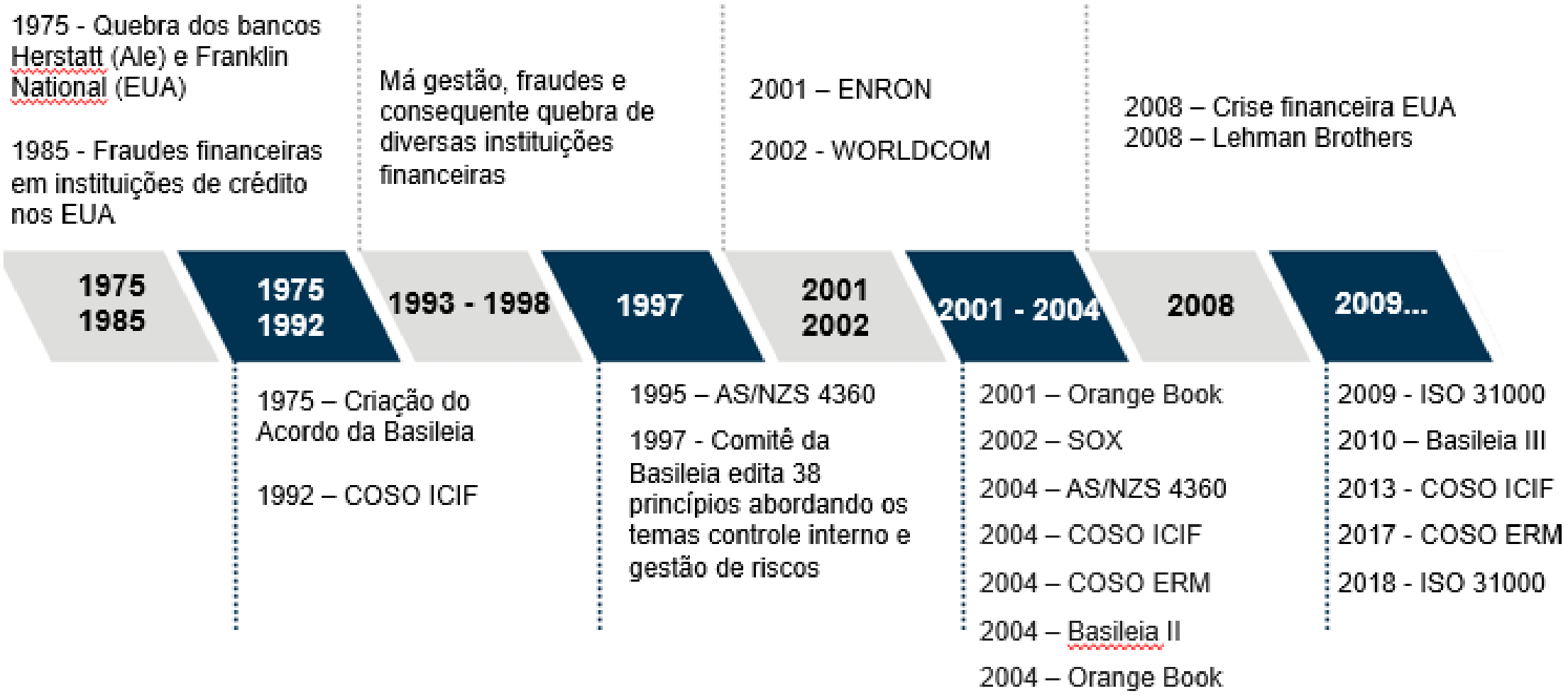
Fontenelle, 2017

CONTEXTO

MUNDO VICA

- **V**olátil
- **I**ncerto
- **C**omplexo
- **A**mbíguo

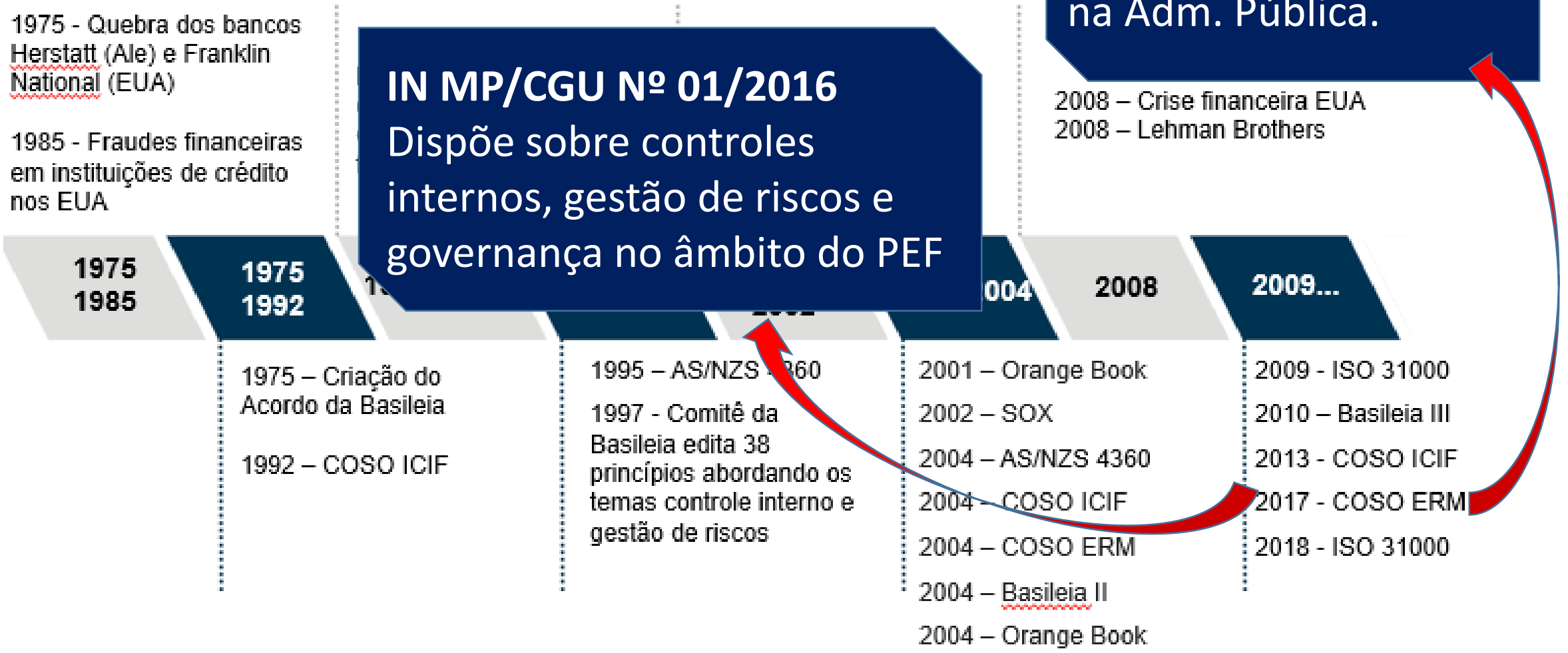
EVOLUÇÃO HISTÓRICA – CONTROLE & RISCO



EVOLUÇÃO HISTÓRICA – CONTROLE & RISCO

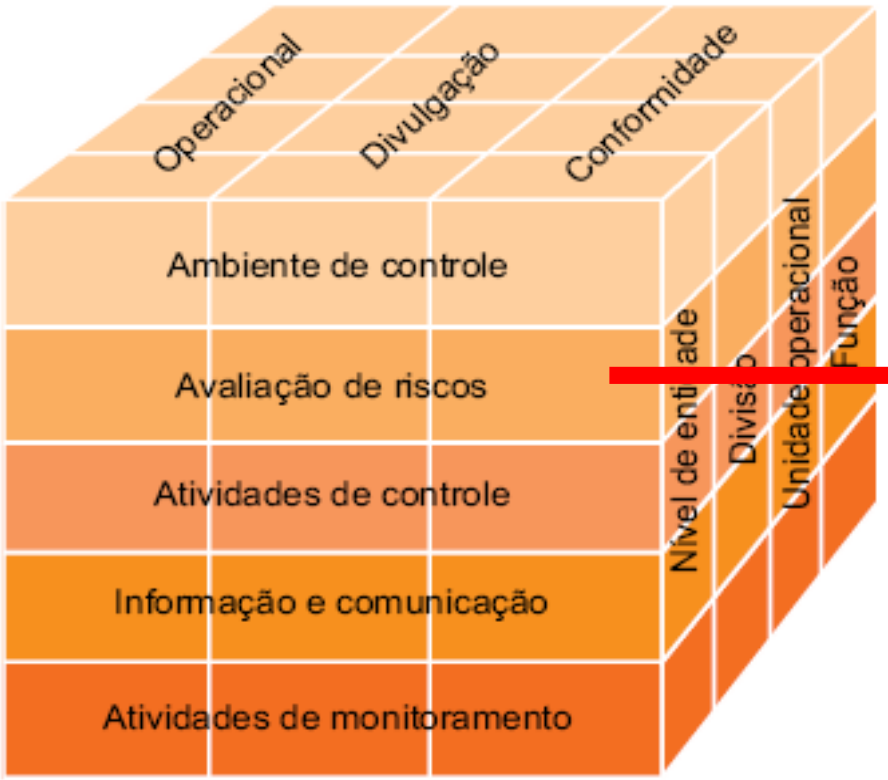
DECRETO nº 9.203/2017: Política de Governança na Adm. Pública.

IN MP/CGU Nº 01/2016 Dispõe sobre controles internos, gestão de riscos e governança no âmbito do PEF



Comparativo COSO ICIF x COSO ERM

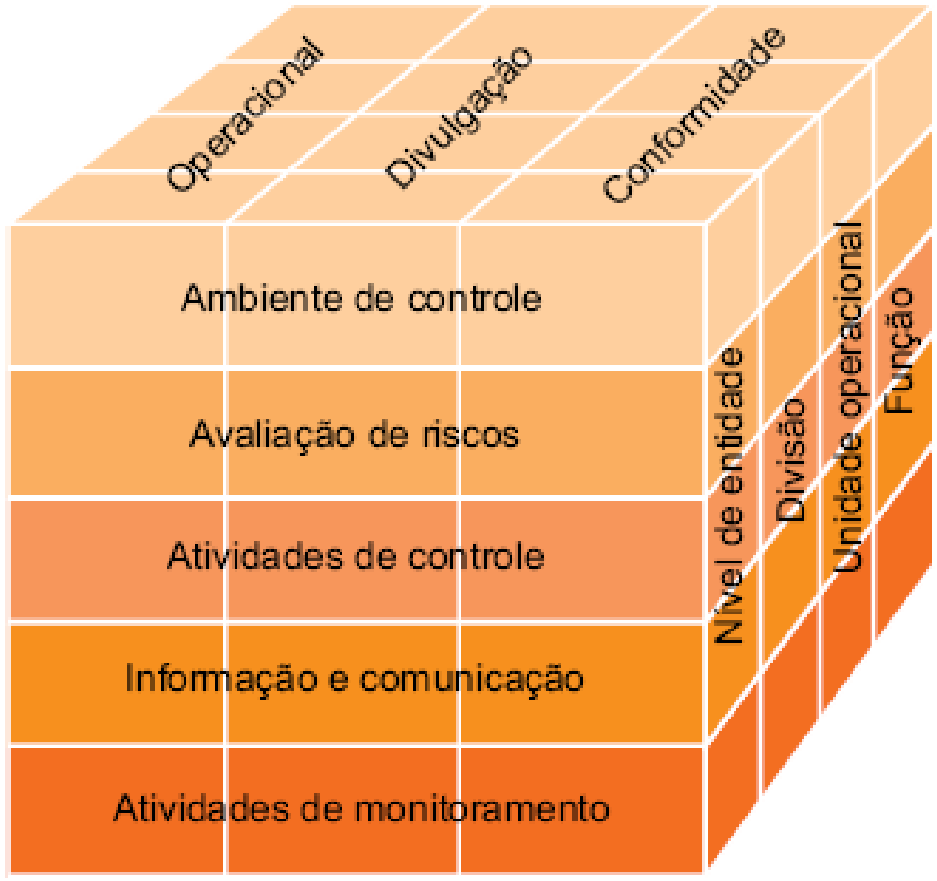
COSO ICIF



COSO ERM

PROCESSO DO CONTROLE INTERNO

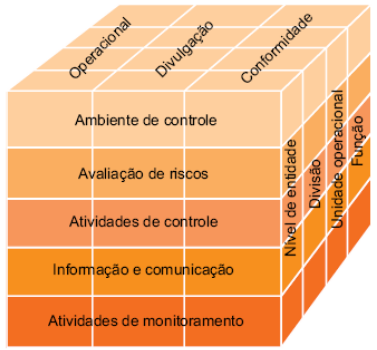
PRINCÍPIOS PARA O CONTROLE INTERNO EFICAZ – para cada dimensão



Ambiente de controle **ETC.**

1. Aderência à integridade e a valores éticos
2. Competência da alta administração em exercer a supervisão do desenvolvimento e do desempenho dos controles internos da gestão
3. Coerência e harmonização da estrutura de competências e reponsabilidades dos diversos níveis de gestão do órgão ou entidade
4. Compromisso da alta administração em atrair, desenvolver e reter pessoas com competências técnicas, em alinhamento com os objetivos da organização
5. Clara definição dos responsáveis pelos diversos controles internos da gestão no âmbito da organização

PROCESSO DO CONTROLE INTERNO



AMBIENTE DE CONTROLE

C 1. AMBIENTE DE CONTROLE (p. 38)

- **P 1. Demonstra comprometimento com a integridade e os valores éticos (p. 40)**
  - PF 1.1. Liderar pelo exemplo (p. 40)
  - PF 1.2. Estabelecer normas de conduta (p. 42)
  - PF 1.3. Avaliar a adesão às normas de conduta (p. 44)
  - PF 1.4. Tratar desvios de forma oportuna (p. 44)
- **P 2. Cumpre a responsabilidade de supervisão (p. 46)**
  - PF 2.1. Estabelecer as responsabilidades pela supervisão (p. 46)
  - PF 2.2. Utilizar experiências relevantes (p. 47)
  - PF 2.3. Operar de forma independente (p. 47)
  - PF 2.4. Exercer a supervisão do sistema de controle interno (p. 49)
- **P 3. Estabelece a estrutura, a autoridade e a responsabilidade (p. 51)**
  - PF 3.1. Considerar todas as estruturas da entidade (p. 51)
  - PF 3.2. Estabelecer linhas de subordinação (p. 53)
  - PF 3.3. Definir, atribuir e limitar autoridades e responsabilidades (p. 54)
- **P4. Demonstra comprometimento com a competência (p.55)**
  - PF 4.1. Estabelecer políticas e práticas (p. 55)
  - PF 4.2. Avaliar a competência e tratar as deficiências (p. 56)
  - PF 4.3. Atrair, desenvolver e reter talentos (p. 57)
  - PF 4.4. Planejar e preparar a sucessão (p. 57)
- **P 5. Reforça a responsabilidade pela prestação de contas (p. 58)**
  - PF 5.1. Exigir a prestação de contas por meio de estruturas, autoridades e responsabilidades (p. 58)
  - PF 5.2. Estabelecer métricas, incentivos e recompensas de desempenho (p. 60)
  - PF 5.3. Avaliar continuamente a relevância de métricas, incentivos e recompensas de desempenho (p. 62)
  - PF 5.4. Considerar pressões excessivas (p. 61)
  - PF 5.5. Avaliar o desempenho e recompensar ou disciplinar as pessoas

Coso, 2013

FRAMEWORK: COSO ERM (2017)

COSO ERM (2017)

GOVERNANÇA E CULTURA

1. Exercer a supervisão dos riscos pela alta direção
2. Estabelecer estruturas operacionais
3. Definir a cultura desejada
4. Demonstrar compromisso com valores centrais
5. Atrair, desenvolver e reter capacidades individuais

COSO ERM (2017)

ESTRATÉGIA E DEFINIÇÃO DE OBJETIVOS

6. Analisar o contexto do negócio
7. Definir o Apetite ao Risco
8. Avaliar Estratégias Alternativas
9. Formular objetivos do negócio

COSO ERM (2017)

DESEMPENHO

10. Identificar o risco
11. Avaliar a severidade do risco
12. Priorizar Riscos
13. Implementar resposta ao risco
14. Desenvolver a visão de portfólio

COSO ERM (2017)

REVISÃO

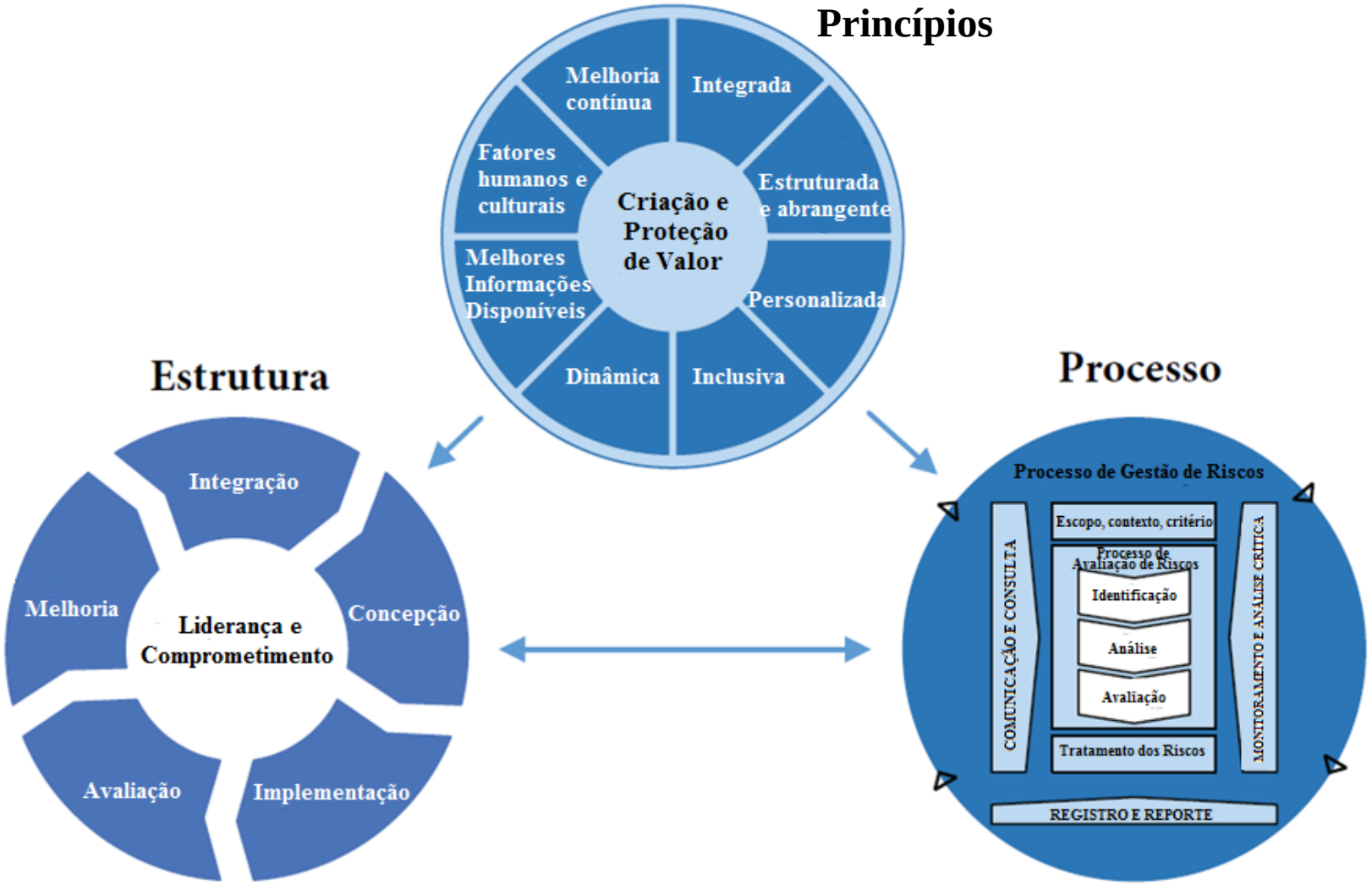
15. Avaliar mudanças substanciais
16. Revisar risco e desempenho
17. Perseguir a melhoria na GRC

COSO ERM (2017)

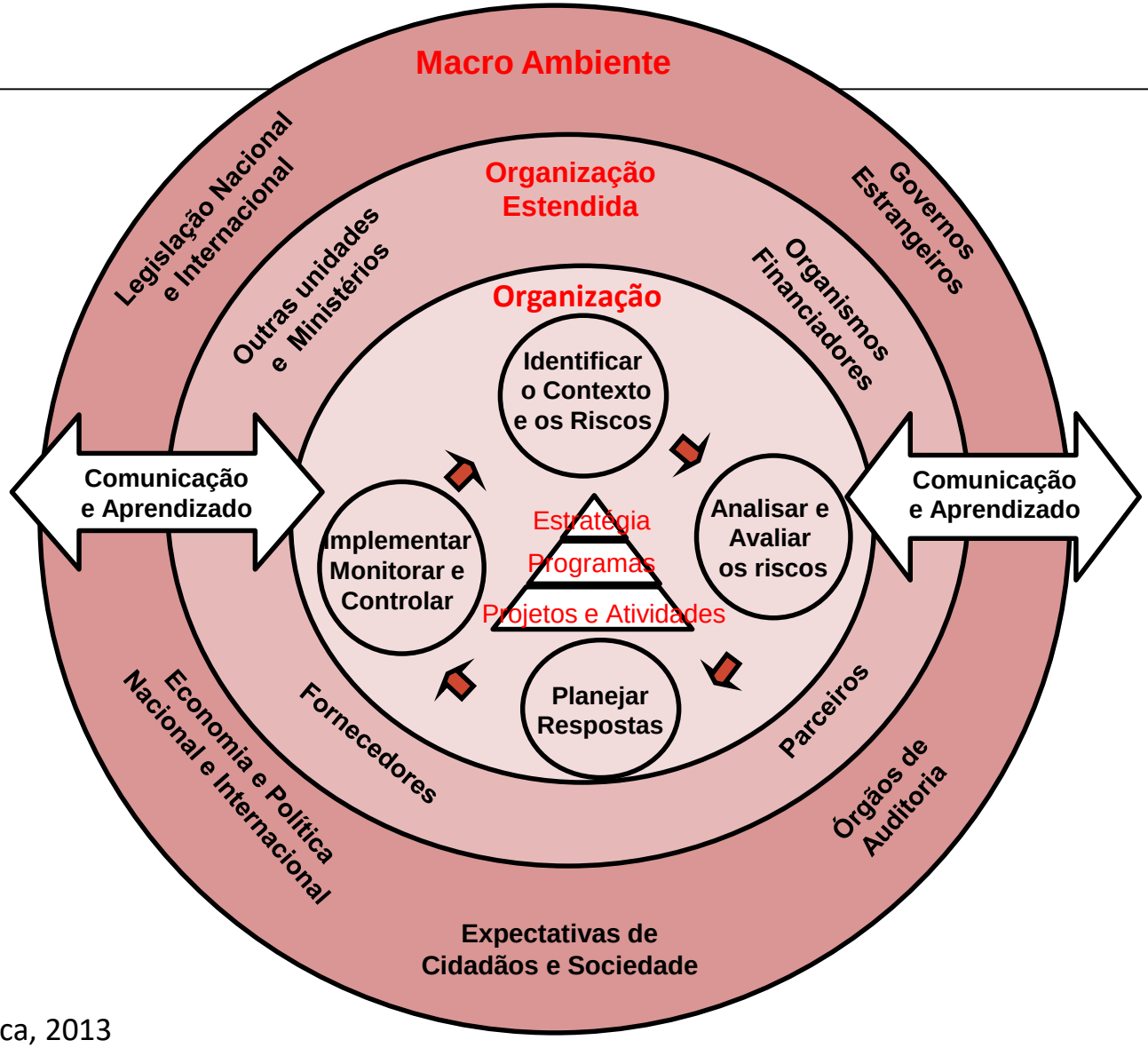
INFORMAÇÃO, COMUNICAÇÃO E REPORTE

18. Alavancar informação e tecnologia
19. Comunicar informações sobre risco
20. Relatar sobre risco, cultura e desempenho

ISO 31000:2018



ORANGE BOOK



Fonte: Gespública, 2013

Outros

COBIT
GOVERNANCE, CONTROL and ASSURANCE for INFORMATION and RELATED TECHNOLOGY

DECRETO nº 9.203, de 22/11/2017

Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional

IN MP/CGU Nº 01, de 10/5/2016

Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal

APLICAÇÕES DO TEMA NO PODER EXECUTIVO FEDERAL

Políticas de GR nos Entes Públicos

Portaria nº 674/2014 – Política de GR da RFB

Portaria nº 627/2014 – Política de GR da PGFN

Portaria nº 426/2016 – Política de Gestão de Integridade, Riscos e Controles Internos da Gestão do MP *

RI nº 020/2016 – Política Corporativa de GR, Controle Interno e Conformidade do SERPRO

Política de Gestão de Riscos do STJ/2016

Resolução nº 287/2017 – Política de GR do TCU

APLICAÇÕES DO TEMA NO PODER EXECUTIVO FEDERAL

GR no Ministério da Saúde

- Portaria 1822/2017: Institui a Política de Gestão de Integridade, Riscos e Controles Internos da Gestão PGIRC no âmbito do Ministério da Saúde

APLICAÇÕES DO TEMA NO PODER EXECUTIVO FEDERAL

GR no Ministério da Economia – Integra aproximadamente 50 órgãos

- Política de Gestão de Riscos, para todo o ME;
- Institucionalização do Sistema AGATHA, desenvolvido pelo MP;
- Abordagem descentralizada, devido à pluralidade de maturidade
- Guia de Gestão de Riscos, em finalização.

https://www.gov.br/economia/pt-br/acesso-a-informacao/acoes-e-programas/integra/governanca/comites-tematicos-de-apoio-a-governanca/comite-de-gestao-de-riscos-transparencia-controle-e-integridade

APLICAÇÕES DO TEMA NO PODER EXECUTIVO FEDERAL

Portaria CGU nº 915/2017 – Política GR da CGU

Princípios

Objetivos da Gestão de Riscos

Processo

- entendimento do contexto
- análise dos riscos
- avaliação dos riscos
- priorização dos riscos
- respostas aos riscos
- comunicação e monitoramento

Competências

- Comitê de Gestão Estratégica
- Comitê Gerencial
- Núcleo de Gestão de Riscos
- Proprietários dos Riscos

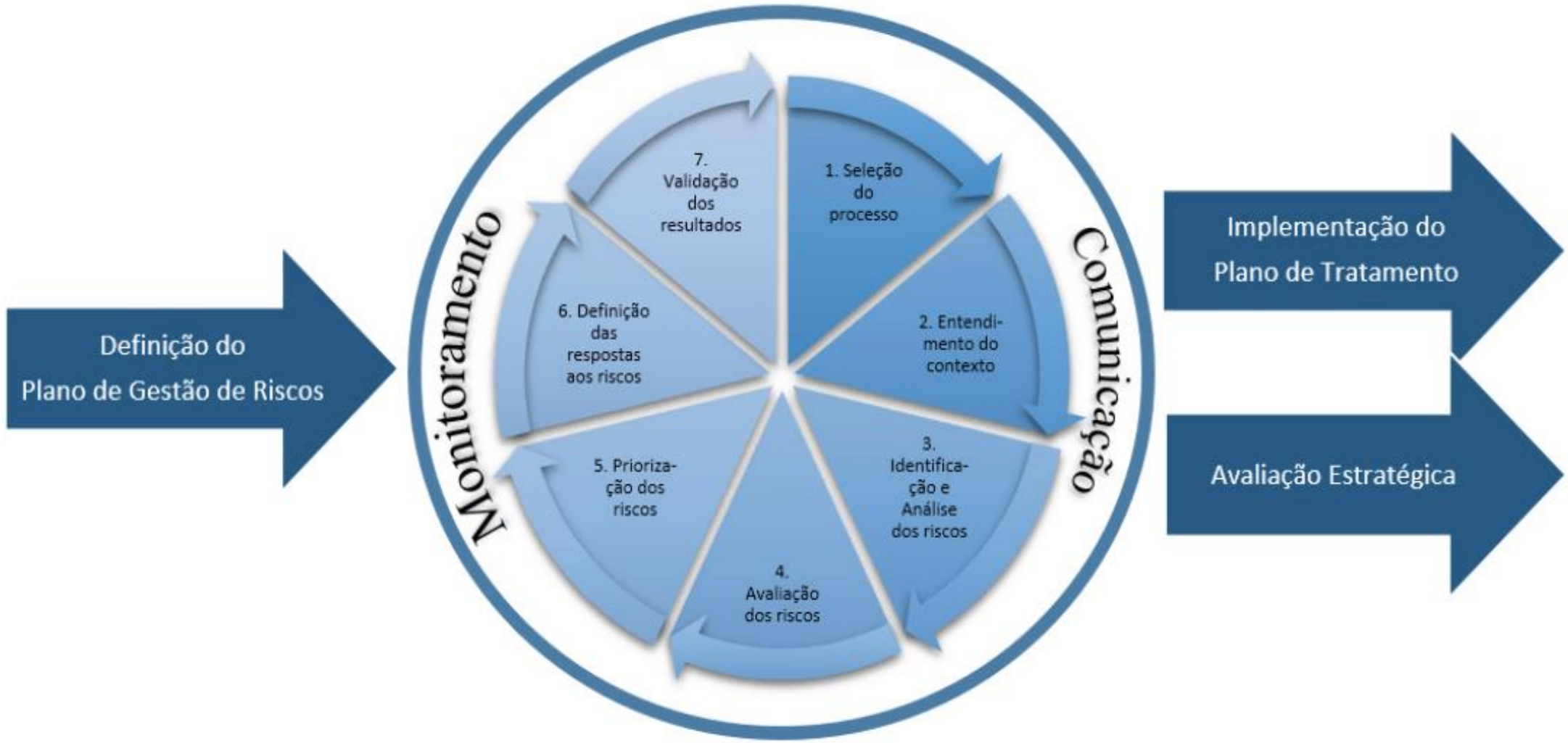
Política de Gestão de Riscos da CGU - Responsabilidades

METODOLOGIA

- **Metodologia de Gestão de Riscos da CGU (Portaria CGU nº 910/2018)**
https://www.gov.br/cgu/pt-br/assuntos/noticias/2018/04/cgu-lanca-metodologia-para-implantacao-da-gestao-de-riscos

PROCESSO DE GESTÃO DE RISCOS

Metodologia CGU - Etapas



ENTENDIMENTO DO CONTEXTO

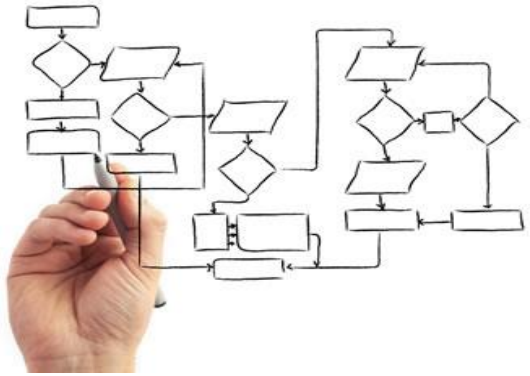
Metodologia CGU – Entendimento do Contexto

- Descrição do processo
- Fluxo (mapa) do processo
- Objetivos do processo organizacional
- Ligação com os objetivos estratégicos
- Leis e regulamentos relacionados ao processo
- Ciclo médio do processo
- Sistemas tecnológicos que apoiam o processo
- Partes interessadas, internas ou externas
- Contexto interno e externo

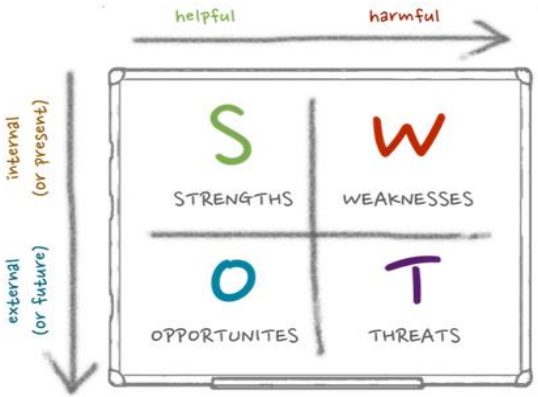
RISCOS – IDENTIFICAÇÃO

Brainstorm

Método Delphi



Mapeamento de Processos



Matriz SWOT

RISCOS – IDENTIFICAÇÃO

FERRAMENTAS & TÉCNICAS (conforme ISO/IEC 31010)	PROCESSO DE AVALIAÇÃO DE RISCOS (conforme ISO 31000)				
	IDENTIFICAÇÃO DE RISCOS	ANÁLISE DE RISCOS			AVALIAÇÃO DE RISCOS *(DECISÃO)*
		CONSEQUÊNCIA	PROBABILIDADE	NÍVEL DE RISCO	
Brainstorming	AA	NA	NA	NA	NA
Entrevistas Estruturadas ou Semi-Estruturadas	AA	NA	NA	NA	NA
Técnica de Delphi	AA	NA	NA	NA	NA
Checklists	AA	NA	NA	NA	NA
Análise Preliminar de Perigos (APP)	AA	NA	NA	NA	NA
Estudo de Perigos e Operabilidade (HAZOP)	AA	AA	A	A	A
Análise de Perigos e Pontos Críticos de Controle (HACCP)	AA	AA	NA	NA	AA
Avaliação de Riscos Ambientais	AA	AA	AA	AA	AA
Técnica Estruturada de *What-If* (SWIFT)	AA	AA	AA	AA	AA

Fonte: ISO 31010:2009

Metodologia CGU – Identificação de Riscos

Que eventos podem...

- EVITAR
- IMPEDIR
- ATRASAR
- PREJUDICAR

... o atingimento de um ou mais objetivos do processo?

Documentos de apoio:
- Organograma
- Opinião de especialistas
- Dados históricos
- Relatórios de auditoria
- Fluxograma do processo

Metodologia CGU - Análise e Revisão

- O evento é um risco que pode comprometer claramente um objetivo do processo?
- O evento é um risco ou uma falha no desenho do processo?
- À luz dos objetivos do processo, o evento é um risco ou uma causa/consequência de um risco?
- O evento é um risco ou uma fragilidade de controle para tratar um risco do processo?

ANÁLISE E REVISÃO - Principais Erros

Negativa do Objetivo:

Não selecionar a proposta mais vantajosa

Descrição Genérica:

Falhas na alimentação do processo

Ótica do Terceiro:

Licitante apresentar informação inidônea

Ótica do Controle:

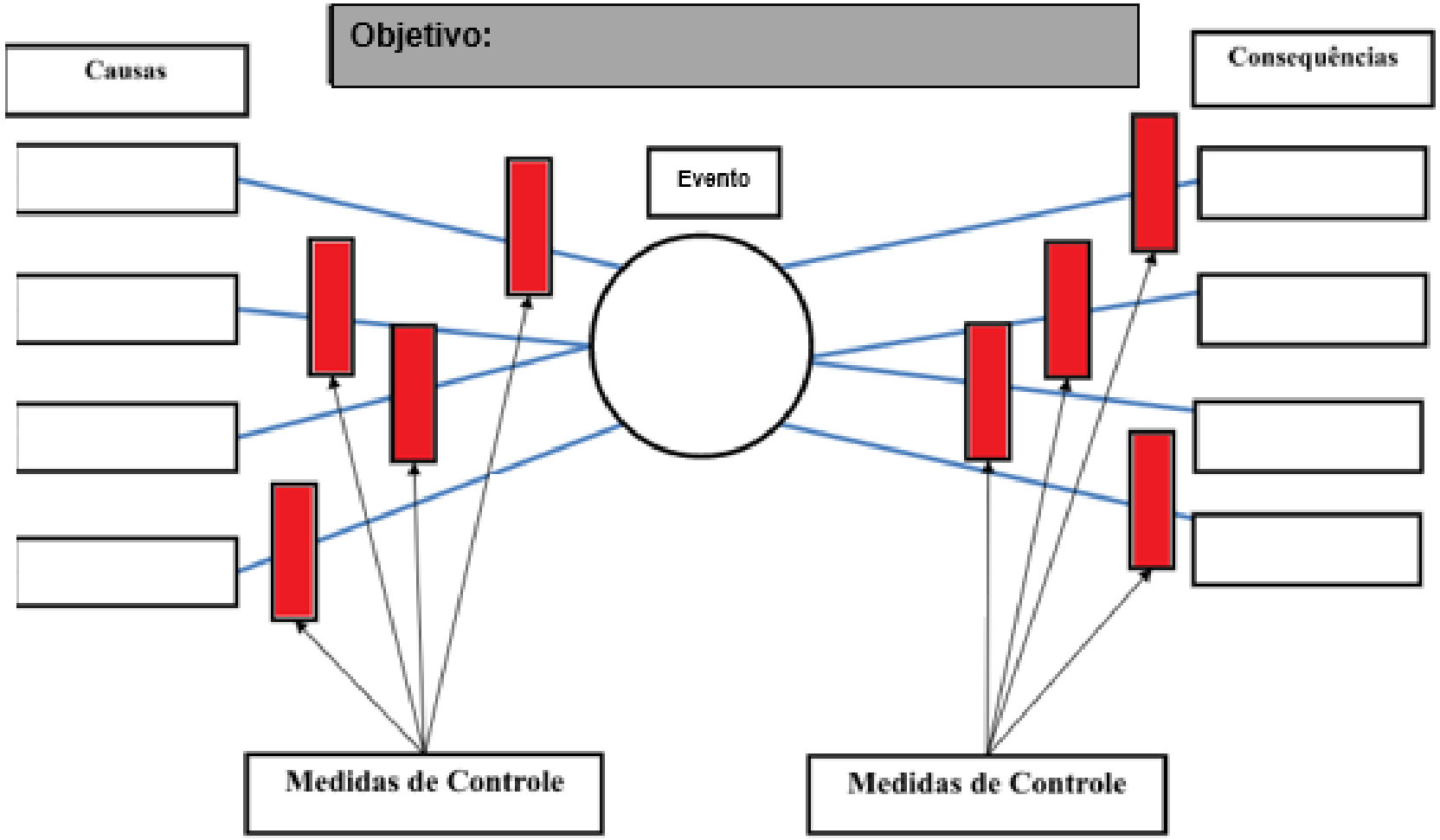
Analista não realizar as conferências exigidas

Metodologia CGU – Identificação e Análise

Para eventos identificados como riscos do processo, deve-se indicar:

- Objetivo do processo/etapa impactado pelo risco
- Categoria do risco:
    - Operacional
    - Legal
    - financeiro/orçamentário
    - integridade

RISCOS – Identificação



Fonte: ISO 31010:2009

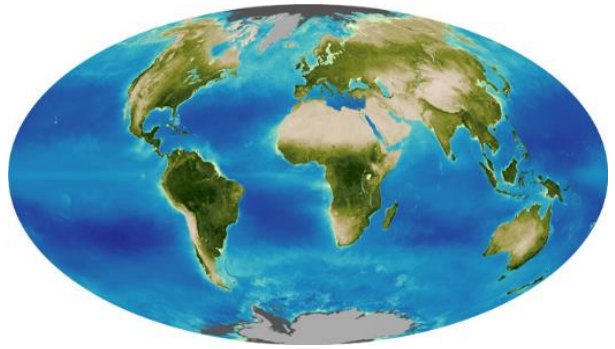
RISCOS – Análise (CAUSA)

- situações ou motivos que podem promover a ocorrência do risco -

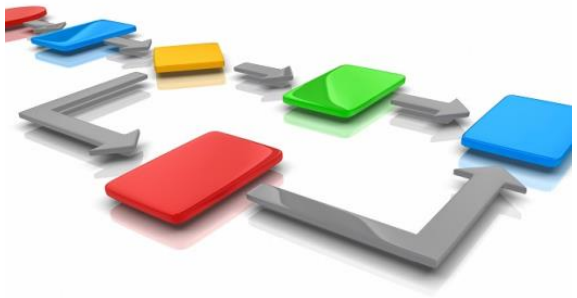
RISCOS – Análise (CAUSA – FONTE DE RISCO)

Pessoas

Sistemas



Eventos Externos



Processos

Infraestrutura

Tecnologia

RISCOS – Análise (CAUSA)

Fator de Risco	Fragilidade
Pessoa	Baixa Capacitação, desmotivada, estressada, negligente, corrupta, etc.
Processo	Ineficiente, mal estruturado, redundante, imaturo, etc.
Sistema	Obsoleto, incompatível, sem documentação, baixa segurança, etc.
Tecnologia	Ultrapassada, alto custo, baixa acessibilidade, alta complexidade, etc.
Infraestrutura	Inadequada, Inacessível, Ineficiente, Precária, etc.
Evento Externo	Desastre Ambiental, Crise Econômica, Influência Política, etc.

Fonte: Elaboração própria

CAUSA

FONTE/FATOR + FRAGILIDADES

RISCOS – Análise (CAUSA)

ATENÇÃO!

Fragilidades nos controles implementados para mitigar um determinado risco NÃO devem ser tratadas como causa primária desse risco.

RISCOS – Análise (CONSEQUÊNCIA)

- resultados do risco que afetam os objetivos -

RISCOS – SINTAXE

DESCRIÇÃO DE RISCOS

Devido a <CAUSAS/FONTES>, poderá acontecer <DESCRIÇÃO DA INCERTEZA>, o que poderá levar a <DESCRIÇÃO DO IMPACTO/CONSEQUÊNCIA/EFEITO> impactando no/na <DIMENSÃO DE OBJETIVO IMPACTADA>

Fonte: TCU, 2013

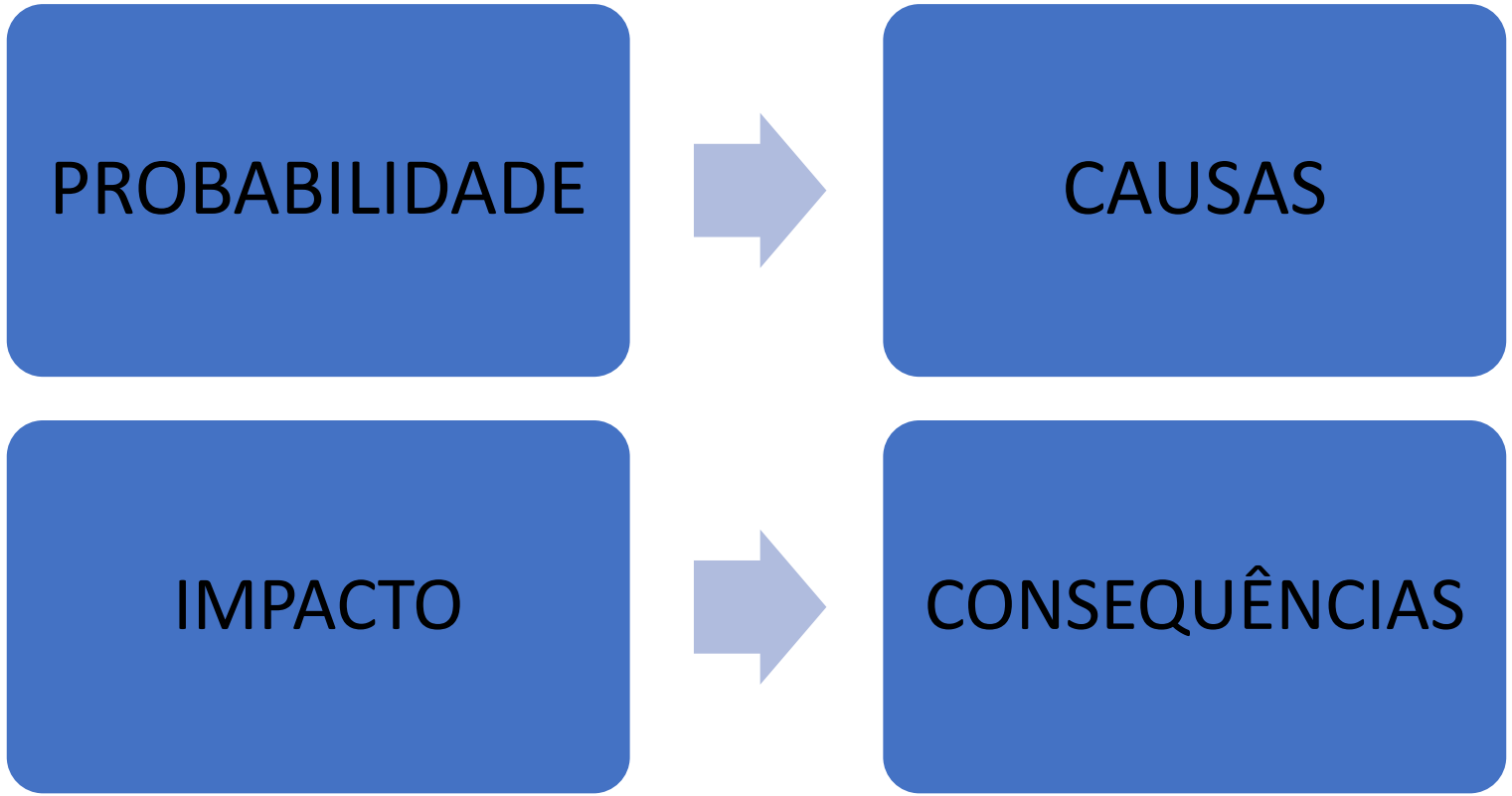
RISCOS – SINTAXE

DESCRIÇÃO DE RISCOS

Devido à ausência de manutenção preventiva, o sistema de climatização poderá não manter a temperatura apropriada, o que poderá ocasionar pane dos servidores de rede do edifício sede, implicando em indisponibilidade temporária de informações e sistemas da unidade.

AVALIAÇÃO DE RISCOS

PROBABILIDADE X IMPACTO



AVALIAÇÃO DE RISCOS – NÍVEL DE RISCO

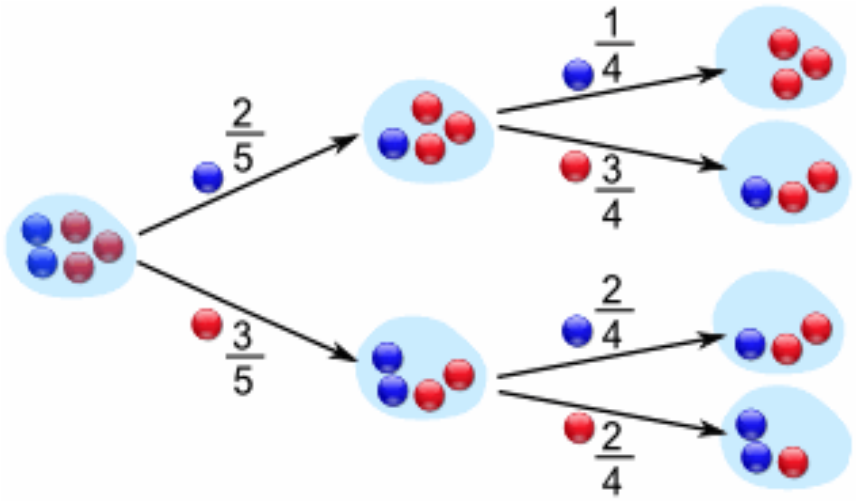
IMPACTO						
	Muito Alto 10	10 RM	20 RM	50 RA	80 RE	100 RE
	Alto 8	8 RB	16 RM	40 RA	64 RA	80 RE
	Médio 5	5 RB	10 RM	25 RM	40 RA	50 RA
	Baixo 2	2 RB	4 RB	10 RM	16 RM	20 RM
	Muito Baixo 1	1 RB	2 RB	5 RB	8 RB	10 RM
		Muito Baixa 1	Baixa 2	Média 5	Alta 8	Muito Alta 10
		PROBABILIDADE				

AVALIAÇÃO DE RISCOS – CRITÉRIOS

Fonte: COSO, 2012

AVALIAÇÃO DE RISCOS – CRITÉRIOS

Qualitativo



Quantitativo

OBSERVAÇÃO:

Uma análise mista, que mistura aspectos quantitativos e qualitativos terá um resultado QUALITATIVO!

AVALIAÇÃO DE RISCOS – CRITÉRIOS

Comparação entre as técnicas de mensuração do risco		
Técnica	**Vantagens**	**Desvantagens**
Qualitativa	• Relativamente rápida e fácil • Fácil compreensão, não requer treinamento em técnicas sofisticadas de análise • Permite avaliações que não se restringem a impacto financeiro e probabilidade, como vulnerabilidade, velocidade e persistência do impacto, segurança, reputação, etc	• Provê diferenciação limitada entre os níveis de risco (ex: muito alto, alto, médio e baixo) • Imprecisa - riscos situados no mesmo nível podem apresentar diferenças consideráveis no valor de seus critérios • Limitação quanto à análise de custo-benefício das respostas ao risco
Quantitativa	• Permite agregação numérica considerando interações dos riscos • Permite análise de custo-benefício na escolha das respostas ao risco • Permite que a alocação do capital seja baseada no risco, visando um retorno ideal • Permite computar a necessidade de capital para manter a solvência da organização em condições extremas	• Requer tempo e recursos, especialmente na construção do modelo de avaliação • Pode implicar em precisão maior que a realidade devido às incertezas dos valores de entrada • Presunções podem não ficar claras • Pode resultar na negligência de impactos qualitativos

Fonte: COSO, 2012

Metodologia CGU – Escala de Probabilidade

Probabilidade	Descrição da probabilidade	Peso
Muito baixa	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	1
Baixa	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	2
Média	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	5
Alta	Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	8
Muito alta	Praticamente certa. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	10

Metodologia MP – Escala de Probabilidade

Probabilidade		
Escala	Descritivo da Escala	Frequência Observada/Esperada
5 - Quase Certo	Evento esperado que ocorra na maioria das circunstâncias	>= 90%
4 - Provável	Evento provavelmente ocorra na maioria das circunstâncias	>= 50% < 90%
3 - Possível	Evento deve ocorrer em algum momento	>= 20% < 50%
2 - Improvável	Evento pode ocorrer em algum momento	>= 10% < 20%
1 - Rara	Evento pode ocorrer apenas em circunstâncias excepcionais	< 10%

AVALIAÇÃO DE RISCOS – CRITÉRIOS

IMPACTO

AVALIAÇÃO DE RISCOS – CRITÉRIOS DE IMPACTO

Critérios de Impacto do Risco		
Rating	**Descrição**	**Definição**
5	Extremo	• Perda Financeira de R$ X milhões ou mais. • Cobertura por muito tempo pela mídia internacional, resultando em perda de mercado significante ao ponto de ser necessário uma mudança completa na estratégia da entidade. • Incidente reportado à regulação, resultando em multas e punições severas, incluindo prisão de líderes da organização. • Falecimento e ferimentos graves em empregados, terceirizados e clientes. • Entrega massiva de cargo pelo alto escalão da entidade.
4	Grande	• Perda Financeira de R$ X milhões a R$ X Milhões. • Cobertura por muito tempo pela mídia nacional, resultando em perda significativa de mercado. • Incidente reportado à regulação, necessitando de projetos grandes para a correção das deficiências. • Lesões físicas, resultando em algumas internações dos empregados, terceirizados e clientes. • Entrega de cargo de alguns gestores, alta debanda de membros experientes da equipe envolvida.

Fonte: COSO, 2012

AVALIAÇÃO DE RISCOS – CRITÉRIOS DE IMPACTO

3	Moderado	• Perda Financeira de R$ X milhões a R$ X Milhões. • Cobertura por pouco tempo pela mídia nacional. • Incidente reportado à regulação, com imediata resposta de correções a serem implementadas. • Lesões físicas, resultando em necessidade de tratamento médico nos empregados, terceirizados e clientes. • Problema generalizado na moral da equipe envolvida com ocorrências constantes de não aceite.
2	Pequeno	• Perda Financeira de R$ X milhões a R$ X Milhões. • Dano a reputação local. • Incidente reportado à regulação, porém sem resposta. • Lesões físicas leves nos empregados, terceirizados e clientes. • A moral da equipe envolvida sofre de problemas gerais e houve aumento de não aceite nas entregas.
1	Incidental	• Perda Financeira de até R$ X milhões. • Atenção apenas pela mídia local facilmente remediável. • Não justifica-se reportar à regulação. • Sem lesões físicas nos empregados, terceirizados e clientes. • Insatisfação isolada nos membros da equipe envolvida.

Fonte: COSO, 2012

Metodologia MP – Escala de Impacto

(http://www.planejamento.gov.br/assuntos/gestao/controle-interno/planilha-documentadora-20-02-2017-2.xlsx/view)

Impacto - Fatores para Análise							
	Estratégico-Operacional					Econômico-Financeiro	Peso
	Esforço de Gestão	Regulação	Reputação	Negócios/Serviços à Sociedade	Intervenção Hierárquica	Orçamentário	
	15%	17%	12%	18%	13%	25%	100%
Orientações para atribuição de pesos	Evento com potencial para levar o negócio ou serviço ao colapso	Determina interrupção das atividades	Com destaque na mídia nacional e internacional, podendo atingir os objetivos estratégicos e a missão	Prejudica o alcance da missão do MP	Exigiria a intervenção do Ministro	> = 25%	5-Catastrófico
	Evento crítico, mas que com a devida gestão pode ser suportado	Determina ações de caráter pecuniários (multas)	Com algum destaque na mídia nacional, provocando exposição significativa	Prejudica o alcance da missão da Unidade	Exigiria a intervenção do Secretário	> = 10% < 25%	4-Grande
	Evento significativo que pode ser gerenciado em circunstâncias normais	Determina ações de caráter corretivo	Pode chegar à mídia provocando a exposição por um curto período de tempo	Prejudica o alcance dos objetivos estratégicos	Exigiria a intervenção do Diretor	> = 3% < 10%	3-Moderado
	Evento cujas consequências podem ser absorvidas, mas carecem de esforço da gestão para minimizar o impacto	Determina ações de caráter orientativo	Tende a limitar-se às partes envolvidas	Prejudica o alcance das metas do processo	Exigiria a intervenção do Coordenador	> = 1% < 3%	2-Pequeno
	Evento cujo impacto pode ser absorvido por meio de atividades normais	Pouco ou nenhum impacto	Impacto apenas interno / sem impacto	Pouco ou nenhum impacto nas metas	Seria alcançada no funcionamento normal da atividade	< 1%	1-Insignificante

Fonte: COSO, 2012

Metodologia CGU – Escala de Impacto

Impacto	Impacto nos objetivos	Peso
Muito baixo	Mínimo impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/ divulgação ou de conformidade)	1
Baixo	Pequeno impacto nos objetivos (idem)	2
Médio	Moderado impacto nos objetivos (idem), porém recuperável	5
Alto	Significativo impacto nos objetivos (idem), de difícil reversão	8
Muito Alto	Catastrófico impacto nos objetivos (idem), de forma irreversível	10

CGU – Escala de Impacto Avaliação Estratégica (adaptado)

ESFORÇO DE GESTÃO (15%)	CEDIBILIDADE (30%)	ESTRATÉGIA (20%)	ABRANGÊNCIA DOS EFEITOS (25%)	ORÇAMENTÁRIO (10%)
EG10 - Evento com potencial para levar a CGU ao colapso	CR10 - Credibilidade na sociedade	ES10 - Prejudica o alcance da missão	PP10 - Pode levar ao colapso de política pública transversal	OR10 - >= 25 % do valor do orçamento da CGU
EG08 - Evento crítico, mas que com a devida gestão pode ser suportado	CR08 - Credibilidade nas instituições de origem nacional e/ou internacional	ES08 - Prejudica o alcance de um ou mais objetivos estratégicos	PP8 - Pode levar ao colapso de política pública	OR08 - >= 10% < 25% do valor do orçamento da CGU
EG06 - Evento significativo que pode ser gerenciado em circunstâncias normais	CR06 - Credibilidade nos produtos da CGU	ES06 - Prejudica o alcance de uma ou mais iniciativas no Planejamento Estratégico	PP6 - Pode prejudicar a política pública e demanda esforço da gestão para minimizar impacto	OR06 - >= 3% < 10% do valor do orçamento da CGU
EG04 - Consequências podem ser absorvidas, mas carecem de esforço da gestão para minimizar o impacto	CR04 - Credibilidade nos representantes da CGU	ES04 - Prejudica o alcance de uma ou mais ações no Planejamento Estratégico	PP4 - Pode prejudicar a política pública, sem demandar esforço da gestão	OR04 - >= 1 % < 3% do valor do orçamento da CGU
EG02 - Evento cujo impacto pode ser absorvido por meio de atividades normais	CR02 - Credibilidade nos servidores da CGU	ES02 - Prejudica o alcance dos objetivos/metas do processo organizacional	PP2 - Não prejudica a política pública, mas aumenta o esforço da gestão desnecessariamente	OR02 - < 1% do valor do orçamento da CGU
EG00 - Evento sem impacto na gestão	CR00 - Não afeta a credibilidade	ES00 - Nenhum impacto nas metas/objetivos do processo organizacional	PP0 - Não há impacto negativo em políticas públicas	OR00 - Sem impacto financeiro

CGU – Escala de Impacto Avaliação Estratégica (adaptado)

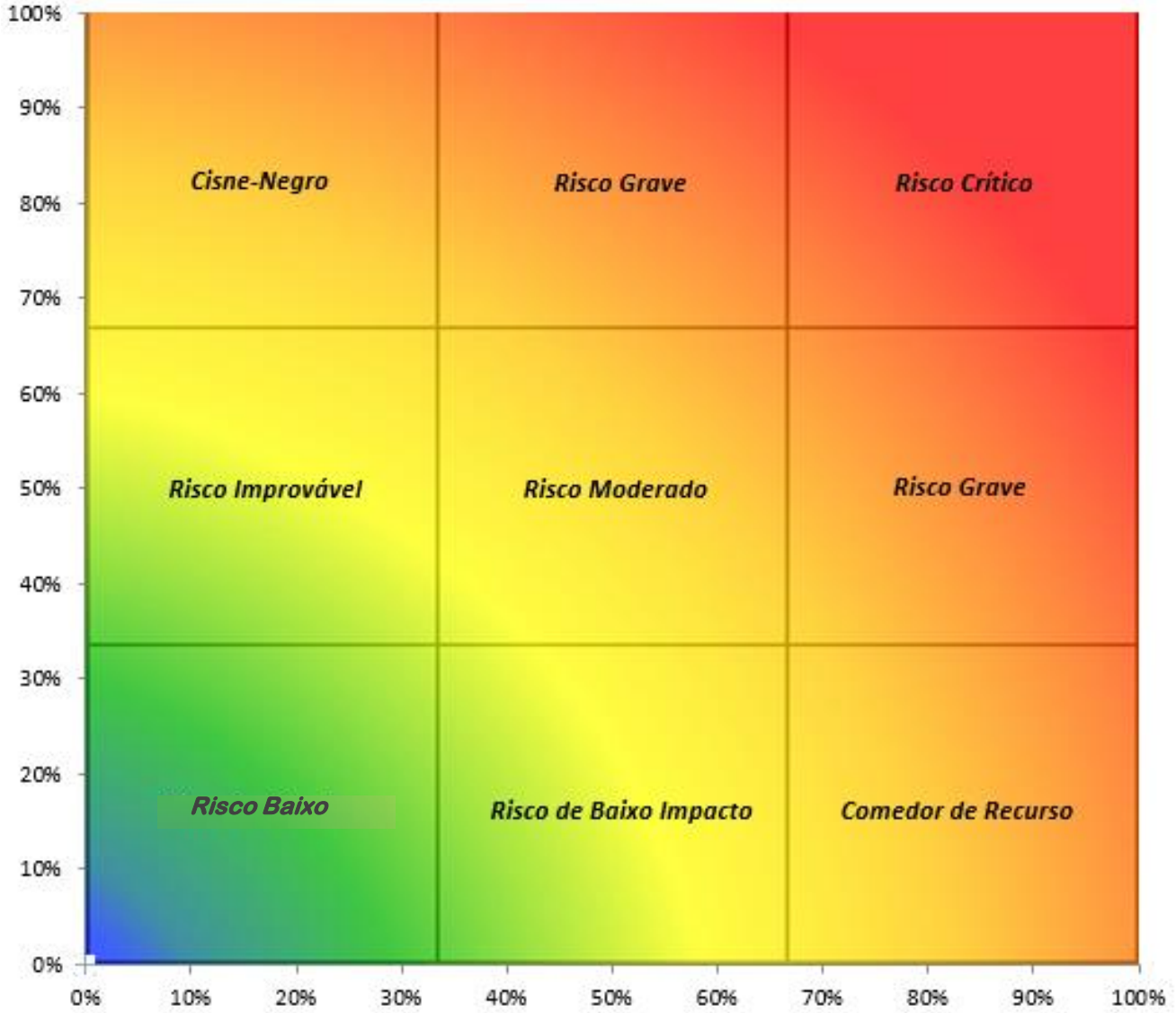
ESFORÇO DE GESTÃO (15%)	CEDIBILIDADE (30%)	ESTRATÉGIA (20%)	ABRANGÊNCIA DOS EFEITOS (25%)	ORÇAMENTÁRIO (10%)
EG10 - Evento com potencial para levar a CGU ao colapso	CR10 - Credibilidade na sociedade	ES10 - Prejudica o alcance da missão	PP10 - Pode levar ao colapso de política pública transversal	OR10 - >= 25 % do valor do orçamento da CGU
EG08 - Evento crítico, mas que com a devida gestão pode ser suportado	CR08 - Credibilidade nas instituições de origem nacional e/ou internacional	ES08 - Prejudica o alcance de um ou mais objetivos estratégicos	PP8 - Pode levar ao colapso de política pública	OR08 - >= 10% < 25% do valor do orçamento da CGU
EG06 - Evento significativo que pode ser gerenciado em circunstâncias normais	CR06 - Credibilidade nos produtos da CGU	ES06 - Prejudica o alcance de uma ou mais iniciativas no Planejamento Estratégico	PP6 - Pode prejudicar a política pública e demanda esforço da gestão para minimizar impacto	OR06 - >= 3% < 10% do valor do orçamento da CGU
EG04 - Consequências podem ser absorvidas, mas carecem de esforço da gestão para minimizar o impacto	CR04 - Credibilidade nos representantes da CGU	ES04 - Prejudica o alcance de uma ou mais ações no Planejamento Estratégico	PP4 - Pode prejudicar a política pública, sem demandar esforço da gestão	OR04 - >= 1 % < 3% do valor do orçamento da CGU
EG02 - Evento cujo impacto pode ser absorvido por meio de atividades normais	CR02 - Credibilidade nos servidores da CGU	ES02 - Prejudica o alcance dos objetivos/metas do processo organizacional	PP2 - Não prejudica a política pública, mas aumenta o esforço da gestão desnecessariamente	OR02 - < 1% do valor do orçamento da CGU
EG00 - Evento sem impacto na gestão	CR00 - Não afeta a credibilidade	ES00 - Nenhum impacto nas metas/objetivos do processo organizacional	PP0 - Não há impacto negativo em políticas públicas	OR00 - Sem impacto financeiro

Se continuar Risco Extremo ou é de Integridade → Comitê de Gestão Estratégica

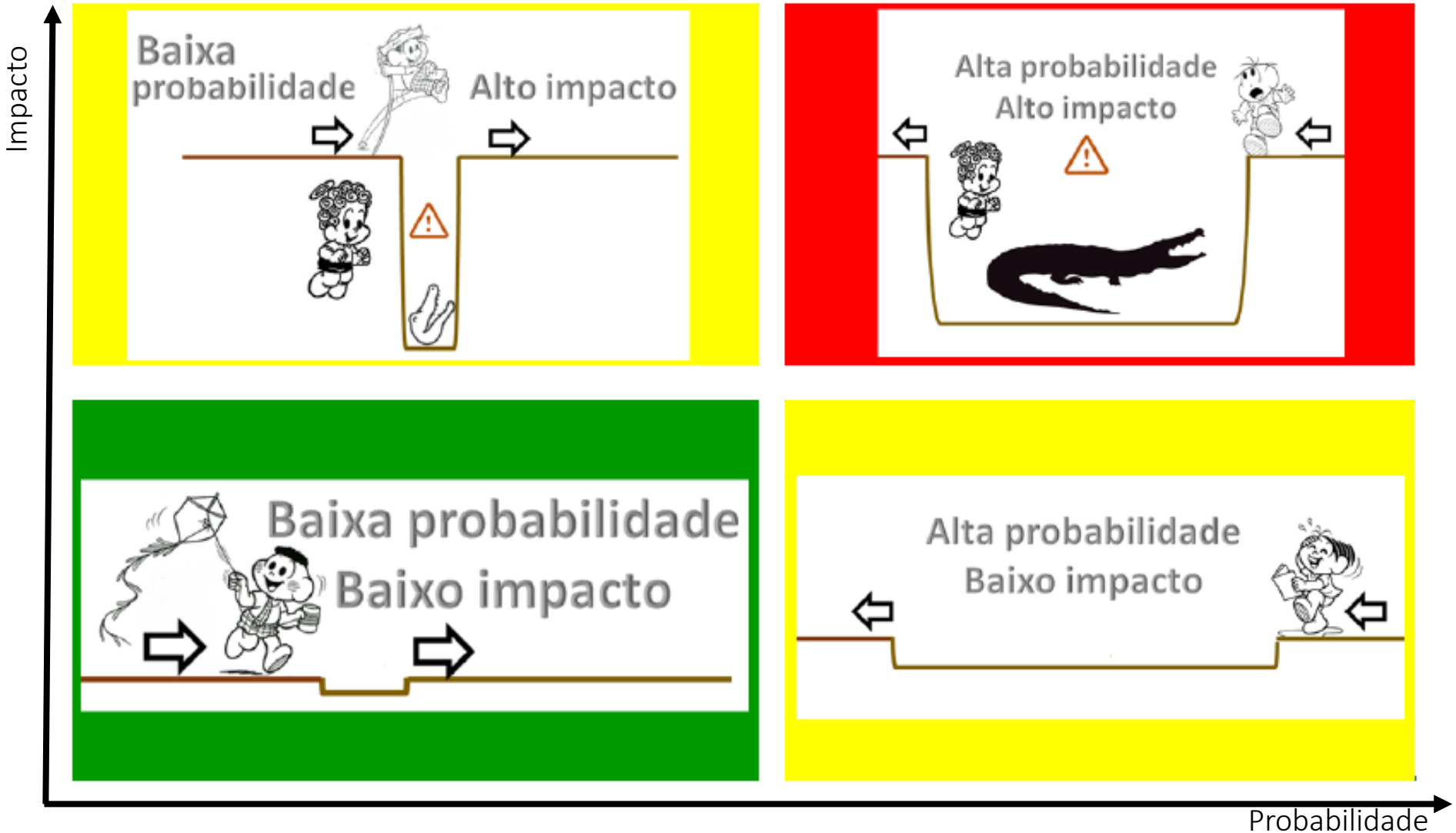
AVALIAÇÃO DE RISCOS – NÍVEL DE RISCO

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				

AVALIAÇÃO DE RISCOS – NÍVEL DE RISCO

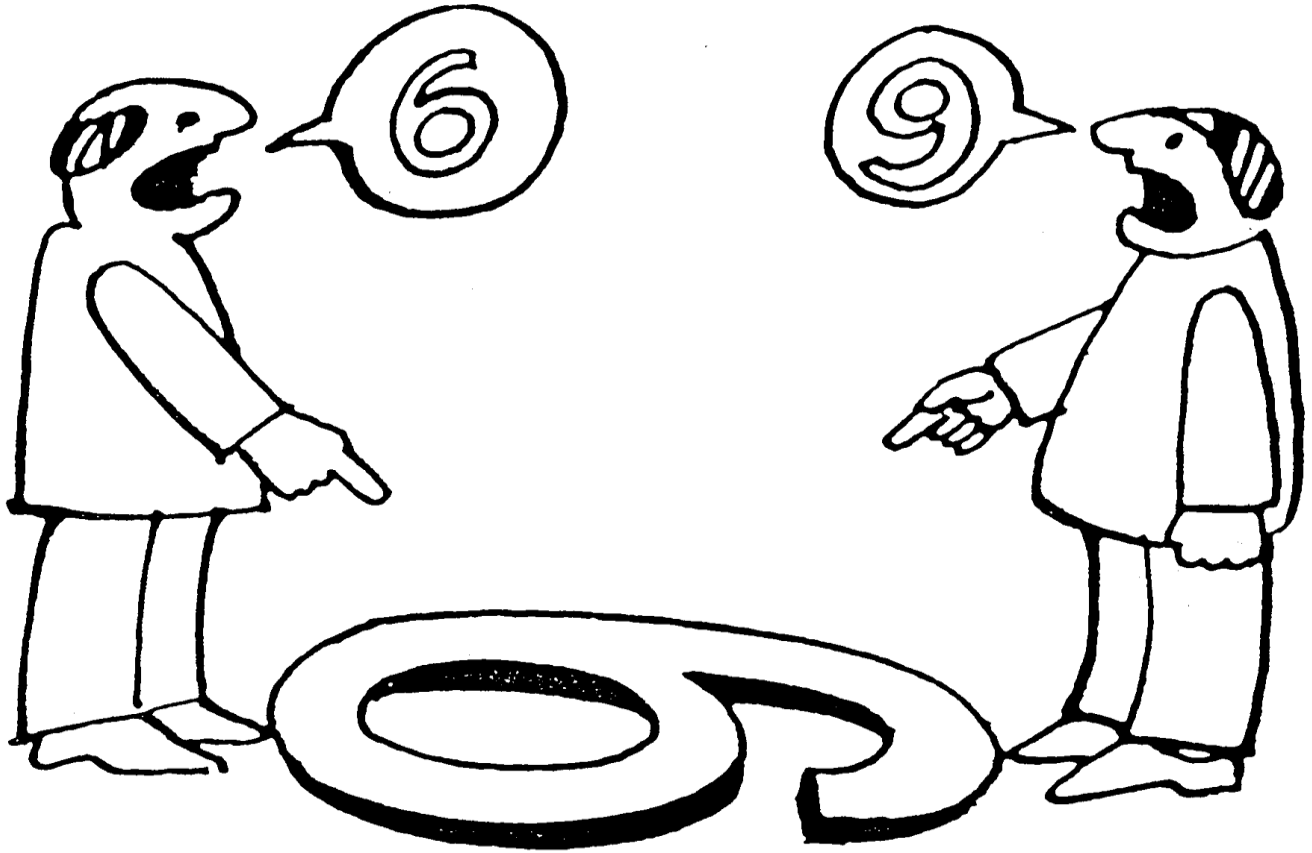


AVALIAÇÃO DE RISCOS – NÍVEL DE RISCO



RISCOS – AVALIAÇÃO – NÍVEL DE RISCO

OUTRAS VISÕES DO NÍVEL DE RISCO



AVALIAÇÃO DE RISCOS – NÍVEL DE RISCO

DECOMPONDO A PROBABILIDADE

A Probabilidade da materialização de um risco depende da correlação entre as vulnerabilidades e as ameaças presentes no processo

AVALIAÇÃO DE RISCOS – NÍVEL DO RISCO

Outras Visões do Nível de Risco: Vulnerabilidade x Impacto

Terremoto Haiti – 2010
Magnitude: 7.0
Mortos: 250.000

Terremoto Japão – 2016
Magnitude: 7.0
Mortos: 16

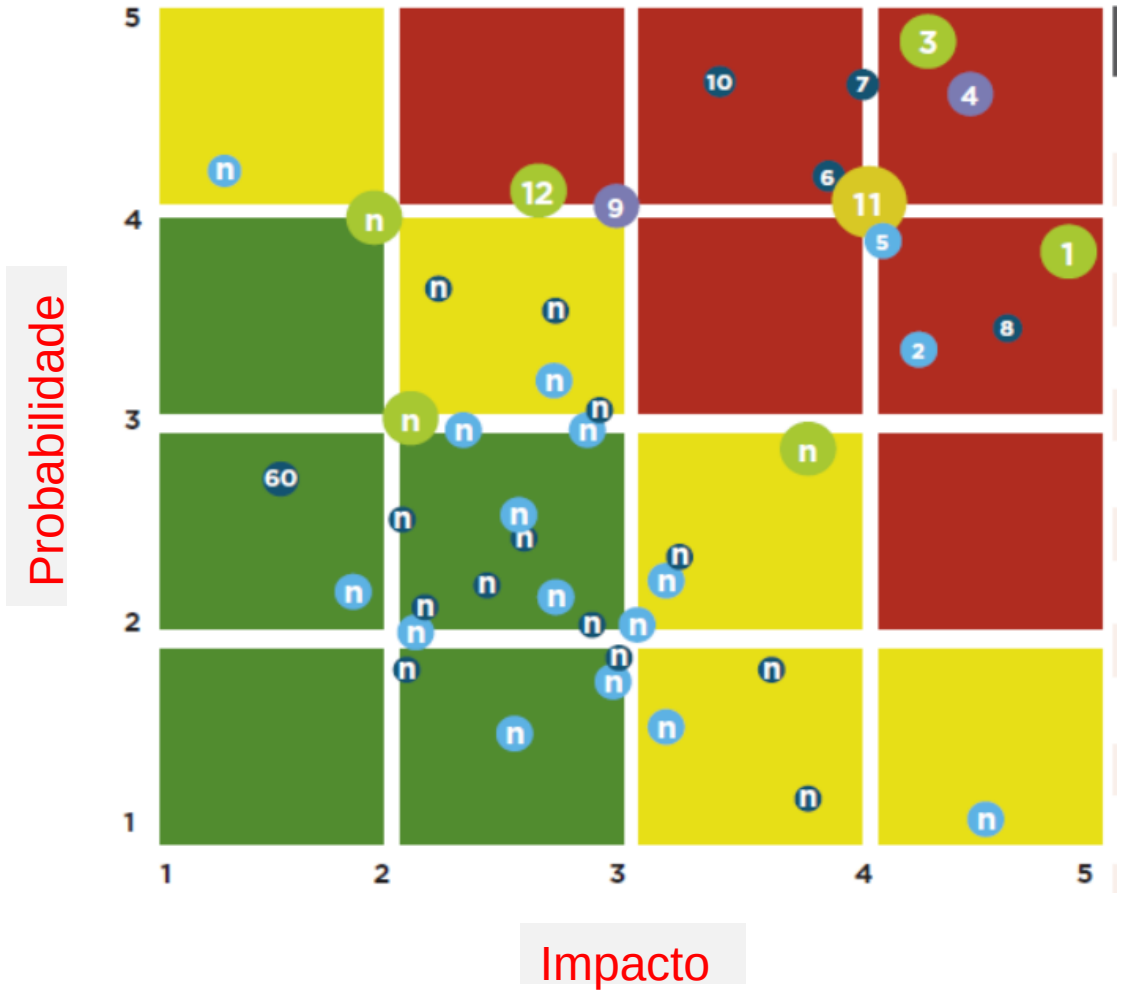
AVALIAÇÃO DE RISCOS – NÍVEL DE RISCO

DEFININDO OS CRITÉRIOS DE VULNERABILIDADE

Critérios de Vulnerabilidade do Risco		
Rating	**Descrição**	**Definição**
5	Muito Alto	• Não há planejamento de cenários. • Inexistência de capacidades nas respostas aos riscos. • Inexistência de controles implementados. • Inexistência de gestão de contingência e crise.
4	Alto	• Planejamento de cenários levando em consideração riscos chaves. • Baixa maturidade nas respostas aos riscos. • Controles parcialmente implementados e não alcance de vários objetivos. • Pouca gestão de contigência e crise implementada
3	Médio	• Realiza análise de cenários sensíveis e testes de stress. • Maturidade média nas respostas aos riscos. • Controles implementados e alcance dos objetivos na maioria dos casos. • Boa parte da gestão de contingência e crise implementada com ensaios limitados.
2	Baixo	• Opções estratégicas definidas. • Maturidade variando entre alta e média nas respostas aos riscos. • Controles implementados resultando em alcance dos objetivos a não ser em condições extremas. • Gestão de Contingência e crise implementada, com alguns ensaios.
1	Muito Baixo	• Opções reais implementadas para maximizar a flexibilidade estratégica. • Alta maturidade em todos seus processos nas respostas aos riscos. • Mecanismos de redundância implementados e com regular testes de seus riscos críticos. • Gestão de contingência e crise implementada e com ensaios regulares.

AVALIAÇÃO DE RISCOS – NÍVEL DE RISCO

OUTRAS VISÕES DO NÍVEL DE RISCO: Probabilidade X Impacto X (Vulnerabilidade, Velocidade, Persistência)



AVALIAÇÃO DE RISCOS – NÍVEL DO RISCO

OUTRA VISÃO DO NÍVEL DE RISCO: VELOCIDADE DO IMPACTO

AVALIAÇÃO DE RISCOS – NÍVEL DE RISCO

OUTRA VISÃO DO NÍVEL DE RISCO: PERSISTÊNCIA DO IMPACTO

'Recuperação da bacia do Rio Doce pode levar até 30 anos', diz ministra

Para Izabella Teixeira, Samarco ainda tem muitas perguntas a responder

Fonte: O GLOBO, 2015

RISCO INERENTE

É o risco intrínseco à atividade que está sendo realizada, está presente no estado atual das coisas, antes da adoção de medidas de resposta ao risco

RISCO RESIDUAL

É o risco remanescente após a adoção de medidas de resposta ao risco

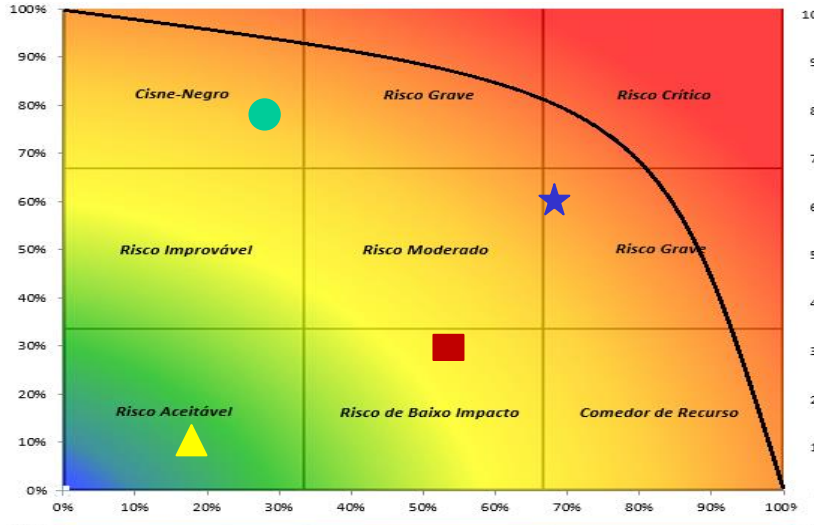
APETITE AO RISCO

APETITE A RISCO =
Nível de risco que uma organização está disposta a aceitar

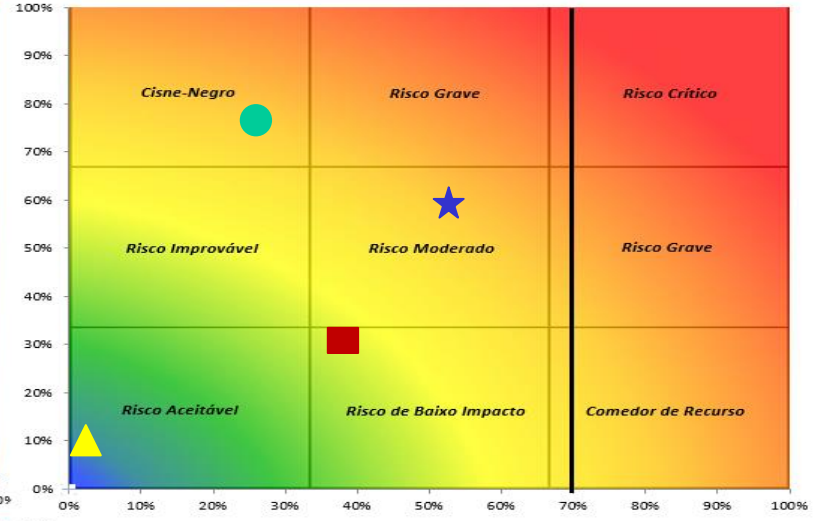
APETITE AO RISCO

APETITE AO RISCO

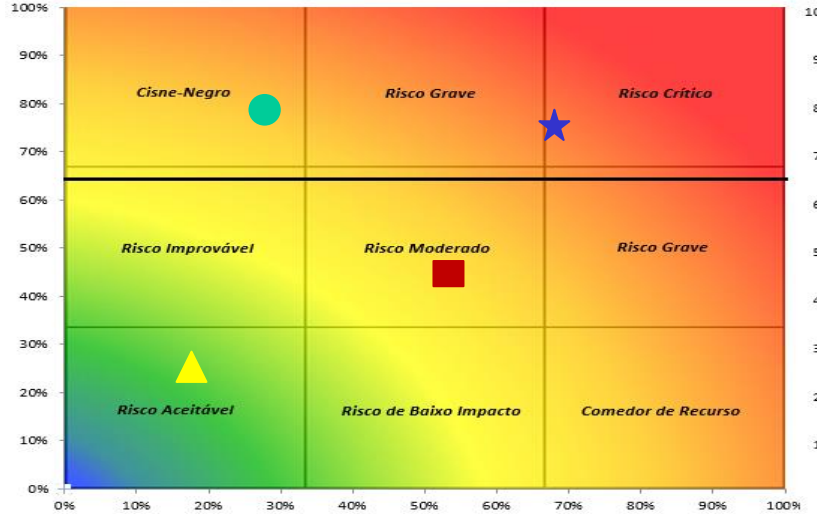
OK



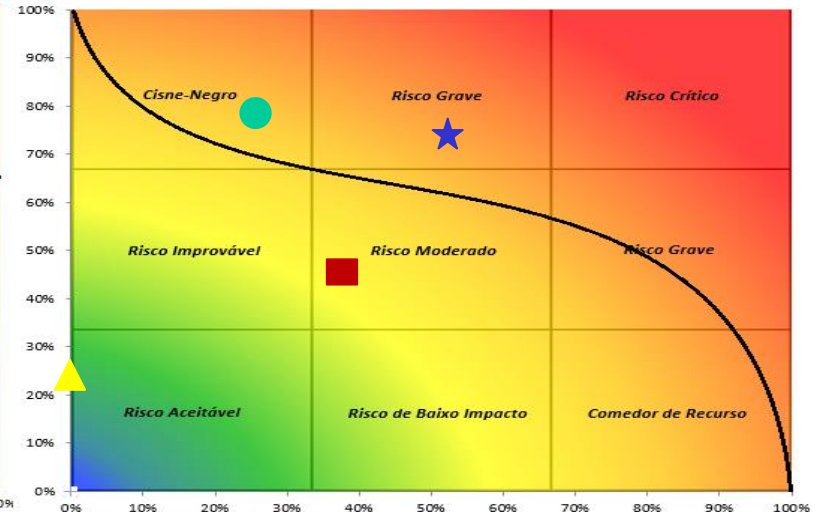
OK



Fora do apetite!



Fora do apetite!



APETITE AO RISCO

ÁREA	DECLARAÇÃO DO APETITE A RISCO
COMPLIANCE	A empresa habilita e espera o pleno cumprimento de todas as leis e regulamentos aplicáveis
ÉTICA	Todas as pessoas que representam a empresa devem agir de acordo com os mais altos padrões éticos em todos os momentos
REPUTAÇÃO	A reputação da empresa é valiosa demais para ser colocada em risco
REPORTES FINANCEIROS	Distorções relevantes nas demonstrações financeiras não são aceitáveis
SEGURANÇA	Risco de segurança aos funcionários e público não é aceitável
AMBIENTE	Nenhum risco de danos a longo prazo para o meio ambiente é aceitável

APETITE AO RISCO

ÁREA	DECLARAÇÃO DO APETITE A RISCO
CRESCIMENTO E AQUISIÇÃO	Aceitar o risco calculado é incentivado nas decisões de aquisição e investimento de capital, como o reconhecimento de que alguma probabilidade de falha sempre acompanha ação rápida para aproveitar as oportunidades
INOVAÇÃO	Benefícios da inovação e do desenvolvimento são obtidos através de uma visão de portfólio que reconhece que alguns novos produtos/serviços não terão sucesso

APETITE AO RISCO

ÁREA	DECLARAÇÃO DO APETITE A RISCO
RECURSOS HUMANOS	Algum risco é aceitável se o custo de reter e atrair os indivíduos mais qualificados é insustentável no contexto da economia de mercado de trabalho
CONTINUIDADE DE NEGÓCIOS E GESTÃO DE CRISES	Os custos são equilibrados com a exposição de forma prioritária
GLOBALIZAÇÃO	Riscos calculados em entrar em geografias novas e emergentes são aceitáveis
MOEDA E GESTÃO DE COMMODITIES	Volatilidade deve ser gerida de forma ativa, mas a especulação é inaceitável
PROPRIEDADE INTELECTUAL	O custo para fazer cumprir direitos de propriedade intelectual é ponderado em relação ao valor da PI
CADEIA DE SUPRIMENTOS	Algum risco de ruptura no aprovisionamento é aceitável se o custo para garantir o abastecimento for excessivo

APLICAÇÕES DO TEMA NO PODER EXECUTIVO FEDERAL

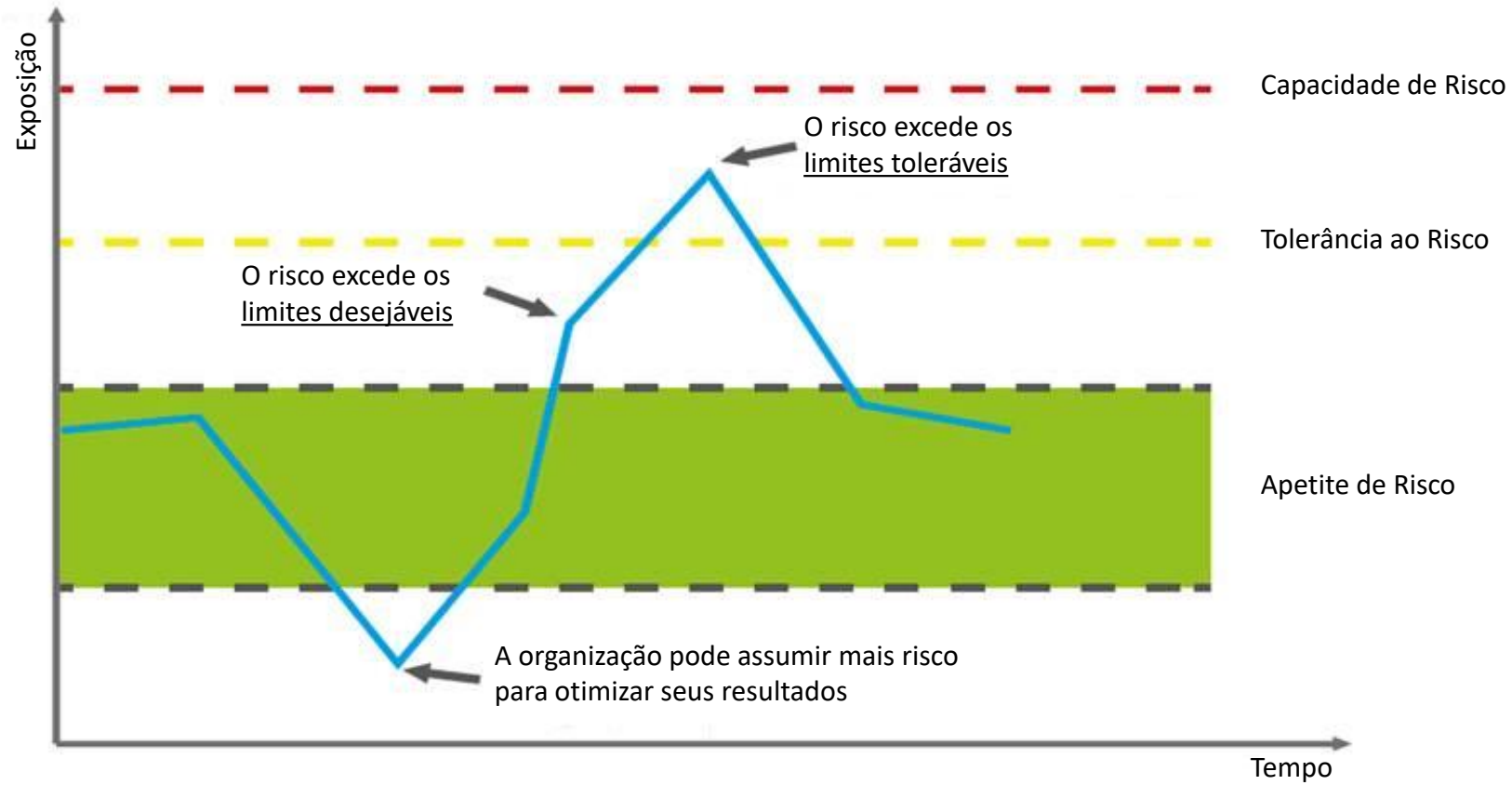
Metodologia CGU – Apetite ao Risco

Classificação	Ação necessária	Exceção
Risco Baixo	Nível de risco dentro do apetite. Pode haver oportunidades de maior retorno a serem exploradas assumindo-se mais riscos, avaliando a relação custo x benefício, como diminuir o nível de controles	Caso o risco seja priorizado para implementação de medidas de tratamento, deve haver justificativa da unidade e aprovação do dirigente máximo
Risco Médio	Nível de risco dentro do apetite. Nenhuma medida adicional é necessária, porém requer atividades de monitoramento específicas e atenção da unidade na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais	Caso o risco seja priorizado para implementação de medidas de tratamento, deve haver justificativa da unidade e aprovação do dirigente máximo
Risco Alto	Nível de risco além do apetite a risco. Qualquer risco nesse nível deve ser comunicado ao dirigente máximo da unidade e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do dirigente máximo da unidade	Caso o risco não seja priorizado para implementação de medidas de tratamento, deve haver justificativa da unidade e aprovação pelo dirigente máximo
Risco Extremo	Nível de risco muito além do apetite a risco. Deve ser objeto de Avaliação Estratégica, comunicado ao CGE e ao dirigente máximo da unidade e ter resposta imediata. Postergação de medidas só com autorização do CGE	Caso o risco não seja priorizado para implementação de medidas de tratamento, deve haver justificativa da unidade e aprovação pelo dirigente máximo e pelo CGE

APETITE X TOLERÂNCIA

APETITE = TOLERÂNCIA?

Apetite x Tolerância: visão gráfica



Fonte: IIA Espanha


CONTROLES
INTERNOS

TEMAS A SEREM ABORDADOS

- Conceitos sobre Controles na Administração Pública
- Princípios, Objetivos e Características dos Controles
- Tipos e Funções dos Controles
- Formulação dos Controles Internos
- Limitações e desafios na implementação dos controles

CONCEITO

Controles Internos da Gestão: processos operacionalizados de forma integrada e contínua pela direção e pelo corpo de funcionários das organizações, destinados a enfrentar os riscos e fornecer segurança razoável de que os objetivos e a missão da entidade sejam alcançados. (IN MP/CGU nº 01/2016)

Definição de Controles Internos

O Que?	Como?	Pra Que?
• Regras; • Diretrizes; • Rotinas; • Procedimentos; • Conferências; • Protocolos; • Entre outros.	Operacionalizados de forma integrada e contínua pela direção e pelo corpo de servidores das organizações.	Destinados a enfrentar os riscos e fornecer segurança razoável de que os objetivos da entidade serão atingidos.

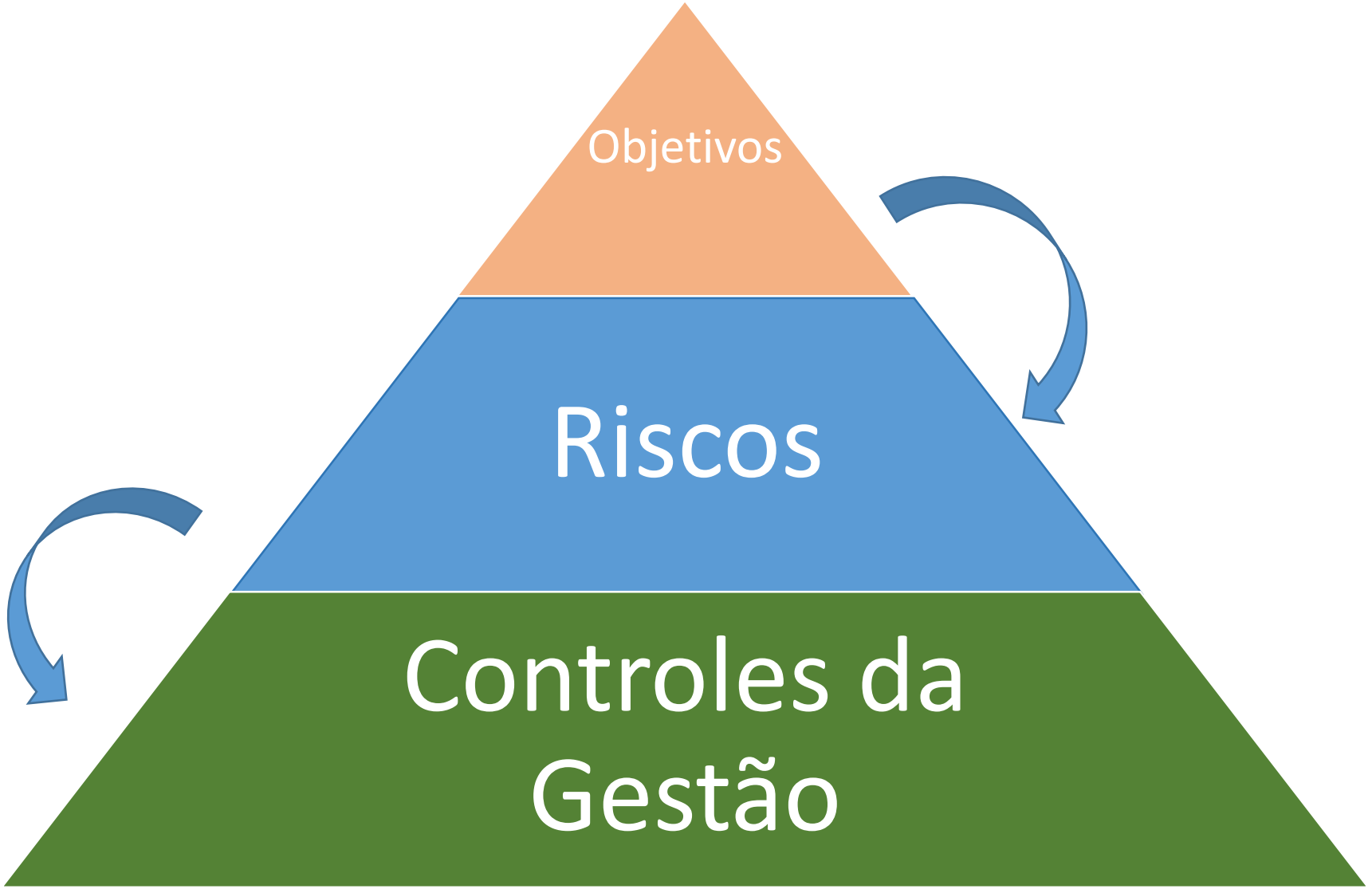
CONTROLES INTERNOS

PESQUISA KPMG (2004): A FRAUDE NO BRASIL

Causas

- ✓ Controles internos burlados: 26%
- ✓ Insuficiência no sistema de CI: 71%

Recuperação de Ativos Judicialmente é de aproximadamente 10% do total


Objetivos
Riscos
Controles da Gestão

Controles Internos – Pressupostos

- ✓ Estabelecimento de metas e objetivos claros
- ✓ Participação de toda a unidade
- ✓ Pessoas capacitadas adequadamente
- ✓ Instruções devidamente formalizadas
- ✓ Processo de aprendizagem organizacional

Controles Internos - Objetivos

- ✓ Segurança *razoável* de que os objetivos da organização sejam alcançados
- ✓ Produção e divulgação de informações confiáveis, relevantes, completas, oportunas e de qualidade para tomada de decisões dos gestores
- ✓ Salvaguarda dos ativos da unidade
- ✓ Garantia de que os processos estejam em conformidade com as leis e regulamentos
- ✓ Aumento da economicidade, eficiência, eficácia e efetividade às operações da unidade

Ciclo de Gestão – Objetivos, Riscos e Controles

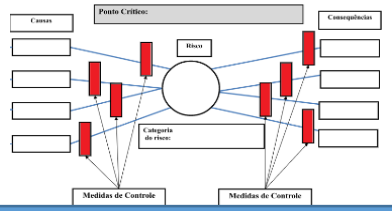
Gerenciamento de Riscos

Cada risco mapeado e avaliado deve estar associado a um agente responsável formalmente designado, com alçada suficiente para orientar e acompanhar as ações de mapeamento, avaliação e mitigação do risco.

- Identificação: Riscos e suas causas e efeitos.
- Mensuração: Probabilidade de ocorrência e Impacto nos Objetivos
- Tratamento: Instituição de Controles Internos

RISCOS – OPÇÕES DE TRATAMENTO

RESPOSTAS AO RISCO = SÃO AÇÕES GERENCIAIS DESTINADAS A MITIGAR O RISCO



CAIXA SEGUROS

"Existe o risco que você não pode jamais correr, e existe o risco que você não pode deixar de correr." (Peter Drucker)

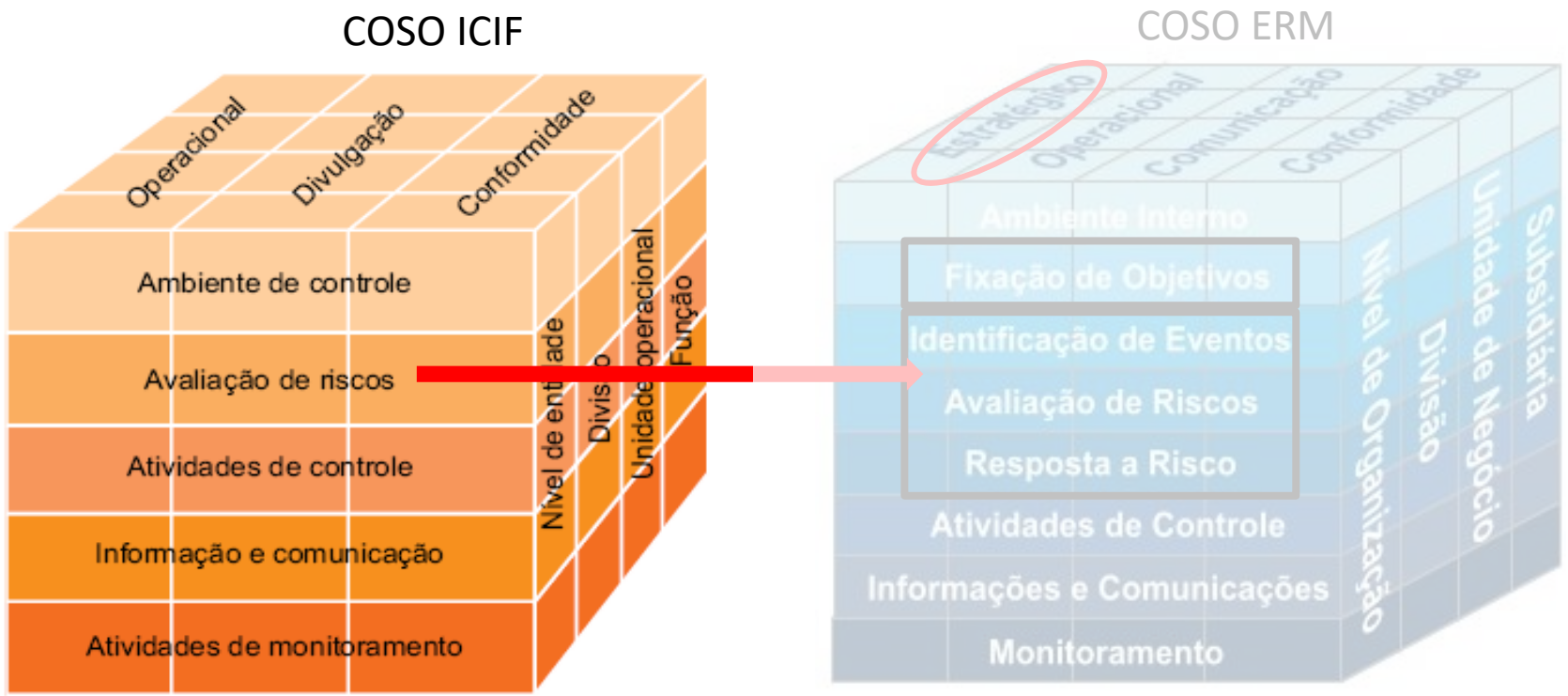
reduzir probabilidade e/ou impacto • Monitoramento para garantir o risco em nível aceitável	consequências (impacto)	compartilhamento de uma porção do risco • Exemplos: terceirização; seguros	

Controles Internos - Formulação

- ✓ Segregação de Funções (autorização, execução, registro e controle).
- ✓ Limites de Alçadas
- ✓ Nível de automação dos processos
- ✓ Adequada Relação Custo-Benefício (nem além do necessário e nem aquém)

CONTROLES INTERNOS

- Controle interno é um processo constituído de 5 elementos inter-relacionados entre si.



CONTROLES INTERNOS

IN MP/CGU Nº 01/2016 – Art. 12

Responsabilidades pelos Controles Internos da Gestão

- **Alta Administração**
- **Gestores**

→

- Estabelecimento
- Manutenção
- Monitoramento
- Aperfeiçoamento

- **Servidores e Funcionários**

→

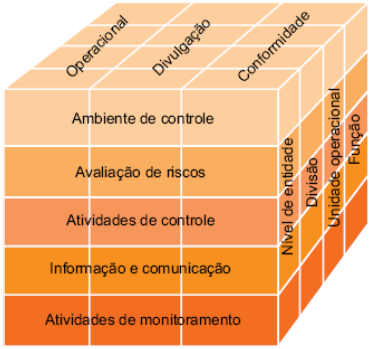
- Operacionalização

Controles Internos - Funções

- Controles Preventivos ou Prévios
- Controles Detectivos ou Concomitantes
- Controles Corretivos ou Posteriores
- Controles Compensatórios

PROCESSO DO CONTROLE INTERNO

ATIVIDADES DE CONTROLE



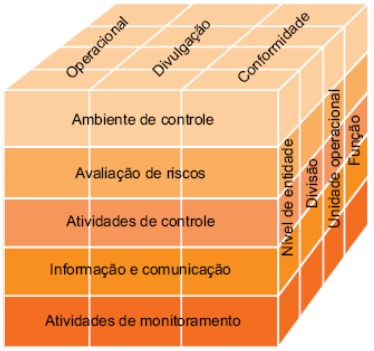
Controles Preventivos

- Finalidade de reduzir a materialização de eventos de risco.
- Agem sobre as causas, reduzindo a probabilidade de ocorrência do risco.

Exemplos: normas, manuais, controles de alçada, controles de acesso, segregação de funções, etc.

PROCESSO DO CONTROLE INTERNO

ATIVIDADES DE CONTROLE



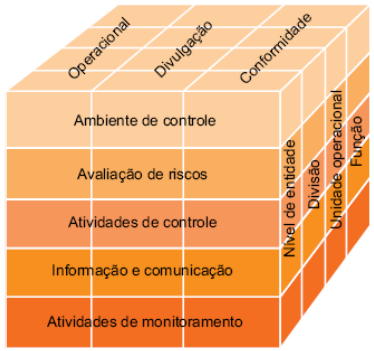
Controles Detectivos

- Identificam eventos (efetivos ou potenciais), sem impedir sua ocorrência
- Indicam desvios do padrão, alertando a gestão para adotar ações corretivas tempestivamente

Exemplos: indicadores, avaliação de desempenho operacional, reconciliações, cruzamento de bases de dados, etc

PROCESSO DO CONTROLE INTERNO

ATIVIDADES DE CONTROLE



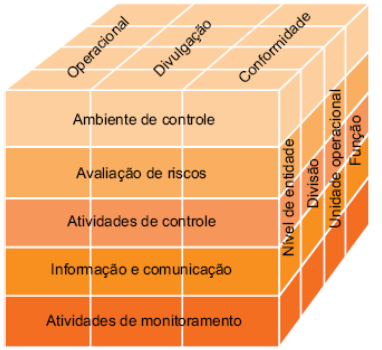
Controles Corretivos

- Constituem medidas corretivas/retificadoras aplicadas em face de falhas, desvios, irregularidades ou ilegalidades ocorridas
- Podem envolver ações de natureza punitiva ou sancionatória

Exemplos: TCE, Apuração de responsabilidade, planos de contingências pós catástrofes etc.

PROCESSO DO CONTROLE INTERNO

ATIVIDADES DE CONTROLE

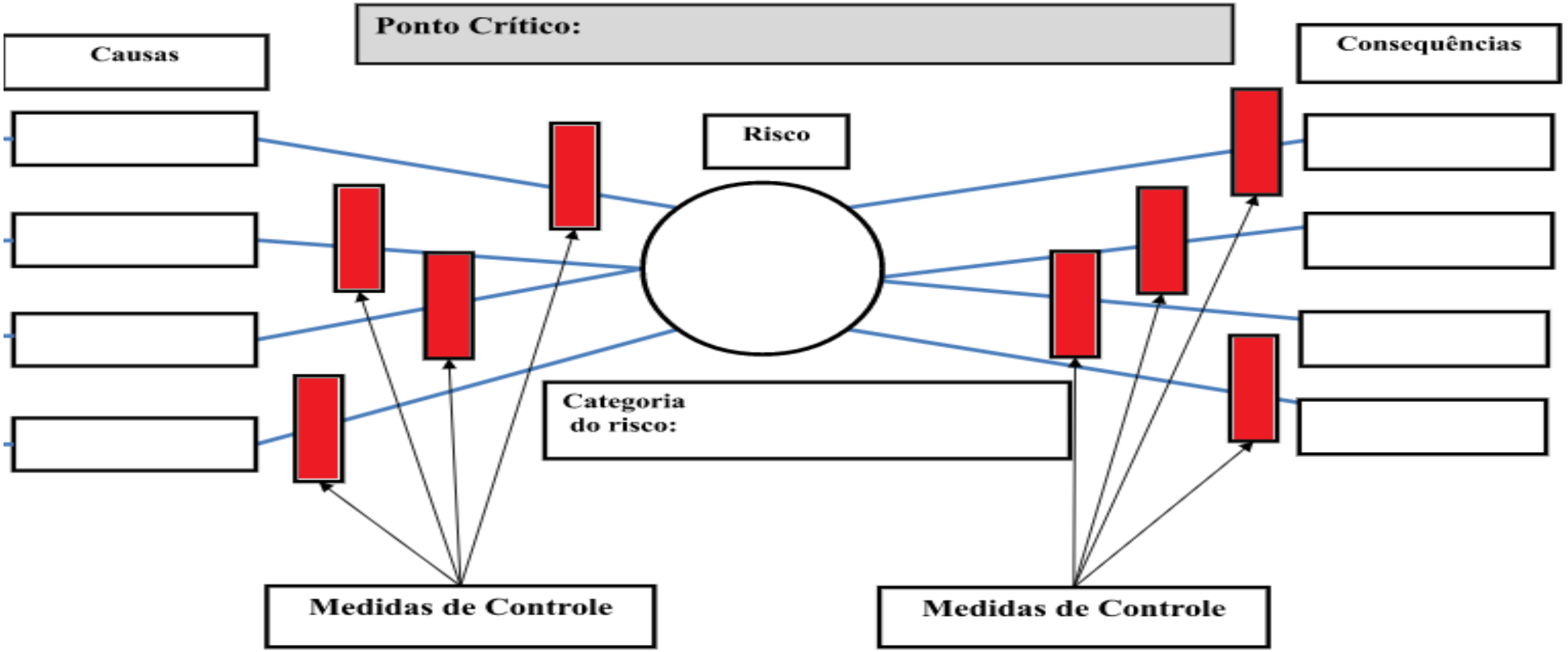


Controles Compensatórios

- Destinados a compensar a não adoção de outros controles mais apropriados ou contrabalancear falhas em controles já existentes
- A adoção desse tipo de controle normalmente acontece por razões de custo-benefício

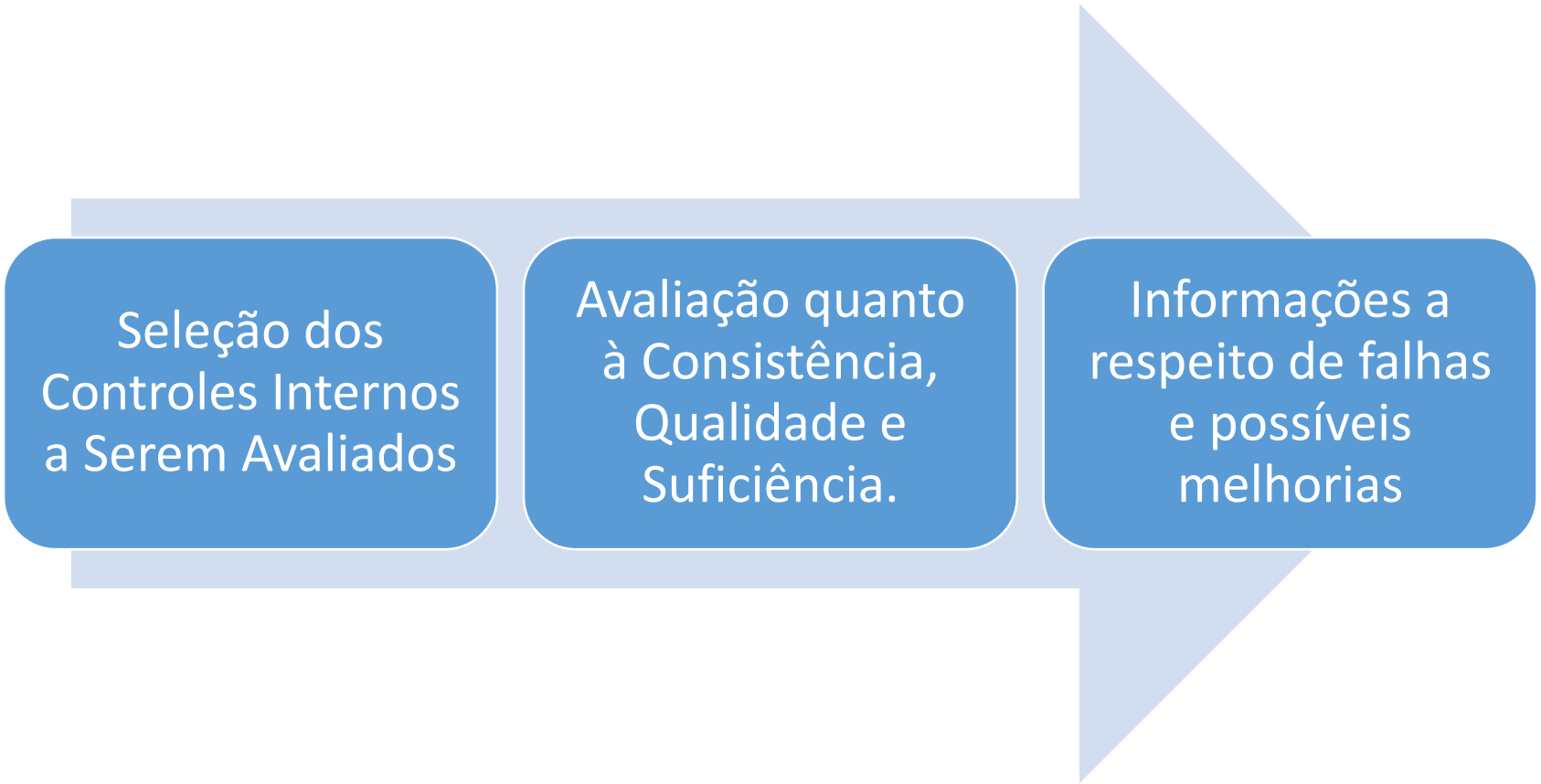
Exemplos: utilização de planilhas eletrônicas para controle de transações em vez de sistema específico etc.

Controle Interno - Formulação



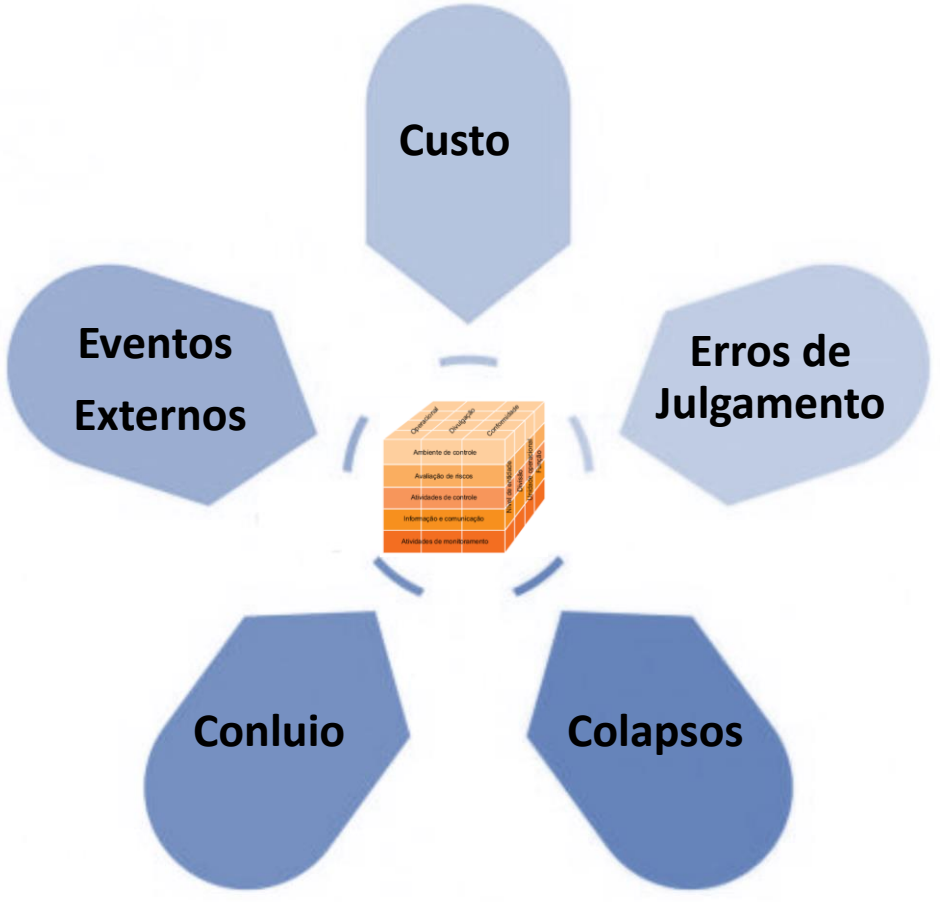
Fonte: ISO 31010:2009

CONTROLE INTERNO - Avaliação da Suficiência e Qualidade



PROCESSO DO CONTROLE INTERNO

LIMITAÇÕES À EFICÁCIA DO CONTROLE INTERNO



PROCESSO DO CONTROLE INTERNO

DESAFIOS AO PROCESSO DE CONTROLE INTERNO

- Falta de consciência (**cultura**) sobre a necessidade de gerenciar riscos por meio de controles internos e outras respostas

- **Resistência** de unidades organizacionais e pessoas

- Falta de **documentação** de atividades/processos (políticas, manuais, normas, fluxos)

- Falta de **conhecimento** do negócio e do ambiente interno e externo da organização (contexto onde os objetivos são buscados)

RISCOS – PLANO DE TRATAMENTO

Trata-se de um plano de ação para a implementação das medidas de tratamento dos riscos do processo organizacional

Risco	Medida de Tratamento	Unidade Responsável	Unidades Corresponsáveis	Responsável pela Implementação	Como será implementado	Custo Previsto	Data Início	Data Término	Situação

RISCOS – COMUNICAÇÃO

- processo contínuo
- fortalece o envolvimento da liderança
- possibilita que os responsáveis pelo GR e partes interessadas:
  - compreendam os fundamentos para a tomada de decisão
  - entendam as razões pelas quais ações específicas são requeridas
  - desenvolvam senso de inclusão e propriedade em relação ao processo de GR

COSO ERM

Informação, comunicação e divulgação

Princípios:

- Alavanca sistemas de informação;
- Comunica informações sobre riscos (canais de comunicação estabelecidos);
- Divulga informações de riscos, cultura e performance.

ISO 31000:2018

Estabelecimento comunicação e consulta

Convém que a organização estabeleça uma abordagem aprovada para comunicação e consulta para apoia a estrutura e facilitar a aplicação eficaz da gestão de riscos.

Comunicação envolve compartilhar informações com o públicos-alvo.

A consulta também envolve o fornecimento de retorno pelos participantes, com expectativa que isto contribuirá para as decisões e sua formulação ou outras atividades.

- **Convém que reflita as expectativas das partes interessadas;**
- **Convém que sejam oportunas e assegrem que a informação pertinente seja coletada, consolidada, sintetizada e compartilhada como apropriado e que o retorno seja fornecido e as melhorias sejam implementadas.**

Metodologia CGU - Comunicação

A comunicação sobre os processos de gerenciamento de riscos e seus resultados deve ser conduzida de maneira formal, utilizando o sistema definido pela CGU.

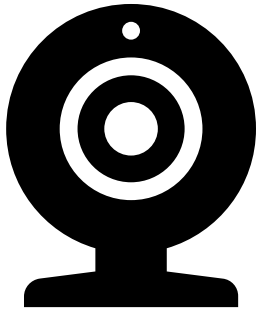
De forma geral, as informações produzidas durante as etapas do processo de gerenciamento de riscos têm caráter restrito. Esse nível de restrição deve ser observado pelos servidores da CGU e demais partes.

Demais comunicações sobre a Gestão de Riscos da CGU serão feitas por meio da elaboração de banners e materiais, publicações na IntraCGU e na página da CGU na internet, por exemplo.

É mais específica e prática, por estar em uma metodologia, e não em um modelo (framework)

RISCOS – MONITORAMENTO

- Parte integrante do processo de GR
- Responsabilidades devem ser claramente definidas
- Base para melhoria contínua do processo de GR
- Objetivos:
  - assegurar que os controles estão operando de forma eficiente e eficaz
  - possibilitar a análise das ocorrências dos riscos
  - detectar mudanças que requeiram revisão dos controles e/ou do plano de tratamento
  - Identificar riscos emergentes



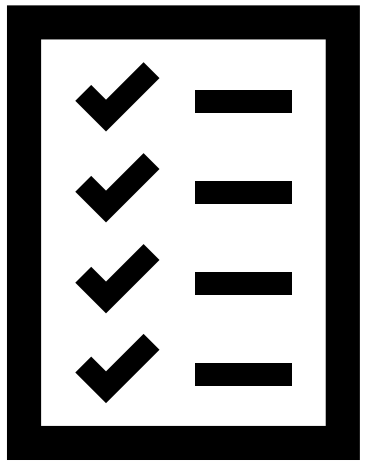
Metodologia CGU – Comunicação e Monitoramento

MATRIZ RACI	CGE	CG	NGR	Dirigente	Resp GR	Equipe Técnica	Resp implement	Servidores
Definir Plano de GR	A	C	I	R	C	I	I	I
Selecionar Processo	A	I	C	R	C	I		
Entendimento Contexto	I	I	C	A	R	R		
Identific e Análise Riscos	I	I	C	A	R	R		
Avaliação dos Riscos	I	I	C	A	R	R		
Priorização dos Riscos	I	I	C	A	R	R		
Def Respostas aos Riscos	I	I	C	A	R	R		
Validar Riscos Levantados	I	I	C	R	C	C		
Implem Plano Tratamento	I	I	C	A	I	C	R	
Monitorar	I/R	I	C	A	R	I	C	R
Avaliação Estratégica	A	C	R	C	C	R		

R – Responsável; A – Autoridade; C – Consultado; I - Informado

RISCOS – DOCUMENTAÇÃO

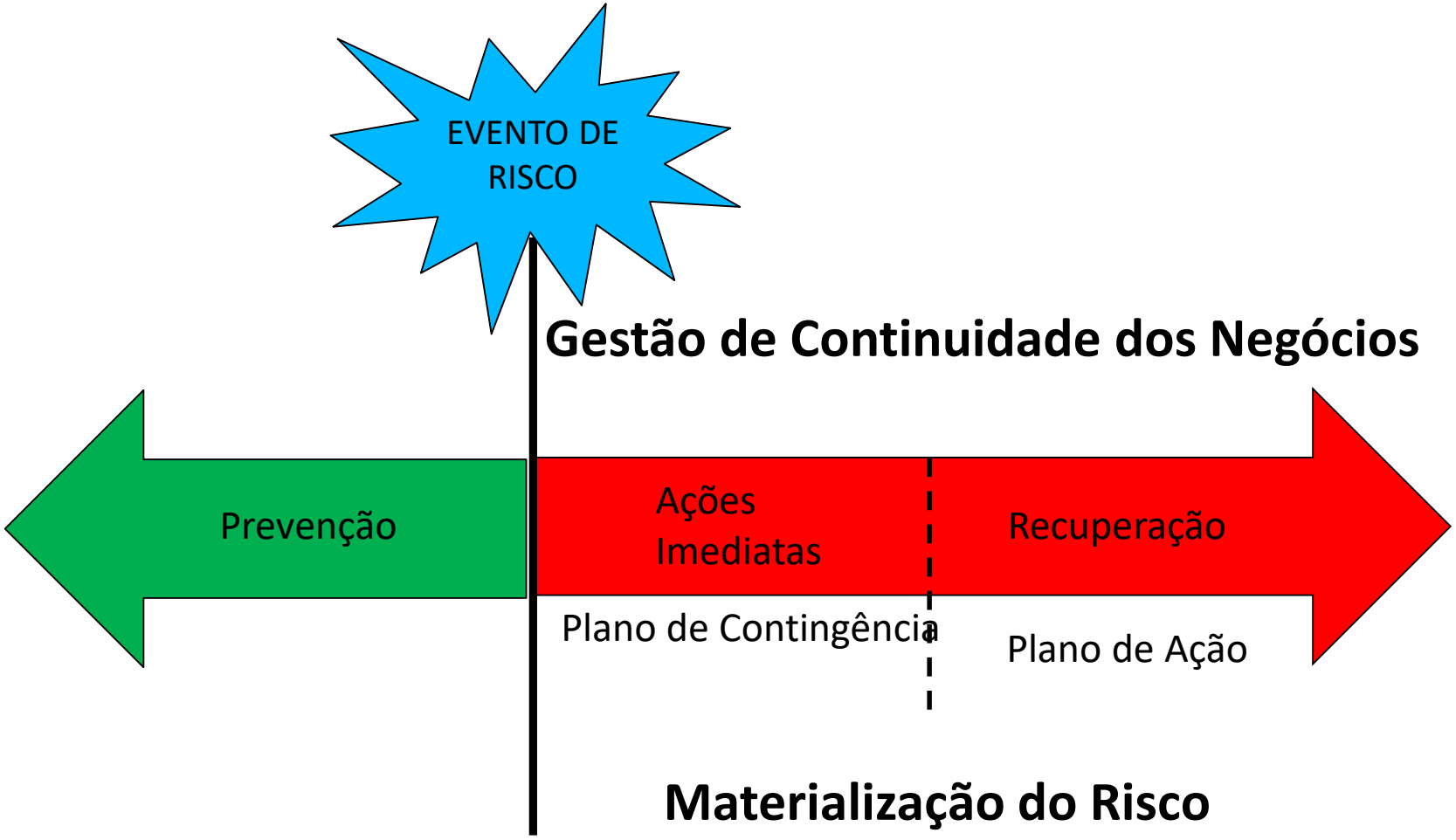
- Fornece os fundamentos para a melhoria dos processos, métodos e ferramentas
- A adequada documentação do processo de GR possibilita:



  - Rastreabilidade dos procedimentos realizados e decisões tomadas
  - Aprendizado contínuo
  - Atendimento a requisitos legais, regulatórios, operacionais e auditoria

RISCOS – E QUANDO O RISCO SE MATERIALIZA?

RISCOS – GERENCIAMENTO DE CONTINUIDADE DE NEGÓCIO



RISCOS – PLANO DE CONTIGÊNCIA

Definição de responsabilidades, áreas e sistemas envolvidos para atender a uma emergência

Tem o objetivo de treinar, organizar, orientar, facilitar, agilizar e uniformizar as ações necessárias às respostas de controle e combate às ocorrências anormais

Também chamado de planejamento de riscos, plano de continuidade de negócios ou plano de recuperação de desastres

RISCOS – PLANO DE AÇÃO E MONITORAMENTO

Planos de ação devem indicar (5W2H):

- **O que será feito (*What*)** – descrever claramente a ação que será realizada
- **Porque será feito (*Why*)** – indicar objetivo da ação e justificar necessidade de sua realização
- **Quem fará (*Who*)** – nominar e individualizar responsabilidades para cada ação do plano
- **Quando fará (*When*)** – estabelecer as datas previstas de início e fim de execução de cada ação
- **Onde fará (*Where*)** – local, unidade, processo, sistema, programa, ação etc.
- **Como fará (*How*)** – maneira, método ou solução adotada
- **Quanto custará (*How much*) –** custo das ações

ATRIBUTOS DE UMA GESTÃO DE RISCOS AVANÇADA

ALTO NÍVEL DE DESEMPENHO

ATRIBUTOS	POSSÍVEIS INDICADORES DE DESEMPENHO
Melhoria Contínua	• Metas explicitas de desempenho
Responsabilização integral pelos riscos	• Responsáveis pela gestão de riscos devidamente registrados em descrições de cargo/posição, em banco de dados ou sistemas de informação

Fonte: ABNT NBR ISO 31000:2009, Anexo A

ATRIBUTOS DE UMA GESTÃO DE RISCOS AVANÇADA

ALTO NÍVEL DE DESEMPENHO

ATRIBUTOS	POSSÍVEIS INDICADORES DE DESEMPENHO
Aplicação da gestão de riscos em todas as tomadas de decisão	• Registros de reuniões e decisões que demonstrem que discussões explícitas sobre os riscos ocorreram; • Representação de todos os componentes da gestão de riscos dentro dos processos-chave para a tomada de decisão na organização.
Comunicação contínua	• Reportes externos e internos, abrangentes e frequentes, sobre os riscos significativos e sobre o desempenho da gestão de riscos.
Integração total na estrutura de governança da organização	• Importantes materiais escritos que utilizam o termo incerteza em conexão com riscos; • Entrevista com gestores e evidência de suas ações e declarações.


Vamos
refletir!!!

Desafios à implementação da GR