Avaliação do Risco

"A mudança organizacional é muito mais eficaz quando é entendida como um desporto onde todos querem jogar" (João Alberto Catalão).

Critérios para avaliação de riscos

- Para determinar os níveis de risco, é preciso definir **escalas** para estimar a probabilidade e o impacto, bem como estabelecer quando a combinação desses dois fatores representa um risco baixo, médio, alto, etc.
- A seguir, são exemplificadas escalas qualitativas para auxiliar na estimativa de probabilidades e impactos de eventos, bem como uma **matriz Impacto x Probabilidade**, definindo níveis de risco decorrentes da combinação desses dois fatores.

Avaliação de um risco

- Um risco é avaliado, racionalmente, em termos de probabilidade de ocorrência e de impacto sobre os objetivos organizacionais.
- Quanto maior a probabilidade e maior o impacto, maior é o nível do risco.

Nível do Risco = Probabilidade x Impacto

- "O desafio da governança nas organizações do setor público é determinar quanto risco aceitar na busca do melhor valor para os cidadãos e demais partes interessadas, o que significa prestar serviço de interesse público da melhor maneira possível (INTOSAI, 2007). O instrumento de governança para lidar com esse desafio é a gestão de riscos" (Referencial Básico de Governança, TCU, 2ª ed, 2014, p. 57).
- Governança no setor público engloba mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade (IN Conjunta 1, de 2016). Ver Portaria/CGU nº 1.308, de 22/05/2015, a qual instituiu a estrutura de governança para implantação e acompanhamento da gestão estratégica, no âmbito do Ministério da Transparência, Fiscalização e Controladoria-Geral da União-CGU.

Probabilidade e impacto

➢Observe que:

- enquanto a probabilidade está associada a um incidente ou ocorrência potencial (chance de o evento vir a ocorrer, a partir de fontes internas ou externas)
- o impacto está associado à consequência do evento ocorrido (materialização do risco)

Avaliação leiga

- “Uma estimativa probabilística de risco produzida por um cientista, embora baseada em teorias e evidências científicas, tende a incluir a sua própria avaliação profissional sobre a importância relativa de diferentes desfechos, a aceitabilidade da incerteza e assim por diante.

- A **estimativa de riscos feita por um leigo**, embora menos sistemática do que a abordagem científica, **é intuitivamente sofisticada e pode refletir considerações importantes** que, talvez, não estejam presentes em uma avaliação científica” (HILL, S.; DINSDALE, G. Uma base para o desenvolvimento de estratégias de aprendizagem para a gestão de riscos no serviço público. *Cadernos Enap*, Brasília, 2003. p. 16, grifos nossos).

“A mudança organizacional é muito mais eficaz quando é entendida como um desporto onde todos querem jogar” (João Alberto Catalão).

Avaliação qualitativa da probabilidade

Descritor	Descrição	Nível
Muito Baixa	Evento extraordinário para os padrões conhecidos da gestão e operação do processo. Embora possa assumir dimensão estratégica para a manutenção do processo, não há histórico disponível de sua ocorrência...	**1**
Baixa	Evento casual, inesperado. Muito embora raro, há histórico conhecido de sua de ocorrência por parte dos principais gestores e operadores do processo...	**2**
Média	Evento esperado, que se reproduz com frequência reduzida, porém constante. Seu histórico de ocorrência é de conhecimento da maioria dos gestores e operadores do processo...	**3**
Alta	Evento usual, corriqueiro. Devido à sua ocorrência habitual ou conhecida em uma dezena ou mais de casos, aproximadamente, seu histórico é amplamente conhecido por parte de gestores e operadores do processo...	**4**
Muito Alta	Evento se reproduz muitas vezes, se repete seguidamente, de maneira assídua, numerosa e, não raro, de modo acelerado. Interfere de modo claro no ritmo das atividades, sendo evidente para os que conhecem o processo...	**5**

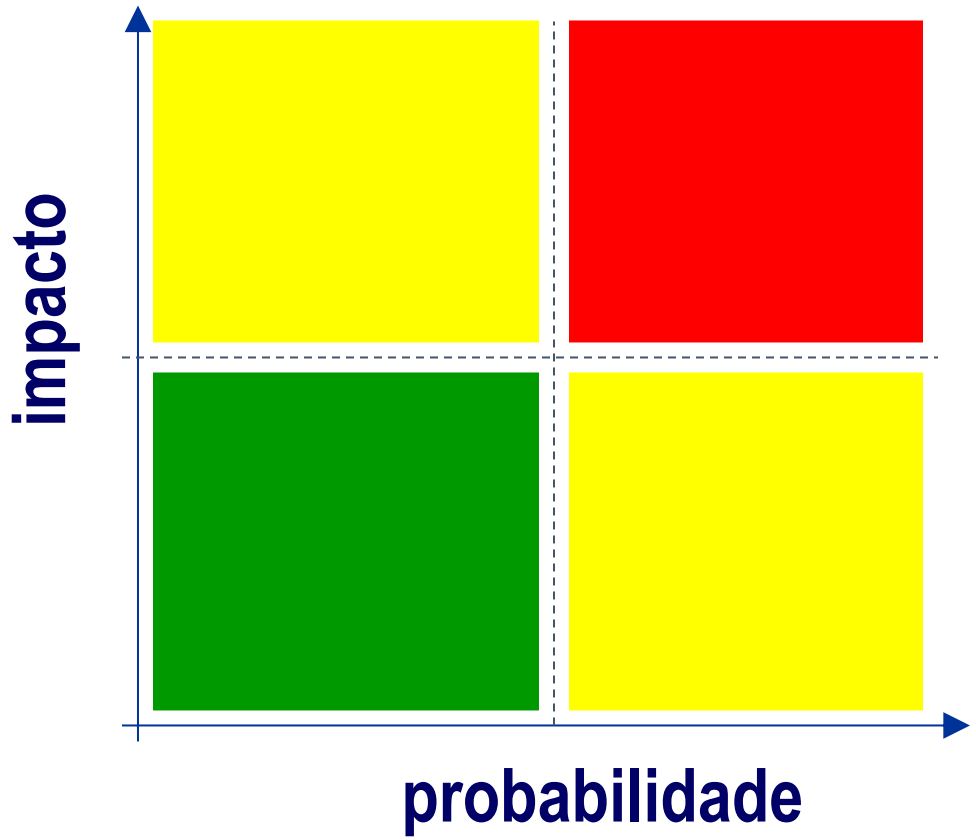
"É impossível que o improvável nunca aconteça" (Emil Gumbel, estatístico alemão, 1891-1966).

Avaliação qualitativa do impacto

Nível	Descritor	Descrição
1	**Muito Baixo**	Degradação de operações, atividades, projetos, programas ou processos da organização, porém causando **impactos mínimos** nos objetivos (de tempo, prazo, custo, quantidade, qualidade, acesso, escopo, imagem, etc.) relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas (clientes internos/externos, beneficiários).
2	**Baixo**	Degradação de operações, atividades, projetos, programas ou processos da organização, causando **impactos pequenos** nos objetivos.
3	**Médio**	Interrupção de operações ou atividades da organização, de projetos, programas ou processos, causando **impactos significativos** nos objetivos, **porém recuperáveis**.
4	**Alto**	Interrupção de operações, atividades, projetos, programas ou processos da organização, causando **impactos de reversão muito difícil** nos objetivos.
5	**Muito Alto**	Interrupção abrupta de operações, atividades, projetos, programas ou processos da organização, **impactando fortemente outros processos**, causando **impactos de dificílima reversão** nos objetivos.

"O risco vem de não saber o que você está fazendo" (Warren Buffett, investidor norte-americano, 1930-).

Diagrama de riscos



Nem todos os riscos precisam e/ou devem ser controlados. Quando a probabilidade de um risco é baixa e o impacto nos objetivos organizacionais (em decorrência do risco) também é baixo, pode-se aceitar o risco e não estabelecer controles.

Diagrama de cálculo de risco (5 colunas)

Legenda Nível de Risco Extremo Alto Médio Baixo		Probabilidade				
		1 Muito Baixa	2 Baixa	3 Média	4 Alta	5 Muito Alta
Impacto	5 Muito Alto	5	10	15	20	25
	4 Alto	4	8	12	16	20
	3 Médio	3	6	9	12	15
	2 Baixo	2	4	6	8	10
	1 Muito Baixo	1	2	3	4	5

Extremo

Alto

Médio

Baixo

Notação: Matriz de cálculo de risco, sendo Extremo: > 15 a 25; Alto: > 8 a 12; Médio: > 3 a 6; e Baixo: 1 a 2.

"Não se encontra a cura de uma desordem na confusão"
(William Shakespeare; 1564-1616; Romeu e Julieta).

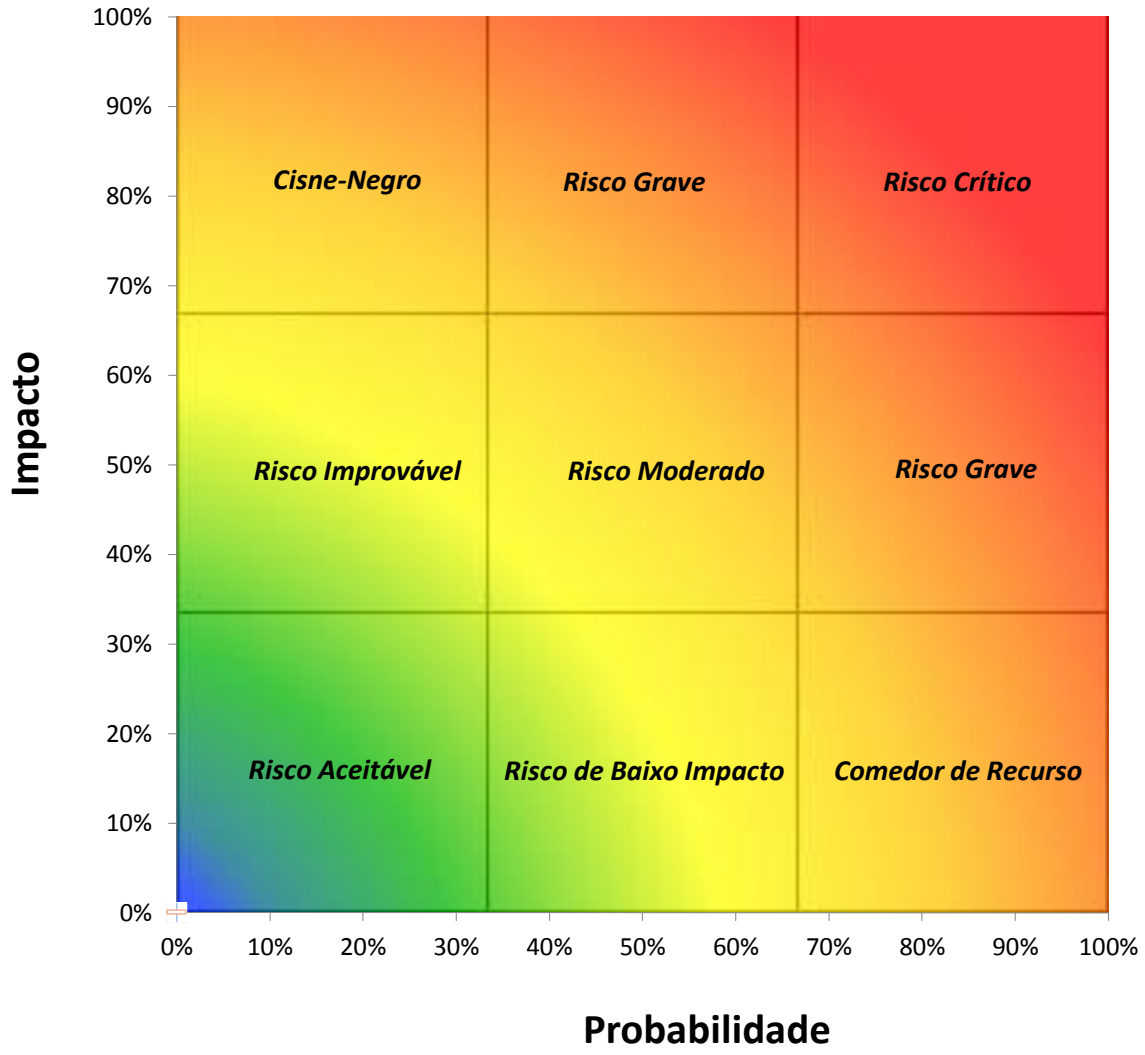
Diagrama de cálculo de risco (3 colunas)

PROBABILIDADE DE CONCRETIZAÇÃO DA AMEAÇA	IMPACTO		
	BAIXO (10)	MÉDIO (50)	ALTO (100)
Alto (1.0)	Baixo - 10 x 1.0 = 10	Médio - 50 x 1.0 = 50	Alto - 100 x 1.0 = 100
Médio (0.5)	Baixo - 10 x 0.5 = 5	Médio - 50 x 0.5 = 25	Médio - 100 x 0.5 = 50
Baixo (0.1)	Baixo - 10 x 0.1 = 1	Baixo - 50 x 0.1 = 5	Baixo - 100 x 0.1 = 10

Notação: Matriz de cálculo de risco, sendo Alto: >50 a 100; Médio: >10 a 50 e Baixo: 1 a 10

Fonte: **matriz de cálculo de risco**, criada por STONEBURNER, Gary *et al*. Risk Management Guide for Information Technology Systems. NIST Special Publication 800-30. National Institute of Standards and Technology. 2002, p. 25.

Diagrama qualitativo de classificação de riscos

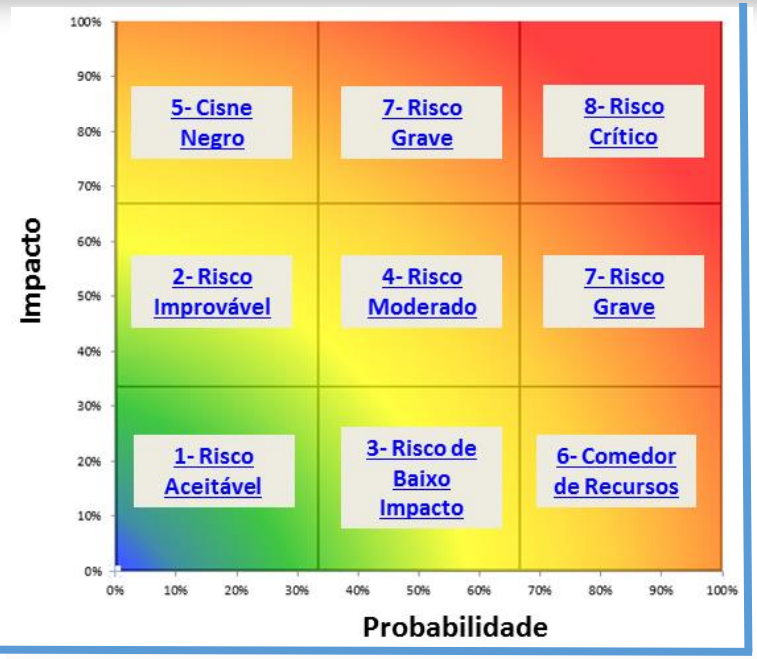


Vamos olhar a figura ao lado com muita atenção!

Fonte: CGU

"Muitas vezes, a perda de recursos e de eficiência pode ter origem nas ações que não fazem estardalhaço" (Mario Sergio Cortella).

Respostas aos riscos



Respostas aos riscos - COSO:

Risco Aceitável — Por tratar-se de um risco com **baixa probabilidade** e **baixo impacto** o gestor pode optar por **aceitá-lo.**

Risco Improvável — Por tratar-se de um risco com **baixa probabilidade,** porém com **impacto moderado**, o gestor pode optar por **aceitá-lo desde que o monitora frequentemente.**

Risco de Baixo Impacto — Por tratar-se de um risco com **baixo impacto**, porém com **probabilidade moderada**, o gestor pode optar por **aceitá-lo desde que o monitore frequentemente.**

Risco Moderado — Por tratar-se de um risco **probabilidade e impacto moderados**, recomenda-se que o gestor envide esforços com vistas a **reduzi-lo.**

Risco Grave — Por tratar-se de um risco com **alta probabilidade** e **impacto moderado OU com alto impacto** e **probabilidade moderada**, é considerado um Risco Grave e o gestor deve envidar todos os esforços possíveis de forma a **reduzi-lo**. Caso os custos para o gerenciamento desse risco sejam inviáveis, o gestor deve estudar a hipótese de **evitar** o risco, descontinuando as atividades que são inerentes a ele.

Risco Crítico — Nenhuma organização sobrevive por muito tempo quando apresenta esse tipo de risco. Por tratar-se do pior extremo possível com **alto impacto** e **alta probabilidade**, muitas vezes o gestor não terá opção a não ser **evitar** o risco descontinuando as atividades inerentes a ele.

Cisne Negro — O risco apresenta **baixa probabilidade** e **alto impacto**. Normalmente representa desastres naturais, ataques terroristas. Devido a sua característica fortuita, recomenda-se que o gestor **transfira** esse risco ou **compartilhe** parte dele. Alguns exemplos são: apólice de seguros, terceirização do serviço, backup remoto, etc.

Comedor de Recursos — O risco apresenta **baixo impacto** e **alta probabilidade**. Por ter alta frequência, os gestores costumam gastar recursos de forma contínua para mitigá-los. Recomenda-se que nesses casos, o gestor faça um estudo de viabilidade na **transferência ou compartilhamento** desse risco (normalmente por terceirização do serviço) e também nas consequências a médio a longo prazo, caso opte por **aceitá-lo.**

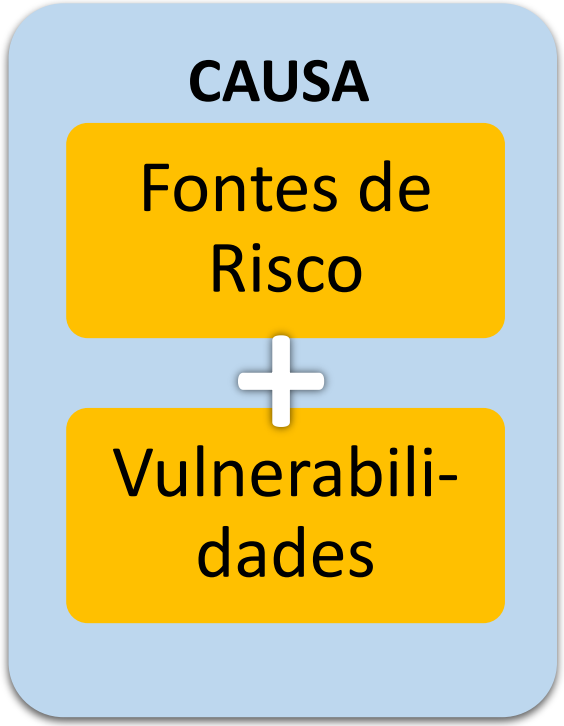
Fonte: CGU

Terminologia relacionada aos riscos

Causas do risco

- Condições que dão origem à possibilidade de um evento acontecer.

- Causas também são chamadas **fatores de riscos** e podem ter origem no ambiente externo ou interno à organização sob análise.



Causa = fonte + vulnerabilidade

- **Fonte de risco:** elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco:
  - pessoas (erro não-intencional; qualificação; fraude...)
  - processos (modelagem; transação; conformidade; controle; técnico...)
  - sistemas de gestão
  - infraestruturas física e organizacional (departamentalização; descentralização...)
  - tecnologia de produto ou de produção (equipamentos; sistemas informatizados; confiabilidade da informação...)
  - eventos externos (não gerenciáveis)
  - Fatores de risco: materialidade em valor; liquidez de ativos; competência gerencial; qualidade dos controles internos da gestão; grau de mudança ou estabilidade, tempo decorrido desde o último trabalho da auditoria interna; complexidade; relações com empregados e governo, etc. (cf. PA/IPPF/IIA nº 2010-2).
- **Vulnerabilidade:** inexistências, inadequações ou deficiências em uma fonte de risco.

Exemplos de causas

- **Da Fonte**
  - **Pessoas**
- **Vulnerabilidades**
  - Em número insuficiente
  - Sem capacitação
  - Perfil inadequado
  - Desmotivadas
  - Ardilosas ...

Exemplos de causas

- **Da Fonte**
  - **Processos**

- **Vulnerabilidades**
  - Mal concebidos (fluxo, desenho, centralização, custosos...)
  - Sem manuais ou instruções formalizadas (procedimentos e rotinas)
  - Ausência de segregação de funções ...

Exemplos de causas

- **Da Fonte**
  - **Sistemas informatizados**

- **Vulnerabilidades**
  - Obsoletos
  - Sem integração
  - Sem manuais de operação
  - Inexistência de controles de acesso lógico / *backups* ...

Exemplos de causas

- **Da Fonte**
  - **Estrutura organizacional**
- **Vulnerabilidades**
  - Falta de clareza quanto às funções e responsabilidades
  - Deficiências nos fluxos de informação e comunicação
  - Centralização de responsabilidades
  - Delegações exorbitantes ...

Exemplos de causas

- **Da Fonte**
  - **Infraestrutura física**
- **Vulnerabilidades**
  - Localização inadequada
  - Instalações ou leiaute inadequados
  - Inexistência de controles de acesso físico ...

Exemplos de causas

Da Fonte

- **Tecnologia** (de produto ou de produção)

Vulnerabilidades

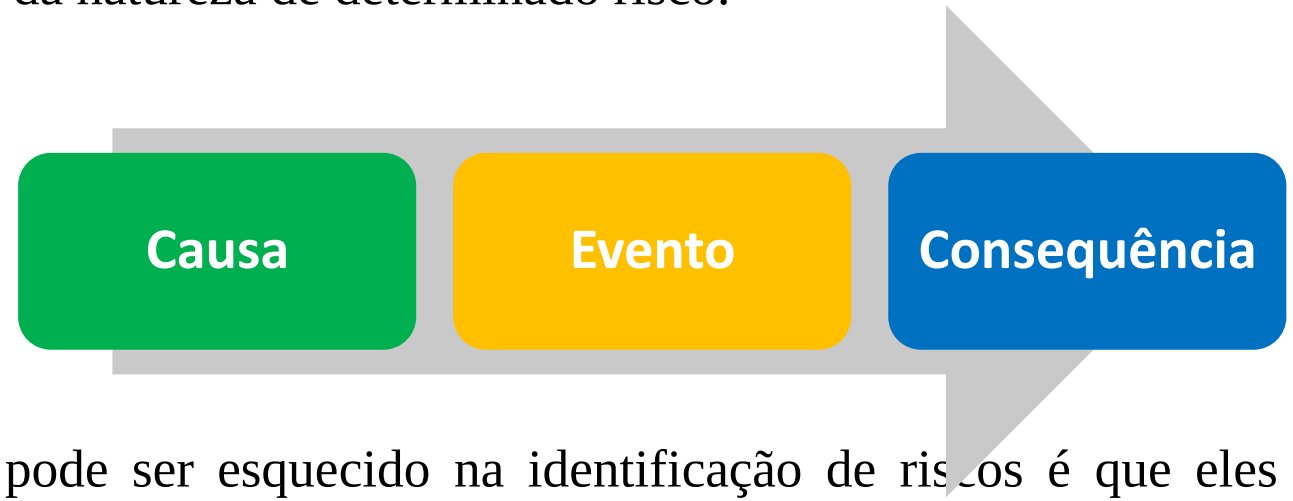
- Técnica de produção ultrapassada / produto obsoleto
- Inexistência de investimentos em pesquisa e desenvolvimento
- Tecnologia sem proteção de patentes
- Processo produtivo (tecnologia) sem proteção contra espionagem

Conceito de identificação de riscos

"O acaso não é, não pode ser, senão a causa ignorada de um efeito desconhecido" (Voltaire, 1694-1778).

Conceito de identificação de riscos

- **Processo organizável de busca, reconhecimento e descrição de riscos** (ABNT NBR ISO 31000:2009)
- Envolve a identificação de fontes de risco, **eventos**, suas **causas** e suas **consequências** potenciais, num esforço de compreensão da natureza de determinado risco.



- Um princípio que não pode ser esquecido na identificação de riscos é que eles **se relacionam com os objetivos da organização**, **do processo**, **do projeto**, etc.
- A identificação de riscos pode basear-se em dados históricos, análises teóricas, opiniões de pessoas capacitadas em GRC e especialistas, e nas necessidades das partes interessadas.

Componentes do risco

CAUSA

- Fontes do risco
- Vulnerabilidades

EVENTO

- Incidente
- Irregularidade

CONSEQUÊNCIA

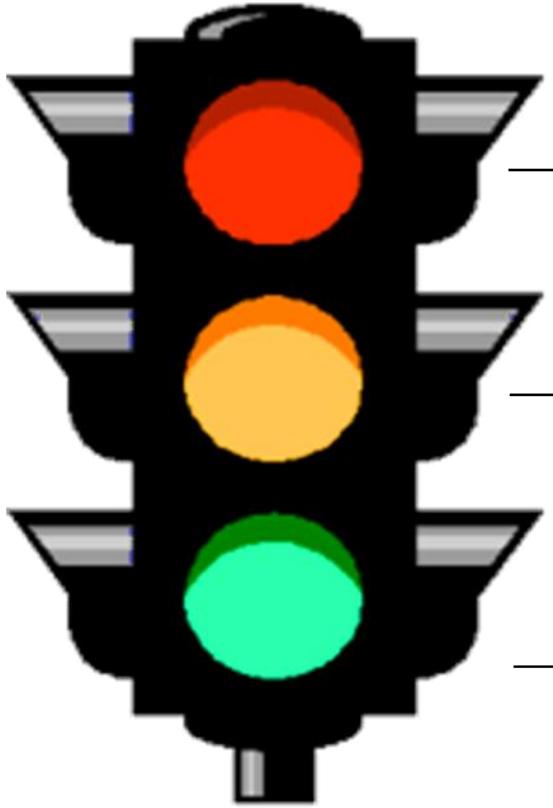
- Impacto em um objetivo
- Ganho/Perda

"Elimine a causa e o efeito cessa" (Miguel de Cervantes, 1547-1616).

Tomada de decisão

"Mude, mas comece devagar, porque a direção é mais importante do que a velocidade" (Clarice Lispector, 1920-1977).

Percepção x Decisão



Vermelho (Estímulo) → **Proibido passar** (Conhecimento) → **Pare!** (Decisão)

Amarelo (Estímulo) → **Atenção** (Conhecimento) → **Reduz!** (Decisão) / **Acelera!** (Decisão)

Verde (Estímulo) → **Permitido passar** (Conhecimento) → **Acelera!** (Decisão)

"Os grandes navegadores devem sua reputação aos temporais e tempestades" (Epicuro, 341 a.C. – 270 a.C., filósofo grego).

Tomada de decisão

- Como o risco afeta a tomada de decisão?

- Fatores que influenciam:
  - Percepção/consciência dos riscos;
  - perfil;
  - situação conjuntural (circunstancial; binômio forças impulsionadoras e/ou forças restritivas).

"Mude, mas comece devagar, porque a direção é mais importante do que a velocidade" (Clarice Lispector, 1920-1977).

Quatro elementos associados ao risco

- Diante disso, com o GRC, busca-se melhorar a capacidade de previsibilidade e ampliar a quantidade de variáveis monitoradas, dentro do contexto; ou seja, “transformar a incerteza em riscos, de forma a poder enfrentá-los” (Sabbag, 2002).

“É perdoável ser derrotado, mas nunca ser surpreendido”
(Frederico II, “o Grande” Rei da Prússia, 1712-1786).

Risco calculado a partir da percepção/consciência

"O automobilismo é um risco calculado. Fico mais preocupado ao fazer viagens comuns, entre São Paulo e minha fazenda em Araraquara, que largando numa corrida" (Emerson Fittipaldi).

Aspectos Normativos

IN Conjunta nº 01/MP-CGU/2016

Art. 12. A responsabilidade por estabelecer, manter, monitorar e aperfeiçoar os controles internos da gestão é da alta administração da organização, sem prejuízo das responsabilidades dos gestores dos processos organizacionais e de programas de governos nos seus respectivos âmbitos de atuação.

Parágrafo único. **Cabe aos demais funcionários e servidores a responsabilidade pela operacionalização dos controles internos da gestão e pela identificação e comunicação de deficiências às instâncias superiores.**

IN Conjunta nº 01/MP-CGU/2016

Art. 13. **Os órgãos e entidades do Poder Executivo federal deverão implementar, manter, monitorar e revisar o processo de gestão de riscos, compatível com sua missão e seus objetivos estratégicos, observadas as diretrizes estabelecidas nesta Instrução Normativa**.

Art. 15. São **objetivos da gestão de riscos**:

I - assegurar que os responsáveis pela tomada de decisão, em todos os níveis do órgão ou entidade, tenham acesso tempestivo a informações suficientes quanto aos riscos aos quais está exposta a organização, inclusive para determinar questões relativas à delegação, se for o caso;

II - aumentar a probabilidade de alcance dos objetivos da organização, reduzindo os riscos a níveis aceitáveis; e

III - agregar valor à organização por meio da melhoria dos processos de tomada de decisão e do tratamento adequado dos riscos e dos impactos negativos decorrentes de sua materialização.

E agora? Vamos iniciar!

E agora? Vamos iniciar!

“ Resultado eu não tenho condição de assegurar... mas desempenho e trabalhar pra isso, sim ...”

(Tite – Treinador da Seleção Brasileira de Futebol)