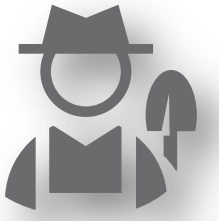
t-Risk
Método de Avaliação de Riscos

INTRODUÇÃO

Gestão de Riscos de acordo com a ISO 31000 e Plataforma t-Risk

Revisado em abril / 2024 B

Evolução da Segurança



HOMEM NATUREZA

SOCIEDADE **COLETORA/PRODUTORA**

ECONOMIA AGRÍCOLA

SEGURANÇA FAMILIAR

PRESERVAÇÃO DO TERRITÓRIO

HOMEM MÁQUINAS

SOCIEDADE **URBANA**

ECONOMIA INDUSTRIAL

SEGURANÇA PATRIMONIAL

PROTEÇÃO DO MEIO DE PRODUÇÃO

HOMEM CONHECIMENTO

SOCIEDADE **INFORMAÇÃO**

ECONOMIA INTANGÍVEL

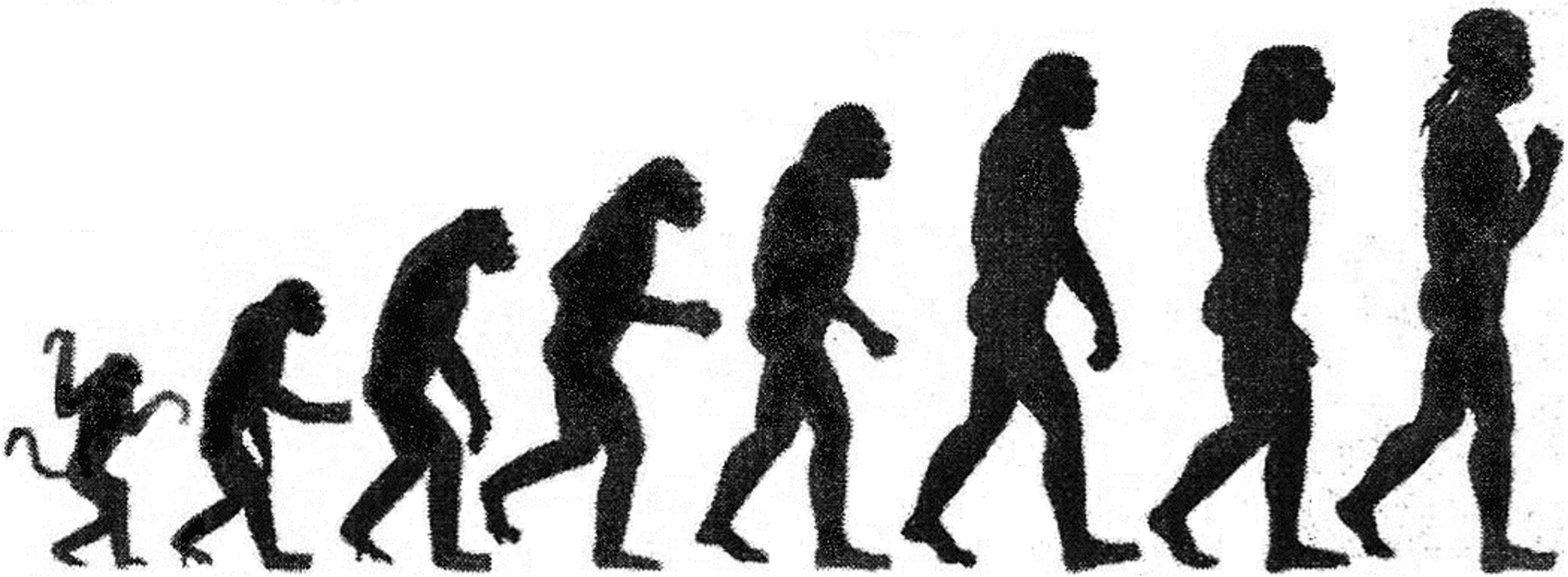
SEGURANÇA INTEGRAL

GESTÃO DE RISCOS

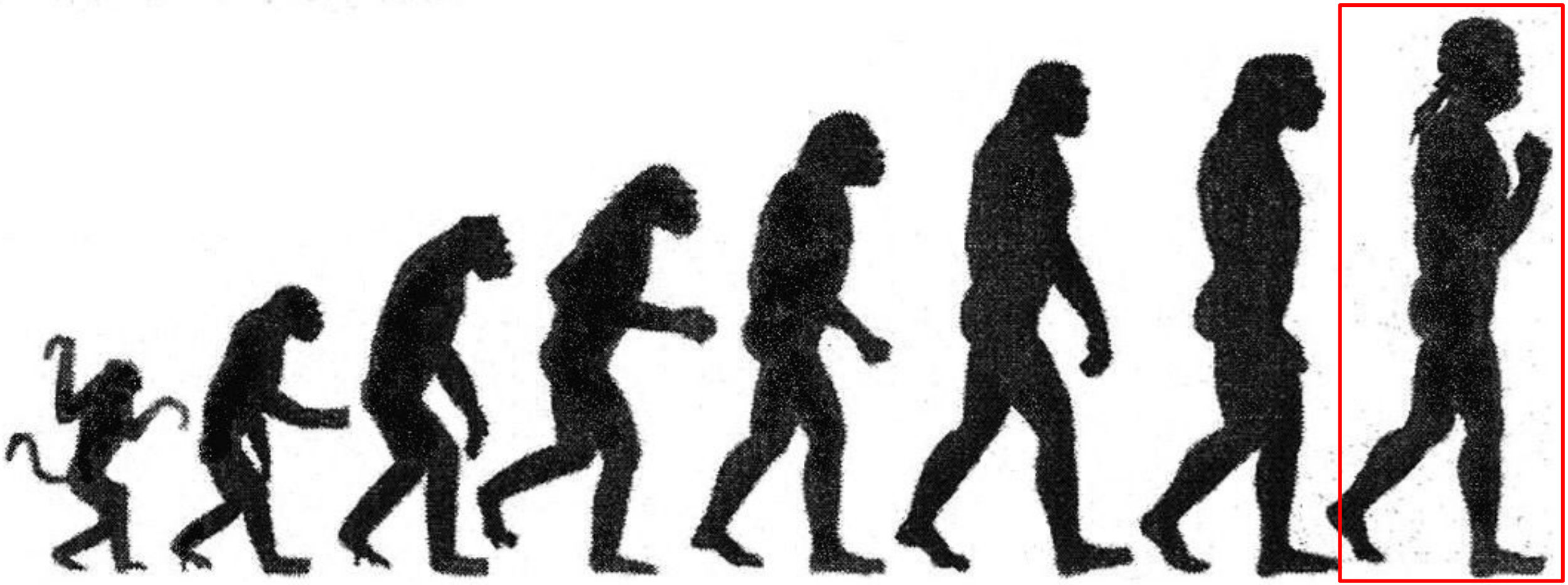
Equação do Risco (Método Total Risk*)

**A Equação do Risco está descrita no livro Gestão de Riscos na Segurança Patrimonial de Tácito Leite e faz parte do Método Total Risk.*

Porque somos bons em gerenciar riscos?



Porque NÃO somos bons em gerenciar riscos HOJE?



Exemplos de riscos na cadeia produtiva do setor joalheiro

ROUBO DE CARGA | FURTO | FRAUDE | COMPLIANCE | ACIDENTE

GARIMPO

LOGÍSTICA

FÁBRICA

REPRESENTANTE

LOJA

FUGA DE INFORMAÇÃO | SABOTAGEM | ROUBO | DANOS À IMAGEM | PERDA E QUEBRA

Único padrão de risco aplicável a todos os tipos de riscos e para todos os tipos de organização!

Evolução da família ISO 31000

- ISO Guia 73:2002
- ISO 31000: 2009
- ISO Guia 73:2009
- ISO 31010: 2012
- ISO 31004: 2015
- ISO 31000: 2018
- ISO 31010: 2021
- ISO 31073: 2022
- Handbook 31000: 2023
- ISO 31050: 2023

Visão geral do processo de gestão de riscos

Identificação dos riscos

- Convém que a organização identifique as fontes de risco, áreas de impactos, eventos e suas causas e consequências potenciais.
- A finalidade desta etapa é gerar uma lista abrangente de riscos **baseada nestes eventos** que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar **a realização dos objetivos da organização**.
- Incluir **reação em cadeia**, efeito cumulativo, em cascata e **cruzado**.
- Importante usar técnicas e ferramentas adequadas e envolver pessoas com conhecimento compatível.

Importância da identificação dos eventos

O risco, com base em seu significado geral (ISO 31000:2018), é definido como o **efeito da incerteza nos objetivos**.

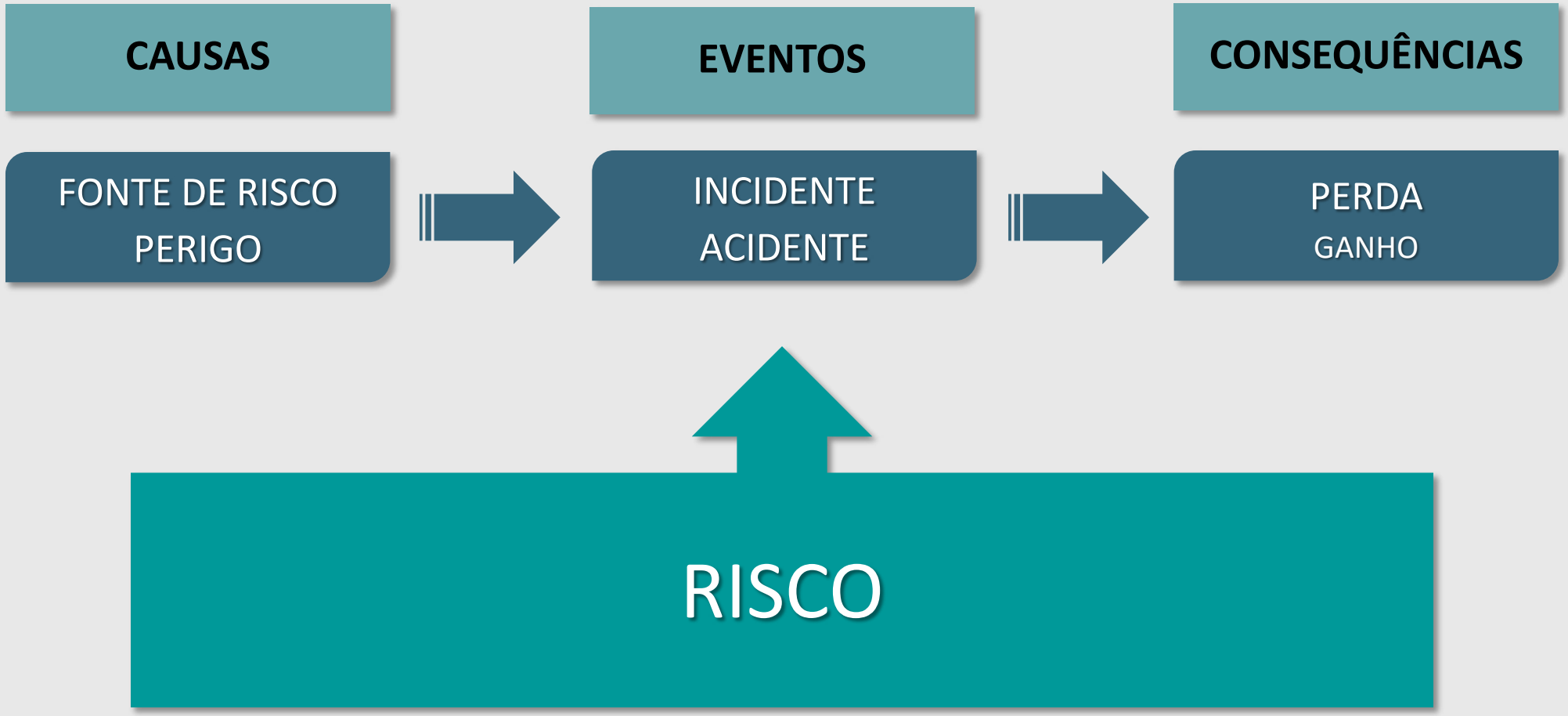
DE ONDE DERIVA A INCERTEZA?

Eventos são coincidências de espaço e tempo entre ameaças (oportunidades) e vulnerabilidades (resiliência).

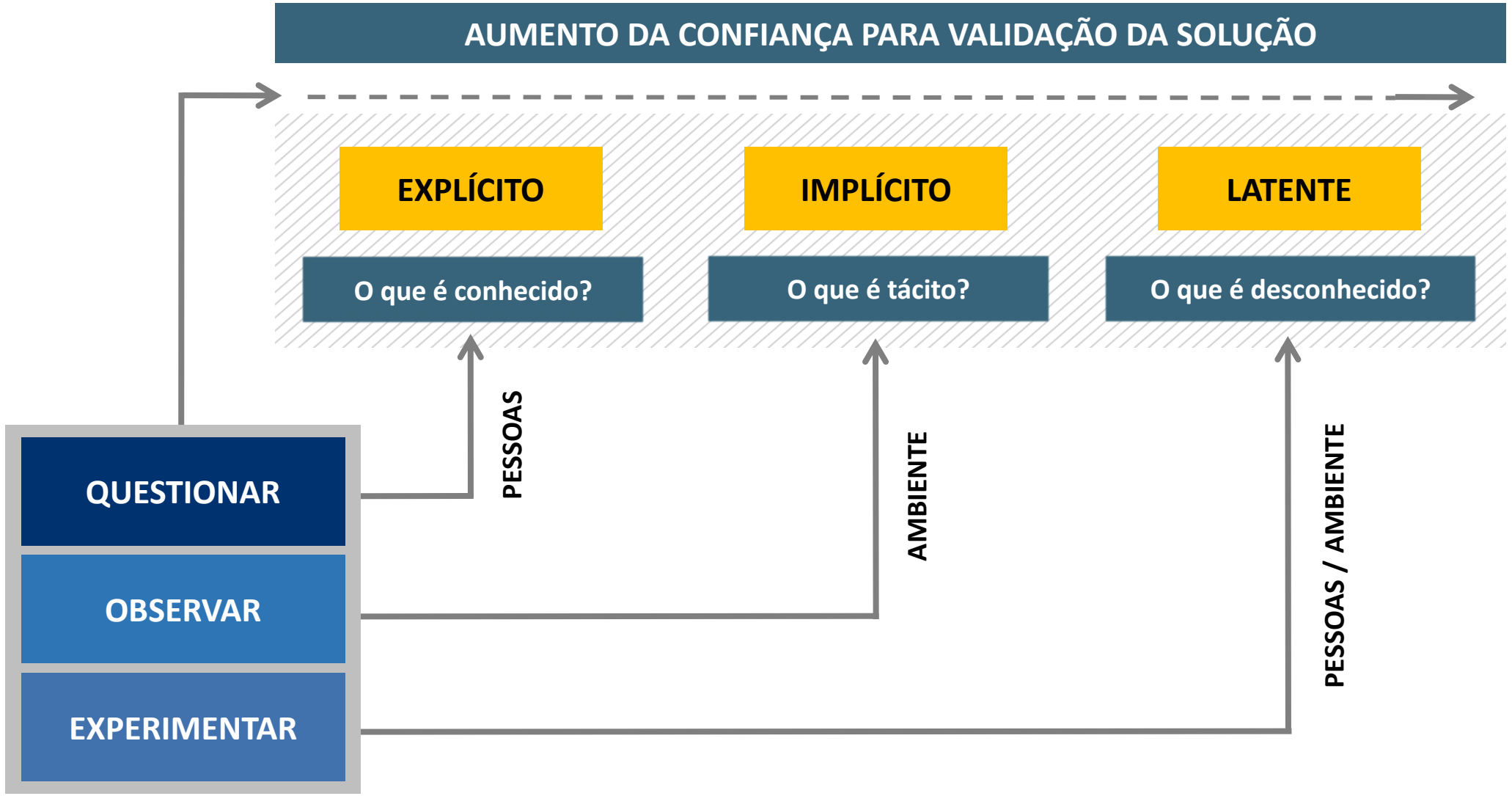
Impacto e Consequências são provocados pelos eventos.

Desvios nos objetivos são provocados pelos impactos e consequências.

Análise de causa, evento e consequência descritos na ISO 31000



Como identificar riscos?



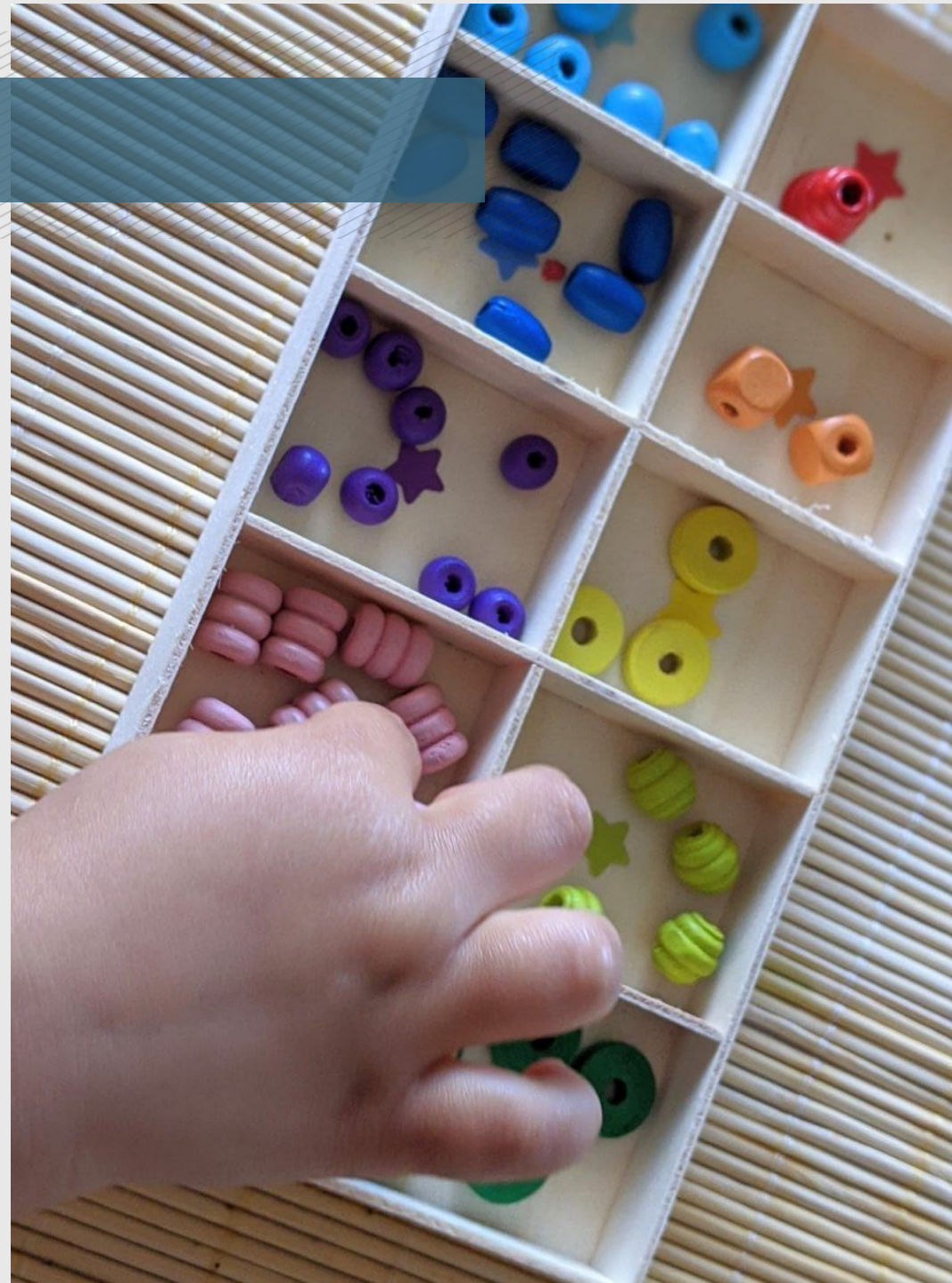
Classificação de risco

O que é classificação de risco?

- É um processo que consiste em **dividir os riscos identificados em categorias** ou grupos, com base em **critérios pré-definidos**, que podem ser a natureza do risco, a sua origem, a sua magnitude, entre outros.

Para que serve a classificação de risco?

- Priorização; Alocação de recursos; compreensão e comunicação; desenvolvimento de estratégias de mitigação; monitoramento e análise; melhora contínua; e garantir conformidade.



Análise dos riscos

- A análise de riscos envolve desenvolver a **compreensão dos riscos**.
- O risco é analisado determinando-se, no mínimo, as **consequências** e suas **probabilidades (ISO 31000:2009).**
- A análise dos riscos considera as **incertezas, fontes de risco, consequências, probabilidades, eventos, cenários, controles** e sua **eficácia (ISO 31000:2018).**
- A análise de riscos pode ser realizada com **diversos graus de detalhe**. Dependendo das circunstâncias, a análise pode ser **qualitativa**, **semiquantitativa**, **quantitativa**, ou uma **combinação destas**.

Avaliação dos riscos

- A finalidade da avaliação de riscos é **auxiliar na tomada de decisões** (com base na comparação dos resultados da análise de riscos e os critérios de risco estabelecidos), sobre quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento.
- A avaliação de riscos envolve comparar o nível de risco encontrado durante o processo de análise com os critérios de risco estabelecidos quando o contexto foi considerado.
- As decisões sobre tipo de tratamento serão influenciadas pela **atitude perante o risco**.

Tratamento dos riscos

- O tratamento de riscos envolve a seleção de uma ou mais opções para modificar os riscos e a implementação dessas opções.

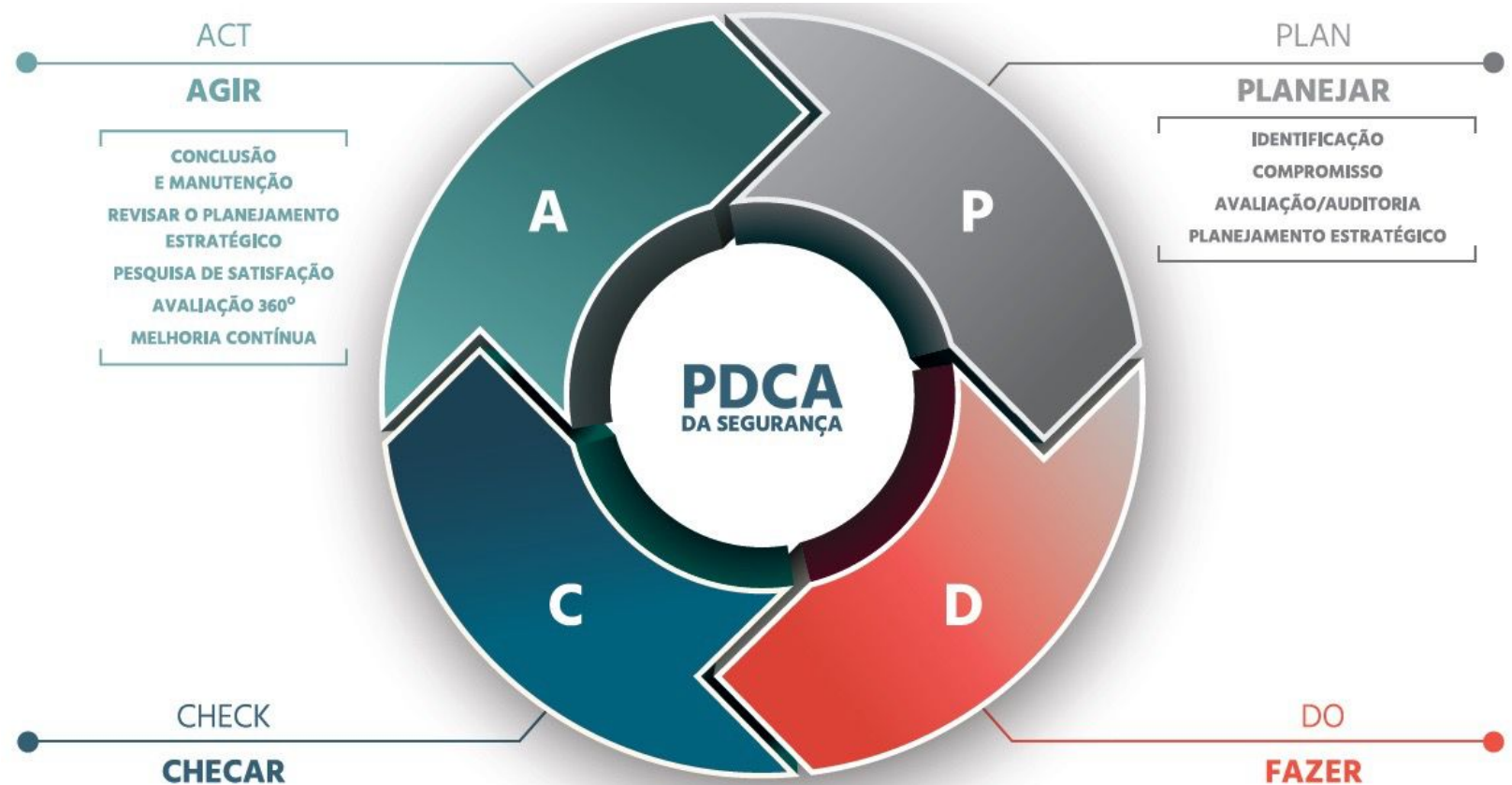
- Tratar riscos envolve um processo cíclico composto por:
  - Avaliação do tratamento de riscos já realizado;
  - Decisão se os níveis de risco residuais são toleráveis; entre outros.

Opções para tratamento dos riscos

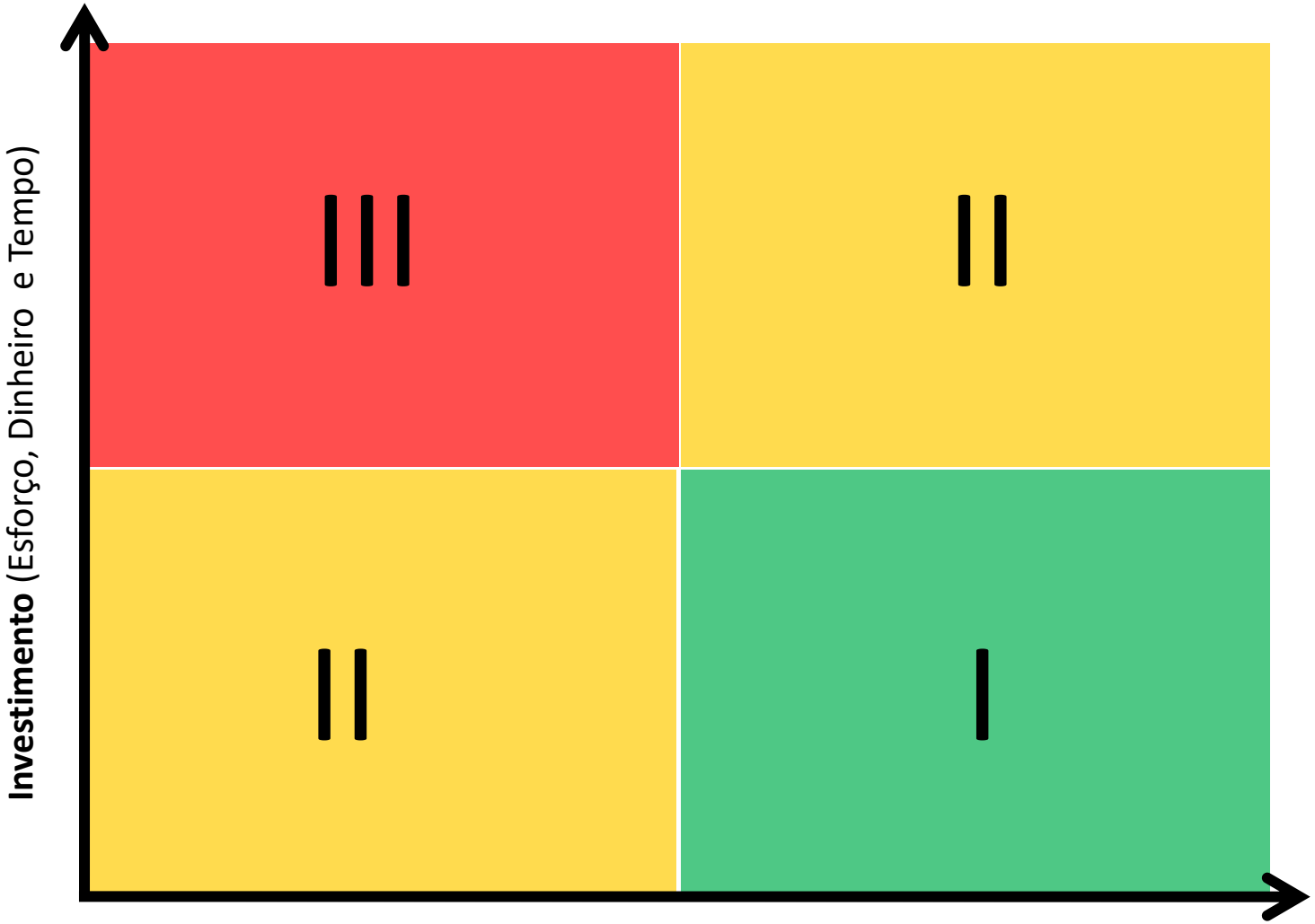
1. **EVITAR** o risco não iniciando ou descontinuando a atividade que origina o risco.
2. **ASSUMIR OU AUMENTAR** o risco para tirar proveito da oportunidade (risco positivo).
3. **REMOVER A FONTE** do risco.
4. **MUDAR A PROBABILIDADE** do risco.
5. **MUDAR AS CONSEQUÊNCIAS** do risco.
6. **COMPARTILHAR** o risco (ex.: através de contratos e seguros).
7. **RETER** o risco de forma consciente e embasada.

Observação: essas opções NÃO são necessariamente excludentes.

PDCA da segurança com base na gestão de riscos



Implantação dos controles & Prioridade de investimento



LEI DE PARETO
20% RECURSOS DE SEGURANÇA INDICADO
80% RISCOS EXISTENTES
20% RISCOS EXISTENTES
80% PERDA ESPERADA

Investimento eficiente em controles de segurança

SEGURANÇA INADEQUADA

FALTA DE INVESTIMENTO EM SEGURANÇA

N.S.N. ≠ N.S.E.

RISCO	Alto
IMPACTO	Alto
ROI	Impreciso

SEGURANÇA INADEQUADA

INVESTIMENTO INEFICIENTE EM SEGURANÇA

N.S.N. ≠ N.S.E.

RISCO	Oscilante
IMPACTO	Oscilante
ROI	Baixo

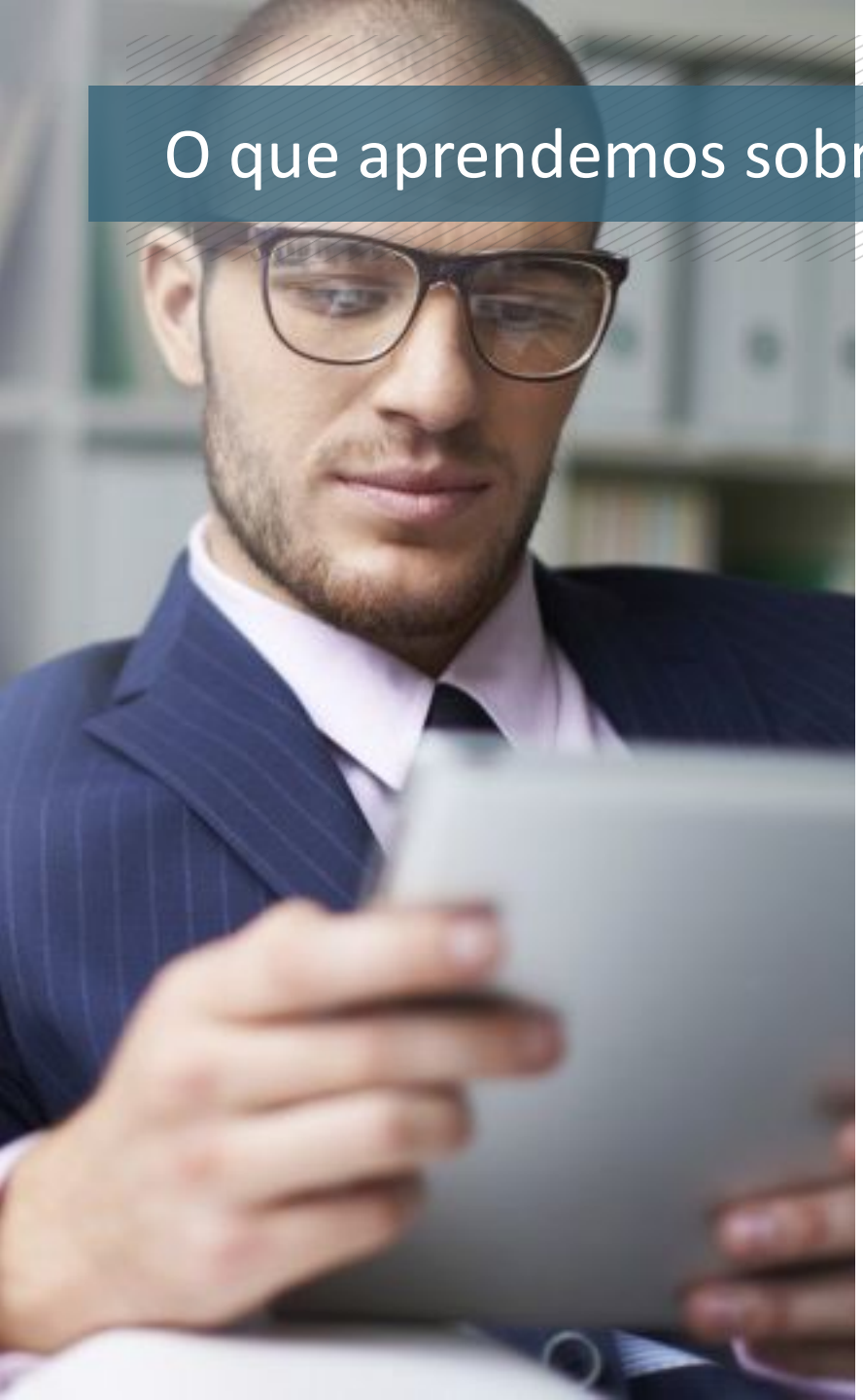
SEGURANÇA ADEQUADA

INVESTIMENTO EFICIENTE EM SEGURANÇA

N.S.N. = N.S.E.

RISCO	Baixo
IMPACTO	Baixo
ROI	Alto

*N.S.N. = Nível de Segurança Necessário
*N.S.E. = Nível de Segurança Existente



O que aprendemos sobre gestão de riscos?

- Desenvolver **processos** de gestão de riscos e avaliação de riscos em *compliance* com base na **ISO 31000**.

- As principais etapas da implantação do Processo de Gestão de Riscos, são:

1. **Comunicação e controle;**
2. **Estabelecimento do contexto;**
3. **Identificação de riscos;**
4. **Análise de riscos;**
5. **Avaliação de riscos;**
6. **Tratamento de riscos, e;**
7. **Monitoramento e análise crítica.**

Comunique valor

Reflexão: GRC – Governança / Risco / Conformidade

1

Governança – O que deve e o que não pode ser feito na empresa para que ela consiga atingir seus objetivos.

2

Risco – Quais os riscos do negócio (sistêmicos & integrados) que podem impedir (total/parcial) a concretização dos objetivos.

3

Conformidade – As ações desejadas estão sendo realizadas? As ações indesejadas ocorreram? Os controles definidos na avaliação de riscos são efetivos/eficientes? A organização está conseguindo atingir seus objetivos?

www.totalrisk.com.br

Bibliografia de referência

Consulte também:
www.bibliotecadeseguranca.com.br

t-Risk

Método de Avaliação de Riscos

Badge t-Risk Practitioner

Adicione a *Badge* t-Risk ao seu histórico profissional e compartilhe-a!

Para mais informações, fale conosco.