





SEGURANÇA DA INFORMAÇÃO

TÓPICOS ESPECIAIS EM ENGENHARIA
GESTÃO DE RISCOS



AGENDA

- ✕ ISO 27005
- ✕ Avaliação do Risco
- ✕ Análise de Risco



ISO 27000

- ✗ Information Security Management
- ✗ 2005
- ✗ +40 normas
- ✗ 27005 → Gestão de Riscos

GESTÃO DE RISCOS

Processo de planejar, organizar, conduzir e controlar as atividades de uma organização com objetivo de mitigar os efeitos do risco sobre o capital e lucro



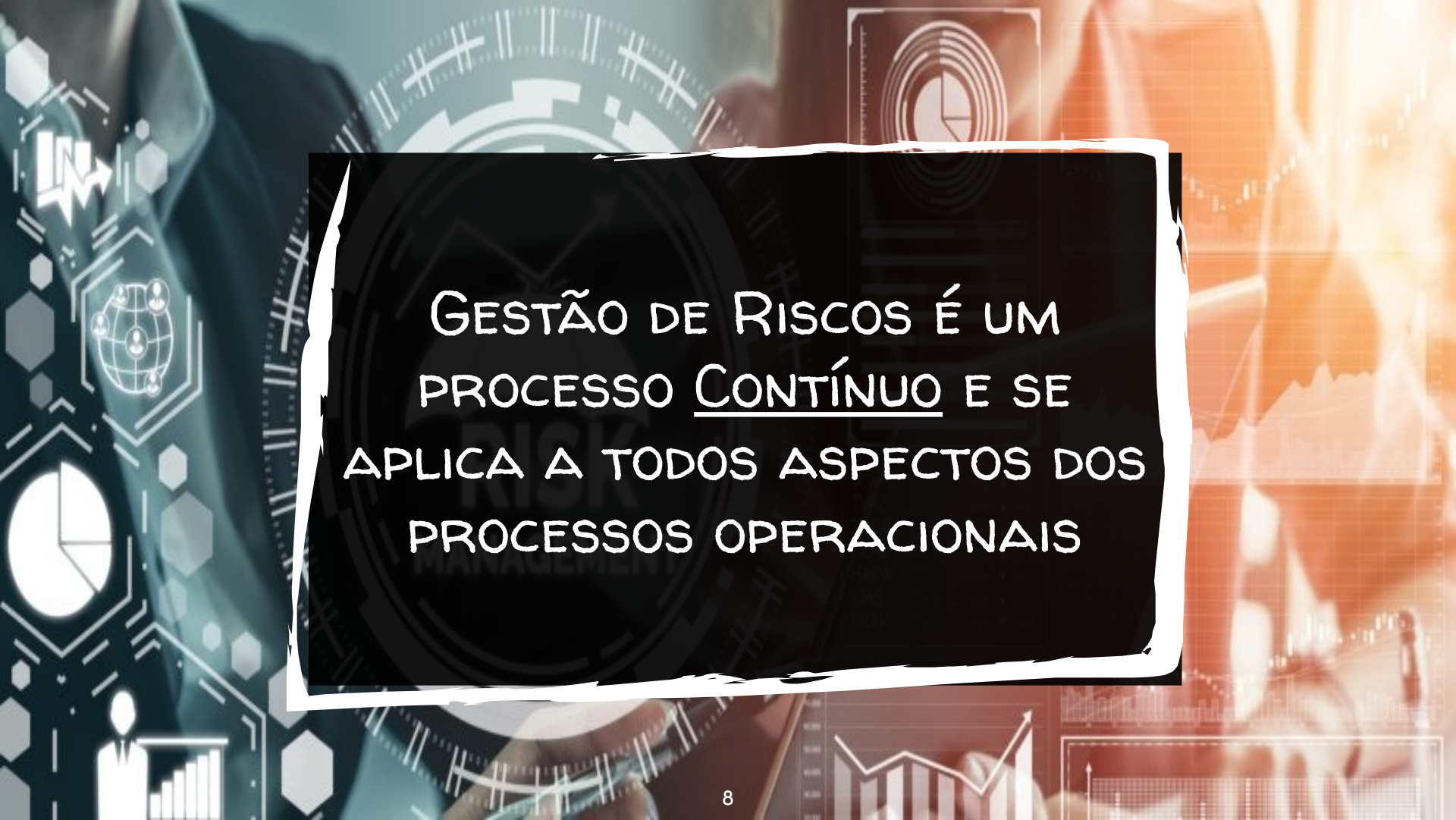
DE ONDE PODE VIR OS RISCOS?

- ✗ Incerteza do mercado financeiro
- ✗ Falhas de projetos
- ✗ Responsabilidades Legais
- ✗ Acidentes
- ✗ Desastres
- ✗ Ataques



O QUE FAZER COM OS RISCOS? (ESTRATÉGIA)

- ✗ Transferir
- ✗ Evitar
- ✗ Reduzir o efeito negativo
- ✗ Aceitar algumas ou todas consequências

The background is a complex collage of business and technology-related imagery. On the left, there are blue-toned icons including a globe with nodes, a pie chart, and a bar chart. In the center, a large, faint clock face is visible. On the right, there are orange-toned elements like a line graph, a bar chart, and a circular diagram. The overall aesthetic is modern and professional, suggesting a focus on data and risk management.

GESTÃO DE RISCOS É UM
PROCESSO CONTÍNUO E SE
APLICA A TODOS ASPECTOS DOS
PROCESSOS OPERACIONAIS



REQUISITOS DA SEGURANÇA DA INFORMAÇÃO

Avaliação de Riscos

Identificação de ameaças a ativos
Vulnerabilidade
Probabilidade de ocorrência
Potencial Impacto

Requisitos Legais

Estatutos, regulamentos e contratos.
Parceiros comerciais, contratantes e provedores de serviço.
Ambiente Sociocultural

Tratamento

Princípios, objetivos e requisitos de negócio para manuseio, processamento, armazenamento, comunicação e arquivamento da informação.



QUANTO DEVO INVESTIR NESSES CONTROLES?



Equalizar de acordo com os prejuízos de negócio que a ausência dos controles trarão.

AVALIAÇÃO DO RISCO

ISO 27002:2005:Capítulo 4 | 27002:2013:....



O QUE É AVALIAÇÃO DO RISCO?

- ✗ Identificar
- ✗ Quantificar
- ✗ Priorizar
 - Critérios de aceitação do risco
 - Objetivos relevantes para organização
- ✗ Resultados guiarão as ações de gestão e prioridade(s)
- ✗ Processo deve ser iterativo



O QUE DEVE INCLUIR A AVALIAÇÃO DO RISCO?

Análise do Risco

Abordagem sistemática para estimar a magnitude de cada risco

Estimativa do Risco

Processo de comparação do risco estimado em relação a um critério para ser determinada a importância do risco.



QUAL CONTEXTO DEVO EXECUTAR A AVALIAÇÃO?

- ✗ Onde for viável, realista e útil
- ✗ Exemplos
 - Toda a organização
 - Parte da organização
 - Software específico
 - Componentes específicos
 - Serviços específicos

ANÁLISE DE RISCO

Segundo ISO 27005

“Análise de Riscos é o processo de definir e analisar os perigos pelos quais indivíduos, empresas e agências governamentais passam em decorrência de potenciais eventos adversos naturais ou causados pelo homem”

TI: Relatório de Análise de Riscos pode ser usado para alinhar objetivos de tecnologia aos objetivos de negócio



CONTEXTO DA ANÁLISE DE RISCO

- ✗ Nível de segurança apropriado (junto com as medidas de segurança associadas) pode ser determinado após esclarecer quais ameaças são relevantes
- ✗ Segurança é a resistência a danos
 - “secura”: “despreocupado”
 - Conceitual e nunca plenamente estabelecido
 - ISECOM: “uma forma de proteção onde é criada uma separação entre os ativos e a ameaça”
- ✗ Análise de Risco ajuda avaliar os riscos e estabelecer medidas de segurança corretas e equilibradas



OBJETIVOS DA ANÁLISE DE RISCO

- ✗ Identificar ativos e seus valores
- ✗ Determinar vulnerabilidades e ameaças
- ✗ Determinar risco de ameaças se concretizarem e interromperem o negócio
- ✗ Estabelecer equilíbrio entre custos de um incidente e custos de medida de segurança



PRINCIPAIS GRUPOS DE ANÁLISES DE RISCOS

Quantitativa

Qualitativa



ANÁLISE QUANTITATIVA DO RISCO

- ✗ Objetivo: calcular, com base no impacto do risco, o nível de prejuízo financeiro e a probabilidade da ameaça virar um incidente
- ✗ Custo das medidas de segurança
- ✗ Valor do próprio estabelecimento
- ✗ $\text{Custo das medidas} < \text{Valor do objeto protegido}$



ANÁLISE QUALITATIVA DO RISCO

- ✗ Números e \$\$\$ não são atribuídos a componentes e perdas
- ✗ Levantamento de cenários de possibilidades de risco
- ✗ Classificação da gravidade das ameaças
- ✗ Validade de possíveis contramedidas
- ✗ Técnicas incluem bom senso, melhores práticas, intuição e XP
- ✗ Exemplos de técnicas: brainstorming, storyboard, grupos de discussão, pesquisas, etc.

CÁLCULO DO RISCO



COMO CALCULAR O RISCO

- ✗ SLE: Single loss expectancy / Expectativa de perda singular
- ✗ ALE: Annualize loss expectancy / Expectativa de perda anual
- ✗ ARO: Annualized rate of occurrence / Taxa de ocorrência anual
- ✗ EF: Exposure Factor / Fator de exposição
 - % de perda que uma ameaça ocorrida pode ter sobre o ativo
- ✗ Valor do ativo * EF = SLE
- ✗ SLE * ARO = ALE

Probabilidade de Londres ser
Inundada: 1 a cada 100 anos
ARO 0,01

ISO 27001:2013

MITIGANDO RISCOS



CONTROLES

- ✗ Salvaguardas ou contramedidas técnicas ou administrativas
- ✗ Evitam / Neutralizam / Minimizam perdas devido a ameaças agindo sobre vulnerabilidades



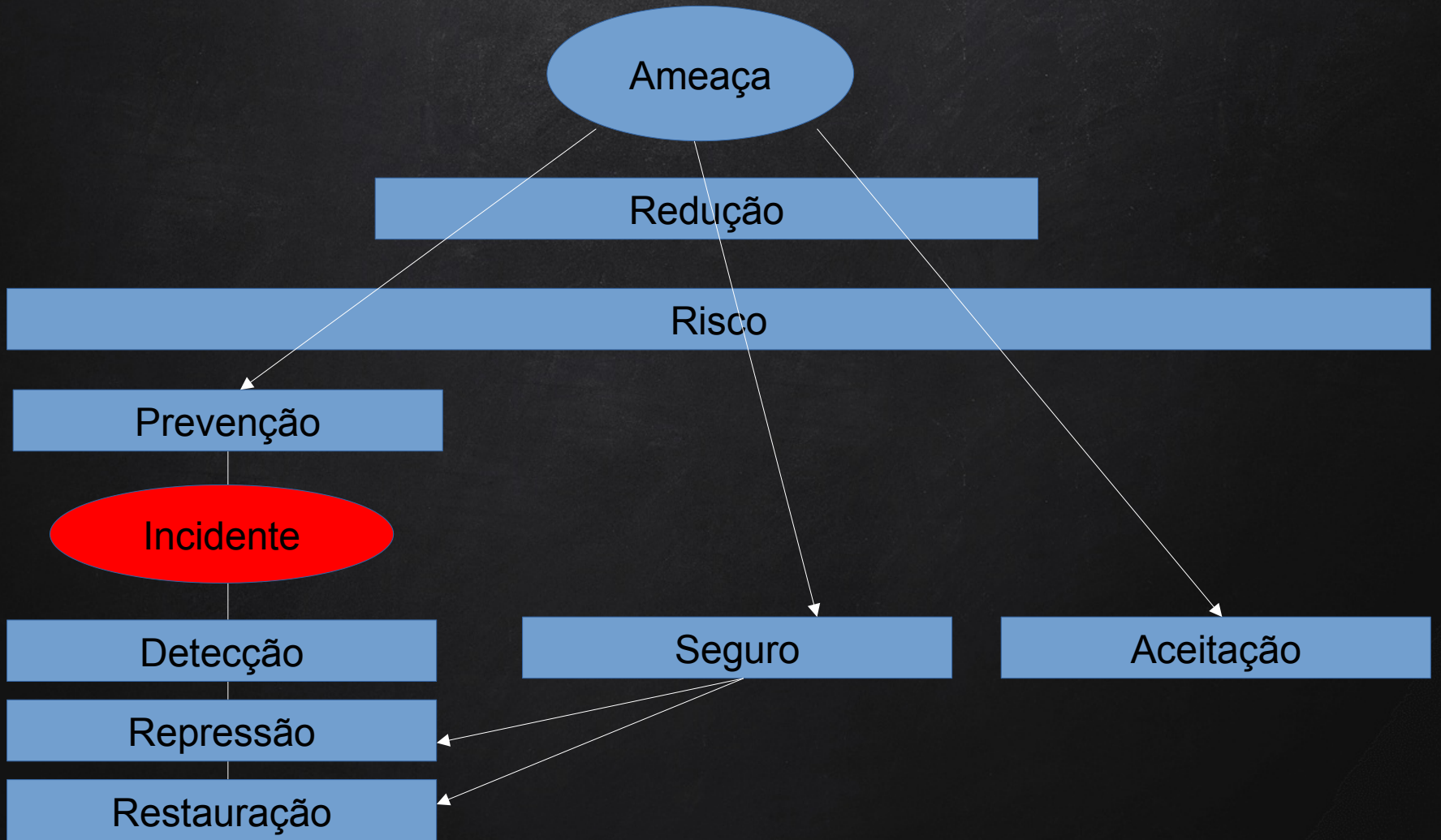
CONTRAMEDIDAS PARA MITIGAR RISCOS

- ✗ Reduzir chances de um evento ocorrer
- ✗ Minimizar consequências
- ✗ Combinação das duas



CATEGORIAS DE CONTRAMEDIDAS

- ✗ Preventivas: evitar incidentes
- ✗ Redução: diminuir probabilidade de uma ameaça ocorrer
- ✗ Detecção: detectar incidentes
- ✗ Repressivas: limitar um incidente
- ✗ Corretivas: recuperação de dados causados por um incidente
- ✗ Aceitação dos riscos



AMEAÇAS



TIPOS DE AMEAÇAS

X Humanas

- Intencional
 - Engenharia social
- Não-intencional
 - Delete sem confirmação
 - Pen drive com virus

X Não-humanas



DÚVIDAS?

Não esqueça de enviar sua
maior dúvida pelo link que está
no github.

ezarpelao@unaerp.br

<https://github.com/elizarp/unaerp>

CREDITS

Special thanks to all the people who made and released these awesome resources for free:

- ✕ Presentation template by [SlidesCarnival](#)
- ✕ Photographs by [Unsplash](#)