

# Segurança e Gestão de Risco

2ºSem 2023/24

**Information Security**

**and Applicable Standards**

**LUIS AMORIM**

**17 Fev 2024**

# Síntese da Aula Anterior

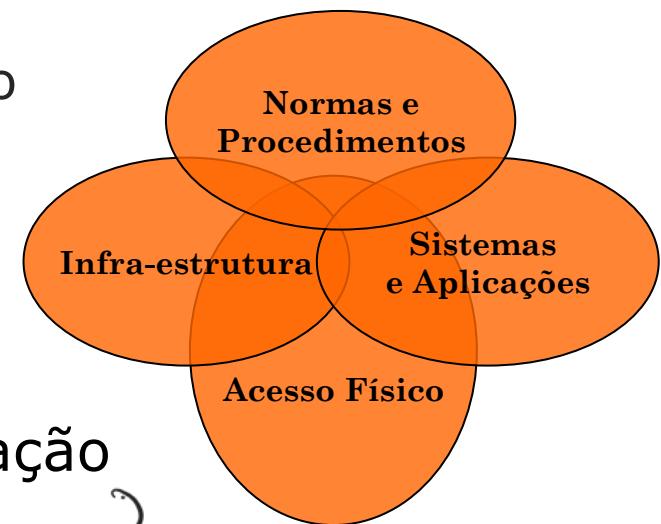
- Segurança da Informação
- Abordagem integrada à segurança
- Requisitos: Normas, Regulamentação e Legislação Aplicável

# Síntese da Aula Anterior

- Segurança da Informação
  - Segurança da Informação <> Segurança dos Sistemas de Informação
    - mas atualmente os Sistemas são a base da Informação
  - A informação (conjunto de dados devidamente ordenados) é atualmente considerada o ativo mais importante nas Organizações
  - Importante identificar os activos a “segurar”
    - Atenção às várias formas de Informação (Visual, Áudio, Escrita, ..., Electrónica)
  - Os 3 atributos essenciais para a segurança da informação: C-I-A
  - A probabilidade de uma ameaça vir a usar uma vulnerabilidade para causar dano resulta num risco para a organização.

# Síntese da Aula Anterior

- Abordagem integrada à segurança
  - A Segurança da informação deve ser um processo integrado, que abrange toda a organização
- Requisitos: Normas, Regulamentação e Legislação Aplicável
  - Devem ser considerados os requisitos
    - Normativos
    - Legais
    - Contratuais

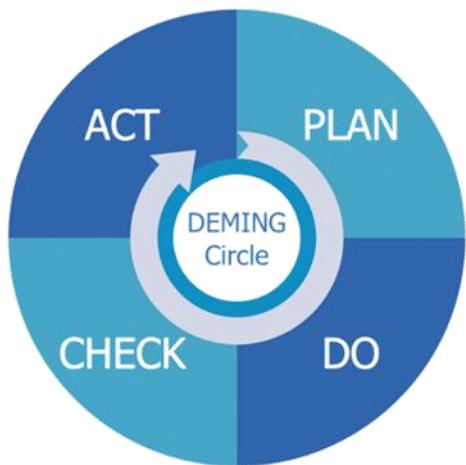


3 respeitar regras  
oficiais do local  
a csiw

# Síntese da Aula Anterior

- Introdução à ISO 27001

- “A exclusão de quaisquer dos requisitos especificados nas cláusulas 4 a 10 não é aceitável para uma organização que reivindica conformidade com a esta Norma” [ISO 27001]



Cap. 0 a 3

- Introdução
- Âmbito
- Referências normativas
- Termos e Definições

Cap. 4 a 10

- Cláusulas 4 a 10
  - Contexto da organização
  - Liderança
  - Planeamento
  - Suporte
  - Operação
  - Avaliação de desempenho
  - Melhoria

Anexos

- Anexos
  - Anexo A (normativo) Objetivos de controlo e controlos
  - Anexo B (informativo) Correspondência entre os termos em inglês e em português

# Exemplificação

- Ameaça: Inundação



( <http://www.youtube.com/watch?v=ttcQy3bCiiU> )

# Exemplificação

- Ameaça: Social Engineering

(<https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402>)

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <https://www.djreprints.com>.

<https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402>

PRO CYBER NEWS

## Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies



PHOTO: SIMON DAWSON/BLOOMBERG NEWS

By [Catherine Stupp](#)

Updated Aug. 30, 2019 12:52 pm ET

Criminals used artificial intelligence-based software to impersonate a chief executive's voice and demand a fraudulent transfer of €220,000 (\$243,000) in March in what cybercrime experts described as an unusual case of artificial intelligence being used in hacking.

The CEO of a U.K.-based energy firm thought he was speaking on the phone with his boss, the chief executive of the firm's German parent company, who asked him to send the funds to a Hungarian supplier. The caller said the request was urgent, directing the executive to pay within an hour, according to the company's insurance firm, Euler Hermes Group SA.

# Exemplificação

- Ameaça: Social Engeneering

(<https://www.reuters.com/article/us-facc-cyber-arrest-china-idUSKCN1110PR>)

AEROSPACE AND DEFENSE AUGUST 26, 2016 / 9:16 AM / UPDATED 6 YEARS AGO

03/2023

## Chinese man arrested in Hong Kong over FACC cyber attack in Austria

By Reuters Staff

3 MIN READ



VIENNA (Reuters) - A Chinese citizen has been arrested in Hong Kong in connection with a cyber attack that cost Austrian aerospace parts maker FACC 42 million euros (\$47.39 million), Austrian police said on Friday.

FACC fired its chief executive and chief financial officer after the attack, which involved hoax emails asking an employee to transfer money for a fake acquisition project - a kind of scam known as a "fake president incident". FACC's customers include Airbus and Boeing.

A 32-year-old man, who was an authorized signatory of a Hong Kong-based firm that received around 4 million euros from FACC, was arrested on July 1 on suspicion of money laundering, a spokesman for Austria's Federal Office for Crime said.

Such attacks, also known as "business email compromise", involve thieves gaining access to legitimate email accounts inside a company – often those of top executives – to carry out unauthorized transfers of funds. The technique, which relies on simple trickery or more sophisticated computer intrusions, typically targets businesses working with international suppliers that regularly perform wire transfers.

A spokesman for FACC said the company was working on getting back 10 million euros which had been found and frozen on accounts in different countries around the world. These 10 million euros are not included in the 42 million euro hit the group has already booked.

In June, the U.S. Federal Bureau of Investigation (FBI) said identified losses from this scam totaled \$3.1 billion and had risen by 1,300 percent in the past 18 months.

8

# Exemplificação

## • Ameaça: Phishing

(<https://www.wsj.com/articles/beware-of-qr-code-scams-11647625020?page=1>)



JOURNAL REPORTS: TECHNOLOGY

## Beware of QR Code Scams

It's so easy to click on a QR code. Criminals are counting on it.

By Heidi Mitchell

Updated March 19, 2022 8:00 am ET

During the Super Bowl in February, one ad grabbed a lot of attention: a mysterious bouncing QR code that enticed viewers to point their phones at their screens and click through to an unknown website. (Spoiler alert: It was for [Coinbase](#). [COIN -1.83% ▼](#)) Within seconds, more than 20 million people had done just that, crashing the cryptocurrency-exchange platform.

The incident illustrated just how willing people are to click on QR codes, but unfortunately for consumers, marketers aren't the only group that understands this. Two months before, in December, a much darker scenario involving QR codes unfolded when malicious actors placed QR-code stickers on parking meters [in major Texas cities](#), directing drivers to a fraudulent website where they supposedly could pay for parking.

“People were tricked into putting in their credit-card information,” says Eric Chien, security threat researcher at Symantec, part of Broadcom Software’s security technology and response division. “It was a really well-done attack.”

# AGENDA

## ➤ **Introdução à Segurança da Informação - ISO 27001**

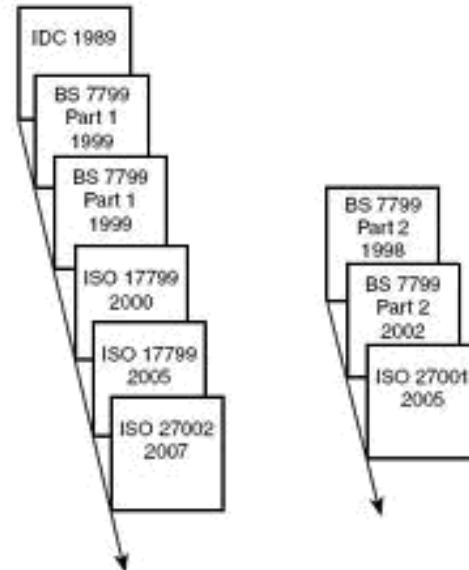
- Introdução à Gestão de Continuidade de Negócio
- A avaliação e gestão de riscos
- Tratamento dos Riscos

# Introdução à ISO 27001

- ISO/IEC 27001- Information Security Management Systems
  - “specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.
  - It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.
  - The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature”
- ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls
  - “Gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).
  - It is designed to be used by organizations that intend to:
    - select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;
    - implement commonly accepted information security controls;
    - develop their own information security management guidelines.”

# 12 Introdução à ISO 27001

- Histórico dos Standards
- Publicação da BS 7799 Parte 1 – Fevereiro 1995
- Publicação da BS 7799 Parte 2 – Fevereiro 1998
- Publicação da BS 7799:1999 Parte 1 e 2 - Abril 1999
- Publicação da ISO 17799 (BS 7799-1) - Dezembro 2000
- Publicação da BS 7799 Parte 2 - Setembro 2002
- Revisão da ISO 17799 (BS 7799-1) - Julho 2005
- Publicação da ISO 27001 (BS 7799-2) – Out 2005
- Publicação da ISO 27001:2013 – Set 2013
- Publicação da ISO 27002:2013 – Out 2013
- Publicação da ISO 27001:2022 – Out 2022
- Publicação da ISO 27002:2022 – Out 2022



# Introdução à ISO 27001

- ISO/IEC 27001
  - Requisitos para a Implementação de um Sistema de Gestão de Segurança da Informação
- Sistema de Gestão (Qualidade, Segurança, Ambiente, ...)
  - O Sistema de Gestão é uma ferramenta que conduz ao controlo e sistematização dos processos, permitindo também a avaliação da eficácia das ações tomadas, na procura da melhoria contínua
- Sistema de Gestão Integrado (Qualidade + Segurança + Ambiente + ...)
  - Um sistema de gestão integrado (quando bem implementado) minimiza e otimiza os processos e as componentes dos diferentes sistemas, conduzindo à concentração num conjunto único de processos, que permitem uniformizar os procedimentos

os vários sistemas têm fórmulas equivalentes

# Introdução à ISO 27001

- ISO/IEC 27001:2013
  - Evolução da ISO 27001:2005 (baseada na BS 7799-2)
    - Publicada em 25 de Setembro de 2013
    - Em conjunto com a ISO/IEC 27002:2013
    - Em simultâneo foi publicada, pelo IPQ, a NP ISO/IEC 27001
  - Especifica os requisitos para o estabelecimento, implementação e documentação de um Sistema de Gestão de Segurança da Informação (ISMS - Information Security Management System)
  - Especifica os requisitos para os controlos de segurança a serem implementados de acordo com as necessidades individuais das organizações

INTERNATIONAL  
STANDARD  
**ISO/IEC  
27001**  
Second edition  
2013-10-01

Information technology — Security  
techniques — Information security  
management systems — Requirements  
Technologien der Information — Sicherheitstechniken — Spezifizierung  
der Verwaltung eines Sicherheitsmanagements — Anforderungen

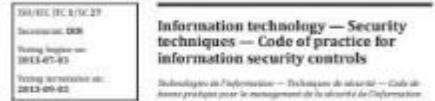
Reference number:  
ISO/IEC 27001:2013/E  
© ISO/IEC 2013

15

# Introdução à ISO 27001

- ISO/IEC 27002:2013 (ex 17799, baseada na BS 7799-1)
  - Código de boas práticas para a gestão da segurança da informação
  - Para utilização como documento de referência
  - Possui um conjunto comprehensivo de controlos de segurança (114)
  - As melhores práticas de segurança atuais
  - Possui 14 secções de controlo
  - Não pode ser utilizado para análise(auditória) e/ou certificação

INTERNATIONAL  
STANDARD  
ISO/IEC  
FDIS  
27002



# Introdução à ISO 27001

- Composição da ISO 27001

- No essencial contém
  - 7 cláusulas
  - 114 Controlos

Cap. 0 a 3

- Introdução
- Âmbito
- Referências normativas
- Termos e Definições

Cap. 4 a 10

- Cláusulas 4 a 10
  - Contexto da organização
  - Liderança
  - Planeamento
  - Suporte
  - Operação
  - Avaliação de desempenho
  - Melhoria

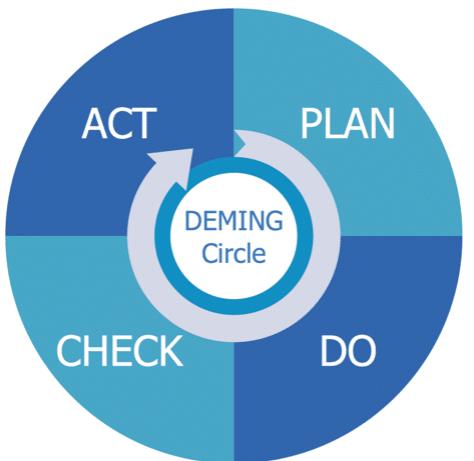
Anexos

- Anexos
  - Anexo A (normativo) Objetivos de controlo e controlos
  - Anexo B (informativo) Correspondência entre os termos em inglês e em português

- Sendo as cláusulas a componente principal e obrigatória
  - “A exclusão de quaisquer dos requisitos especificados nas cláusulas 4 a 10 não é aceitável para uma organização que reivindica conformidade com a esta Norma” [ISO 27001]

# Introdução à ISO 27001

- Modelo PDCA aplicado ao ISMS
  - Plan (establish the ISMS)
    - Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
  - Do (implement and operate the ISMS)
    - Implement and operate the ISMS policy, controls, processes and procedures.
  - Check (monitor and review the ISMS)
    - Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
  - Act (maintain and improve the ISMS)
    - Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.



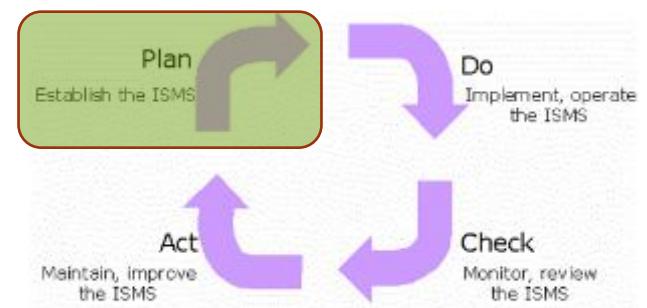
# Introdução à ISO 27001

## • Sistema de Gestão

- 4 Contexto da organização
  - 4.1 - Compreender a organização e o seu contexto
  - 4.2 - Compreender as necessidades e expectativas das partes interessadas
  - 4.3 - Determinar o âmbito do sistema de gestão de segurança da informação
  - 4.4 - Sistema de gestão de segurança da informação

*Dependendo do local where problems  
mudar.*

*stakeholders*



# Introdução à ISO 27001

## • Sistema de Gestão

- 4 Contexto da organização
  - 4.1 - Compreender a organização e o seu contexto
    - A organização **deve** determinar as questões internas e externas que são relevantes para a sua finalidade e que afetam a sua capacidade para alcançar o(s) resultado(s) pretendido(s) do seu sistema de gestão de segurança da informação.
  - NOTA: A determinação destas questões relaciona-se com o estabelecimento do contexto externo e interno da organização considerado na Cláusula 5.3 da NP ISO 31000:2012.

# Introdução à ISO 27001

## • Sistema de Gestão

- 4 Contexto da organização
  - 4.2 Compreender as necessidades e expectativas das partes interessadas
    - A organização deve determinar as partes interessadas e os seus requisitos:
      - a) as partes interessadas que são relevantes para o SGSI
      - b) os requisitos, destas partes interessadas, relevantes para a segurança da informação

# Introdução à ISO 27001

## • Sistema de Gestão

- 4 Contexto da organização
  - 4.3 - Determinar o âmbito do sistema de gestão de segurança da informação
    - A organização deve determinar os limites e aplicabilidade do SGSI, de forma documentada e disponível
    - Ao determinar este âmbito, a organização deve considerar:
      - a) questões externas e internas referidas em 4.1
      - b) requisitos referidos em 4.2;
      - c) interfaces e dependências entre as atividades desempenhadas pela organização, e aquelas que são desempenhadas por outras organizações.

# Introdução à ISO 27001

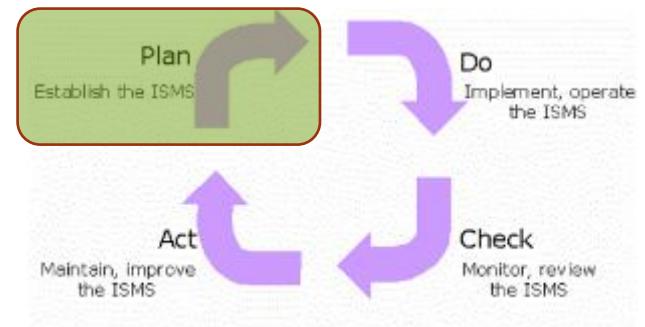
- **Sistema de Gestão**

- 4 Contexto da organização
  - 4.4 - Sistema de gestão de segurança da informação
    - A organização deve estabelecer, implementar, manter e melhorar de forma contínua um SGSI

# Introdução à ISO 27001

- Sistema de Gestão

- 5 Liderança
  - 5.1 - Liderança e comprometimento
  - 5.2 - Política
  - 5.3 - Funções, responsabilidades e autoridades na organização



# Introdução à ISO 27001

- **Sistema de Gestão**

- 5 Liderança
  - 5.1 - Liderança e comprometimento
  - A gestão de topo deve demonstrar liderança e comprometimento para com o SGSI:
    - a) assegurando que a política de segurança da informação e os objetivos de segurança da informação estão estabelecidos e são compatíveis com a orientação estratégica da organização
    - b) assegurando a integração dos requisitos do SGSI nos processos da organização
    - c) assegurando que os recursos necessários para o SGSI estão disponíveis
    - d) comunicando a importância de uma gestão de segurança da informação eficaz e em conformidade com SGSI
    - e) assegurando que o sistema de gestão de segurança da informação atinge os resultados pretendidos
    - f) orientando e apoiando as pessoas para contribuir para a eficácia do SGSI
    - g) promovendo a melhoria contínua
    - h) apoiando outras funções de gestão relevantes a demonstrarem a sua liderança, conforme aplicável às suas áreas de responsabilidade

# Introdução à ISO 27001

- **Sistema de Gestão**

- 5 Liderança
  - 5.2 - Política
  - A gestão de topo deve estabelecer uma política de segurança da informação, que:
    - a) seja apropriada ao propósito da organização
    - b) inclua os objetivos de segurança da informação (ver 6.2) ou proporcione um modelo de referência para definir objetivos de segurança da informação
    - c) inclua um comprometimento para satisfazer os requisitos aplicáveis relacionados com a segurança da informação
    - d) inclua um comprometimento para a melhoria contínua do sistema de gestão de segurança da informação
    - e) estar disponível, como informação documentada;
    - f) ser comunicada dentro da organização
    - g) estar disponível para as partes interessadas, conforme apropriado

# Introdução à ISO 27001

- **Sistema de Gestão**

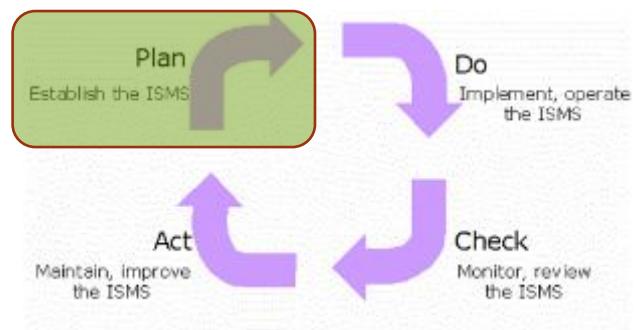
- 5 Liderança
  - 5.3 - Funções, responsabilidades e autoridades na organização
  - A gestão de topo deve atribuir a responsabilidade e a autoridade para:
    - a) assegurar que o sistema de gestão de segurança da informação está em conformidade com os requisitos desta Norma
    - b) reportar à gestão de topo o desempenho do sistema de gestão de segurança da informação
  - NOTA: A gestão de topo pode também atribuir responsabilidades e autoridades para reportar o desempenho do SGSI

# Introdução à ISO 27001

## • Sistema de Gestão

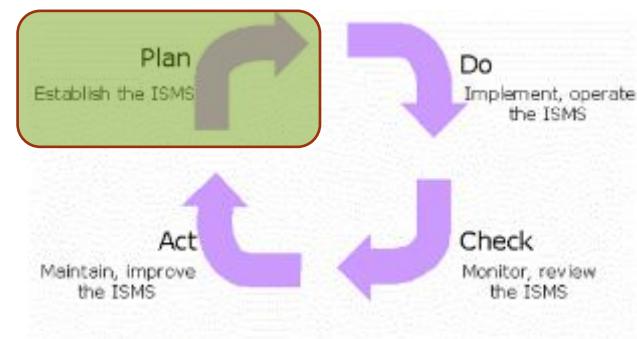
- 6 Planeamento
  - 6.1 - Ações para endereçar riscos e oportunidades
    - 6.1.1 Generalidades
    - 6.1.2 Avaliação dos riscos de segurança da informação
    - 6.1.3 Tratamento dos riscos de segurança da informação
  - 6.2 - Objetivos de segurança da informação e planeamento para os alcançar

com 2 quocic s d<sup>e</sup> m<sup>o</sup> o c<sup>o</sup>s  
d<sup>e</sup> o que é b<sup>a</sup>n<sup>o</sup> p<sup>o</sup>r c<sup>o</sup>rir  
de um p<sup>o</sup>rm<sup>c</sup>



# Introdução à ISO 27001

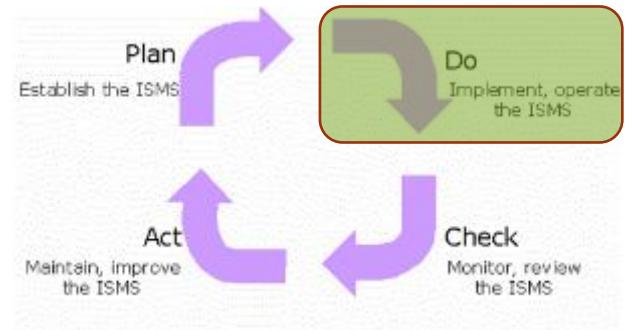
- Sistema de Gestão
  - 7 Suporte
    - 7.1 - Recursos
    - 7.2 - Competência
    - 7.3 - Consciencialização
    - 7.4 - Comunicação
    - 7.5 - Informação documentada
      - 7.5.1 Generalidades
      - 7.5.2 Criar e atualizar
      - 7.5.3 Controlo da informação documentada



# Introdução à ISO 27001

- Sistema de Gestão

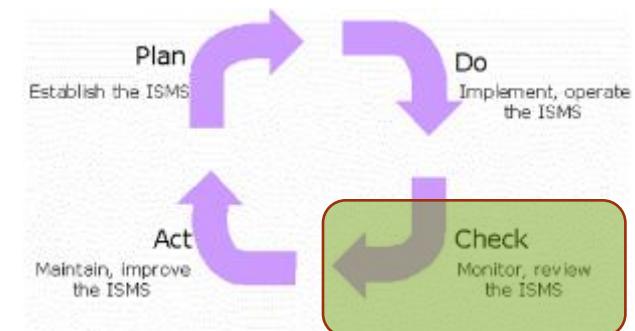
- 8 Operação
  - 8.1 - Planeamento e controlo operacional
  - 8.2 - Avaliação dos riscos da segurança da informação
  - 8.3 - Tratamento dos riscos da segurança da informação



# Introdução à ISO 27001

- Sistema de Gestão

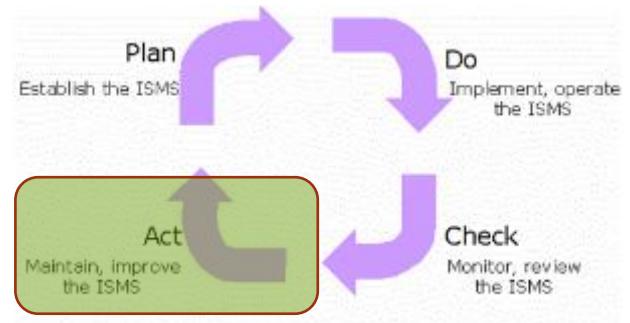
- 9. Avaliação de desempenho
  - 9.1 Monitorização, medição, análise e avaliação
  - 9.2 Auditoria interna
  - 9.3 Revisão pela gestão



# Introdução à ISO 27001

- Sistema de Gestão

- 10. Melhoria
  - 10.1 Não conformidade e ação corretiva
  - 10.2 Melhoria contínua



# Introdução à ISO 27001

## • Annex A – Controlos

- A selecção dos controlos a aplicar depende de cada Organização e dos requisitos do ISMS
  - Factores de negócio (ex. sector financeiro)
  - Processos de negócio (ex. desenv. de software)
  - Âmbito do ISMS (ex. pessoas, processos e/ou facilities)
- Implementação dos controlos detalhada na ISO 27002
- Poderão ser necessários controlos adicionais
  - Sector de mercado
    - (ex. lotarias, banca, saúde, defesa nacional, requisitos legais)
  - Imposições legais
  - Requisitos contratuais

# Introdução à ISO 27001:2013

- **Anexo A - Controlos A5 a A18**

- A.5 Políticas de segurança da informação
- A.6 Organização da segurança da informação
- A.7 Segurança na gestão de recursos humanos
- A.8 Gestão de activos
- A.9 Controlo de acessos
- A.10 Criptografia
- A.11 Segurança física e ambiental
- A.12 Gestão das operações e comunicações
- A.13 Segurança de comunicações
- A.14 Aquisição, desenvolvimento e manutenção de sistemas de informação
- A.15 Relações com fornecedores
- A.16 Gestão de incidentes de segurança da informação
- A.17 Aspetos de segurança da informação relativos à gestão da continuidade do negócio
- A.18 Conformidade

# Introdução à ISO 27001

- Annex A – Controlos
  - A.8 Gestão de activos
    - A.8.1 Responsabilidade pelos activos
      - A.8.1.1 Inventário de activos
      - A.8.1.2 Responsabilidade pelos activos
      - A.8.1.3 Utilização aceitável dos activos
      - A.8.1.4 Devolução de ativos
    - A.8.2 Classificação da informação
      - A.8.2.1 Classificação da informação
      - A.8.2.2 Etiquetagem da informação
      - A.8.2.3 Manuseamento de ativos
    - A.8.3 Manuseamento de suportes de dados
      - A.8.3.1 Gestão de suportes de dados amovíveis
      - A.8.3.2 Eliminação de suportes de dados
      - A.8.3.3 Transporte de suportes de dados

# Introdução à ISO 27001

- Annex A – Controlos (ISO 27002)
  - A.8 Gestão de activos
    - A.8.1 Responsabilidade pelos activos
      - A.8.1.1 Inventário de activos
        - Implementation guidance
        - An organization should identify assets relevant in the lifecycle of information and document their importance. The lifecycle of information should include creation, processing, storage, transmission, deletion and destruction. Documentation should be maintained in dedicated or existing inventories as appropriate.
        - The asset inventory should be accurate, up to date, consistent and aligned with other inventories.
        - For each of the identified assets, ownership of the asset needs should to be assigned (see 8.1.2) and the classification needs should to be identified (see 8.2).
        - Other information
          - Inventories of assets help to ensure that effective protection takes place, and may also be required for other purposes, such as health and safety, insurance or financial (asset management) reasons.

# Introdução à ISO 27001:2022

- Anexo A - Controlos A5 a A8

- 114 Controlos na versão de 2013 > 93 Controlos em 2022
  - Fusão de 56 controlos, em 24
  - 23 Controlos renomeados
  - 3 Controlos removidos
  - 11 novos controlos
- Agrupados em 4 áreas temáticas, face aos 14 domínios anteriores
  - A 5 – Controlos Organizacionais
  - A 6 – Controlos relacionados com as Pessoas
  - A 7 – Controlos físicos
  - A 8 – Controlos Tecnológicos

# AGENDA

- Introdução à Segurança da Informação - ISO 27001
- **Introdução à Gestão de Continuidade de Negócio**
- A avaliação e gestão de riscos
- Tratamento dos Riscos

# AGENDA

## ➤ **Introdução à Gestão de Continuidade de Negócio**

- A avaliação e gestão de riscos
- Tratamento dos Riscos
- Controlos de segurança
  - Tecnológicos, Operacionais e de Gestão

# Introdução à Gestão de Continuidade de Negócio

- A caracterização e implementação de um Business Continuity Management (BCM), ou Gestão Continuidade de Negócio deve fazer parte da Gestão de Risco de uma organização.
- O processo de Gestão Continuidade de Negócio conduz à produção de planos e procedimentos que permitem, a uma organização, responder a incidentes mantendo ou reactivando em tempo útil os seus serviços críticos ou essenciais para o negócio
- A dependência das organizações face aos Sistemas de Informação e os riscos a que se expõem torna necessário conceber e operacionalizar uma estratégia de Gestão Continuidade de Negócios.
- Actualmente o standard a seguir nesta área é a ISO 22301:2012
  - Revisão da versão 2012 (ainda utilizada)
  - Provém da BS25999 do BSI

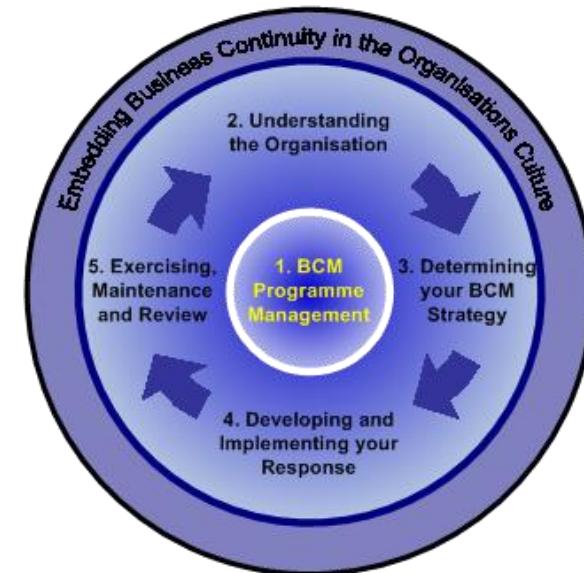


# Introdução à Gestão de Continuidade de Negócio

10/03/2023

- Business Continuity Management Lifecycle (ISO 22301)

- BCM program management
- Understanding the organization
- Determining BCM strategies
- Developing & implementing a BCM response
- Exercising, maintaining and reviewing BCM
- Embedding BCM in the organization's culture



# Introdução à Gestão de Continuidade de Negócio

- Uma Gestão de Continuidade de Negócio eficiente permite à Organização:
  - Identificar os processos/informação/sistemas críticos para o negócio
  - Identificar os impactos de uma eventual descontinuação dos serviços;
  - Preparar a resposta a incidentes, que permitam minimizar esses impactos para o negócio;
  - Definir processos e organização da equipa na sua implementação, testes e ativação;
- Oferece à organização uma vantagem competitiva
  - Em caso de incidentes, oferecendo uma maior preparação e rápida resposta
  - Pode ser explorado em termos de marketing

# Introdução à Gestão de Continuidade de Negócio

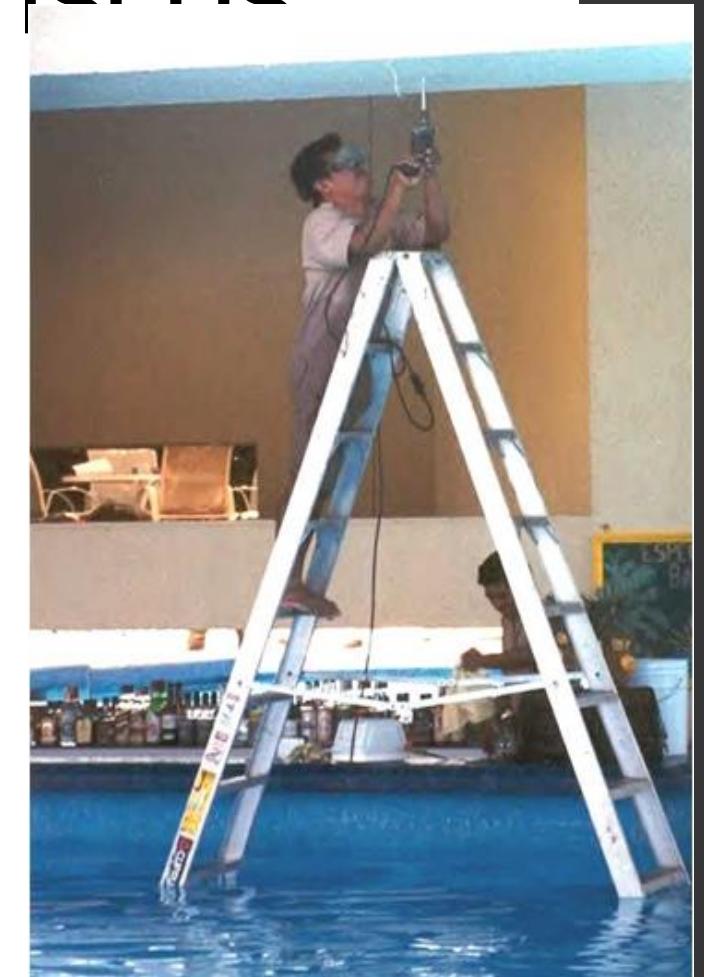
- Uma Gestão de Continuidade de Negócio eficiente permite à Organização:
  - Identificar os processos/informação/sistemas críticos para o negócio
  - Identificar os impactos de uma eventual descontinuação dos serviços;
  - Preparar a resposta a incidentes, que permitam minimizar esses impactos para o negócio;
  - Definir processos e organização da equipa na sua implementação, testes e ativação;
- Oferece à organização uma vantagem competitiva
  - Em caso de incidentes, oferecendo uma maior preparação e rápida resposta
  - Pode ser explorado em termos de marketing

# AGENDA

- Introdução à Segurança da Informação - ISO 27001
  - Introdução à Gestão de Continuidade de Negócio
- **A avaliação e gestão de riscos**
- Tratamento dos Riscos

# A Avaliação e gestão dos riscos

- Análise de Risco?
- Gestão do Risco?



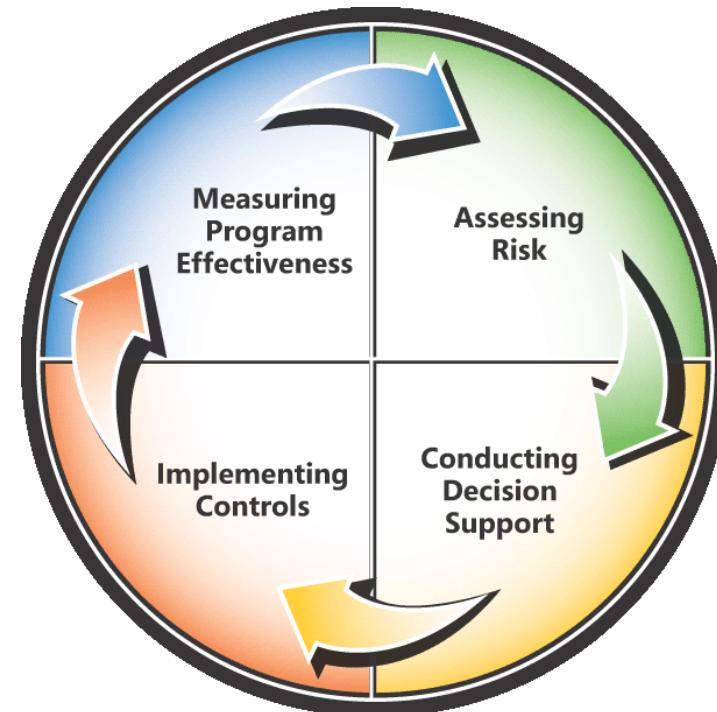
# A Avaliação e gestão dos riscos

- Avaliação de Risco

Vs

- Gestão de Risco

- É um processo:
  - Avaliação de Risco
  - Decisões sobre opções
  - Implementação de controlos
  - Reavaliação/monitorização



# A Avaliação e gestão dos riscos

- Gestão de Riscos

- Tem como objetivo permitir à organização atingir os objetivos a que se propôs:
- Mantendo em segurança os sistemas de informação que guardam, processam ou transmitem informação da organização
- Permitindo à gestão a tomada de decisões devidamente fundamentadas que justifiquem os investimentos e custos das Tis
- Assistir a gestão na acreditação dos sistemas de IT com base na documentação resultante das atividades desenvolvidas na Gestão de Risco
- É um processo, não um projeto

# A Avaliação e gestão dos riscos

- A aplicação da Avaliação e Análise de Risco:
  - Sobre os processos e sistemas implementados
  - Sobre novos processos e sistemas
- Ter em atenção que
  - O custo para correção de problemas de um sistema de informação apresenta um acentuado crescimento com a fase de vida do projeto, em que se tomam as necessárias medidas.
    - O ideal é ser realizada uma análise cuidada na fase de conceção
  - A acrescer aos custos de correção, temos os custos inerentes às consequências para o negócio (produtividade, indisponibilidade, confiança, imagem, ...)

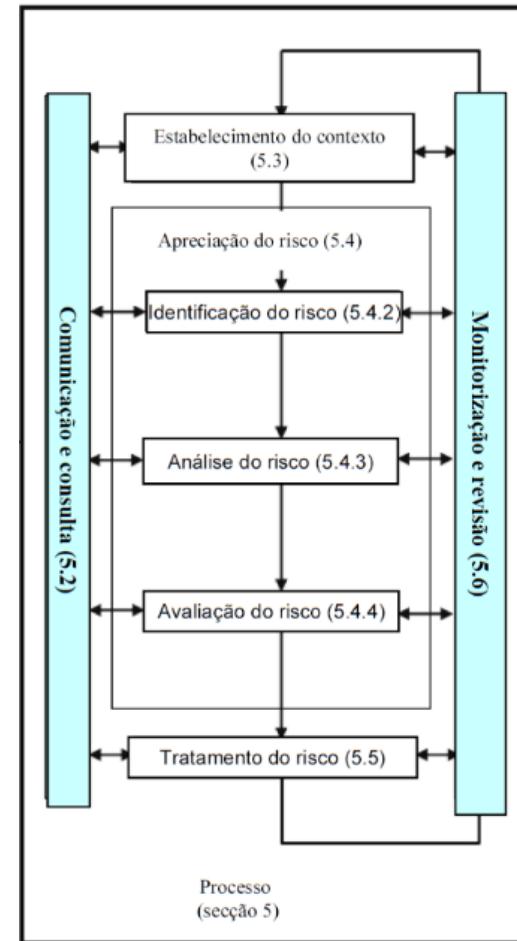


# A Avaliação e gestão dos riscos

- Outras utilizações da Avaliação e Gestão dos Riscos
  - Project Impact Analysis ou Avaliação dos Riscos de Projeto
    - É utilizada para fundamentar as razões pelas quais o processo deve ser (ou não) implementado
    - Depois de analisado e aprovado, a avaliação serve para identificar as ameaças inerentes a esse projeto, e possível redução de riscos
  - Resultados principais
    - Identificação das ameaças e Valorização dos Riscos
    - Identificação de possível formas de mitigação
    - Análise custo benefício da implementação

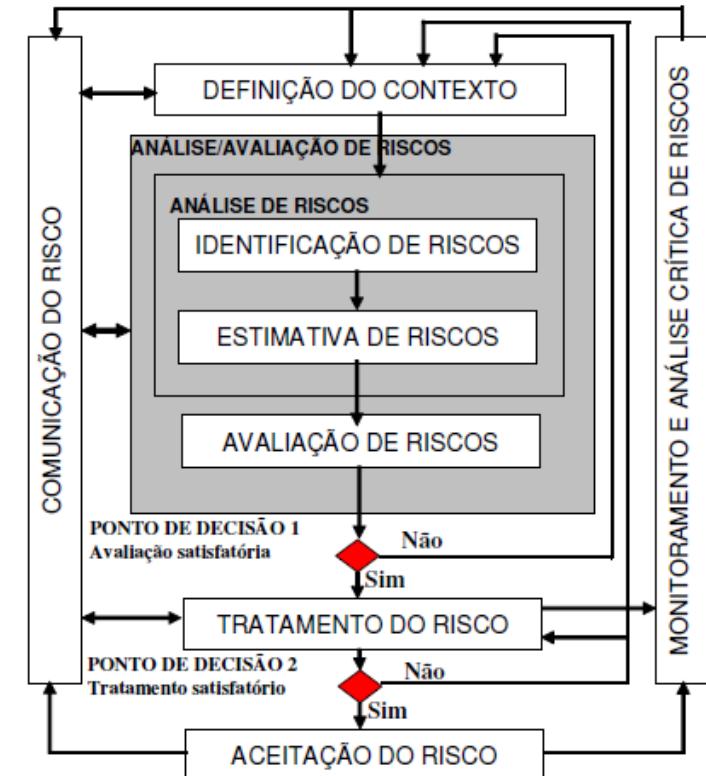
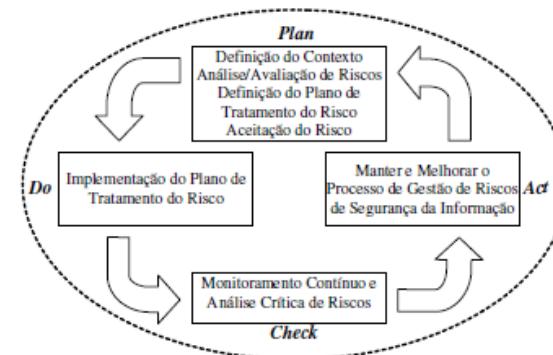
# A Avaliação e gestão dos riscos

- ISO 31000:2018 - Risk management - Principles and guidelines
- Norma ISO genérica que define metodologia de Gestão de Risco



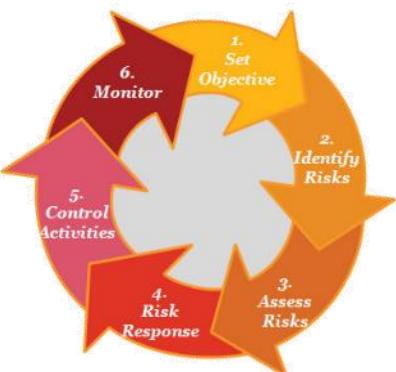
# A Avaliação e gestão dos riscos

- ISO 27005 - Norma adaptada à Gestão de Risco de Segurança da Informação
- Alinhada com o modelo PDCA da ISO 27001



# A Avaliação e gestão dos riscos

- ERM / COSO - Enterprise Risk Management, do COSO (Committee of Sponsoring Organizations of the Treadway Commission)
  - Componentes ERM
    - cruzando categorias de objetivos (estratégicos, operacionais, de comunicação e conformidade) com a Organização (nível de organização, divisão, unidade de negócio e subsidiária)



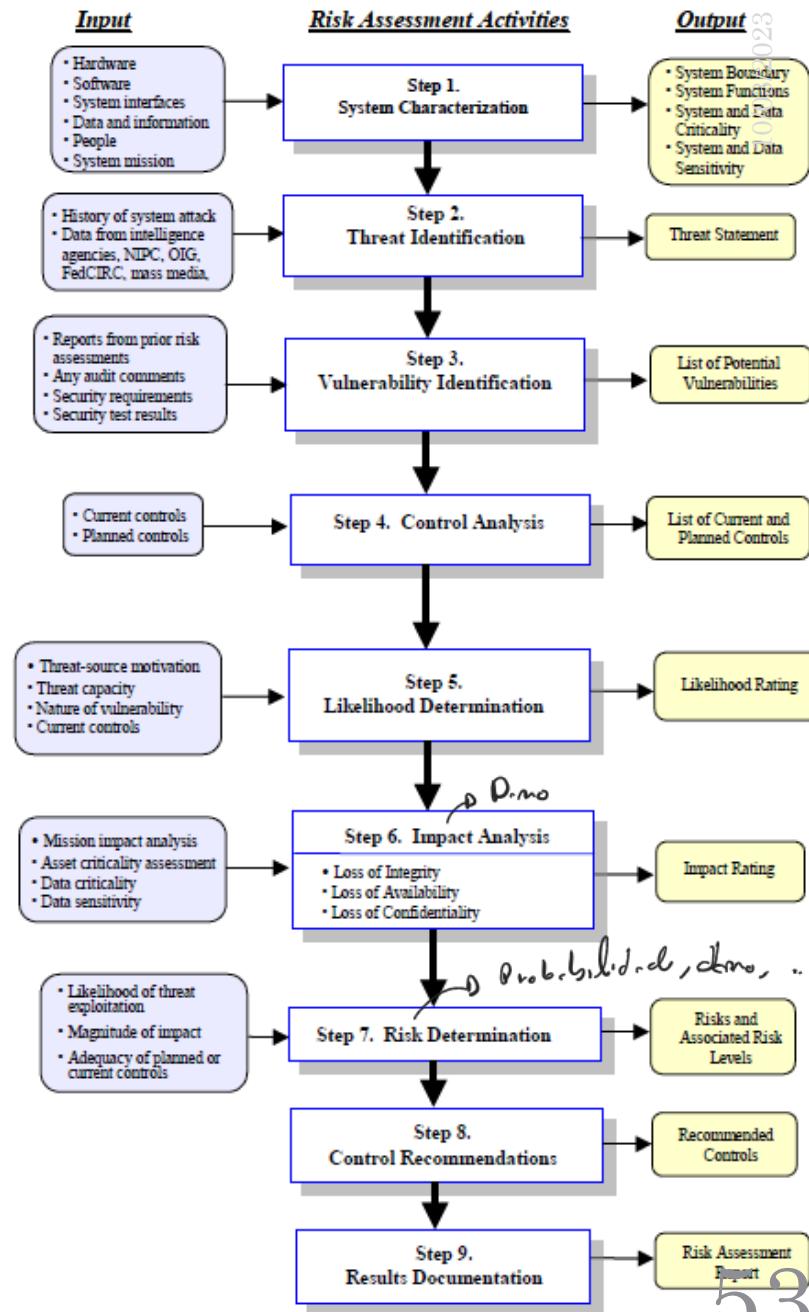
# Exercício de Grupo

- Escolher uma área/sistema da Universidade
- Identificar possíveis
  - Ameaças
  - Vulnerabilidades
  - Riscos
- Identificar controlos a implementar

# A Avaliação e gestão dos riscos

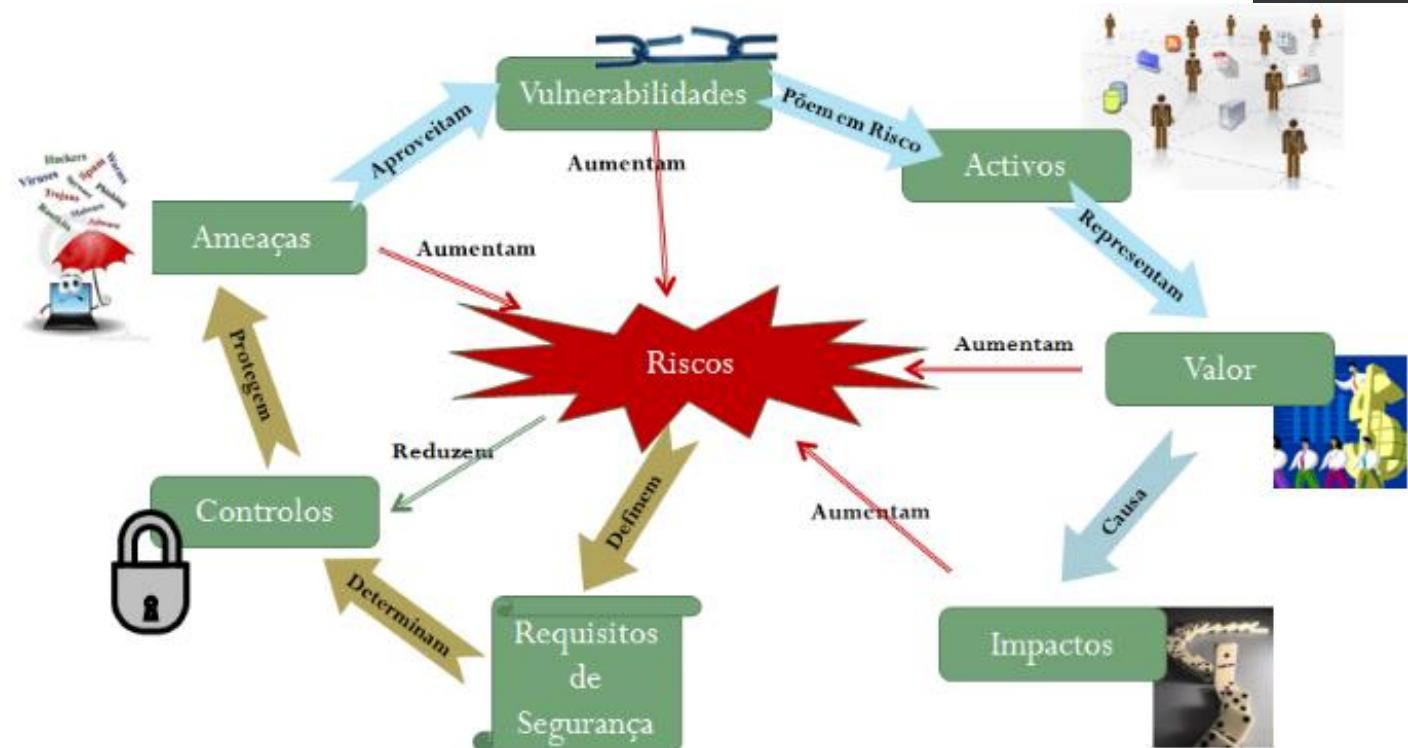
- As etapas de uma Avaliação de Riscos (segundo o NIST - National Institute of Standards and Technology)
  - Caracterização do sistema
  - Identificação das ameaças
  - Identificação das Vulnerabilidades
  - Análise de controlos
  - Determinação de probabilidades
  - Análise de impacto
  - Determinação do Risco
  - Recomendação de Controlos a implementar
  - Documentação final

Apresenta pormenores cuja adoção poderá beneficiar a metodologia a adotar
- (NIST SP800-30 - Risk Management Guide for IT Systems)



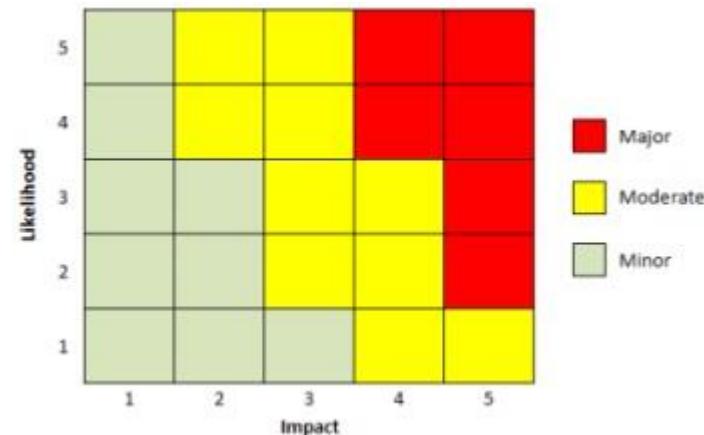
# A Avaliação e gestão dos riscos

- Mas:
- Como quantificar o Risco?
- Como estimar a probabilidade?
- Como avaliar o Risco?



# A Avaliação e gestão dos riscos

- Formas de quantificar o Risco?
- Avaliação quantitativa, recorrendo a valores numéricos
- Avaliação qualitativa, através de níveis de valores, utilizando categorias e níveis de risco
- Ou uma avaliação mista



		Matriz de Probabilidade x Impacto				
		5	4	3	2	1
Probabilidade	5	5	10	15	20	25
	4	4	8	12	16	20
3	3	6	9	12	15	
2	2	4	6	8	10	
1	1	2	3	4	5	
Impacto	1	2	3	4	5	



# A Avaliação e gestão dos riscos

- Formas de quantificar o Risco?
  - Avaliação qualitativa vs Avaliação quantitativa

“Many discussions of security risk analysis methodologies mention a distinction between quantitative and qualitative risk analysis, but virtually none of those discussions clarify the distinction in a rigorous way”

(Posted By Jeff Lowder On September 4, 2008 @ 6:00 am In Risk Analysis)

- Quantitative Risk Analyses assign fixed numerical values (within a margin of error) to both the probability and utility (business impact) of an outcome;
- Qualitative Risk Analyses don't. Instead, they represent both the probability and utility of an outcome using an interval scale, where each interval includes a range of numerical values (beyond the margin of error) and each interval is typically represented by a non-numerical label (such as the words “High”, “Medium”, “Low”), not the ranges of values those labels represent.

# A Avaliação e gestão dos riscos

- Avaliação de risco

- Existem várias formas de calcular o risco
  - Em função da metodologia adoptada
  - No entanto, tem que ser sistemática e repetível

- Alguns exemplos de fórmulas de cálculo de risco:

- Risco = Probabilidade x Consequência x Severidade
- Risco = Valor\_Ativo x Probabilidade x Impacto
- Risco = Probabilidade x Impacto

- Preferencialmente, devem ser utilizados valores quantitativos (1, 2, 3, 4, 5) em vez de qualitativos (alto, médio, baixo)

- A ISO27005 refere:

“Qualitative risk analysis may be used:  
- As an initial screening activity to identify risks that require more detailed analysis  
- Where this kind of analysis is appropriate for decisions  
- Where the numerical data or resources are inadequate for a quantitative risk analysis”

caso não haja dados suficientes para quantificação

# A Avaliação e gestão dos riscos

- Avaliação quantitativa, recorrendo a valores monetários

- SLE – Single Loss Expectancy
- ALE – Annualized Loss Expectancy
- ARO – Annualized Rate of Occurrence
- AV – Asset value
- EF – Exposure Factor: % Loss that is expected to occur.

$$\overbrace{\text{ALE} = (\text{AV} \cdot \text{EF}) \cdot \text{ARO}}^{\text{SLE}}$$

Asset Value (AV)	2000000	Replacement / Recovery / Reporting /
Exposure Factor (EF)	75.00%	Percentage of asset loss caused by identified threat (Single Event)
Single Loss Expectancy (SLE)	1500000	AV x EF
Annualized Rate of Occurance (ARO)	0.02	Estimated frequency a threat will occur (or fraction thereof)..
Annualized Loss Expectancy (ALE)	30000	SLE x ARO

# A Avaliação e gestão dos riscos

- Avaliação quantitativa
  - Através da aplicação deste método, os fatores do risco (probabilidade e severidade) são classificados através da atribuição de um valor (numérico ou verbal) que está integrado numa escala de valores relativos.
  - Cada valor da escala é associado a uma descrição explicativa.
    - Mas atenção à subjetividade

1	Raramente	Pouco credível que alguma vez aconteça
2	Improvável	Pode ocorrer ocasionalmente
3	Possivelmente	É possível que aconteça, mas não é esperado
4	Provavelmente	Provavelmente irá acontecer
5	Quase certo	Acontecerá com alguma frequência

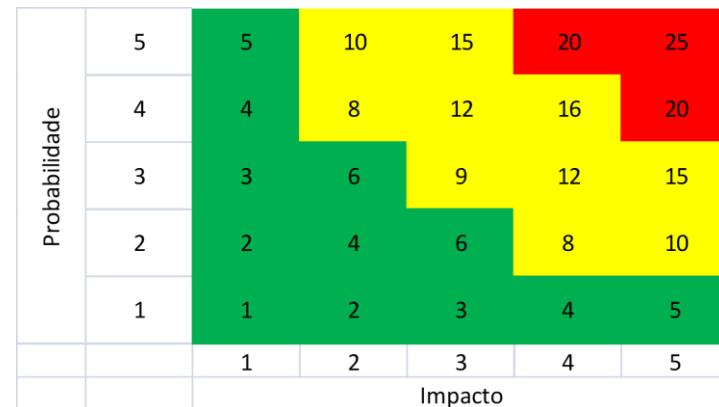
# A Avaliação e gestão dos riscos

- Avaliação quantitativa
- Considerados níveis de avaliação de 1 a 5
- Neste caso o Risco é de 45, considerando:
  - o valor de 5 para o activo
  - 3 para a probabilidade da ameaça se concretizar
  - e 3 para o impacto da vulnerabilidade

Risk	Valor
Dados de Clientes	5
Roubo de informação interno	3
Dados em claro na Base de dados (apesar de controlo de acessos)	3
<b>Total</b>	<b>45</b>

# A Avaliação e gestão dos riscos

- Exemplo de cálculo de risco



Probabilidade		
Níveis	Probabilidade	Ocorrências por ano
Nível 1	Improvável	0 a 1 vez
Nível 2	Pouco provável	1 a 2 vezes
Nível 3	Provável	2 a 3 vezes
Nível 4	Bastante provável	3 a 4 vezes
Nível 5	Muito Provável	Mais de 4
Impacto		
Níveis	Impacto	Descrição do nível de impacto
Nível 1	Muito Baixo	Um posto de trabalho parado
Nível 2	Baixo	Um sistema/processo parado
Nível 3	Médio	Um departamento parado
Nível 4	Alto	Mais que um departamento parado
Nível 5	Muito alto	A organização pára completamente

	Actual				Mitigação			
	Actual				Mitigação			
	Actual				Mitigação			
Risco = função(Ameaça,vulnerabilidade, consequência)	Controlos Existentes	Probabilidade	Impacto	Valor Risco = P * I	Novo Controlo	Probabilidade2	Impacto2	Novo Risco = P2 * I2
Acesso de colaboradores a documentos classificados, por privilégios mal configurados	-	3	5	15	implementar serviços de directório, com controlo de acessos por perfil	1	5	5

# A Avaliação e gestão dos riscos

- Formas de estimar a probabilidade
  - Através de dados e input interno
  - Recorrendo a dados externos

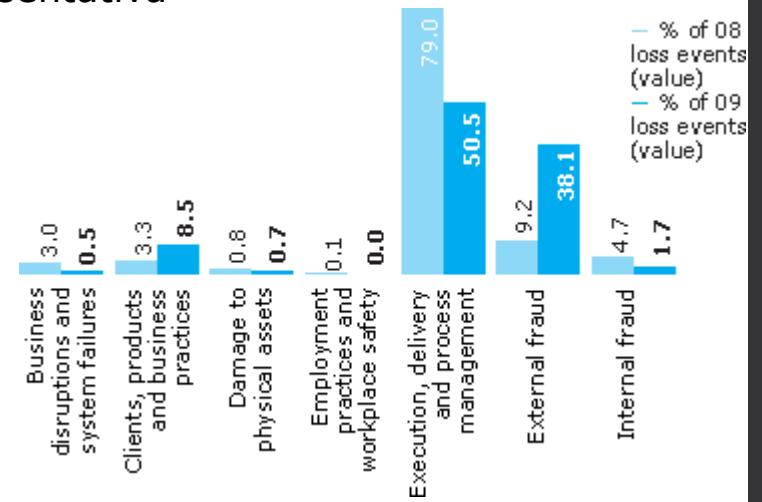
# A Avaliação e gestão dos riscos

- Estimar a probabilidade através de dados e inputs internos
  - Utilizar histórico dos incidentes para determinar os riscos actuais
    - Carece de mecanismos de recolha e análise de dados
      - IDS, CSIRT (Computer Security Incident Response Team), Security Event Correlation and Analysis...
      - Pressupõe que os dados recolhidos são representativos
      - Pressupõe padrão semelhante de comportamento no futuro
    - Recorrer ao conhecimento e experiência dos colaboradores e especialistas internos em segurança
    - Através de metodologias estruturadas de recolha de dados:
      - Com questionários;
      - E discussões de grupo.

# A Avaliação e gestão dos riscos

- Estimar a probabilidade através de dados externos

- Dados partilhados por outras organizações
  - Pressupõe uma exposição ao risco semelhante
  - Implica analisar e escolher com cuidado uma amostra representativa
- Recorrer a dados partilhados por
  - Information Security Forum (ISF)
  - Operational Riskdata eXchange Association
  - ...
  - Ou relatórios de entidades privadas  
como [barclaysannualreport.com](http://barclaysannualreport.com)



# A Avaliação e gestão dos riscos

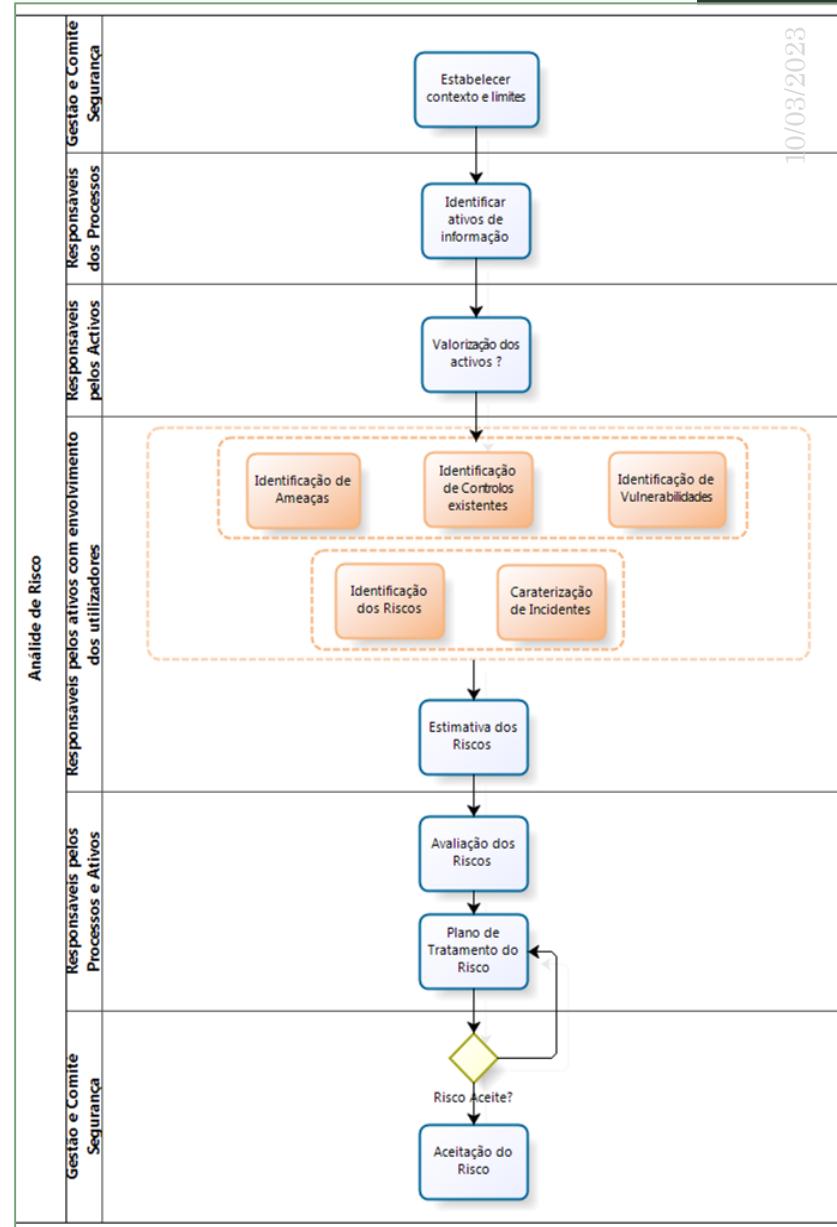
- Avaliar o Risco

- Analisando a gravidade do risco
- O nível de aceitação do risco pode ser estabelecido pela intersecção da escala da probabilidade e severidade.
- No exemplo o nível de aceitação do risco é 25.
- Riscos estimados com valores superiores a 68 são considerados intoleráveis, devendo ser evitados.

RISK ASSESSMENT SCORING MATRIX										
LIKELIHOOD	1	2	3	4	5	6	7	8	9	10
Certain	10	20	30	40	50	60	70	80	90	100
Almost certain	9	18	27	36	45	54	63	72	81	90
Very likely	8	16	24	32	40	48	56	64	72	80
Probable	7	14	21	28	35	42	49	56	63	70
Likely	6	12	18	24	30	36	42	48	54	60
Likely	5	10	15	20	25	30	35	40	45	50
May happen	4	8	12	16	20	24	28	32	36	40
Improbable	3	6	9	12	15	18	21	24	27	30
Unlikely	2	4	6	8	10	12	14	16	18	20
Very unlikely	1	2	3	4	5	6	7	8	9	10
SEVERITY										
KEY	Insignificant injury	Minor injury	Minor injury	Illness - Injury	Illness - Injury	Major Injury	Major Injury	Single fatality	Fatality	Multiple Fatalities
Not Significant	0 to 3									
Very Low	4 to 12									
Low	13 to 25									
Moderate	26 to 42									
High	43 to 67									
Very High	68 to 100									

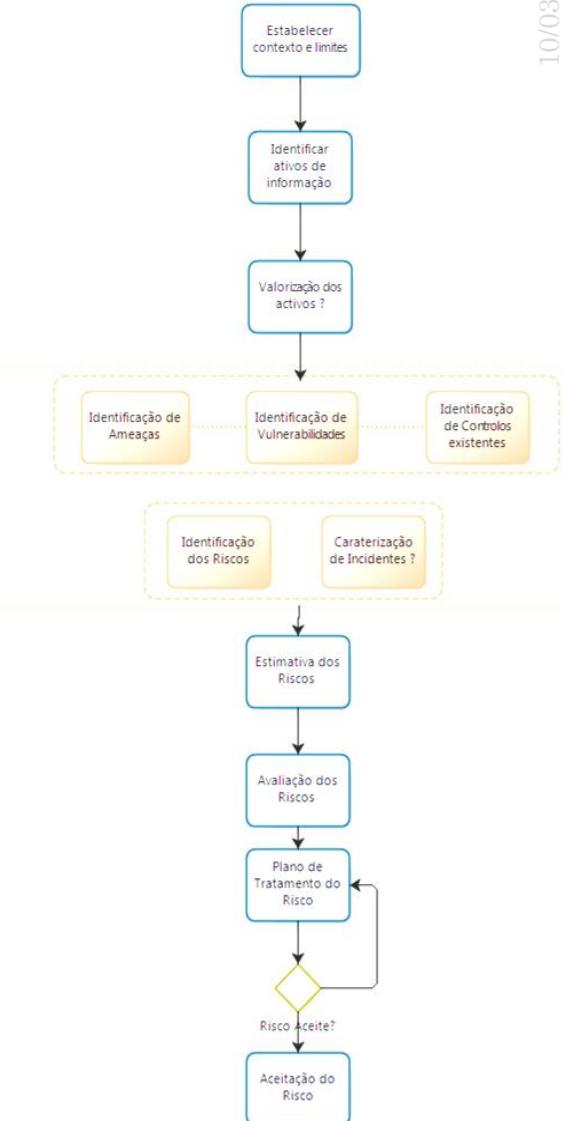
# Análise e Avaliação de Risco

- Detalhe do processo de Análise e Avaliação de Risco
  - Baseado na ISO27005



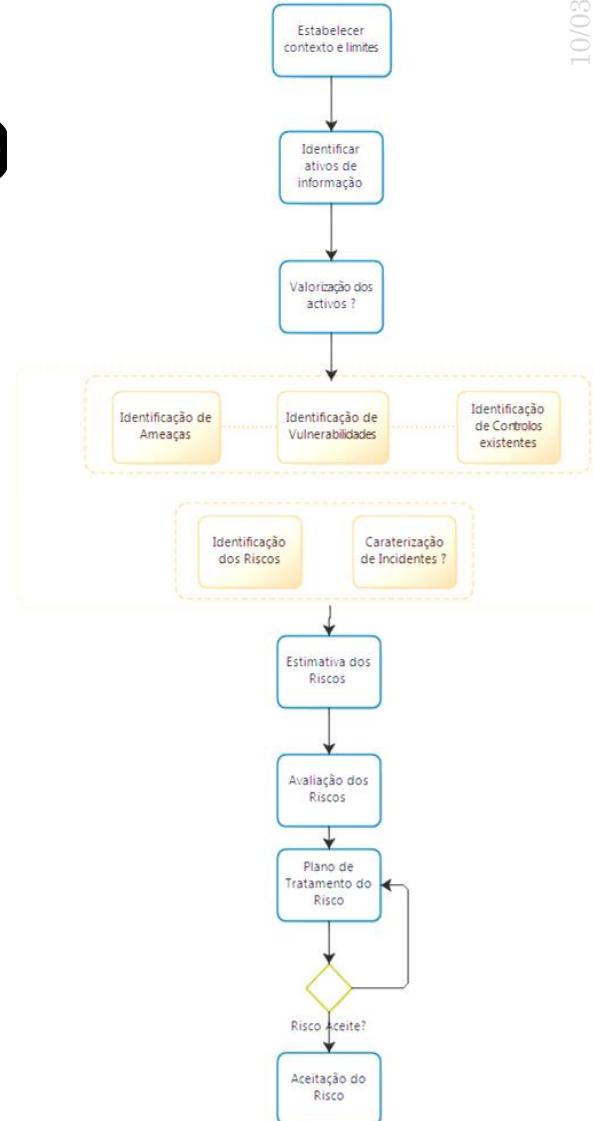
# Análise e Avaliação de Risco

- Estabelecer o contexto e limites
  - Caracterizar as atividades e processos de negócio que se encontram dentro do âmbito do SGSI, bem como identificar os pontos de contato com outras atividades e processos com os quais interagem.
  
- Definir os princípios orientadores para a análise e avaliação dos riscos:
  - Forma e níveis de avaliação a serem utilizados;
    - Formula de estimativa de riscos
    - Níveis e descrição dos critérios de avaliação da fórmula
  - Valor mínimo dos ativos a abranger na análise de risco;
  - Valor do Risco aceitável, acima do qual requer o tratamento do risco.



# Análise e Avaliação de Risco

- Identificação dos Ativos de Informação
  - Identificar todos os ativos relevantes, com informação
    - Nome
    - Descrição
    - Tipo de Ativo
    - Responsável
    - Localização
    - Dependências (de outros ativos)
  - Agrupar por tipos de ativos:
    - Instalações
    - Equipamentos e Dispositivos Informáticos
    - Outros Equipamentos
    - Software de Base (S.O.: SGBD, ERP, ..)
    - Software Aplicacional
    - Informação lógica
    - Informação Física
    - Colaboradores Internos
    - Colaboradores Externos
    - Serviços externos de suporte
    - Ativos organizacionais



# Análise e Avaliação de Risco

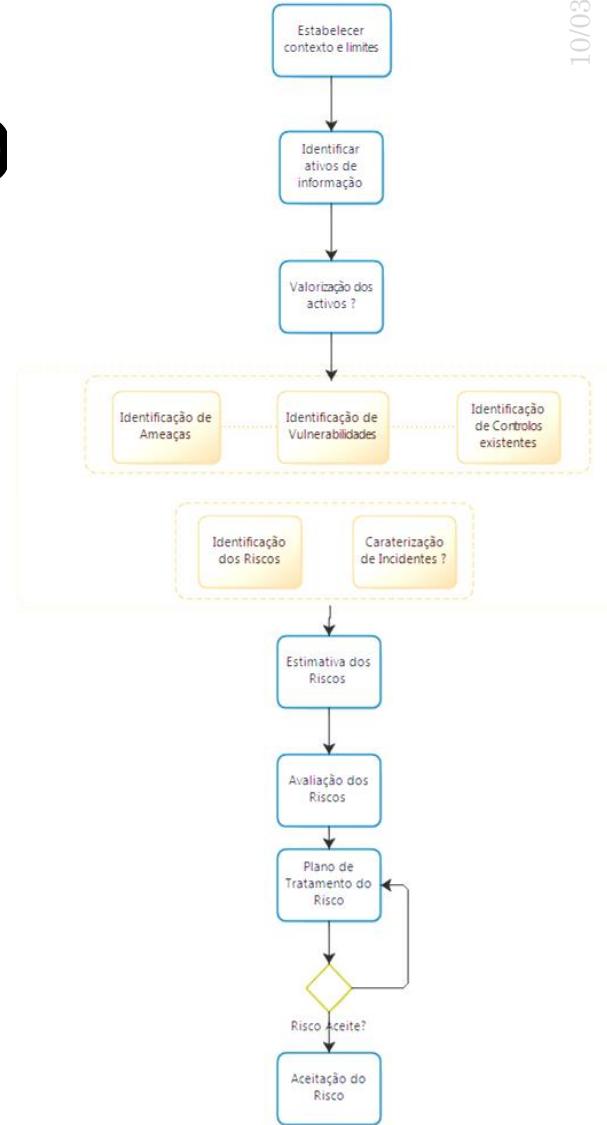
- Valorização dos Ativos

- Atribuição de um nível de valor (numa escala de 1 a 4) para cada ativo, em função da sua importância comercial ou operacional

- Triagem dos ativos que carecem de análise de risco, em função do seu valor

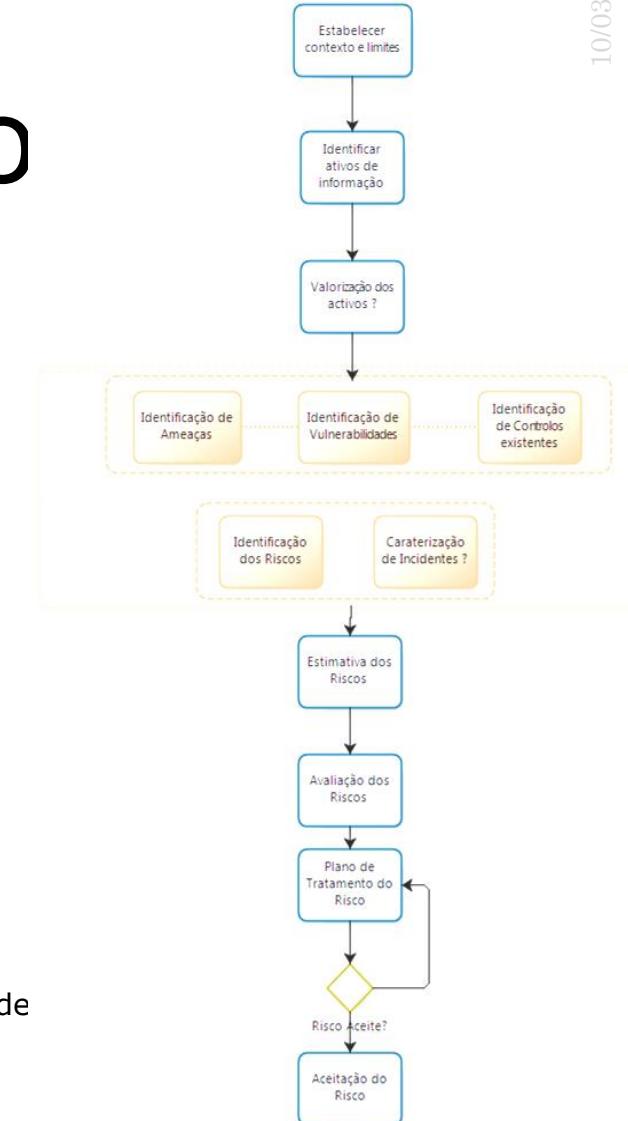
- p.e. só analisar ativos de valor Médio, Alto ou Muito Alto

Valor	Descrição
4	<b>Muito Alto.</b> O processo não se executará conforme o estipulado, comprometendo acordos comerciais
3	<b>Alto.</b> O processo não se executará conforme o estipulado,
2	<b>Médio.</b> O processo será executado, mas existirão impactos negativos na operação
1	<b>Baixo.</b> O processo executará normalmente, podendo existir pequenos impactos na operação



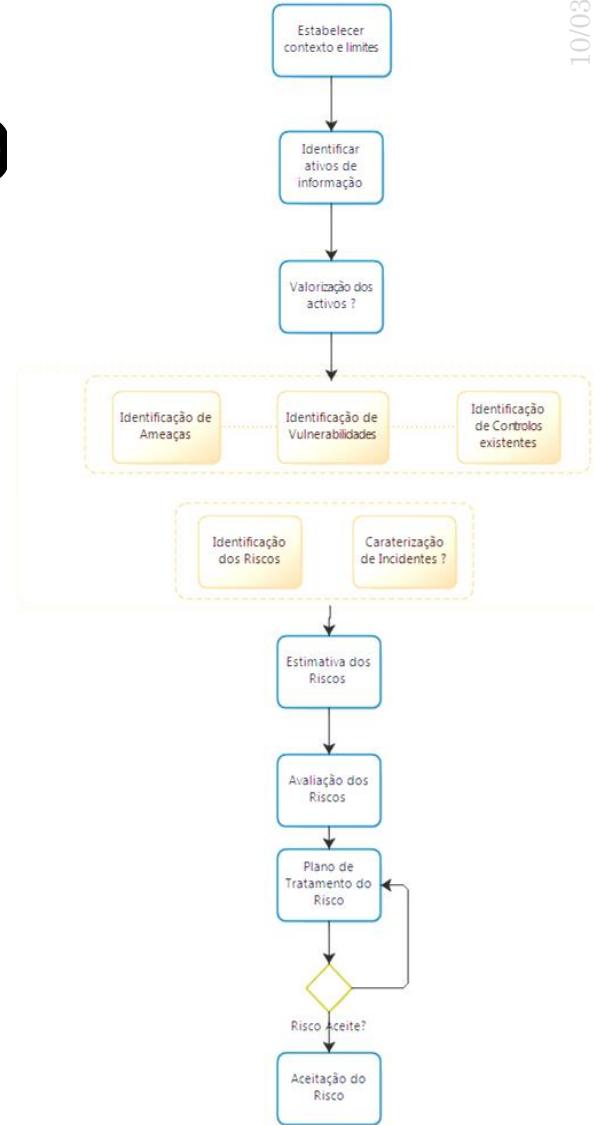
# Análise e Avaliação de Risco

- Identificação de Ameaças
  - Por tipo de Ativo
- Identificação de Vulnerabilidades
  - Por Tipo de Ativo
- Identificação de Controlos existentes
  - Por tipo de ativo
  - Verificar listagem de controlos da norma ISO27001
- Identificação de Riscos
  - O risco como a consequência de uma ameaça explorar uma vulnerabilidade
  - Depois de identificadas as ameaças e riscos devem ser encontrados os pares Ameaça+Vulnerabilidade que façam sentido
  - Estes Ameaça+Vulnerabilidade devem estar associados a vários tipos de ativos
- Caraterização de Incidentes
  - Quando a possibilidade de concretização de uma ameaça+vulnerabilidade resulta num conjunto de riscos



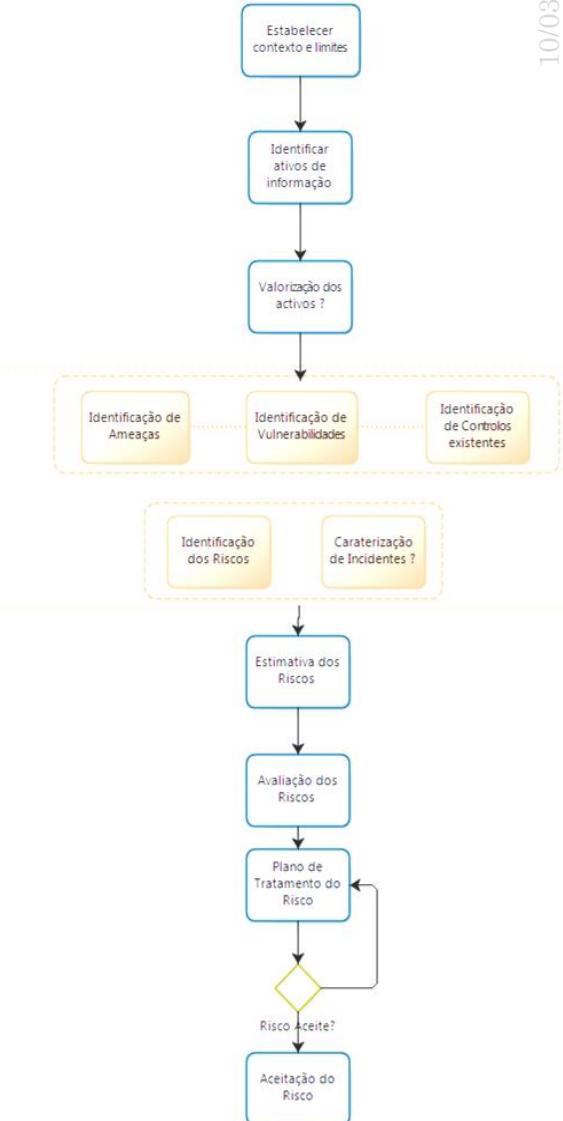
# Análise e Avaliação de Risco

- Estimativa dos Riscos
- Estimar a probabilidade de um risco se concretizar
- Risco Operacional
  - Estimar o impacto operacional de um risco se concretizar
  - Impacto operacional – indisponibilidade do(s) serviço(s)
  - Calcular o valor do Risco (O) = Probabilidade \* Impacto Operacional
- Risco Financeiro
  - Estimar Impacto financeiro em valor monetário
  - Impacto financeiro = perdas financeiras decorrentes de ocorrências e de reposição da atividade normal
- Calcular o valor do Risco (F) = Probabilidade \* Impacto Financeiro
- Escolher o maior nível de risco



# Análise e Avaliação de Risco

- Avaliação dos Riscos
  - Identificar os riscos que se encontram dentro dos limites aceitáveis e os que carecem tratamento
  
- Plano de Tratamento do Risco
  - Identificar as formas de tratamento dos riscos
  - Caracterizar os controlos a implementar, por forma a reduzir os riscos a valores aceitáveis, reavaliando os riscos
  
- Aceitação do Risco
  - Aceitação pela gestão dos riscos e do plano de tratamento traçado



# AGENDA

- Introdução à Segurança da Informação - ISO 27001
  - Introdução à Gestão de Continuidade de Negócio
  - A avaliação e gestão de riscos
- **Tratamento dos Riscos**

# Tratamento dos Riscos

- Opcões de Tratamento de Risco (ISO27005/Segurança da Informação)
  - Assumir o Risco
    - Aceitar o Risco continuando com o sistema em operação
    - Podendo/devendo ir implementando controlos tendentes à redução do risco
  - Evitar o Risco
    - Eliminando a causa do risco ou as consequências (desactivar certas funcionalidades ou, mesmo, desligar o sistema)
  - Transferênciа de Risco
    - Utilizando opções que permitam compensação em caso de perdas (p.e. seguros)
  - Aplicação de Controlos ou Mitigação dos Riscos
    - Controlos de segurança apropriados às ameaças e vulnerabilidades encontradas no sentido de reduzir o risco final

# Tratamento dos Riscos

- Opções de Tratamento de Risco (ISO 31000)
  - “As opções para o tratamento do risco poderão envolver uma ou mais das seguintes opções:
    - evitar o risco ao decidir não iniciar ou continuar com a atividade que origina o risco;
    - aceitar ou aumentar o risco de modo a explorar uma oportunidade;
    - remover a fonte do risco;
    - alterar a verosimilhança;
    - alterar as consequências;
    - partilhar o risco (p.e. através de contratos, aquisição de seguros);
    - reter o risco mediante decisão informada

# Tratamento dos Riscos

- Opções de Tratamento dos Riscos (NIST)

- Assumir o Risco

- Aceitar o Risco continuando com o sistema em operação
    - Podendo/devendo ir implementando controlos tendentes à redução do risco

- Evitar o Risco

- Eliminando a causa do risco ou as consequências (desativar certas funcionalidades ou, mesmo, desligar o sistema)

- Transferência de Risco

- Utilizando opções que permitam compensação em caso de perdas (p.e. seguros)

- Planeamento de Risco

- Gerir o risco, desenvolvendo um plano de mitigação que prioriza, implementa e mantem os controlos

- Limitar o Risco

- Implementar os controlos capazes de minimizar o impacto de certas ameaças sobre alguma vulnerabilidade
    - Necessário implementar medidas de detecção, prevenção e suporte
    - (se for verificado um determinado incidente, desligar sistema, ou repor sistema...)

- Reconhecimento e Desenvolvimento de controlos

- De forma a baixar o risco, à medida que as vulnerabilidades são reconhecidas, é implementado um plano de desenvolvimento e implementação de controlos que permitam corrigir ou minimizar a vulnerabilidade

# Tratamento dos Riscos

## - técnico e/ou administrativo

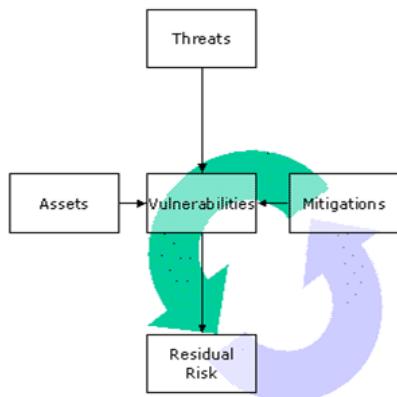
- Mitigação técnica ou administrativa ?
- Assumir o Risco
- Evitar o Risco
- Transferência de Risco
- Planeamento de Risco
- Limitar o Risco
- Reconhecimento e Desenvolvimento de controlos

**Predominantemente técnicos**

# Tratamento dos Riscos

## • Risk Mitigation Checklist (extraído do NIST)

- Each proposed risk mitigation option should be examined from the following perspectives:
  - Effectiveness.



- Will it reduce or eliminate the identified risks? To what extent do alternatives mitigate the risks? Effectiveness can be viewed as being somewhere along a continuum, as follows:
  - Level One (Engineering actions): The safety action eliminates the risk, for example, by providing interlocks to prevent thrust reverser activation in flight;
  - Level Two (Control actions): The safety action accepts the risk but adjusts the system to mitigate the risk by reducing it to a manageable level, for example, by imposing more restrictive operating conditions; and
  - Level Three (Personnel actions): The safety action taken accepts that the hazard can neither be eliminated (Level One) nor controlled (Level Two), so personnel must be taught how to cope with it, for example, by adding a warning, a revised checklist and extra training.

# Tratamento dos Riscos

- **Cost/benefit.**

- Do the perceived benefits of the option outweigh the costs? Will the potential gains be proportional to the impact of the change required?

- **Practicality.**

- Is it doable and appropriate in terms of available technology, financial feasibility, administrative feasibility, governing legislation and regulations, political will, etc.?

- **Challenge.**

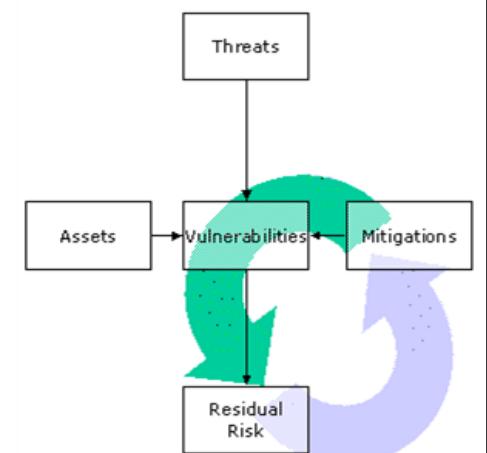
- Can the risk mitigation measure withstand critical scrutiny from all stakeholders (employees, managers, stockholders/State administrations, etc.)?

- **Acceptability to each stakeholder.**

- How much buy-in (or resistance) from stakeholders can be expected? (Discussions with stakeholders during the risk assessment phase may indicate their preferred risk mitigation option.)

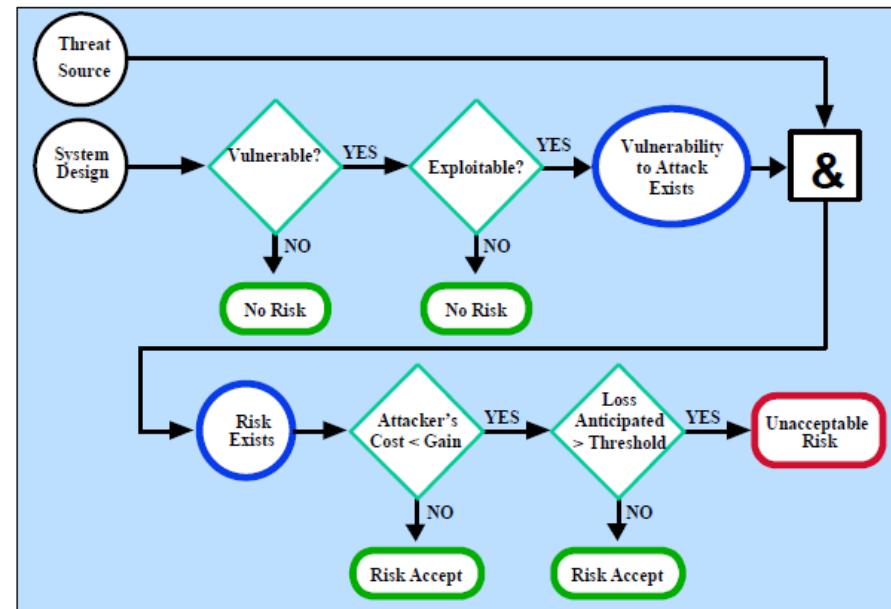
# Tratamento dos Riscos

- **Enforceability.**
  - If new rules (SOPs, regulations, etc.) are implemented, are they enforceable?
- **Durability.**
  - Will the measure withstand the test of time? Will it be of temporary benefit or will it have long-term utility?
- **Residual risks.**
  - After the risk mitigation measure is implemented, what will be the residual risks relative to the original hazard? What is the ability to mitigate any residual risks?
- **New problems.**
  - What new problems or new (perhaps worse) risks will be introduced by the proposed change?



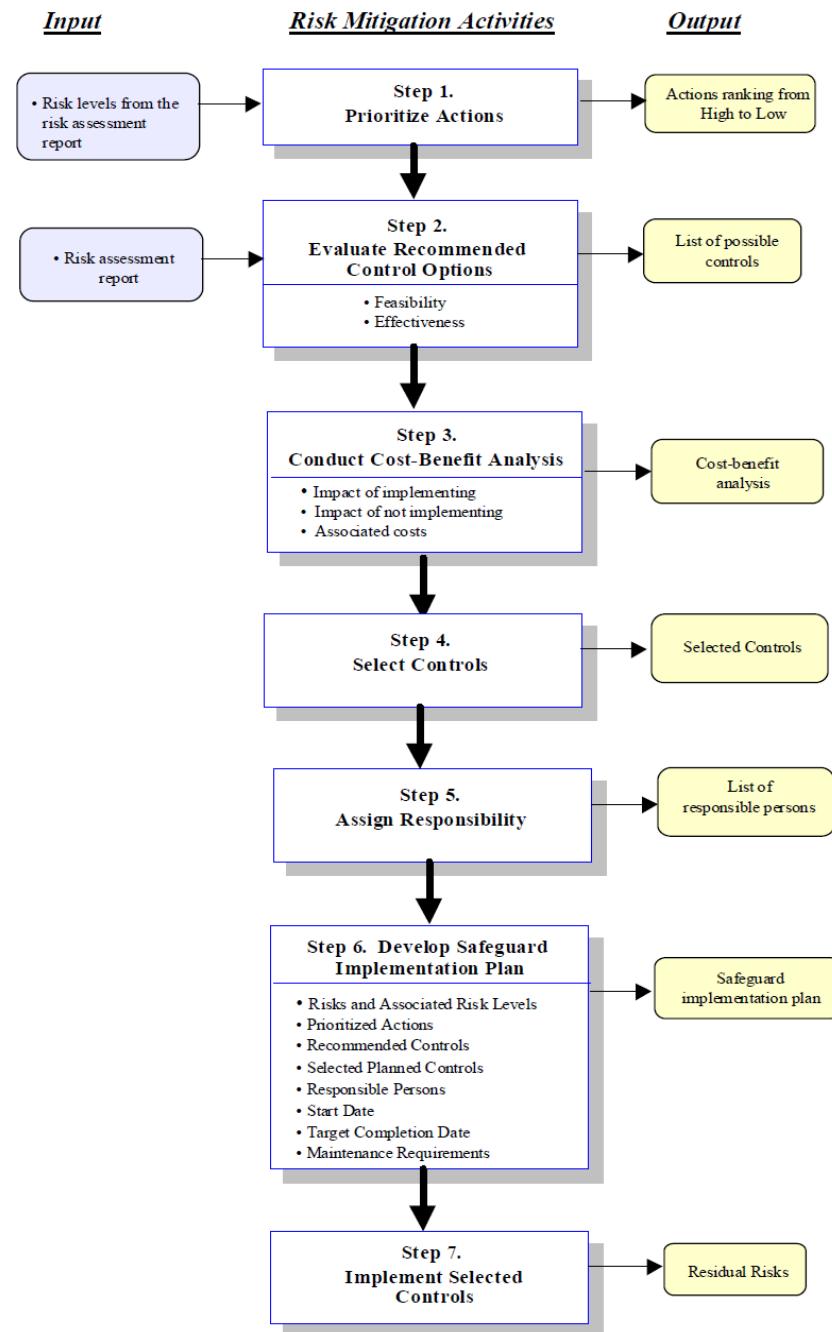
# Tratamento dos Riscos

- Fluxo de aceitação de riscos
- Ou não aceitação e implementação de controlos



# Tratamento dos Riscos

- 7 passos para a implementação de controlos
  - Step 1- Prioritize Actions
    - Output -Actions ranking from High to Low
  - Step 2- Evaluate Recommended Control Options
    - Output from - List of feasible controls
  - Step 3 - Conduct Cost-Benefit Analysis
    - Output - Cost-benefit analysis describing the cost and benefits of implementing or not implementing the controls
  - Step 4 - Select Control
    - Output from - Selected control(s)
  - Step 5 - Assign Responsibility
    - Output - List of responsible persons
  - Step 6 - Develop a Safeguard Implementation Plan
    - Output - Safeguard implementation plan
  - Step 7 - Implement Selected Control(s)
    - Output from - Residual risk



# Segurança e Gestão de Risco

2ºSem 2023/24

**Information Security**

**and Applicable Standards**

**LUIS AMORIM**

17 Fev 2024



