

SEGURANÇA E GESTÃO DE RISCO

2ºSEM 2021/22

**SEGURANÇA DA INFORMAÇÃO
E NORMAS APLICÁVEIS**

LUIS AMORIM

19 Mar 2022



2 SÍNTESE DA SESSÃO ANTERIOR

- Segurança da Informação
- Abordagem integrada à Segurança

3 SÍNTESE


- Segurança da Informação

- Segurança da Informação, mas actualmente os Sistemas são a base da Informação
- A informação (conjunto de dados devidamente ordenados) é actualmente considerada o activo mais importante nas Organizações
- Importante identificar os activos a “segurar”
- Atenção às várias formas de Informação (Visual, Áudio, Escrita, ..., Electrónica)
- Importante o Controlo de acesso à Informação (âmbito e classificação)
- 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.
- A Segurança da informação deve ser um processo integrado, que abrange toda a organização

- Abordagem integrada à Segurança

4 EXEMPLOS

- **Biggest data breaches (since 2000)**

- 
1. Yahoo, August 2013 > 3 billion accounts
 2. Alibaba, November 2019 > 1.1 billion pieces of user data
 3. LinkedIn, June 2021 > 700 million users
 4. Sina Weibo, March 2020 > 538 million accounts
 5. Facebook, April 2019 > 533 million users
 6. Marriott International (Starwood), September 2018 > 500 million customers
 7. Yahoo, 2014 > 500 million accounts
 8. Adult Friend Finder, October 2016 > 412.2 million accounts
 9. MySpace, 2013 > 360 million user accounts
 10. NetEase, October 2015 > 235 million user accounts
 11. Court Ventures (Experian), October 2013 > 200 million personal records
 12. LinkedIn, June 2012 > 165 million users
 13. Dubsmash, December 2018 > 162 million user accounts
 14. Adobe, October 2013 > 153 million user records
 15. My Fitness Pal, February 2018 > 50 million user accounts

(fonte: <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>)

Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing

Dec. 11, 2018

WASHINGTON — The cyberattack on the Marriott hotel chain that **collected personal details of roughly 500 million** guests was part of a Chinese intelligence-gathering effort that also hacked health insurers and the security clearance files of millions more Americans, according to two people briefed on the investigation.

The **hackers**, they said, **are suspected of working on behalf of the Ministry of State Security, the country's Communist-controlled civilian spy agency**. The discovery comes as the Trump administration is planning actions targeting China's trade, cyber and economic policies, perhaps within days.

Those moves include indictments against Chinese hackers working for the intelligence services and the military, according to four government officials who spoke on the condition of anonymity. The Trump administration also plans to declassify intelligence reports to reveal Chinese efforts dating **to at least 2014 to build a database containing names of executives** and American government officials with security clearances.

5 EXEMPLOS

- Ameaça: Terrorismo

Planos de ataques da Al Qaeda escondidos em pornografia

Entre eles estavam sequestros de navios de cruzeiros e atentados na Europa semelhantes aos de Bombaim, em 2008

Por: tv24 | 1-5-2012 0:37

Gosto

48
pessoas
gostam
disto.

Like

48

Send

[Casino](#)
[da](#)
[Sorte](#)
[Português](#)
[Jogue](#)
[sem](#)
[necessidade](#)
[de](#)
[depósito](#)
[Ou](#)



A polícia alemã descobriu planos de ataques da Al Qaeda escondidos num vídeo pornográfico que um jovem austríaco tinha escondido na roupa interior.

Entre os alvos encontravam-se navios de cruzeiro e estavam previstos ataques na Europa ao estilo dos que ocorreram na cidade indiana de Bombaim, em Novembro de 2008, em que uma dezena de operacionais armados espalhou o terror durante três dias, matando 164 pessoas.

Esta descoberta só agora revelada foi feita já no ano passado. De acordo com a CNN, tudo começou quando as autoridades germânicas detiveram em Berlim Maqsood Lodin, um austríaco de 22 anos, que estivera recentemente no Paquistão e entrara na Alemanha por terra, depois de ter regressado à Europa através da Hungria.

6 EXEMPLOS

- Ameaça: Roubo de documentos

Expresso

Roubados documentos dos submarinos

Vários documentos foram "cirurgicamente" roubados de um carro ontem em Lisboa.

10:01 | Quarta feira, 3

O contrato entre o Estado e a empresa alemã Ferrostaal sobre as contrapartidas pela venda a Portugal de dois submarinos foi ontem roubado, segundo revela hoje o "Correio da Manhã".

Os documentos foram roubados do carro quando Christoph Mollenbeck, representante da Ferrostaal, jantava com um amigo em Lisboa, perto da Cinemateca.

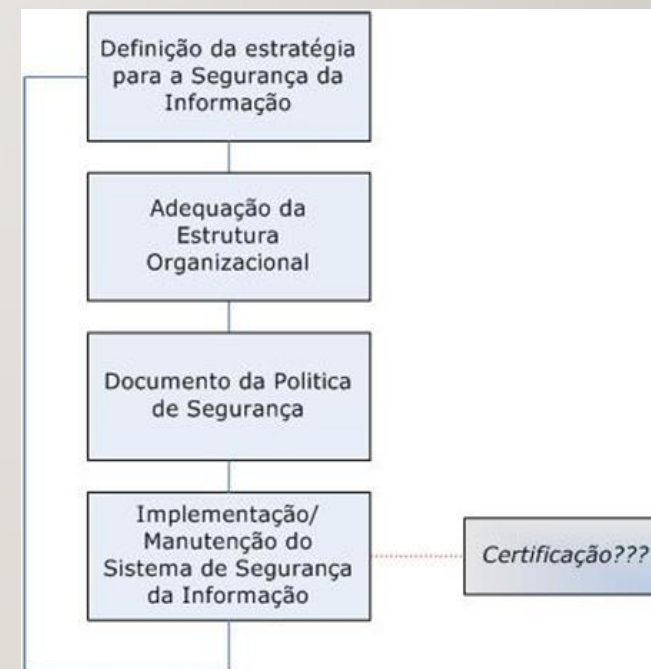
Segundo o mesmo diário, o Audi A6 foi "cirurgicamente assaltado" e não tinha quaisquer "sinais de arrombamento". Só quando Mollenbeck e o amigo e compatriota Kai Jusec chegaram a casa é que deram pela falta da pasta e do portátil.

Às autoridades, Christoph Mollenbeck disse que as contrapartidas foram ontem renegociadas entre a empresa e o Estado. Do carro também desapareceu o memorando de entendimento entre a Ferrostaal e o Laboratório de Tecnologias de Informação.

O caso está a ser investigado pelo DIAP de Lisboa, liderado por Maria José Morgado.

7 SÍNTESE

- Segurança da Informação
- Abordagem integrada à Segurança
 - A Segurança de um Sistema de Informação só se consegue atingir considerando de forma integrada
 - Normas e Procedimentos
 - Sistemas e Aplicações
 - Infra-estrutura lógica e física
 - Importante estabelecer um Roadmap de forma a estabelecer a Política de Segurança



8 AGENDA

➤ Normas e legislação aplicável

- Introdução à ISO 27001
- Introdução à Gestão de Risco

9 NORMAS E LEGISLAÇÃO APLICÁVEL

- O recurso a normas e boas práticas permite
 - Utilização de Metodologias testadas e comprovadas
 - Incorporação de conhecimento real (modelos/regras) a nível de uma comunidade alargada
 - Possibilidade de aferição e comparação
- O conhecimento e adoção de requisitos legais permite
 - Cumprimento da lei, assegurando a legalidade

10 NORMAS E LEGISLAÇÃO APLICÁVEL

- (alguns) Standards relacionados com a segurança
 - ISO/IEC 27001:2013 (BS7799-2) - Information Security Management Systems - Requirements
 - ISO/IEC 27002 – ex ISO/IEC 17799- Code of practice for Information Security Management
 - ISO/IEC 27003:2010 - Information security management system implementation guidance
 - ISO/IEC 27004:2009 - Information security management - Measurement
 - ISO/IEC 27005:2008 (BS7799-3) - Information security risk management
 - ISO/IEC 27006:2007 - Requirements for bodies providing audit and certification of information security management systems
 - ISO/IEC TR 27015:2012 — Information technology — Security techniques — Information security management guidelines for financial services
 - ISO/IEC 27033-2:2012 Security techniques -- Network security -- Part 2: Guidelines for the design and implementation of network security
 - ISO/IEC 27035:2016 Information technology -- Security techniques -- Information security incident management
- ISO/IEC 15408:2005 - Security techniques — Evaluation criteria for Itsecurity (Common Criteria)
- ISO 24760 - A Framework for Identity Management -This has not yet been published.
- ISO 22301:2019 (BS25999) – Business Continuity Management System - requirements

II NORMAS E LEGISLAÇÃO APLICÁVEL

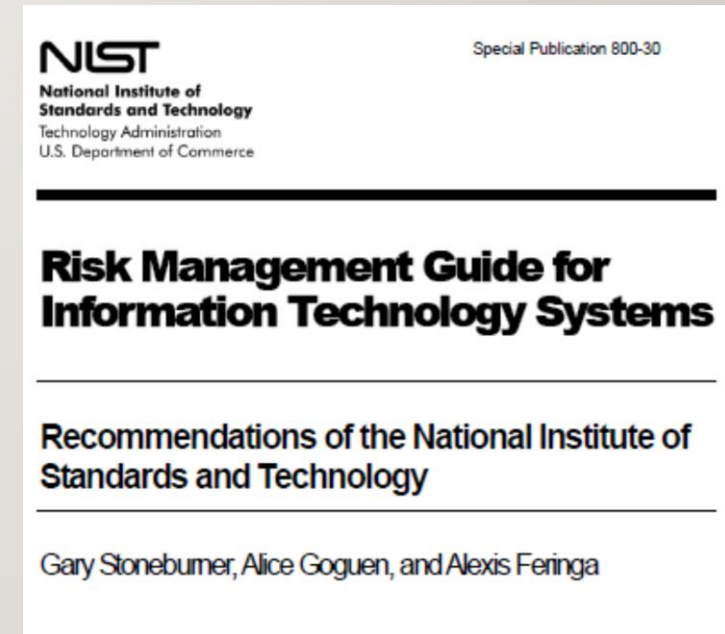
- ISO/IEC 15408 - Security techniques-Evaluation criteria for ITsecurity
 - ISO/IEC 15408-1 - Part 1: Introduction and general model
 - defines two forms for expressing IT security functional and assurance requirements:
 - the protection profile (PP) construct allows creation of generalized reusable sets of these security requirements. The PP can be used by prospective consumers for specification and identification of products with IT security features which will meet their needs.
 - the security target (ST) expresses the security requirements and specifies the security functions for a particular product or system to be evaluated, called the target of evaluation (TOE). The ST is used by evaluators as the basis for evaluations conducted in accordance with ISO/IEC 15408
 - Part 2: Security functional requirements
 - defines the required structure and content of security functional components for the purpose of security evaluation. It includes a catalogue of functional components that will meet the common security functionality requirements of many IT products and systems.
 - Part 3: Security assurance requirements
 - defines the assurance requirements of ISO/IEC 15408. It includes the evaluation assurance levels (EALs) that define a scale for measuring assurance, the individual assurance components from which the assurance levels are composed, and the criteria for evaluation of protection profiles and security targets

I2 NORMAS E LEGISLAÇÃO APLICÁVEL

- ISO/IEC 18028 - Security techniques - IT network security
 - Part 1: Network security management
 - Part 2: Network security architecture
 - Part 3: Securing communications between networks using security gateways
 - Part 4: Securing remote access
 - Part 5: Securing communications across networks using Virtual Private Networks

I3 NORMAS E LEGISLAÇÃO APLICÁVEL

- NIST Special Publication 800-30
- (abordagens diferentes)
 - Os controlos a implementar podem ser agrupados em
 - Tecnológicos
 - Não tecnológicos: Gestão, Operacionais e Organizacionais



14 NORMAS E LEGISLAÇÃO APLICÁVEL

- Outras normas e legislação com implicação na segurança
 - IT Governance
 - ITIL (ISO/IEC 20000) – procedimentos de operação, no que respeita à segurança
 - COBIT, na implementação de controlos
 - Legislação
 - SEGNACs – GNS – Manuseamento de matéria classificada
 - Lei nº 109/ 2009 - Lei do cibercrime
 - Lei nº 58/2019 – Lei da Proteção de Dados Pessoais
 - Lei nº 46/2018 – Lei que estabelece o regime jurídico da segurança do ciberespaço
 - Decreto-Lei nº 65/2021- regulamentação de aspetos relacionados com os requisitos de segurança e regras de notificação de incidentes
 - Regras específicas de determinados sectores
 - Sarbanes-Oxley Act - visa garantir a criação de mecanismos de auditoria e segurança
 - Basileia II - acordo internacional que determina as regras de gestão de risco para os bancos
 - PCI DSS - Payment Card Industry Data Security Standard
 - HIPAA - Health Insurance Portability and Accountability Act

I5 NORMAS E LEGISLAÇÃO APLICÁVEL

- Mas também normas ligadas à qualidade e processos da organização
 - ISO 9001 - Quality management systems - Requirements
 - ISO 14001 Environmental management systems - Requirements with guidance for use
 - OHSAS 1800 > ISO 45001 - Occupational health and safety management systems — Requirements with guidance for use
- “NOTE: If an organization already has an operative business process management system (e.g. in relation with ISO 9001 or ISO 14001), it is preferable in most cases to satisfy the requirements of this International Standard within this existing management system.” [ISO 27001]

16 NORMAS E LEGISLAÇÃO APLICÁVEL

- Mas também outras normas ligadas às tecnologias
 - ISO/IEC 21559-1 - Telecommunications and information exchange between systems
 - ISO/IEC 25000:2005 - Software product
 - Quality Requirements and Evaluation (SQuaRE)



17 NORMAS E LEGISLAÇÃO APLICÁVEL LIGAÇÃO DA QUALIDADE À SEGURANÇA

- Conseguiremos ter Qualidade sem nos preocuparmos com a Segurança de um Sistema de Informação?
- Conseguiremos atingir os níveis de Segurança adequados, sem ter Qualidade, ao nível do produto e do processo de desenvolvimento e manutenção?
- Tanto a Qualidade como a Segurança devem estar presentes ao longo de todo o ciclo de vida de um Sistema de Informação



18 NORMAS E LEGISLAÇÃO APLICÁVEL

- Os requisitos a considerar podem ser
 - Normativos
 - Legais
 - Contratuais



19 AGENDA

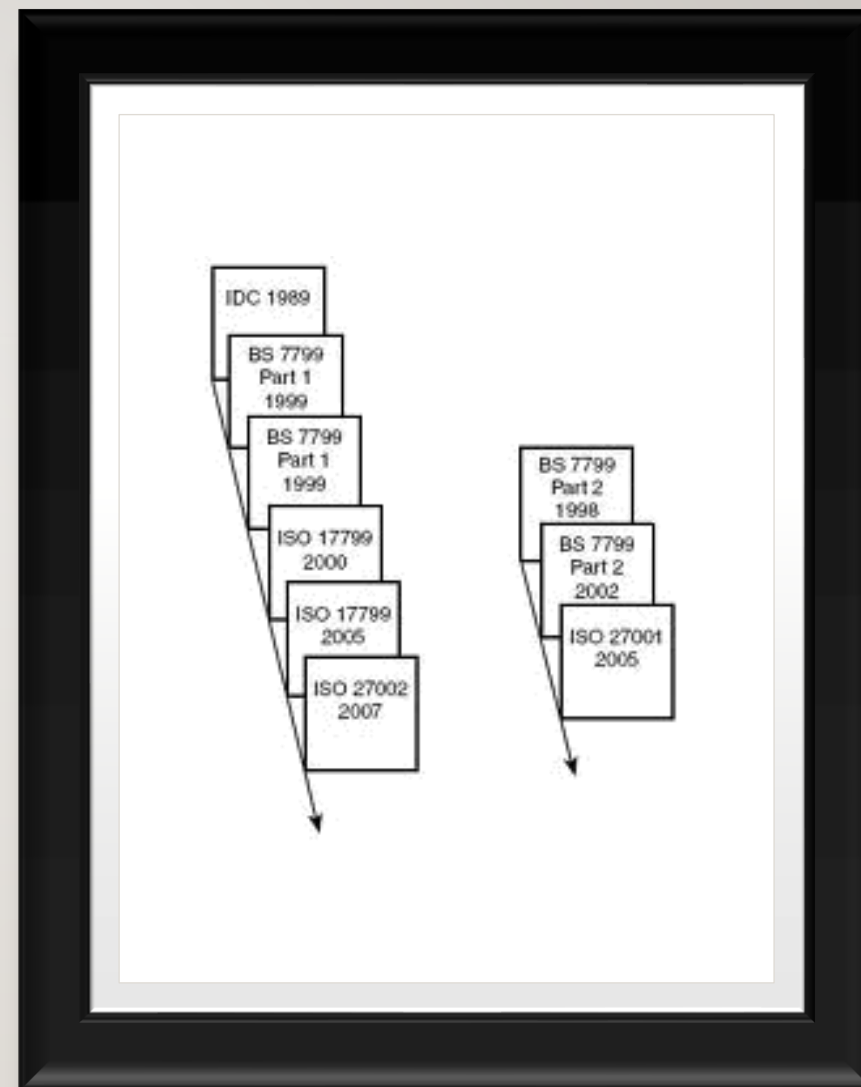
- Normas e legislação aplicável
- **Introdução à ISO 27001**
- Introdução à Gestão de Risco

20 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.”

21 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

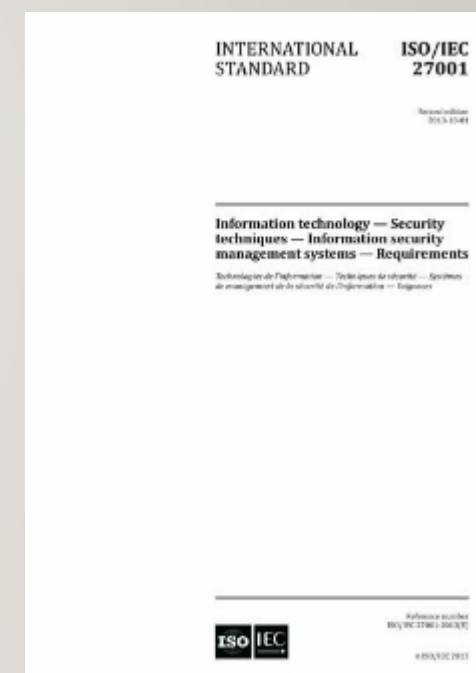


22 INTRODUÇÃO À ISO 27001

- 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

23 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



24 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 compreensivo de controlos de segurança (114)
 - As melhores práticas de segurança atuais
 - Possui 14 secções de controlo
 - Não pode ser utilizado para análise(auditoria) e/ou certificação



25 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

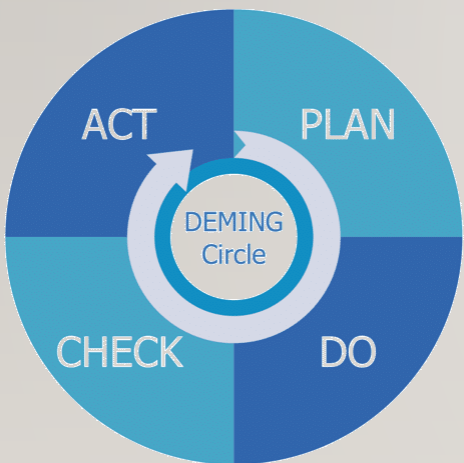
- **Cláusulas 4 a 10**
 - Contexto da organização
 - Liderança
 - Planeamento
 - Suporte
 - Operação
 - Avaliação de desempenho
 - Melhoria

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]

26 INTRODUÇÃO À ISO 27001



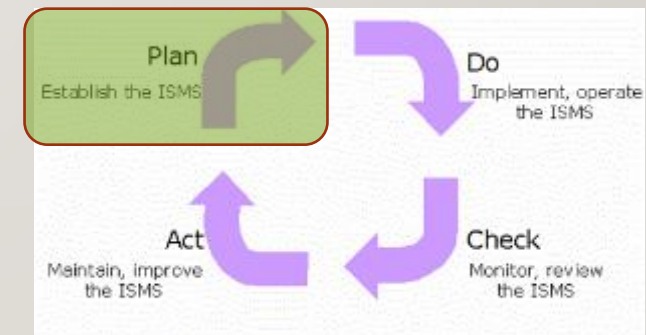
- Modelo PDCA aplicado ao ISMS
 - Plan (establish the ISMS)
 - Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
 - Do (implement and operate 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.

27 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



28 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.

29 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

30 INTRODUÇÃO À ISO 27001

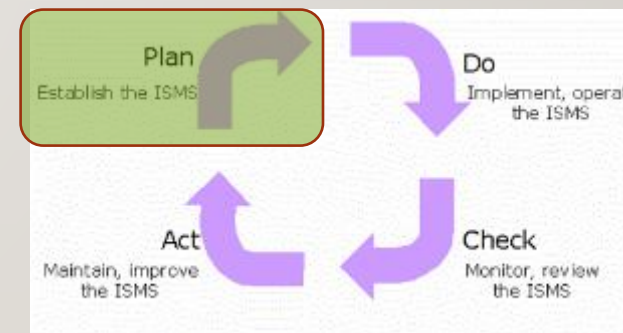
- Sistema de Gestão
 - 4 Contexto da organização
 - 4.3 - Determinar o âmbito do sistema de gestão de segurança da informação
 - A organização deve determinar os limites e aplicabilidade do SGSI, de forma documentada e disponível
 - Ao determinar este âmbito, a organização deve considerar:
 - a) questões 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.

3 | 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

32 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



33 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

34 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:

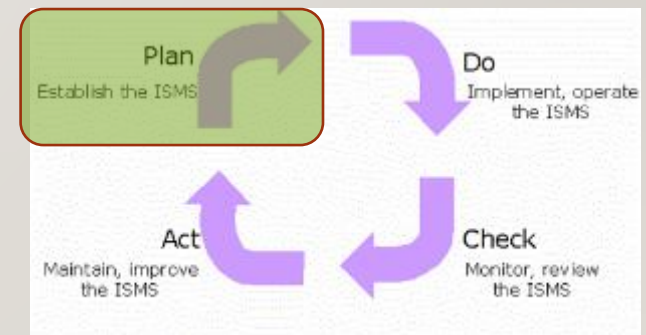
- a) seja apropriada ao propósito da organização
 - b) inclua os objetivos de segurança da informação (ver 6.2) ou proporcione um modelo de referência para definir objetivos de segurança da informação
 - c) inclua um comprometimento para satisfazer os requisitos aplicáveis relacionados com a segurança 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

35 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

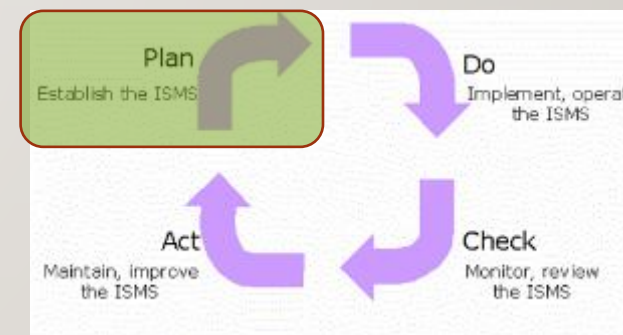
36 INTRODUÇÃO À ISO 27001

- 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



37 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

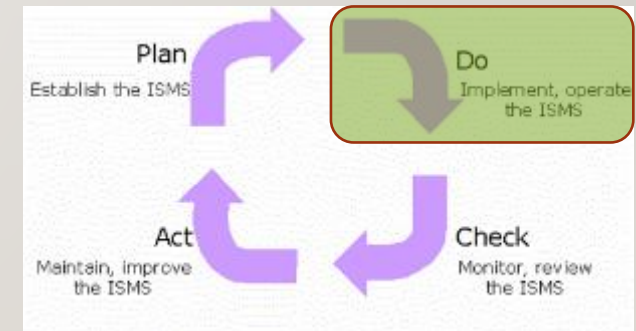


38 INTRODUÇÃO À ISO 27001

- Sistema de Gestão

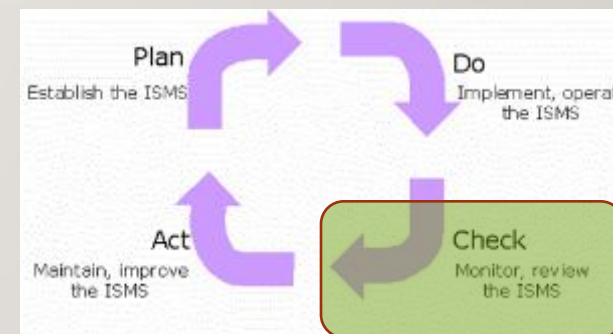
- 8 Operação

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



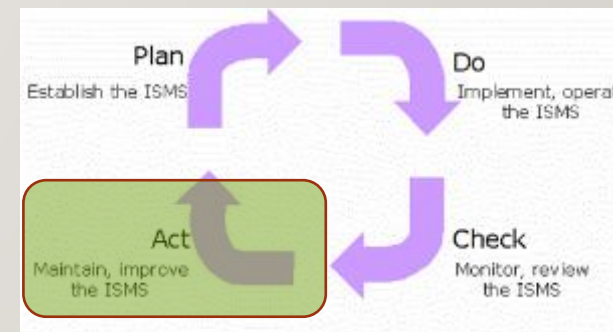
39 INTRODUÇÃO À ISO 27001

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



40 INTRODUÇÃO À ISO 27001

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



4 | 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

42 INTRODUÇÃO À ISO 27001

- 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 Aspectos de segurança da informação relativos à gestão da continuidade do negócio
 - A.18 Conformidade

43 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

44 INTRODUÇÃO À ISO 27001

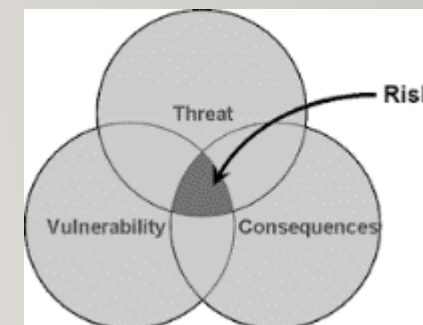
- Annex A – Controlos (ISO 27002)
 - A.8 Gestão de activos
 - A.8.1 Responsabilidade pelos activos
 - A.8.1.1 Inventário de activos
 - Implementation guidance
 - An organization should identify assets relevant in the lifecycle of information and document their importance. The lifecycle of information 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.

45 AGENDA

- Normas e legislação aplicável
- Introdução à ISO 27001
- **Introdução à Gestão de Risco**

46 INTRODUÇÃO À GESTÃO DO RISCO

- Riscos – Risk
 - Risco é a probabilidade de algo mau vir a acontecer e causar danos a um activo de informação
- Outros conceitos relacionados com o Risco, segundo a ISO 27001
 - Risk Analysis
 - “systematic use of information to identify sources and to estimate the risk”
 - Risk Evaluation
 - “process of comparing the estimated risk against given risk criteria to determine the significance of the risk”
 - Risk Assessment
 - “overall process of risk analysis and risk evaluation”
 - Risk Treatment
 - “process of selection and implementation of measures to modify risk”
 - Risk Management
 - “coordinated activities to direct and control an organization with regard to risk”



47 INTRODUÇÃO À GESTÃO DO RISCO

- O risco é avaliado de acordo com parâmetros, cujo peso pode variar de acordo com o método utilizado:
 - Ameaça
 - Vulnerabilidade
 - Probabilidade
 - Valor do asset
 - Impacto
 - Controlos existentes
 - ...

48 INTRODUÇÃO À GESTÃO DO RISCO

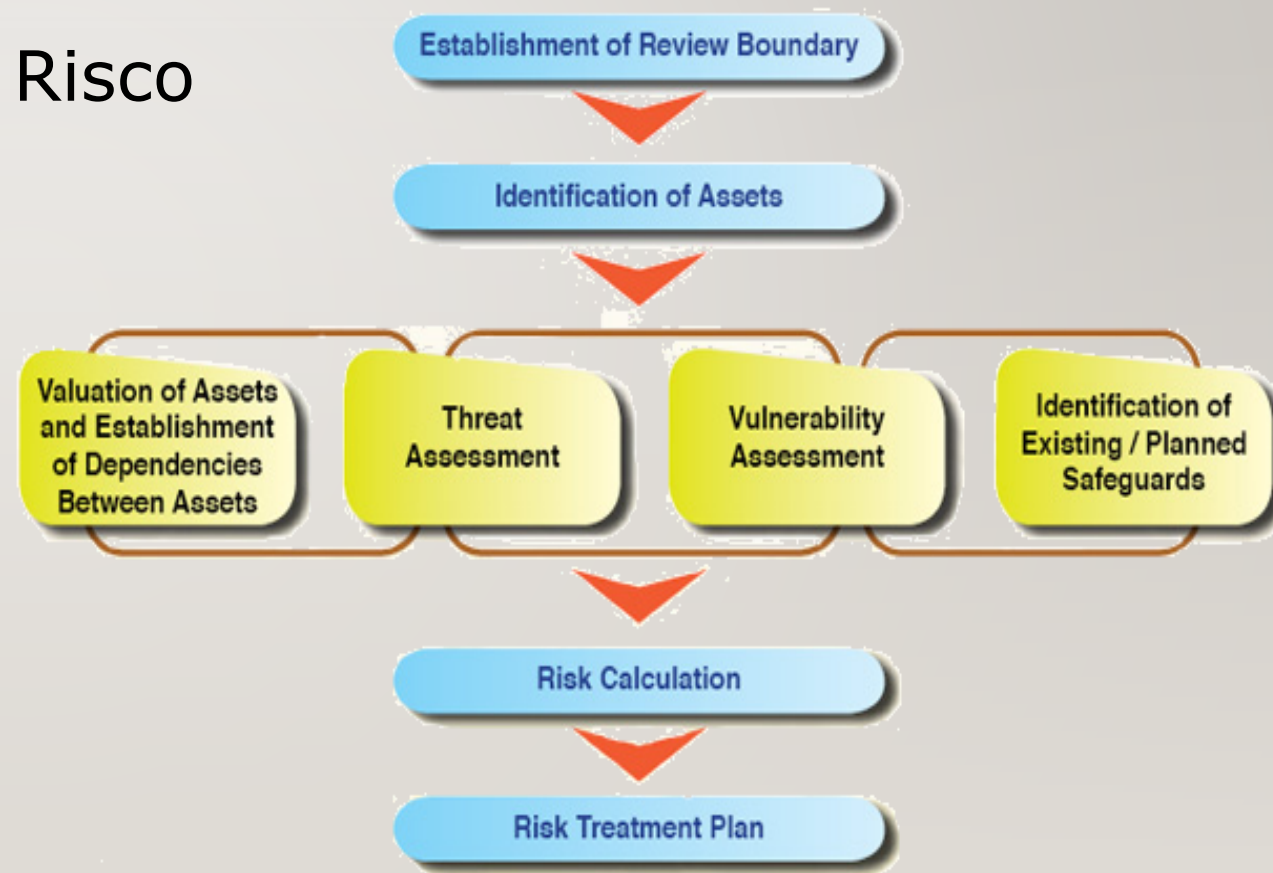
- Ameaças [ISO 27005]
 - Terrorismo
 - Espionagem industrial
 - Uso não autorizado de equipamento
 - Fogo
 - Inundações
 - Terramotos
 - Falha de energia
 - Falha de comunicações
 - Falha de hardware ou software
 - Acesso não autorizado
 - Roubo de informação
 - Corrupção de dados
 - Bugs de software
 - Social engeneering
 - Ataques de vírus
 - Hacking
 - ...
- Vulnerabilidades [ISO 27005]
 - Inexistência de sistemas de detecção e extinção de incêndios
 - Inexistência de sistemas de detecção de Inundações
 - Inexistência de um programa BCM
 - Inexistência de redundância de power e comunicações
 - Testes de software fracos
 - Inexistência de sistemas de proteção contra intrusões (ex. FW, IPS, etc.)
 - Inexistência de sistemas de controlo de acessos físicos (barreiras, seguranças, vídeo, ID cards, etc.)
 - Inexistência de sistemas de controlo de acessos lógicos (login/passwd, id manag, tokens, etc.)
 - ...

49 INTRODUÇÃO À GESTÃO DO RISCO

- 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:
 - $\text{Risk} = \text{Asset value} \times \text{Likelihood}$
 - $\text{Risk} = \text{Asset value} \times \text{Likelihood} \times \text{Impact} \times \text{Threat} \times \text{Vulnerability}$
 - $\text{Risk} = \text{Asset Value} \times \text{Threat} \times \text{Vulnerability} \times \text{Likelihood}$
 - $\text{Risk} = \text{Asset value} \times \text{Group (Threat/Vulnerability/Legal)} \times \text{Likelihood}$
 - Preferencialmente, devem ser utilizados valores quantitativos precisos (1, 2, 3, 4, 5) em vez de qualitativos vagos (alto, médio, baixo)

50 INTRODUÇÃO À GESTÃO DO RISCO

- Processo de Avaliação de Risco



51 INTRODUÇÃO À GESTÃO DO RISCO

- Avaliação do Nível de Risco

RISK ASSESSMENT SCORING MATRIX											
LIKELIHOOD											
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	
	Insignificant injury	Minor injury	Minor injury	Illness - Injury	Illness - Injury	Major Injury	Major Injury	Single fatality	Fatality	Multiple Fatalities	
KEY										SEVERITY	
Not Significant	0 to 3	May be ignored, No further action Required									
Very Low	4 to 12										
Low	13 to 25	Ensure safe working									
Moderate	26 to 42	Refer to Risk Assessment, Safe Working Procedures									
High	43 to 67	Monitor Control Measures									
Very High	68 to 100	Avoid if Possible, Full Method Statement if Not									

52 INTRODUÇÃO À GESTÃO DO RISCO

- Tratamento do risco
 - Após cada avaliação dos Riscos, estes devem ser tratados de acordo com o seu valor e as prioridades para o negócio:
 - Aceitar os riscos (ex. abaixo de um determinado valor);
 - Evitar os riscos (ex. fechar um serviço ou substituí-lo – deve ser feita nova avaliação);
 - Transferir os riscos (seguradoras).
 - Mitigar os riscos
 - Implementar os respectivos controlos (alguns identificados no Annex A da ISO27001);
 - Pode requerer nova avaliação tendo em conta os novos controlos

SEGURANÇA E GESTÃO DE RISCO

2ºSEM 2021/22

**SEGURANÇA DA INFORMAÇÃO
E NORMAS APLICÁVEIS**

LUIS AMORIM

19 Mar 2022

