UNINOVE
Universidade Nove de Julho

PPGI

Disciplina
Segurança da Informação

Aula 02 – Normas para Segurança da Informação

Professor: João Rafael
Email: joao.rafael@uni9.pro.br

São Paulo
2025

As Primeiras Normas Para Segurança da Informação

Normas Para a Segurança da Informação

- Existem instituições **nacionais e internacionais**, reconhecidas como **idôneas** no desenvolvimento de padrões, sendo responsáveis pela **edição**, **publicação** e **revisão** de normas técnicas que deverão ser seguidas por diversas áreas.

- Dentre as organizações, destacam-se:
  - **ISO** (*International Standardization Organization*).
  - **IEC** (*International Electrotechnical Commission*).
  - **ABNT** (Associação Brasileira de Normas Técnicas).

Normas de Segurança da Informação
Cenário Nacional

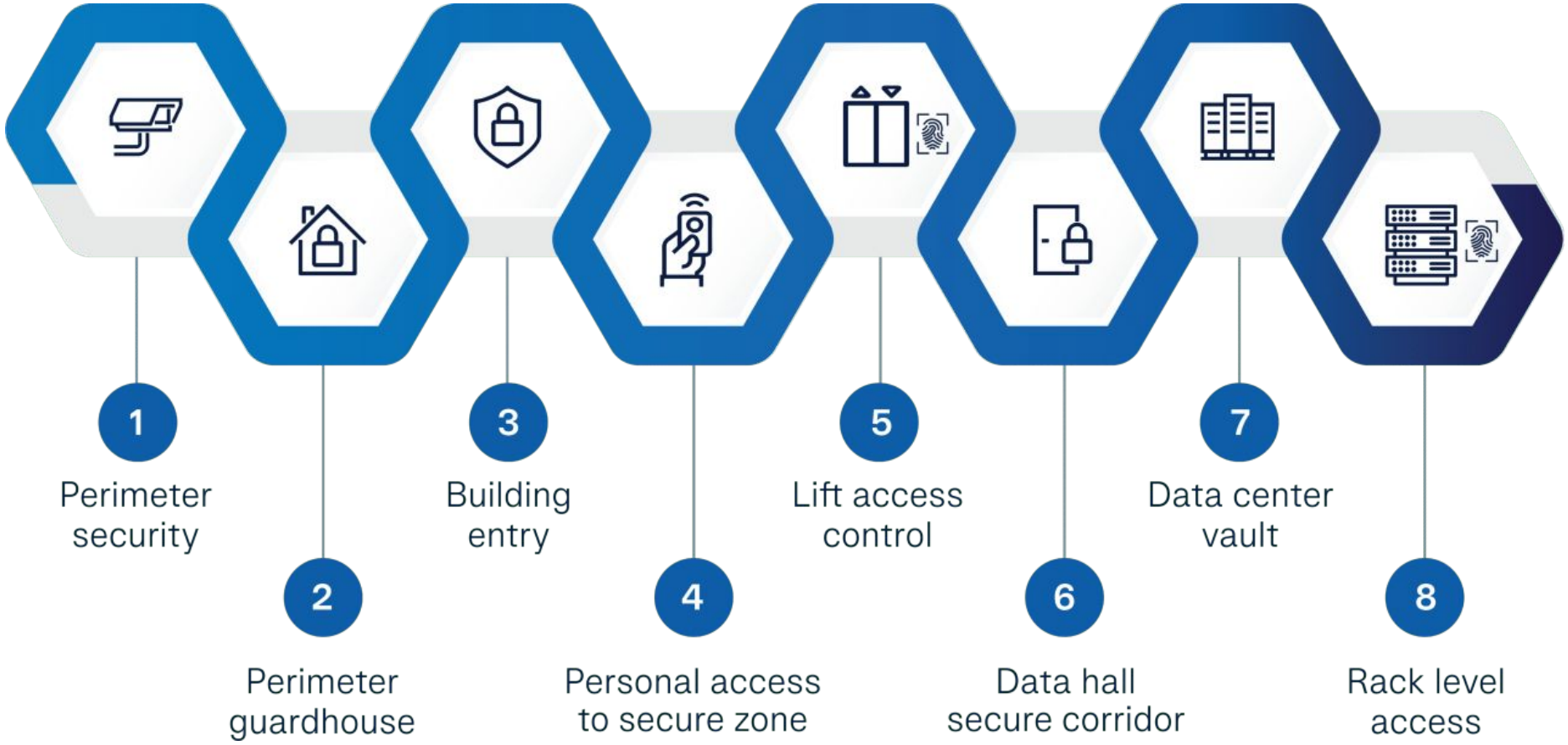
Normas Para a Segurança da Informação – Acesso Físico

- Antes dos computadores estarem conectados em redes, a segurança das informações eram estritamente relacionadas ao **acesso físico**. As primeiras orientações (normas) definidas para a segurança física na área da computação no cenário nacional foi desenvolvida pelas normas técnicas **NBRs**.

Normas Para a Segurança da Informação – Acesso Físico

- NBR 10842, de 11/1989 – Equipamentos para tecnologia da informação e requisitos de segurança.
- NBR 1333, de 12/1990 □ NBR 11514 (2007) – Controle de acesso físico a CPDs.
- NBR 1334, de 12/1990 □ Atualizada em (2003) – Segurança física para armazenamento de dados.
- NBR 1335, de 07/1991 □ NBR 11584 (2007) – Segurança física de microcomputadores e terminais.

Exemplos de Segurança Física



Normas de Segurança da Informação
Cenário Internacional

Normas de Segurança da Informação – Cenário Internacional

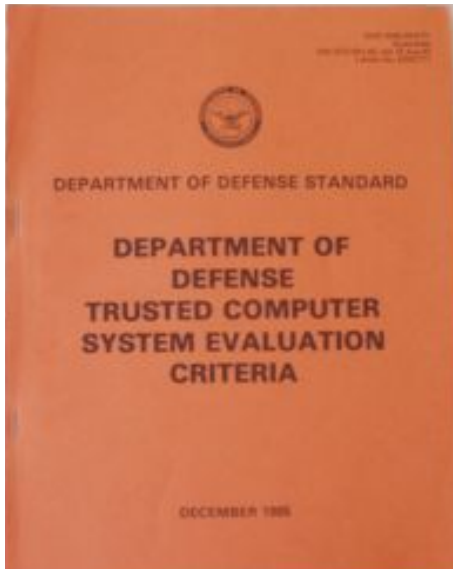
- ***"Security Control for Computer System"*** - Departamento de Defesa (*DoD*): Desenvolveu a primeira documentação conhecida com o objetivo de ***resolver itens de segurança em computadores***. Neste documento continham as seguintes informações:

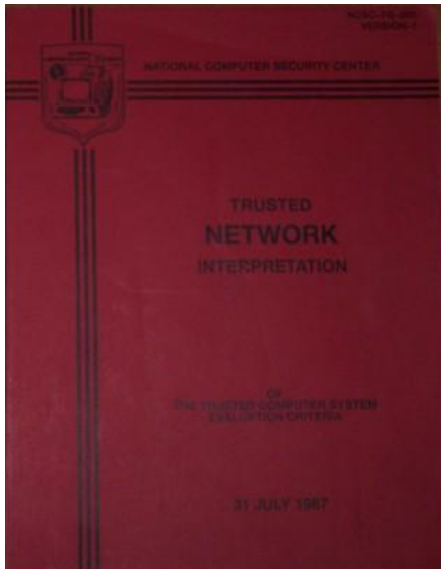
  - Conjunto de regras que deveria ser utilizado nos processos internos;
  - Classificação dos sistemas operacionais em: **Seguro** ou **Não-Seguro**;

The Orange Book & The Red Book

- Com o passar do tempo, o documento produzido pelo **Departamento de Defesa** passou a incorporar **outras regras**, capazes de avaliar e classificar o nível de segurança em **hardwares e softwares.**

- Esse conjunto de regras ficou conhecido informalmente como "***The Orange Book***". Em seguida, desenvolveu-se um novo documento englobando **itens de segurança em redes de computadores**. Este documento foi denominado: ***"The Red Book"***.





Reino Unido - British Standard 7799

- Em 1989, o Departamento de Comércio e Indústria do Reino Unido (UK-DTI) criou o ***"Centro de Segurança de Informação (CCSC)",*** órgão responsável pelo desenvolvimento da primeira versão da documentação: ***"Código de Segurança da Informação - PD 0003".***

- Posteriormente a criação do ***"Código de Segurança da Informação"***, O CCSC produziu diversos outros documentos e códigos-fonte sobre Segurança da informação, inspirados nos documentos: ***The Orange Book*** e ***The Red Book***. A unificação de todos estes recursos em um único documento foi chamado de chamado: **BS7799 (*British Standard* 7799).**

British Standard 7799

- Devido a sua complexidade, a **BS7799** foi dividida em **duas partes**: ***BS7799-1*** e ***BS7799-2***;
  - **BS7799-1:** Documento de referência – "Boas práticas para a área da Segurança da Informação".
  - **BS7799-2:** Guia para criação de um **SGSI (Sistema de Gestão de Segurança da Informação)**.

- Entre 1995 e 1999, a **BS7799-1** já era adotada em outros países, como: África do Sul, Austrália, Suíça e Dinamarca. O problema é que a **BS7799-1** possuía muitos itens característicos do seu país de origem (Reino Unido). Para torná-la padrão e extinguir sua restrição de localidade, a **ISO** homologou a **BS7799-1** em um novo documento universal chamado de: **ISO/IEC 17799:2000.**

ISO/IEC 17799:2000

ISO/IEC 17799:2005

ISO/IEC 17999:2000

- A **ISO/IEC 17799** foi publicada pela **ISO** em 2000. Possui diversos controles e requerimentos que devem ser **atendidos** para garantir a segurança das informações. A ISO/IEC 17999:2000 foi uma das normas pioneiras em **criar mecanismos de certificação** para empresas.

- Uma organização certificada pela ***ISO/IEC 17799:2000*** "**afirma**" que trata as suas informações de **forma segura**, independentemente de como e onde eles estão armazenados.

- Em 2001, a **ABNT**, disponibilizou para consulta pública o ***Projeto 21:204.01-010***. Este projeto deu origem a norma nacional de segurança da informação: **NBR ISO/IEC 17799:2000**.

UNINOVE
Universidade Nove de Julho

Os 10 Controles Principais da NBR ISO/IEC 17999

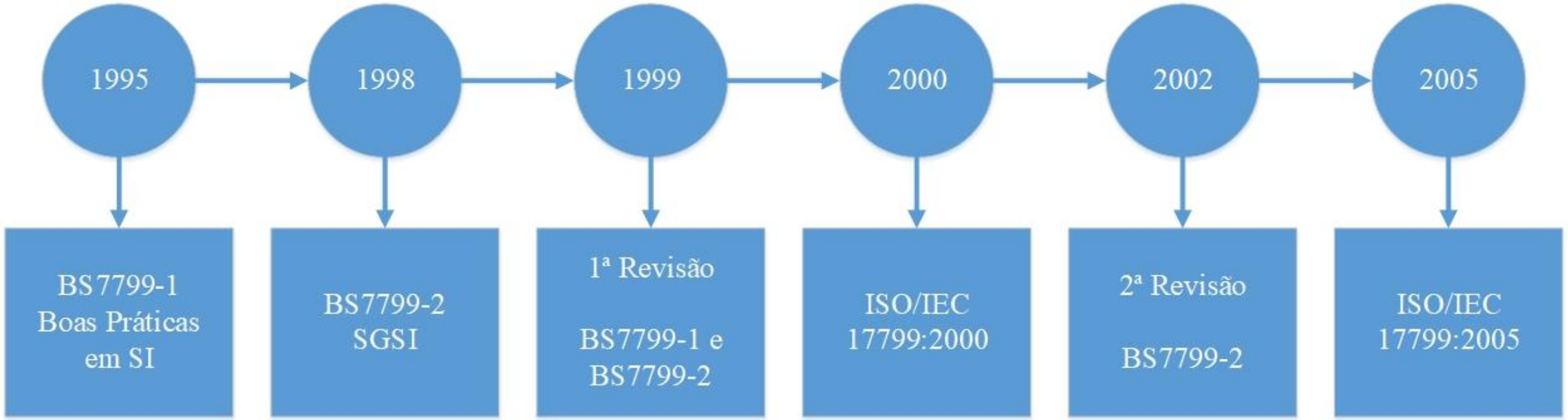
- Políticas de Segurança;
- Segurança Organizacional;
- Classificação e Controle dos Ativos da Informação;
- Segurança de Pessoas;
- Segurança Física e do Ambiente;
- Gerenciamento de Operações e Comunicações;
- Controle de Acesso;
- Desenvolvimento da Segurança de Sistemas;
- Gestão da Continuidade do Negócio;
- Conformidade.

ISO/IEC 17999:2000 e a NBR ISO/IEC 17799:2005

- Em 2001,foi publicada uma atualização da **NBR ISO/IEC-17799.** Esta atualização passou a incluir o Brasil oficialmente na lista de países que adotaram e apoiaram o uso desta norma. Após algumas atualizações, foi publicada a versão mais recente da norma: **NBR ISO/IEC 17799:2005**.

- A **NBR ISO/IEC 17799:2005** teve como principal objetivo, acompanhar o dinamismo da área de segurança da informação, estabelecendo diretrizes para iniciar, implementar, manter e melhorar o **SGSI (Sistema de Gestão da Segurança da Informação)** em uma organização.

Evolução da ISO/IEC 17799



Normas ISO/IEC
27000, 27001 e 27002

ISO/IEC 27000

- A ISO reuniu as normas existentes para Segurança da Informação: **ISO 17799**, **BS7799-1** e **BS7799-2,** e as unificou em uma única série chamada: **ISO/IEC 27000**.

- As normas ISO 27000 fornecem diretrizes para organizações de todos os tipos e tamanhos implementam e monitoram um ***Sistema de Gestão de Segurança da Informação (SGSI)***.

UNINOVE
Universidade Nove de Julho

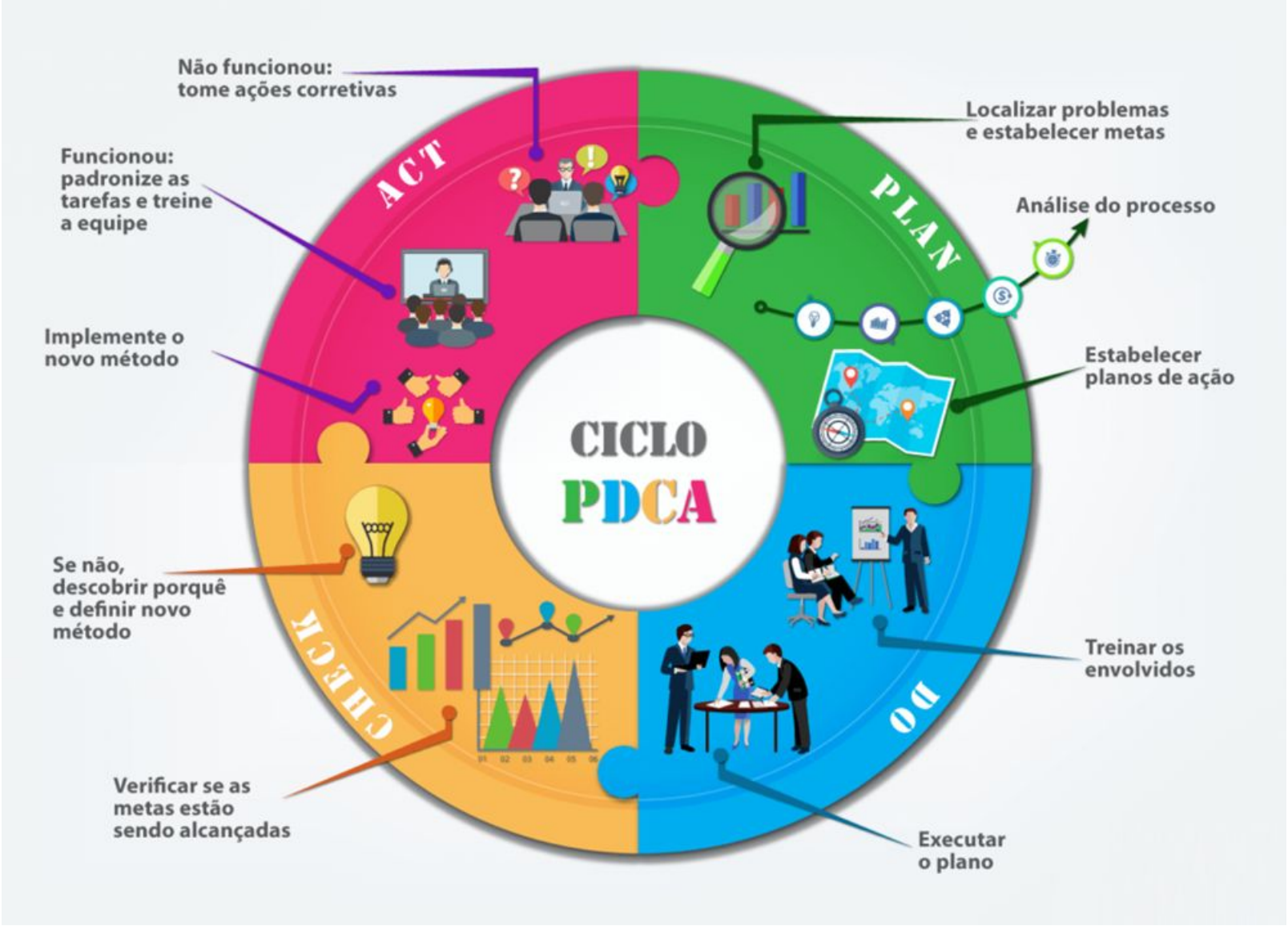
ISO/IEC 27000, ISO/IEC 27001 e ISO/IEC 27002

- **ISO/IEC 27000:** Norma responsável por estabelecer as conceituações gerais da **ISO 27000.** Nesta norma, são definidos os **glossários / vocabulários** utilizados para **SGSI**.

- **ISO/IEC 27001:** Revisão da Norma BS7799-2, contendo melhorias, como: Recomendações para tarefas de Auditoria, o uso de KPI (***Key Performance Indicators***) na avaliação de **SGSI** e a utilização do **Ciclo de Melhoria Contínua (PDCA)**.

- **ISO/IEC 27002 :** Descreve **Boas Práticas** que podem apoiar na implementação e monitoramento de diferentes controles de Segurança da Informação.

Ciclo PDCA (ISO 27001)



Demais Normas ISO/IEC da Série 27000

UNINOVE
Universidade Nove de Julho

Demais Normas ISO/IEC da Série 27000

- **ISO 27003:** Gestão de Risco;
- **ISO 27004:** Produção de relatórios para um SGSI;
- **ISO 27005:** Implantação, monitoramento e melhoria contínua em controles de SI;
- **ISO 27006:** Recuperação e continuidade de negócio das organizações (Auditoria);
- **ISO 27007:** Suporte para auditorias em SGSI;
- **ISO 27008:** Complementa a ISO 27007, mas insere controles de SI.
- **ISO 27009:** Suporte para indústrias específicas que desejam usar a série ISO 27000.
- **ISO 27010:** Guia para a comunicação em um SGSI (interno / externo);
- **ISO 27011:** Guia para SGSI para empresas de telecomunicações;
- **ISO 27012:** Guia para aplicar um SGSI em Organizações Públicas **(Cancelada)**;
- **ISO 27013:** Guia de Implementação da norma ISO 27001 com a ISO 27000;

UNINOVE
Universidade Nove de Julho

Demais Normas ISO/IEC da Série 27000

- **ISO 27014:** Técnicas para a Governança da SI;
- **ISO 27015:** Aborda a aplicação de um SGSI em empresas com serviços financeiros;
- **ISO 27016:** Semelhante a norma ISO/IEC 27015, mas focada no setor de economia;
- **ISO 27017:** Guia com controles específicos para *Cloud Computing*;
- **ISO 27018:** Aborda PII (*Personally Identifiable Information*) para *Cloud Computing*;
- **ISO 27019:** Controles específicos para a indústria de energia;
- **ISO 27031:** Guia com definições para a área da Segurança da Informação;
- **ISO 27032:** Guia com definições para a área de *Cybersecurity*;
- **ISO 27033:** (Dividida em 6 Normas): Segurança em redes, inspirada na ISO 18028;
- **ISO 27034:** (Dividida em 6 Normas): Segurança em desenvolvimento de Software;
- **ISO 27035:** Gestão de incidentes em Segurança da informação;

UNINOVE
Universidade Nove de Julho

Demais Normas ISO/IEC da Série 27000

- **ISO 27036:** Segurança da informação no relacionamento com fornecedores;
- **ISO 27037:** Gestão para o tratamento de evidências forenses digitais;
- **ISO 27038:** Especificação para a proteção de redações digitais;
- **ISO 27039:** Guia para gestão de sistemas IDS, IPS e IDPS;
- **ISO 27040:** Aspectos de SI para infraestruturas de Armazenamento de Dados;
- **ISO 27041:** Regulamentação dos métodos utilizados para investigações forense;
- **ISO 27042:** Diretrizes para análise e coleta de evidências digitais;
- **ISO 27043:** Princípios e processos para investigar incidentes de SI;
- **ISO 27044:** Diretrizes para sistemas SIEM (*Security Information and Event Management*);
- **ISO 27799:** Gestão de SI para a área da Saúde;
- **ISO 31000:** Gestão de Riscos

UNINOVE
Universidade Nove de Julho

Resumo - Normas ISO/IEC da Série 27000

Vocabulário	27000
Requisitos	27001, 27006, 27009
Orientações	27002, 27003, 27004, 27005, 27007, 27013, 27014
Diretrizes Setoriais	27010, 27011, 27015, 27017, 27018, 27019
Diretrizes de Controle Específicas	2703x, 2704x, 2779x

Outras Normas, Leis e Padrões que possuem Controles de Segurança da Informação

Normas, Leis e Padrões que envolvem SI

- **Lei *Sarbannes-Oxley* (SOX–SARBOX):** Criada em 2002 pelo congresso americano para promover transparência na divulgação das informações contábeis, assegurar a prestação de contas e tratar de forma justa e imparcial as partes interessadas. A motivação para sua criação surgiu após os problemas envolvendo fraudes financeiras das empresas **Enron e WorldCom (Xerox)**. A Lei SOX é composta por 11 capítulos, distribuídos em 69 artigos.

- **Basel II Accord (Acordo de Basileia):** Criado em 1988, o Acordo de Basiléia fornece diretrizes para calcular riscos (crédito, mercado e operacionais) de instituições financeiras, para assim, regulamentar o funcionamento de instituições financeiras por meio de uma série de regras.

Normas, Leis e Padrões que envolvem SI

- **PCI-DSS (*Payment Card Industry*):** Criada em 2004 pela iniciativa conjunta das bandeiras de cartão: *Visa*, *MasterCard*, *American Express*, *Discover* e *JCB*, a **PCI-DSS** define padrões para o tratamento de dados de **pagamentos de cartões de crédito** para comerciantes e fornecedores de serviços. Seu principal objetivo é reduzir o **risco de fraudes e roubo de dados de cartões de crédito**.

- **ITIL (*Information Technology Infrastructure Library*):** Biblioteca composta por 5 livros específicos **para Gerenciamento de Serviços de TI**. No ITIL, itens específicos abordam a adoção de Segurança da Informação, principalmente em **planos de continuidade de negócios**.

Normas, Leis e Padrões que envolvem SI

- **COBIT (*Control Objectives for Information and related Technology*):** Trata-se um framework de boas práticas composto por diferentes ferramentas para implementação de outras normas ou padrões. O COBIT é reconhecido por diversos padrões internacionais, incluindo **ITIL** e a **Série ISO 27000**.

Aplicabilidade das
Normas Segurança da Informação

Aplicabilidade das Normas de Segurança da Informação

- Embora exista uma variedade de normas nacionais e internacionais, que abordam processos, técnicas, ferramentas e boas práticas de SGSI, sua aplicação isoladamente **não é o suficiente para solucionar por completo as ameaças** a ativos de informação.

- Para minimizar os riscos ao máximo de uma informação tornar-se insegura, se faz necessário que, juntamente com a aplicação das normas, aplique-se também **Políticas de Segurança da Informação (PSI)**, que atenda às necessidades da organização.

Referências

Referências e Links Úteis

- COELHO, Flávia Estélia Silva, BEZERRA, Edson Kowask, ARAÚJO, Luiz Geraldo Segadas. Gestão da Segurança e da Informação: NBR 27001 e NBR 27002. Escola Superior de Redes, 2013, 212p.
- DIAS, Cláudia. Segurança e Auditoria da Tecnologia da Informação . Rio de Janeiro: Axcel Books, 2000.
- FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. Política de Segurança da Informação: guia prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna, 2006.
- NAKAMURA, Emílio Tissato; GEUS, Paulo. Lício de. Segurança de redes em ambientes cooperativos. São Paulo: Berkeley, 2002.
- SÊMOLA, Marcos. Gestão da Segurança da Informação: uma visão executiva. Rio de Janeiro: Elsevier, 2003.
- VINTEN, Gerald. Auditing and Security. AS/400, NT, Unix, Networks, and Disaster Recovery Plans. Managerial Auditing Journal, v. 17, n. 5, p. 289-290, 2002.

- Segurança Física: https://www.linkedin.com/pulse/how-perform-physical-security-risk-assessment-igor-milkovski-ma
- Information Security Histoty: https://www.pqbweb.eu/platform.php?i=&if=94&ch=2896