


# SEGURANÇA E PROTEÇÃO DE DADOS

Prof. Priscilla Cunha

[pcunha@uni9.pro.br](mailto:pcunha@uni9.pro.br)

# Agenda





# PRINCIPAIS PADRÕES E NORMAS DE SEGURANÇA

- Devido a toda a preocupação com segurança que se tem atualmente nas empresas, percebeu-se a necessidade de se criar regras para se lidar com ela.
- Até pouco tempo atrás, quase não existiam normas e padrões de segurança para orientar as empresas sobre como agir, mas isso mudou!!!

- Os padrões e normas surgiram para proteger a informação...
- Anterior ao 11 de setembro, até existiam algumas preocupações com segurança, mas ela era mais voltada para a parte física.

- Isso vem mudando gradativamente e as empresas começam a ter uma preocupação maior com seu bem mais precioso: a INFORMAÇÃO.
- O rápido crescimento das redes de computadores e da comunicação on line fez as empresas perceberem sua dependência da informação e de seus sistemas.




**NORMAS**

- Norma: documento criado por uma autoridade reconhecida, feita em consenso por uma equipe com alta capacidade técnica sobre o assunto, que permite que seja tirada uma certificação.



- Usada para definir regras e padrões que servirão como meio de controle na realização de determinada atividade.
- As normas de segurança da informação foram criadas para fornecer as melhores práticas, diretrizes e princípios gerais para a implementação de sua gestão para qualquer organização.




# **ÓRGÃOS PADRONIZADORES E PRIMEIRAS NORMAS BRASILEIRAS**

- Existem alguns órgãos nacionais e internacionais reconhecidos e idôneos que elaboram padrões, editam, publicam e revisam normas técnicas.
- Os mais conhecidos são:
  - ISO – International Standardization Organization
  - IEC – International Electrotechnical Commission
  - IEEE – Institute of Electrical and Electronics Engineers
  - ABNT – Associação Brasileira de Normas Técnicas

# Primeiras Normas Brasileiras

- NBR1333 (1990): controle de acesso físico ao CPD
- NBR1334 (1990): critérios de segurança física para o armazenamento das informações
- NBR1335 (1991): segurança física dos terminais dos usuários
- NBR10842 (1989): segurança para os equipamentos de TI



# EVOLUÇÃO DAS NORMAS DE SEGURANÇA

- 1970 – criação de uma força tarefa no departamento de defesa americano que criou o documento Security Control for Computer System
- 1983 – criado um conjunto de regras para classificação dos sistemas operacionais como seguros ou não, chamado de Orange Book; usado para avaliar e classificar o grau de proteção que os SOs ofereciam ao hardware, software e informações armazenados.

- 1987 – criada uma adaptação do orange book, voltado para a segurança de equipamentos de redes, chamado de Red Book.
- [http://en.wikipedia.org/wiki/Rainbow\\_Series](http://en.wikipedia.org/wiki/Rainbow_Series)



- 1995 – foi criada no Reino Unido a BS7799, um padrão de segurança muito bem elaborado e complexo, que foi dividido em 2 partes:
  - BS7799-1: documento de referência para implementar "Boas Práticas" para a segurança da informação.
  - BS7799-2: proporcionar a base para a criação de um sistema de Gestão da Segurança da Informação (SGSI) dentro das empresas.



- Por ter sido uma norma muito bem elaborada e inédita, ela passou a ser usada no mundo todo.
- Porém, ela tinha diversos itens específicos do mercado britânico. Com isso, ela foi adaptada para ser usada internacionalmente.

- 2000 – criada a ISO/IEC 17799, a versão internacional da BS7799-1.
- 2001 – criada a NBR ISO/IEC 17799, a versão brasileira da norma internacional, que foi revisada em 2005.



**SÉRIE ISO  
27000**

- Série composta por 6 normas de segurança, cada uma tratando temas específicos.
  - ISO 27001
  - ISO 27002
  - ISO 27003
  - ISO 27004
  - ISO 27005
  - ISO 27006

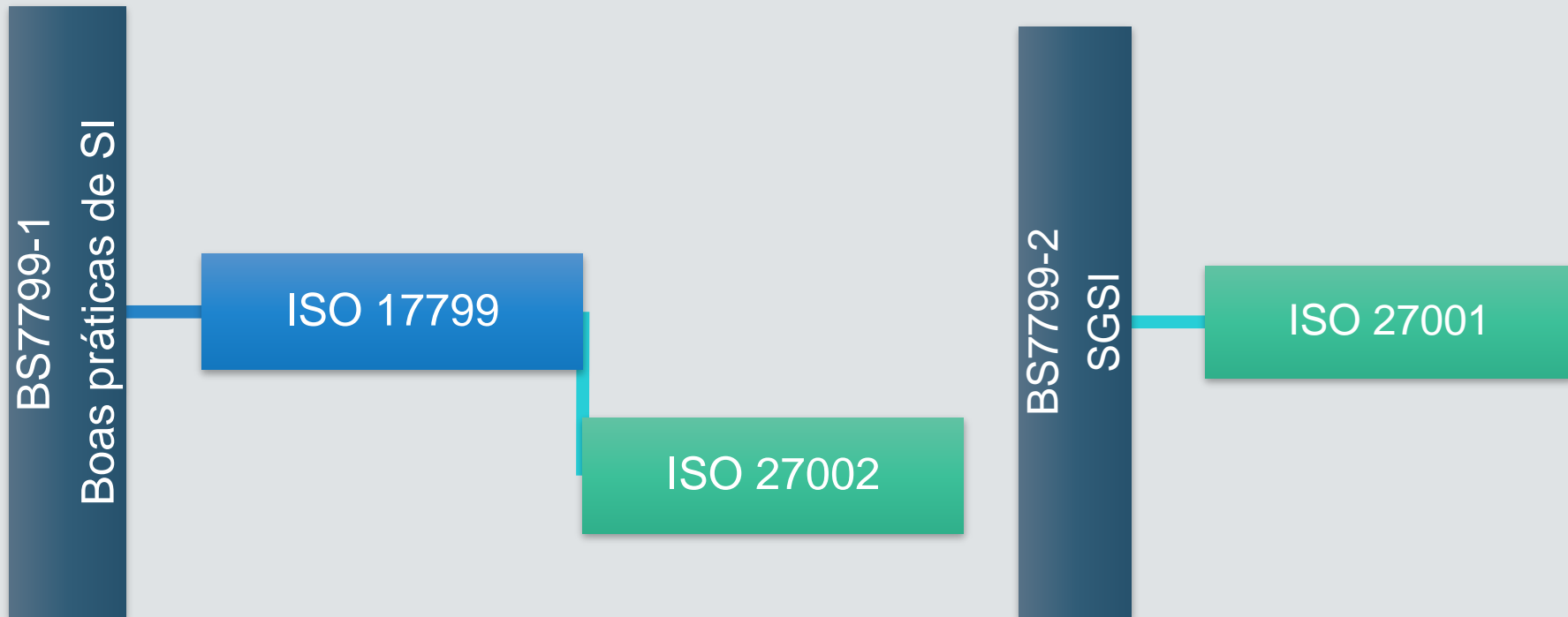
- ISO 27001 (2005)
  - BS7799-2 revisada e melhorada
  - Sistema de Gestão da Segurança da Informação (SGSI)
  - Contempla o ciclo de melhoria contínua.

- ISO 27002 (2005)
  - Voltada para a gestão da segurança da informação
  - Princípios gerais de concepção, implementação, manutenção e melhoria da segurança
  - Guia de boas práticas
  - Substitui a ISO 17799.

- ISO 27003 (2010)
  - Orientação sobre a implementação de SGSI, incluindo técnicas de segurança
  - Fornece instruções de como realizar um planejamento de um projeto SGSI em organizações de todos os tamanhos.
- ISO 27004 (2009)
  - Padrão referente aos mecanismos de medição e relatórios para um SGSI.

- ISO 27005 (2008)
  - Gestão de riscos: fornece diretrizes para o gerenciamento de informações de riscos.
- ISO 27006 (2011)
  - Requisitos para auditorias externas em um SGSI e certificação de sistemas de informação de gestão de segurança.







**OUTRAS  
NORMAS**

- Algumas outras normas, de assuntos não tão voltados a segurança, surgiram, abrangendo um pouco da nossa área.

- 2002 - Sarbanes Oxley (SARBOX ou SOX): criada nos EUA depois da crise financeira criada por causa de escândalos financeiros. Objetivo: dar transparência na divulgação das informações e assegurar a prestação de contas. Responsabiliza diretores, auditores e pessoal de TI por informações falsas apresentadas aos investidores

- BASEL III ACCORD (BASILEIA III): tem o objetivo de manter estabilidade financeira pela implementação de controles que diminuam os riscos dos bancos. Realiza cálculo de riscos (de crédito, do mercado e operacionais).

- PCI (Payment Card Industry) – criada pelas grandes bandeiras de cartão de crédito (AMEX, Discover Financial Services, Japan Credit Bureau, MasterCard e Visa), define um padrão para o manuseio de dados de pagamentos para todos os comerciantes que lidam com armazenamento, transmissão ou processamento de dados de cartões de crédito.

- ITIL (Information Technology Infrastructure Library): modelo de referência para gerenciamento de processos de TI, itens específicos que abordam o assunto da Segurança da Informação, principalmente em planos de continuidade de negócios.

- COBIT (Control Objectives for Information and Related Technology): conjunto de ferramentas de implementação e guia com técnicas de gerenciamento.



- ISO 15408 – criada em 2005, estabelece critérios de segurança para o desenvolvimento de aplicações seguras.
- BS 2599-2: criada em 2007, é uma norma britânica com foco em gestão de continuidade de negócios.
- ISO 31000: norma criada em 2009 e voltada para a gestão de riscos.

- Como podemos ver, temos uma constante evolução das normas de segurança. Isso se deve ao fato de as TI evoluir muito rapidamente, e com ela as ameaças às quais estamos sujeitos. Todos os dias temos novas ameaças e vulnerabilidade, precisando de novos procedimentos e mecanismos para evitá-los.



**CERTIFICAÇÃO**

# Importância da Certificação

- Apesar de não garantir total e completamente a segurança da informação, a certificação mostra aos clientes de uma empresa que a mesma se preocupa com suas informações, o que pode ser um diferencial de mercado.



**LGPD**

- LGPD: Lei Geral de Proteção de Dados
- Lei brasileira que estabelece regras para a proteção de dados pessoais de cidadãos brasileiros.
- A lei foi criada para aumentar a proteção de dados pessoais e garantir que os dados pessoais sejam usados de forma responsável e transparente.

- A LGPD foi criada em 2018 e entrou em vigor em agosto de 2020 e se aplica a empresas de todos os setores.

# Aplicações

1. Proteção de dados pessoais: permite que as empresas estabeleçam controles e processos para garantir que os dados pessoais dos usuários sejam tratados de acordo com as leis de proteção de dados.
2. Conscientização dos usuários: exige que as empresas forneçam aos usuários informações claras e claras sobre como seus dados estão sendo utilizados, bem como sobre seus direitos de proteção de dados.



3. Responsabilidade: estabelece que as empresas sejam responsáveis por seus processos de tratamento de dados, o que inclui o cumprimento de requisitos legais e técnicos.
4. Auditorias: determina que as empresas realizem auditorias regulares para garantir que seus processos de tratamento de dados estejam em conformidade com as leis de proteção de dados.
5. Prevenção de violações de segurança: requer que as empresas implementem medidas de segurança para prevenir violações de dados, tais como criptografia e autenticação forte.

# Vantagens

- Proteção dos direitos dos cidadãos, permitindo que as pessoas tenham mais controle sobre seus dados pessoais.
- Muitas empresas terão que se adequar às novas regras, o que ajudará a aumentar a segurança dos dados pessoais.
- A LGPD aumenta a transparência das empresas, pois obriga que elas informem as pessoas sobre como seus dados estão sendo usados.

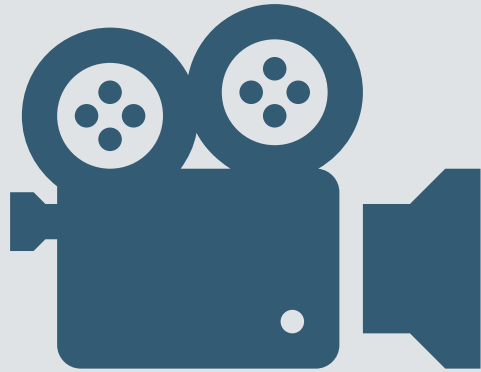
# Desvantagens

- As empresas precisarão se adaptar às novas regras, o que pode resultar em custos adicionais.
- As empresas precisarão ter uma compreensão profunda de como seus sistemas de dados funcionam e de como eles estão protegidos.
- A LGPD pode causar problemas para empresas que usam dados pessoais para fins comerciais, pois os requisitos são mais estritos.





**VÍDEOS**



- ISO 27000 -  
<https://www.youtube.com/watch?v=8kJp1ijbnvM&index=7&list=UUFFzm2qUHce7Gua4tGb6dvQ>
- LGPD - Resumo Geral da Lei -  
<https://www.youtube.com/watch?v=UYAJA2HG6-M>
- Entenda: O que é e pra que serve a LGPD? -  
<https://www.youtube.com/watch?v=oFRROvMVUWQ>



**PARA SABER  
MAIS**



- <https://www.portalgsti.com.br/2013/12/as-normas-da-familia-iso-27000.html>
- <https://www.portalgsti.com.br/2012/11/ebook-gratuito-gestao-da-seguranca-da-informacao.html>
- <https://www.lgpdbrasil.com.br/>



# Dicas para Estudo



Seja “CURIOSO”:

Procure revisar o que foi estudado.

Pesquise as referências bibliográficas.



Seja “ANTENADO”:

Leia a próxima aula.



Seja  
“COLABORATIVO”:

Traga assuntos relevantes para a sala de aula.

Participe da aula.

Proponha discussões relevantes sobre o conteúdo.



Prof. Priscilla Cunha

