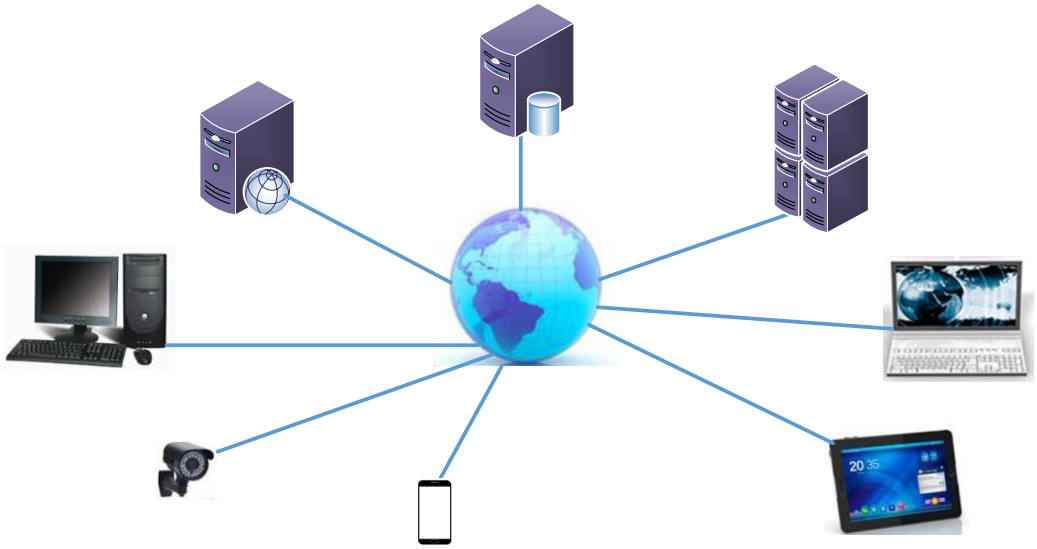
Normas ISO 27000



Prof. Dr. Márcio Andrey Teixeira
Instituto Federal de São Paulo – Campus Catanduva
Catanduva, SP
Membro Sênior do IEEE
marcio.andrey@ifsp.edu.br

CONTEÚDO

- REVISÃO
- INTRODUÇÃO
- VISÃO GERAL DA ISO 27000
- ABNT NBR ISO/IEC 27002:2013
- LEIS E REGULAMENTAÇÕES
- REFERÊNCIAS BIBLIOGRÁFICAS

- SIGLAS:
  - *ABNT = ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS*
  - *NBR = NORMAS BRASILEIRAS*
  - *ISO = INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ORGANIZAÇÃO INTERNACIONAL PARA PADRONIZAÇÃO)*
  - *IEC = INTERNATIONAL ELECTROTECHNICAL COMMISSION (COMISSÃO ELETROTÊCNICA INTERNACIONAL)*

REVISÃO

- ***Ameaças:*** Causa potencial (agente) de um incidente indesejado, que pode resultar em dano para um sistema ou organização [ISO 27002].
- Podem colocar em risco a confidencialidade, integridade e disponibilidade das informações.
- ***São classificadas em:*** *Naturais (natureza), Intencionais (maldades) e Involuntárias (despreparo e desconhecimento humano).*

- ***Vulnerabilidades:*** Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças [ISO 27002].

- ***Riscos:*** é a **Probabilidade** da **AMEAÇA** explorar **VULNERABILIDADES**.
- Causando perdas ou danos aos ativos e consequente impacto no negócio.

REVISÃO

- Esteganografia *(Steganography)*
  - **Do grego** : *steganos* = ***esconder, ocultar, mascarar***
    graphein = ***escrever, escrita***
  - Técnica de segurança utilizada desde a antiguidade (mensageiros a cavalos, pombo correio e outras formas).
  - Ocultar mensagens, ou seja, a arte da escrita encoberta.
  - Atualmente é utilizada para esconder mensagens de texto em imagens, vídeos ou até em outros textos.
  - Segurança por obscuridade.

INTRODUÇÃO

- Apresentar a evolução e o objetivo de cada uma das principais normas que fazem parte da ISO 27000;
- Explicar os objetivos de controle do Código de Prática para Gestão da Segurança da Informação;
- Descrever a relação entre normas, leis e recomendações.

INTRODUÇÃO

- **O que são e para que servem as normas?**
- É aquilo que se estabelece como medida para a realização de uma atividade.
- Uma norma tem como propósito definir regras e instrumentos de controle para assegurar a conformidade de um processo, produto ou serviço.

INTRODUÇÃO

- Conforme definido pela Associação Brasileira de Normas Técnicas (ABNT), os objetivos da normalização são:
  - **Comunicação:** proporcionar meios mais eficientes na troca de informação entre o fabricante e o cliente, melhorando a confiabilidade das relações comerciais e de serviços;
  - **Segurança:** proteger a vida humana e a saúde;
  - **Proteção do consumidor**: prover a sociedade de mecanismos eficazes para aferir qualidade de produtos;
  - **Eliminação de barreiras técnicas e comerciais:** evitar a existência de regulamentos conflitantes sobre produtos e serviços em diferentes países, facilitando assim, o intercâmbio comercial.

A FAMÍLIA 27000

A família **ISO 27000 – *Sistema de Gerenciamento de Segurança:***

- **ISO/IEC 27000:2009** - ***Sistema de Gerenciamento de Segurança*** - Explicação da série de normas, objetivos e vocabulários;

- **ISO/IEC 27001:2013** - ***Sistema de Gestão de Segurança da Informação*** - Esta Norma **especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização**. Esta Norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização

- **ISO/IEC 27002:2013** - ***Código de Melhores Práticas para a Gestão de Segurança da Informação*** - **Mostra o caminho de como alcanças os controles certificáveis na ISO 27001**. Essa ISO é certificável para profissionais e não para empresas.

A FAMÍLIA 27000

- ISO/IEC 27003:2011 - *Diretrizes para Implantação de um Sistema de Gestão da Segurança da Informação* - Segundo a própria ISO/IEC 27003, "O propósito desta norma é **fornecer diretrizes práticas para a implementação de um Sistema de Gestão da Segurança da Informação (SGSI), na organização, de acordo com a ABNT NBR ISO/IEC 27001:2005.**

- ISO/IEC 27004:2010 - *Gerenciamento de Métricas e Relatórios para um Sistema de Gestão de Segurança da Informação* - **Mostra como medir a eficácia do sistema de gestão de SI na corporação.**

- ISO/IEC 27005:2011 - *Gestão de Riscos de Segurança da Informação* - Essa norma é **responsável por todo ciclo de controle de riscos na organização**, atuando junto à ISO 27001 em casos de certificação ou através da ISO 27002 em casos de somente implantação. de segurança da informação deve ocorrer.

A FAMÍLIA 27000

- ISO/IEC 27007:2016 – *Diretrizes para auditoria de sistemas de gestão da segurança da informação* - Esta Norma **fornece diretrizes sobre como gerenciar um programa de auditoria de sistemas de gestão da segurança da informação (SGSI) e sobre como executar as auditorias e a competência de auditores de SGSI, em complementação as diretrizes descritas na ABNT NBR ISO 19011.** Esta Norma é aplicável a todos que necessitam entender ou realizar auditorias internas ou externas de um SGSI ou ainda gerenciar um programa de auditoria de SGSI.

- ISO/IEC 27011:2009 - *Tecnologia da informação - Técnicas de segurança - Diretrizes para gestão da segurança da informação para organizações de telecomunicações baseadas na ABNT NBR ISO/IEC 27002* - Entende-se que toda parte de telecomunicação é vital e essencial para que um SGSI atinja seus objetivos plenos (claro que com outras áreas), para tanto era necessário **normatizar os processos e procedimentos desta área objetivando a segurança da informação corporativa de uma maneira geral.** A maneira como isso foi feito, foi tendo como base os controles e indicações da ISO 27002.

A FAMÍLIA 27000

- ISO/IEC 27014:2013 – *Tecnologia da Informação – Técnicas de Segurança – Governança de segurança da informação* - Esta recomendação | Norma **fornece orientação sobre conceitos e princípios para a governança de segurança da informação**, pela qual as organizações podem avaliar, dirigir, monitorar e comunicar as atividades relacionadas com a segurança da informação dentro da organização.

A FAMÍLIA 27000

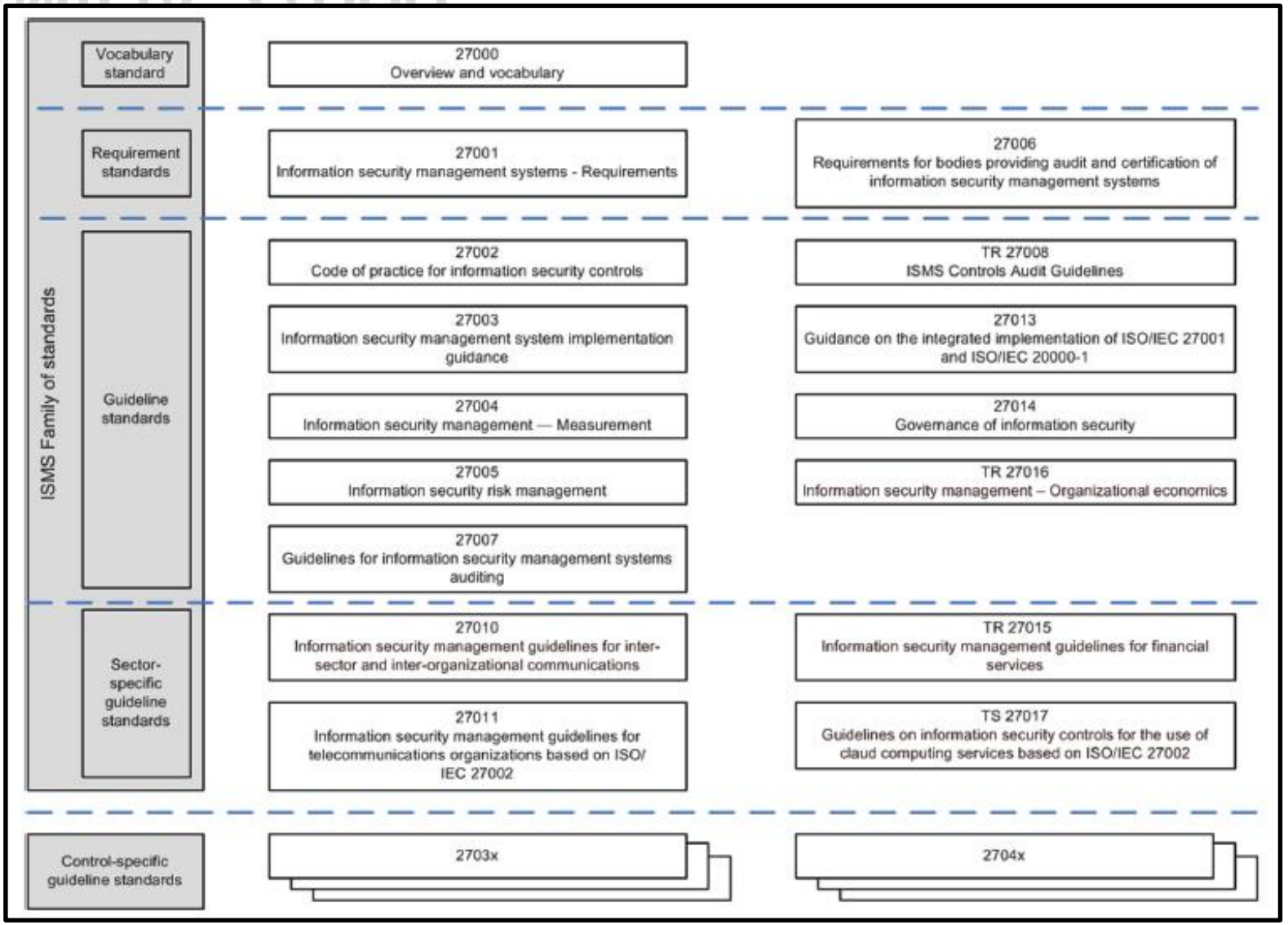
- ISO/IEC 27031:2015 - *Tecnologia da informação - Técnicas de segurança - Diretrizes para a prontidão para a continuidade dos negócios da tecnologia da informação e comunicação* - Esta Norma descreve os conceitos e princípios da prontidão esperada para a tecnologia de comunicação e informação (TIC) na continuidade dos negócios e fornece uma estrutura de métodos e processos para identificar e especificar todos os aspectos (como critérios de desempenho, projeto e implementação) para fornecer esta premissa nas organizações e garantir a continuidade dos negócios.
- É aplicável para qualquer organização (privada, governamental e não governamental, independentemente do tamanho) desenvolvendo a prontidão de sua TIC para atender a um programa de continuidade nos negócios (PTCN), requerendo que os serviços e componentes de infraestrutura relacionados estejam prontos para suportar as operações de negócio na ocorrência de eventos e incidentes e seus impactos na continuidade (incluindo segurança) das funções críticas de negócio. Também assegura que a organização estabeleça parâmetros para medir o desempenho que está correlacionado à PTCN de forma consistente e organizada.

A FAMÍLIA 27000

- ISO/IEC 27032:2015 - *Tecnologia da Informação - Técnicas de segurança - Diretrizes para segurança cibernética* - Esta Norma fornece diretrizes para melhorar o estado de Segurança Cibernética, traçando os aspectos típicos desta atividade e suas ramificações em outros domínios de segurança.

- ISO/IEC 27037:2013 - *Tecnologia da informação — Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidência digital* - Esta Norma fornece diretrizes para atividades específicas no manuseio de evidências digitais que são a identificação, coleta, aquisição e preservação de evidência digital que possam possuir valor probatório.

A FAMÍLIA 27000



ABNT NBR ISO/IEC 27002:2013 – CÓDIGO DE PRÁTICA PARA SI

- As **medidas de segurança são definidas pela norma ISO/IEC 27002**, que dá suporte ao desenvolvimento e normas de planos de segurança da informação e orienta de melhor forma a **Gestão da Segurança da Informação.**

- A norma **ISO 27002** é o novo nome da norma ISO 17799. Esta norma é um guia de boas práticas que descreve os objetivos de controle e os controles recomendados para a ***Segurança da Informação.*** A norma ISO 27001 contém alguns anexos que resumem alguns destes controles.

- **Inclui: A seleção, a implementação e o gerenciamento de controles. Levando em consideração os ambientes de risco da segurança da informação da organização.**

ABNT NBR ISO/IEC 27002:2013 – CÓDIGO DE PRÁTICA PARA SI

- No Brasil esta norma foi elaborada pelo **Comitê Brasileiro de Computadores e Processamento de Dados** (ABNT/CB-21), pela **Comissão de Estudo de Técnicas de Segurança** (CE-21:027.00).

- Projeto circulado em Consulta Nacional conforme Edital nº 09, de 26.09.2013 a 25.10.2013, número de Projeto ABNT NBR ISO/IEC 27002.

- Versão atual (**2ª edição**) ***substitui*** **e** ***cancela*** a edição anterior (ABNT NBR ISO/IEC 27002:2005)

ABNT NBR ISO/IEC 27002:2013 – ESTRUTURA DA NORMA

- *Contém:*
  - 14 seções de controles de segurança da informação;
  - 35 objetivos de controles e
  - 114 controles

ABNT NBR ISO/IEC 27002:2013 – ESTRUTURA DA NORMA

- **Seções:** define os controles de segurança da informação. Contém um ou mais objetivos de controle.

  Não importa a ordem em que aparecem, ou seja, não implica nem significa o seu grau de importância. Cada organização averigua, escolhe e implementa esta Norma de acordo com sua aplicabilidade para os processos individuais do negócio.

- **Categorias e Controles:** cada seção principal contém:

  Um objetivo de controle declarando o que se espera que seja alcançado;

  Um ou mais controles que podem se aplicados para se alcançar o objetivo do controle.

- **Controle:** define a declaração específica do controle, para atender ao objetivo de controle.

ABNT NBR ISO/IEC 27002:2013 – ESTRUTURA DA NORMA

- **Diretrizes para implementação:** apresenta informações mais detalhadas para apoiar a implementação do controle e alcançar o objetivo do controle.

- **Informações adicionais:** apresenta mais dados que podem ser considerados, como exemplo, questões legais e referências normativas.

ABNT NBR ISO/IEC 27002:2013 – ESTRUTURA DA NORMA

- Estrutura da Norma

5. Política de Segurança da Informação (1) Seção

5.1 Política de Segurança da Informação Categoria ou Objetivos de Controle

Objetivo: "Prover uma orientação de apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes“

5.1.1 Documento da Política de Segurança da Informação

"Convém que um documento da política de SI seja aprovado pela direção ..."

5.1.2 Análise Crítica da Política de Segurança da Informação

"Convém que a política de SI seja analisada criticamente a intervalos planejados ou quando mudanças ...

ABNT NBR ISO/IEC 27002:2013 – ESTRUTURA DA NORMA

- Seções (Categorias):
- 5 - Política de Segurança da Informação (1)
- 6 - Organizando a Segurança da Informação (2)
- 7 - Segurança em Recursos Humanos (3)
- 8 - Gestão de Ativos (3)
- 9 - Controle de Acesso (4)
- 10 – Criptografia (1)
- 11 - Segurança Física e do Ambiente (2)
- 12 - Segurança nas operações (7)
- 13 – Segurança nas comunicações (2)
- 14 – Aquisição, desenvolvimento e manutenção de sistemas (3)
- 15 – Relacionamento na cadeia de suprimento (2)
- 16 - Gestão de Incidentes de SI (1)
- 17 – Aspectos da segurança da informação na gestão da continuidade do negócio (2)
- 18 - Conformidade (2)

ABNT NBR ISO/IEC 27002:2013 – SEÇÕES E OBJETIVOS DE CONTROLE

5. Política de Segurança da Informação (1)
    5.1 Orientação da direção para segurança da informação

6. Organizando a Segurança da Informação (2)
    6.1 Organização interna
    6.2 Dispositivos móveis e trabalho remoto

7. Segurança em recursos humanos (3)
    7.1 Antes da contratação
    7.2 Durante a contratação
    7.3 Encerramento e mudança da contratação

8. Gestão de Ativos (3)
    8.1 Responsabilidade pelos ativos
    8.2 Classificação da informação
    8.3 Tratamento de mídias

ABNT NBR ISO/IEC 27002:2013 – SEÇÕES E OBJETIVOS DE CONTROLE

9. Controle de acesso (4)
   - 9.1 Requisitos do negócio para controle de acesso
   - 9.2 Gerenciamento de acesso do usuário
   - 9.3 Responsabilidades dos usuários
   - 9.4 Controle de acesso ao sistema e à aplicação

10. Criptografia (1)
   - 10.1 Controles criptográficos

11. Segurança física e do ambiente (2)
   - 11.1 Áreas seguras
   - 11.2 Equipamentos

ABNT NBR ISO/IEC 27002:2013 – SEÇÕES E OBJETIVOS DE CONTROLE

12 – Segurança nas operações (7)

- 12.1 Responsabilidades e procedimentos operacionais
- 12.2 Proteção contra *malware*
- 12.3 Cópias de segurança
- 12.4 Registros e monitoramento
- 12.5 Controle de *software* operacional
- 12.6 Gestão de vulnerabilidades técnicas
- 12.7 Considerações quanto à auditoria de sistemas da informação

13 – Segurança nas comunicações (2)

- 13.1 Gerenciamento da segurança em redes
- 13.2 Transferência de informação

14 – Aquisição, desenvolvimento e manutenção de sistemas (3)

- 14.1 Requisitos de segurança de sistemas de informação
- 14.2 Segurança em processos de desenvolvimento e de suporte
- 14.3 Dados para teste

ABNT NBR ISO/IEC 27002:2013 – SEÇÕES E OBJETIVOS DE CONTROLE

15 - Relacionamento na cadeia de suprimento (2)

15.1 Segurança da informação na cadeia de suprimento

15.2 Gerenciamento da entrega do serviço do fornecedor

16 – Gestão de incidentes de segurança da informação (1)

16.1 Gestão de incidentes de segurança da informação e melhorias

17 – Aspectos da segurança da informação na gestão da continuidade do negócio (2)

17.1 Continuidade da segurança da informação

17.2 Redundâncias

18 – Conformidade (2)

18.1 Conformidade com requisitos legais e contratuais

18.2 Análise crítica da segurança da informação

LEIS E REGULAMENTAÇÕES

- **Objetivo:**

- A seguir serão apresentadas algumas informações básicas sobre leis e regulamentações que possuem relação (impacto) direto na segurança da informação de instituições que estão posicionadas em diferentes mercados.

- O atendimento dessas leis e regulamentações são amparadas pelos controles mencionados anteriormente.

LEIS E REGULAMENTAÇÕES

- **Definições:**

- **Lei:** é a regra jurídica escrita emenda do poder competente;

- **Resolução:** espécie de norma utilizada pelo poder público ou autoridade para regulamentar alguma situação que guarde relação com as suas atribuições.

LEIS E REGULAMENTAÇÕES

- Nos últimos anos observou-se a publicação de muitas leis e regulamentações (em âmbito nacional e internacional) cujo escopo contempla aspectos de Segurança da Informação. Por exemplo:

- SOX *(Sarbanes-Oxley)*
- Bacen 3380 *(Banco Central)*
- CVM *(Comissão de Valores Imobiliários)*
- CFM *(Conselho Federal de Medicina)*

REFERÊNCIAS BIBLIOGRÁFICAS

- ABNT NBR ISO/IEC 27002:2013. **Código de Prática para a Gestão da Segurança da Informação, 2013.**

- **ABNT - Associação Brasileira de Normas Técnicas.**
  site: http://abntcolecao.com.br/ e http://abntcolecao.com.br/ifsp/

- Sêmola, Marcos. **Gestão da Segurança da Informação: Uma Visão Executiva. Rio de Janeiro, Ed. Campus, 2014.**

- Centro de Estudos, Respostas e Tratamento de Incidentes. **CERT.Br** - http://www.cert.br/ e http://cartilha.cert.br