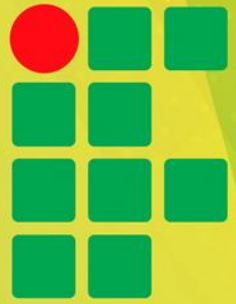
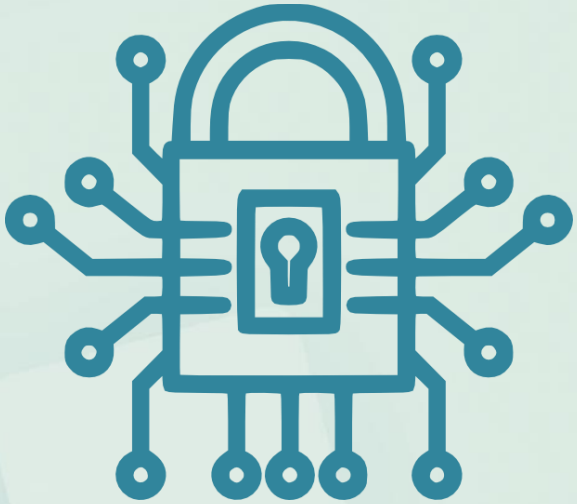


INSTITUTO FEDERAL

Sertão Pernambucano

Segurança da Informação



Leis e Normas

Prof. Heraldo Gonçalves Lima Junior

INSTITUTO FEDERAL
Sertão Pernambucano

1. Introdução

1. 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.

1. O que diz a ABNT

- 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;

1. O que diz a ABNT

- **Segurança:** proteger a vida humana e a saúde;
- **Proteção do consumidor:** prover a sociedade de mecanismos eficazes para aferir qualidade de produtos;

1. O que diz a ABNT

- **Eliminação de barreiras técnicas e comerciais:** evitar a existência de regulamentos conflitantes sobre produtos e serviços em diferentes países, facilitando assim, o intercâmbio comercial.

2. Família ISO 27000

2.1. Família ISO 27000

- É a principal família de normas de Segurança da Informação aceitas internacionalmente;
- Aplicável a qualquer organização, independentemente de tamanho ou segmento;

2.1. Família ISO 27000

- **ISO/IEC 27000:** visão geral/introdução à família ISO 27000.
- **ISO/IEC 27001:** Define os requisitos para um Sistema de Gestão da Segurança da Informação (SGSI).
- **ISO/IEC 27002:** Código de práticas com um conjunto completo de controles que auxiliam aplicação do Sistema de Gestão da Segurança da Informação.

2.1. Família ISO 27000

- **ISO/IEC 27003:** Contém um conjunto de diretrizes para a implementação do SGSI.
- **ISO/IEC 27004:** Define métricas de medição para a gestão da segurança da informação.
- **ISO/IEC 27005:** Cobre a Gestão de Riscos de segurança da informação.

2.1. Família ISO 27000

- Todas as normas presentes nessa família se convertem para o **SGSI**.
- Ele conta com princípios que criam parâmetros para a segurança dos e a melhor maneira de armazenar as informações.

SGSI
Sistema de Gestão de Segurança da Informação

2.1.1. ISO 27000

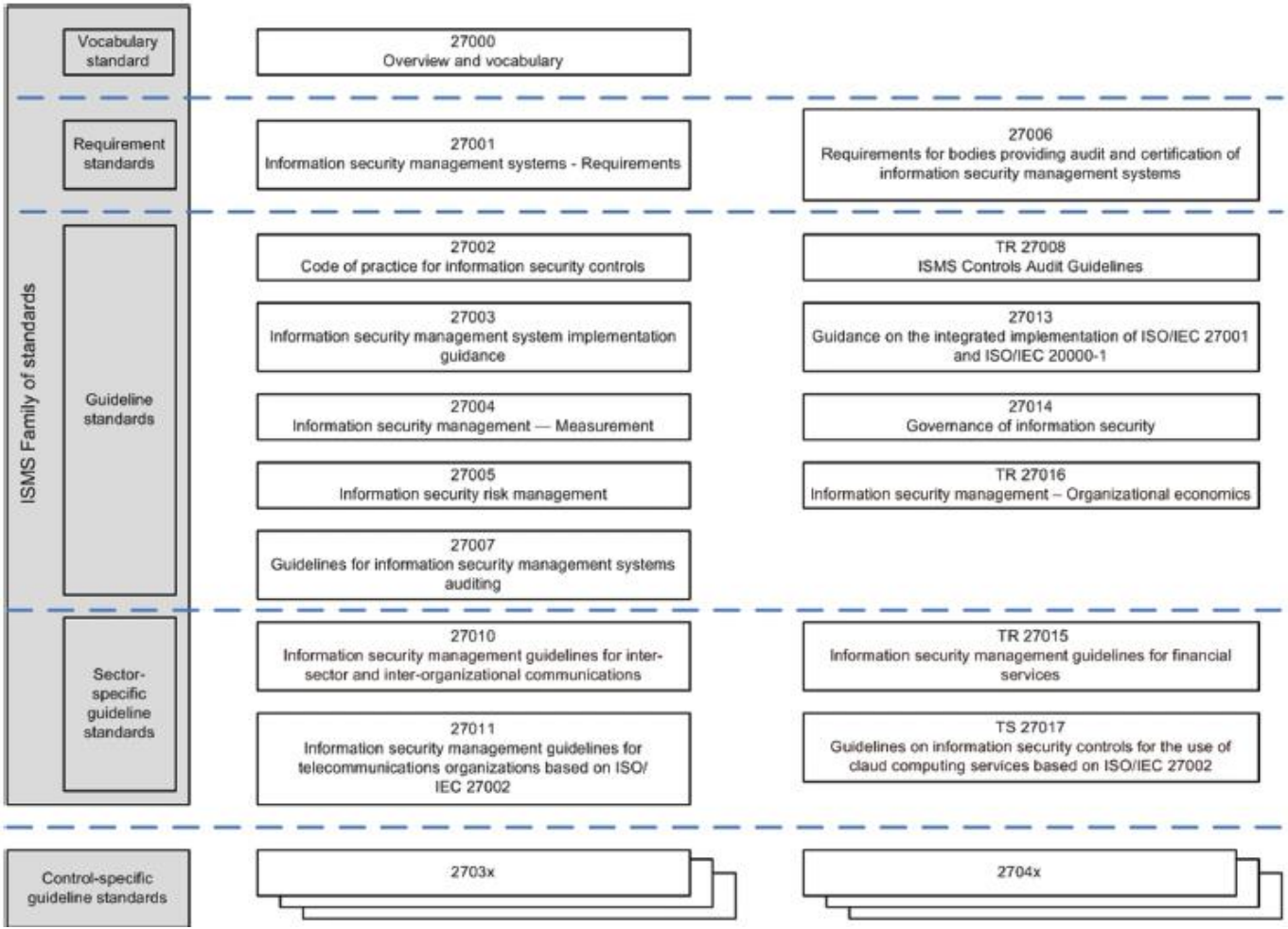
- Base para uma **certificação**, mas pode ser usada mesmo sem esse objetivo.
- oferece uma visão geral do conceito. Atua como uma **norma introdutória**, que traz consigo um **glossário de termos** que prepara para as certificações seguintes.

2.1.1. ISO 27000

- Definição de um **Sistema de Gestão de Segurança da Informação**;
- Objetivos e princípios do SGSI;
- A importância do SGSI para organizações;
- Definições estratégicas de como estabelecer, monitorar, implantar e melhorar seu SGSI;

2.1.1. ISO 27000

- Fatores críticos de sucesso para adoção do SGSI / Segurança da Informação nas organizações;
- Benefícios em se usar uma abordagem padronizada/normatizada para um SGSI;
- Como funciona o relacionamento entre as normas da família 27000.


ISMS Family of standards
Vocabulary standard
27000
Overview and vocabulary
Requirement standards
27001
Information security management systems - Requirements
27006
Requirements for bodies providing audit and certification of information security management systems
Guideline standards
27002
Code of practice for information security controls
TR 27008
ISMS Controls Audit Guidelines
27003
Information security management system implementation guidance
27013
Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
27004
Information security management — Measurement
27014
Governance of information security
27005
Information security risk management
TR 27016
Information security management – Organizational economics
27007
Guidelines for information security management systems auditing
Sector-specific guideline standards
27010
Information security management guidelines for inter-sector and inter-organizational communications
TR 27015
Information security management guidelines for financial services
27011
Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
TS 27017
Guidelines on information security controls for the use of claud computing services based on ISO/IEC 27002
Control-specific guideline standards
2703x
2704x

2.1.2. Por quais motivos minha empresa deve aderir a ISO 27000?

- A implementação da ISO 27000 é o tipo de iniciativa que oferece um excelente retorno sobre o investimento, manifestando-se tanto na construção de uma **boa imagem** para a marca quanto na **organização interna** da empresa.

2.2. ISO 27001

- Padrão de referência internacional para a **gestão de segurança da informação**.
- Provê requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI).

INSTITUTO FEDERAL
Sertão Pernambucano

2.2. ISO 27001

- **2013:** Preparada para fornecer os requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação.

2.2.1. ISO 27001 - Características

- **Análise de risco:**
  - A norma exige que a empresa faça uma análise de riscos de segurança periodicamente e sempre que mudanças significativas forem propostas ou estabelecidas.

2.2.1. ISO 27001 - Características

- **Comprometimento da alta gestão:**
  - A norma também exige que a alta administração demonstre comprometimento com o SGSI, além de ser essa parte da empresa a responsável em si pela segurança da informação.

2.2.1. ISO 27001 - Características

- **Definição de objetivos e estratégias:**
  - Durante o planejamento, a empresa precisa ter muito claro quais são seus objetivos de segurança e quais serão as estratégias estabelecidas para atingir esses objetivos.

2.2.1. ISO 27001 - Características

- **Recursos e competências:**
  - A organização também deve garantir que todos os recursos necessários não só para a implementação, mas também para a manutenção do sistema estejam disponíveis.

2.2.2. ISO 27001: Benefícios

- As organizações podem **aumentar o nível de segurança** das informações e dos sistemas, de acordo com os princípios.
- Identificar de forma continuada **oportunidades de melhorias**, transformando em um processo contínuo;
- **Aumentar a satisfação** dos clientes e parceiros.
- Implementar controle de **análises de riscos**.

2.2.3. ISO 27001 - SGCI

- O SGSI busca preservar a **confidencialidade, integridade e disponibilidade** da informação por meio da aplicação de um processo de **gestão de riscos** e fornece confiança para as partes interessadas (partes internas e externas).

SGSI
Sistema de Gestão de Segurança da Informação

INSTITUTO FEDERAL
Sertão Pernambucano

2.2.4. ISO 27001: Requisitos

- A ordem dos requisitos na norma não reflete sua importância ou implica na ordem pela qual eles devem ser implementados, pois os requisitos são genéricos e podem ser aplicados a todas as organizações.
- Os requisitos do SGSI conforme a ISO 27001:2013 estão separados em 7 seções, vamos conhecê-las.

2.2.4. ISO 27001: Requisitos

- **Contexto da organização:**
  - **Entendimento da organização** e das **necessidades das partes interessadas**, além da **determinação do escopo do SGSI**.

2.2.4. ISO 27001: Requisitos

- **Liderança:**
  - Demonstrar liderança e comprometimento, além da **autoridade**, **responsabilidade e papéis organizacionais**. A Alta Direção deve estabelecer uma **política de segurança da informação (PSI).**

2.2.4. ISO 27001: Requisitos

- **Planejamento:**
  - Planejamento de ações para **abordar riscos e oportunidades**, **objetivos de segurança da informação**.

2.2.4. ISO 27001: Requisitos

- **Apoio:**
  - Fornecer **recursos**, determinar **competência**, determinar a **comunicação** e incluir e assegurar a **informação documentada**.

2.2.4. ISO 27001: Requisitos

- **Operação:**
  - **Planejamento e controle operacionais**, a **avaliação de riscos** e o **tratamento dos riscos**.

2.2.4. ISO 27001: Requisitos

- **Avaliação de Desempenho:**
  - **Monitoramento**, medição, **análise** e **avaliação**, da auditoria interna e da análise crítica pela direção.

2.2.4. ISO 27001: Requisitos

- **Melhoria:**
  - **Não conformidade** e **ações corretivas**. Melhoria contínua.

2.2.5. ISO 27001: Como implementar?

- Para realizar a sua implementação é preciso seguir as diretrizes abordadas na **ISO 27003**. Essa norma fornece um guia e detalha passo a passo o processo de implementação da 27001.
- Contudo, existem cinco passos para a implantação da ISO 27001 à organização, descritos a seguir.

2.2.5. ISO 27001: Como implementar?

- **Entendimento do contexto da empresa:** a primeira etapa tem como objetivo compreender as características e necessidades da empresa, a fim de identificar e estabelecer as políticas e objetivos internos de segurança da informação;

2.2.5. ISO 27001: Como implementar?

- **Avaliação dos riscos:** o segundo passo é a realização da avaliação de riscos, isto é, a identificação das fragilidades dos processos internos e os riscos que envolvem a segurança da informação. A partir disso, cria-se uma classificação de risco para os tópicos identificados;

2.2.5. ISO 27001: Como implementar?

- **Implementação de controles operacionais**: o terceiro passo visa a implementação de controles operacionais nos processos, a fim de controlar, eliminar ou mitigar a classificação dos riscos identificados no tópico anterior;

2.2.5. ISO 27001: Como implementar?

- **Análise de eficácia:** na quarta etapa é preciso realizar uma análise dos resultados obtidos com a implementação dos controles operacionais, identificando aquilo que tem sido eficaz ou não. Essa é a fase em que a empresa realiza uma auditoria;

2.2.5. ISO 27001: Como implementar?

- **Melhoria contínua:** por fim, o último passo consiste na contínua melhoria a partir da obtenção da certificação, garantindo que a organização esteja em constante monitoramento dos riscos e possíveis novos controles operacionais.

2.3. O que é certificação ISO?

- Processo onde a empresa é avaliada para analisar se atende aos requisitos das normas correspondentes ao seu nicho de atuação. A certificação oferece garantia e legitimidade à corporação segundo padrões internacionais.

2.3. O que é certificação ISO?

- Uma empresa certificada mostra que se preocupa e oferece o melhor em segurança da informação, o que significa que seus clientes e fornecedores podem **confiar** suas informações a ela.

Obrigado!
Vlw! Flw!

INSTITUTO FEDERAL
Sertão Pernambucano