UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Segurança da Informação
Aula 9 – Políticas de Segurança

Prof. Dr. Eng. Fred Sauer

http://www.fredsauer.com.br

fsauer@gmail.com

Política de Segurança de Informações

É um documento que serve como mecanismo preventivo de proteção dos dados e processos importantes de uma organização, que define um padrão de segurança a ser seguido pelo corpo técnico e gerencial e pelos usuários, internos ou externos.

Política de Segurança da Informação

– A Política de Segurança é um conjunto de diretrizes, normas, procedimentos e instruções, destinadas respectivamente aos níveis estratégico, tático e operacional, com o objetivo de estabelecer, padronizar e normatizar a segurança tanto no escopo humano como no tecnológico.

Política de Segurança da Informação

- A Segurança da Informação "inicia" através da definição de uma política clara e concisa acerca da proteção das informações.
- Através de uma Política de Segurança da Informação, a empresa formaliza suas estratégias e abordagens para a preservação de seus ativos.

Política de Segurança da Informação

- A Política de Segurança da Informação deve ser compreendida como a tradução das expectativas da empresa em relação a segurança considerando o **alinhamento** com os seus objetivos de negócio, estratégias e cultura.

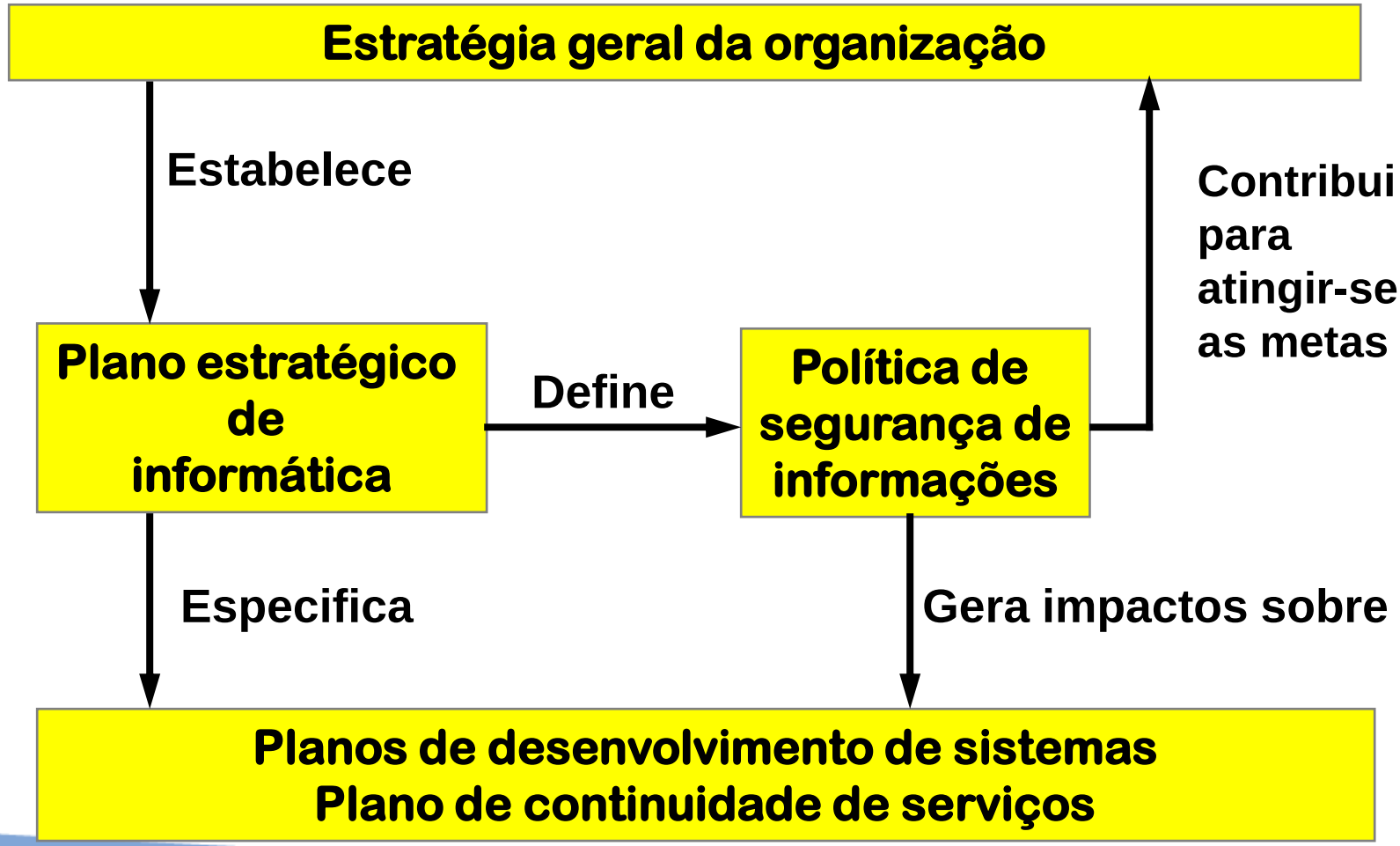
Política de Segurança da Informação

Política de Segurança de Informações

- Deve estabelecer os papéis e responsabilidades das funções relacionadas com a segurança
- Deve discriminar as principais ameaças, riscos e impactos envolvidos.
- Deve integrar-se às políticas institucionais relativas à segurança em geral, às metas de negócios da organização e ao plano estratégico de informática.
- Gera impactos sobre todos os projetos de informática, tais como *planos de desenvolvimento de novos sistemas* e *plano de contingências*.
- Não envolve apenas a área de informática, mas todas as informações da organização.

Política de Segurança da Informação

Relacionamentos da política de segurança de informações:



Política de Segurança da Informação

- **Objetivos e Escopo**
- Prover uma orientação da direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

[ISO 27002:2013]

Política de Segurança da Informação

- **Elaboração da política**
- As atividades básicas do **desenvolvimento** da Política de Segurança da Informação são:
  - Estruturar o Comitê de Segurança;
  - Definir Objetivos;
  - Realizar Entrevistas e Verificar a Documentação Existente;
  - Elaborar o Glossário da Política de Segurança;
  - Estabelecer Responsabilidades e Penalidades;
  - Preparar o Documento Final da PSI;
  - Oficializar a Política da Segurança da Informação;
  - Sensibilizar os Colaboradores.

Participação na Política de Segurança

Devem estar envolvidos:

- A alta gerência;
- A gerência de segurança de informações;
- Os vários gerentes e proprietários dos sistemas informatizados e, finalmente;
- Os usuários.

Política de Segurança da Informação

Ciclo de vida da informação

- Manuseio
  - Refere-se ao instante em que a informação é criada e/ou passa a ser manipulada
- Armazenamento
  - Como / onde armazenar determinados tipos de informações
- Transporte
  - Abrange todo o tipo de transporte possível para uma informação (fax, e-mail, entrega via transportadora, etc.)
- Descarte
  - Procedimentos a serem adotados no momento da exclusão de um informação e quando o descarte deve ocorrer .

Política de Segurança da Informação

Classificação da Informação

- Objetivos
  - Identificar quais os níveis de proteção que as informações disponíveis na organização requerem;
  - Uma informação pode ser classificada com base em diversos critérios, entre eles: sigilo, valor e criticidade;
  - Definir níveis de proteção e os controles a serem implementados ao longo do ciclo de vida da informação.

Política de Segurança da Informação

Classificação da Informação

- Definição
  - Conjunto de normas, procedimentos e instruções existentes que tratam sobre como proteger as informações
- A política define
  - Tipos de classificação
  - Critérios de avaliação e proteção
  - Responsabilidades

Política de Segurança da Informação

Classificação da Informação

- **Benefícios**
  - Proteção das informações importantes / vitais para o negócio;
  - Define e compartilha responsabilidades entre as partes;
  - Ajuda na tomada de decisões, uma vez que as informações estão bem categorizadas;
  - Ajuda a criar a cultura da segurança da informação (conscientização)
  - Uso racional dos recursos (controles) utilizados para proteger as informações
  - Cria níveis de proteção de acordo com o valor da informação

Política de Segurança da Informação

Classificação da Informação

- Premissas
  - Deve estar em conformidade com a cultura e realidade (complexidade) da organização
  - *Need to Know*, nada mais do que o necessário, apenas isso
    - Privilégio mínimo!
- As informações (independente do seu formato) possuem finalidades específicas e, portanto, destinam-se a determinados grupos de usuários
    - **Confidencialidade**!

Política de Segurança da Informação

Classificação da Informação

- Grau de sigilo
  - Rótulo atribuído a informação.
  - Conteúdo X Público que terá acesso.

- **Empresas:**
  - **Confidencial**
  - **Privada**
  - **Sigilosa**
  - **Pública**

- **Governo/militar:**
  - **Ultra Secreta**
  - **Secreta**
  - **Confidencial**
  - **Reservada**
  - **Não Classificada**

Política de Segurança da Informação

Classificação da Informação

- Prazo de validade da classificação.
  - Estabelecido pelas normas.
- Em geral, quanto maior o sigilo, maior a duração.
- Critérios
  - Valor da Informação
  - Consequência do vazamento dessa informação
  - Consequência da modificação indevida dessa informação
- Revisão da classificação

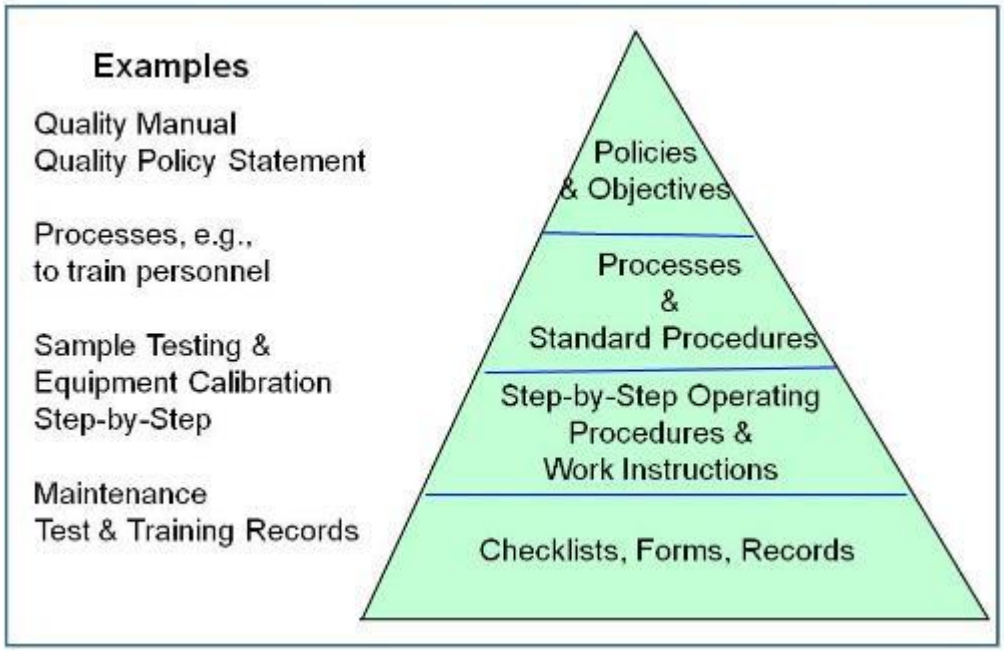
Política de Segurança da Informação

Classificação da Informação

- Proprietário da Informação
  - Normalmente o responsável por atribuir os níveis de classificação.
- Custodiante
  - É aquele que zela pelo armazenamento e preservação de informações que não lhe pertencem.
- Equipe de segurança
  - Responsável por desenvolver, implementar e monitorar estratégias de segurança que atendam aos objetivos da organização.
- Gerente de usuários
  - Reponde pela ação dos usuários;
  - Responsável por solicitar, transferir e revogar as permissões de acesso para os seus funcionários.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Políticas de Segurança



Política de Segurança da Informação

Fases do Processo de Implantação

- ✓ Identificação dos recursos críticos.
- ✓ Classificação das informações.
- ✓ Definição, em linhas gerais, dos objetivos de segurança a serem atingidos.
- ✓ Análise das necessidades de segurança (identificação das possíveis ameaças, análise de riscos e impactos).
- ✓ Elaboração de proposta de política.
- ✓ Discussões abertas com os envolvidos.
- ✓ Apresentação de documento formal à gerência superior.
- ✓ Aprovação.
- ✓ Implementação.
- ✓ Avaliação da política e identificação das mudanças necessárias.
- ✓ Revisão.

SGSI – Sistema de Gestão da Segurança da Informação

Sistema de Gestão

- **Definição**: um **sistema** de gestão é um sistema para estabelecer política e objetivos, e para atingir estes objetivos utilizando:
  - A estrutura organizacional;
  - Processos sistemáticos e recursos associados;
  - Metodologia de medição e avaliação;
  - Processo de análise crítica para assegurar que os problemas são corrigidos e as oportunidades de melhoria são identificadas e implementadas quando necessário.

SGSI – Sistema de Gestão da Segurança da Informação

Elementos de um Sistema de Gestão

- Política (demonstração de compromisso).
- Planejamento (identificação das necessidades, recursos, estrutura e responsabilidades).
- Implementação e operação (construção da consciência organizacional e treinamento).
- Avaliação de desempenho (monitoramento e medição, auditoria e tratamento de não conformidades).
- Melhoria (ação preventiva e corretiva, melhoria contínua).
- Análise crítica pela direção.

SGSI – Sistema de Gestão da Segurança da Informação

- A norma ISO 27001 foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um SGSI.
- A adoção de um SGSI deve ser estratégico para a organização.
- Projeto e implementação: devem ser escalados conforme as necessidades da organização. Uma situação simples requer uma solução simples.
- Espera-se que o SGSI mude com o tempo.

O que é a ISO?

- ✓ ISO é o nome usual com o qual é conhecida a International Organization for Standardization (Organização Internacional de Padronização).

- ✓ É uma entidade fundada em 1947, sediada na Suiça. Congrega organismos de normalização nacionais, cuja principal atividade é a de elaborar padrões para especificações e métodos de trabalho nas mais diversas áreas da sociedade, exceto no setor eletro-eletrônico onde a responsabilidade fica a cargo da International Electrotechical Comission (IEC).

- ✓ O Brasil é representado na ISO através da ABNT - Associação Brasileira de Normas Técnicas.

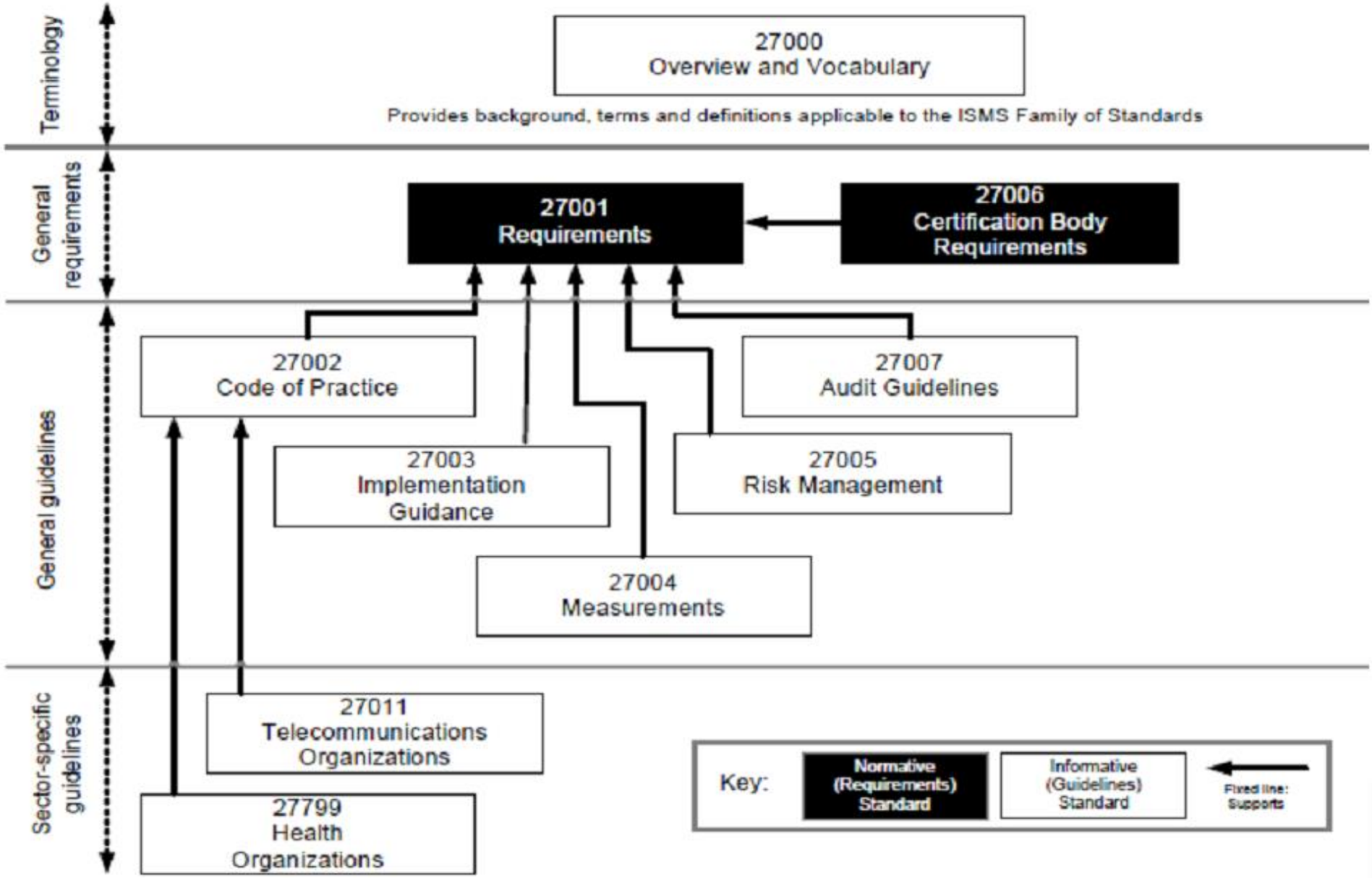
SGSI – Sistema de Gestão da Segurança da Informação

Compatibilidade com outros sistemas de gestão

- **ISO 27001 – Gestão de Segurança da Informação é alinhada com**

  - ✓ **ISO 9001 – Gestão da Qualidade**
  - ✓ **ISO 14001 – Gestão do Meio Ambiente.**
  - ✓ **OSHAS 18001 – Gestão da Saúde e Segurança do Trabalhador.**

IMPORTANTE: possível adaptação a sistemas já existentes na organização


Terminology
27000
Overview and Vocabulary
Provides background, terms and definitions applicable to the ISMS Family of Standards
General requirements
27001
Requirements
27006
Certification Body
Requirements
General guidelines
27002
Code of Practice
27007
Audit Guidelines
27003
Implementation
Guidance
27005
Risk Management
27004
Measurements
Sector-specific guidelines
27011
Telecommunications
Organizations
27799
Health
Organizations
Key:
Normative
(Requirements)
Standard
Informative
(Guidelines)
Standard
Fixed line:
supports

ISO 27001

- ✓ **ISO 27001**: referência da implantação de Processos de Gestão de Segurança da Informação, publicada inicialmente em Outubro de 2005.

- ✓ Esta norma veio tornar padrão internacional o que havia sido desenvolvido e publicado pela entidade normativa inglesa BSI (British Standard Institution), com o designação de BS7799-2.

- ✓ A norma ISO/IEC 27001 (Information Technology - Information Security Management Systems - Requirements) trata da implantação de um Processos de Gestão de Segurança da Informação (ISMS - Information Security Management Systems). Esta norma em conjunto com a ISO/IEC 17799 (Código de Boas Práticas da Gestão de Segurança da Informação) são as principais referências, atualmente, para a quem procura tratar a questão da segurança da informação de maneira eficiente e com eficácia.

ISO 27001 é

- Uma metodologia estruturada reconhecida internacionalmente dedicada a segurança da informação
- Um processo definido para validar, implementar, manter e gerenciar a segurança da informação
- Um grupo detalhado de controles compreendidos das melhores práticas de segurança da informação
- Desenvolvido pelas empresas para as empresas

ISO 27001 não é

- Um padrão técnico
- Um produto ou tecnologia dirigida
- Uma metodologia de avaliação de equipamentos
- Mas pode exigir a utilização de Níveis de Garantia dos Equipamentos

O que é a NBR?

- ✓ Normas nacionais são normas técnicas estabelecidas por um organismo nacional de normalização para aplicação num dado país. No Brasil, as normas brasileiras (NBR) são elaboradas pela ABNT , e em cada país, normalmente, existe um organismo nacional de normalização.

- ✓ A ABNT é reconhecida pelo Estado brasileiro como o Fórum Nacional de Normalização, o que significa que as normas elaboradas pela ABNT - as NBR - são reconhecidas formalmente como as normas brasileiras.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Família ISO 27000

Família 27000		
Número	Ano	Descrição
27000	ABNT: 2012	Fundamentos e vocabulário
27001	ABNT: 2013	Requisitos para um SGSI
27002	ABNT: 2013	Código de pratica para a gestão de segurança da informação
27003	ABNT: 2015	Guia de implementação
27004	ABNT: 2017	Métricas e medidas
27005	ABNT: 2011	Gestão de riscos
27006	ISO: 2007	Requisitos de acreditação para a certificação
27007	ABNT: 2018	Orientações para gestão de auditorias
27008	Em desenv.	Orientações para auditores
27011	ABNT: 2009	Técnicas de segurança - Diretrizes para gestão da segurança da informação para organizações de telecomunicações baseadas na ABNT NBR ISO/IEC 27002
27037	ABNT: 2013	Identificação, coleta, aquisição e preservação de Evidência Digital.
Outras normas não publicadas no Brasil e/ou em fase de desenvolvimento: 27010, 27031, 27032, 27033-X, 27034-X, 27036.		

Fixação

- Uma Política de Segurança deve estar ALINHADA com os objetivos do **Negócio**, a **Estratégia** e a **Cultura** da organização. Deve estabelecer os **Papéis** e **Responsabilidades** de todos com relação à segurança da informação na organização. Entre seus objetivos, o mais importante é prover uma **Orientação da Direção** e o apoio para a SegInfo, de acordo com os objetivos do **Negócio** e com a **Legislação** vigente.
- A SegInfo deve ser desenvolvida para proteger a informação durante todo o seu **Ciclo** de vida, que é: **Manipulação**, **Armazenamento**, **Transporte** e **Descarte**.
- Para se determinar o nível de proteção necessária, faz-se a **Classificação** da informação. Nela, para cada "rótulo" define-se uma proteção específica.
- A ISO **27001:2013**, responsável pela definição de requisitos para um **Sistema** de gestão da SegInfo, é desenhado sobre um ciclo **PDCA** (Demming).