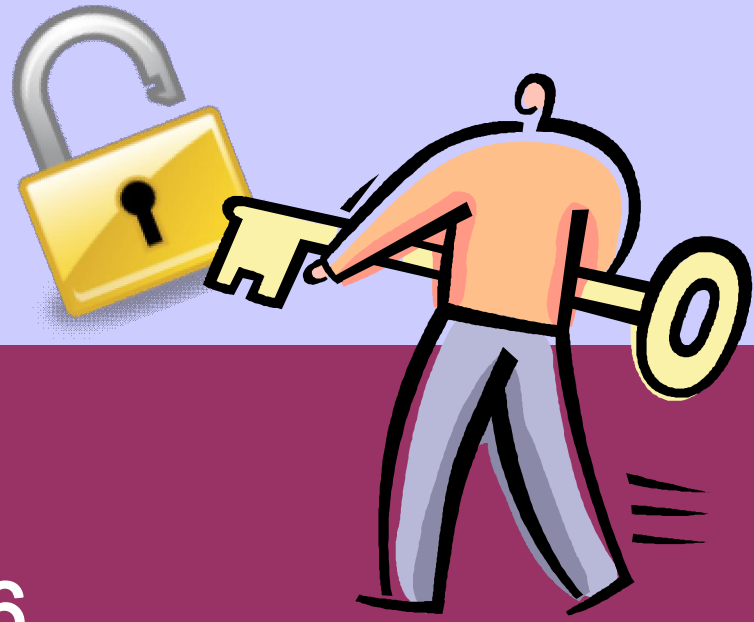
TI.exames

EDUCAÇÃO E TREINAMENTO
PARA ALAVANCAR A SUA CARREIRA

Curso e- Learning

Sistema de Gestão de Segurança da Informação



Interpretação da norma NBR ISO/IEC 27001:2006

Objetivos do Curso

Este curso é dirigido a todos os profissionais que querem conhecer os requisitos da norma NBR ISO/IEC 27001:2006 e adquirir os conhecimentos necessários para implantar e manter um sistema de gestão de segurança da informação adequado e eficaz, conforme os requisitos desta norma.

Durante este curso iremos:

- Entender a organização ISO
- Conhecer dados de certificações no Brasil e no mundo
- Conhecer a evolução das normas de Sistemas de Gestão de Segurança da Informação
- Aprender que a série NBR ISO/IEC 27001 é composta de 2 normas: NBR ISO/IEC 27001 e NBR ISO/IEC 27002 e qual seu conteúdo
- Compreender e manejar princípios, requisitos e controles da norma NBR ISO/IEC 27001
- Entender o objetivo da NBR ISO/IEC 27002
- Entender o processo de certificação
- Colocar em prática os conceitos apresentados

Conteúdo Programático

MÓDULO 1	▪Visão Geral da Organização ISO ▪Visão Geral das normas NBR ISO/IEC 27001 e NBR ISO/IEC 27002
MÓDULO 2	▪Conceitos: informação, segurança da informação, ativos,confidencialidade, integridade, disponibilidade, vulnerabilidades, ameaças, impactos, probabilidade
MÓDULO 3	▪Conceitos: riscos de segurança, processos de avaliação e tratamento do risco, sistema de gestão, sistema de gestão de segurança da informação
MÓDULO 4	▪Interpretação das cláusulas: 0, 1, 2, 3 da NBR ISO/IEC 27001:2006
MÓDULO 5	▪Interpretação das cláusulas: 4 /4.1, 4.2/ 4.2.1, 4.2.2, da NBR ISO/IEC 27001:2006
MÓDULO 6	▪Interpretação das cláusulas: 4.2.3, 4.2.4, 4.3/ 4.3.1, 4.3.2, 4.3.3 da NBR ISO/IEC 27001:2006
MÓDULO 7	▪Interpretação das cláusulas: 5, 6, 7 e 8 da NBR ISO/IEC 27001:2006
MÓDULO 8	▪Visão Geral do Anexo A - objetivos de controle e controles ▪Anexo A - Controles detalhados do A5 ao A9
MÓDULO 9	▪Anexo A - Controles detalhados do A10 ao A12
MÓDULO 10	Anexo A - Controles detalhados do A13 ao A15 Processo de certificação ISO 27001 para empresa

Módulo 1

Visão geral da organização ISO e das normas NBR ISO/IEC 27001 e NBR ISO/IEC 27002

O que é a organização ISO?

International Organization for Standardization

- A ISO - “International Organization for Standardization” é uma organização sediada em Genebra, na Suiça. Foi fundada em 1946.
- A sigla ISO foi originada da palavra isonomia.
- O propósito da ISO é desenvolver e promover normas que possam ser utilizadas igualmente por todos os países do mundo.
- Cerca de 111 países integram esta importante organização internacional, especializada em padronização, cujos membros são entidades normativas de âmbito nacional. O Brasil é representado pela Associação Brasileira de Normas Técnicas – ABNT.

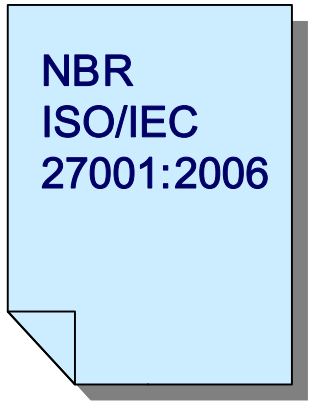
Hoje no Brasil quais são as normas para Sistemas de Segurança da Informação?

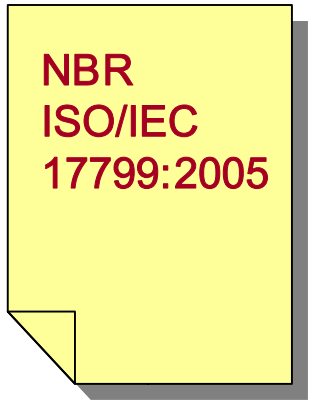
As Normas para segurança da informação foram adotadas e traduzidas pela ABNT recebendo a denominação de:

- NBR ISO/IEC 27001:2006 – Tecnologia da Informação – Técnicas de Segurança – Sistema de Gestão de Segurança da Informação - Requisitos e
- NBR ISO/IEC 17799:2005 - Tecnologia da Informação – Técnicas de Segurança – Código de Prática para Gestão de Segurança da Informação,

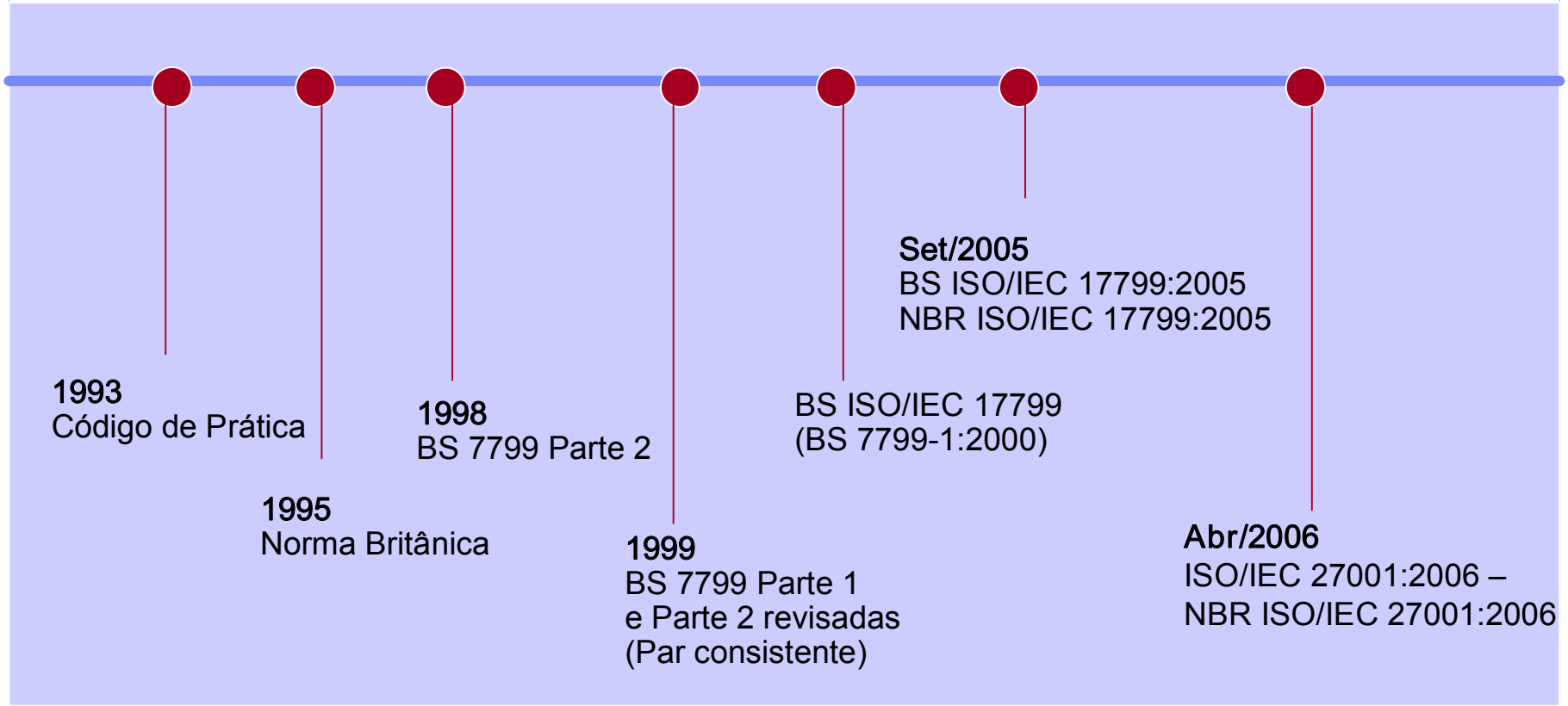
as quais neste treinamento, serão tratadas respectivamente por ISO 27001 e ISO 17799.

A norma ISO 27001 refere-se à quais requisitos de sistemas de gestão da informação devem ser implementados pela organização e a ISO 17799 é um guia que orienta a utilização de controles de segurança da informação. Estas normas são genéricas por natureza.





História das normas ISO 27001:2006 e da 17799:2005



Não existem praticamente diferenças entre a ISO/IEC 27001 e a BS 7799-2

ISO/IEC 17799:2005 – Código de Prática para SGSI

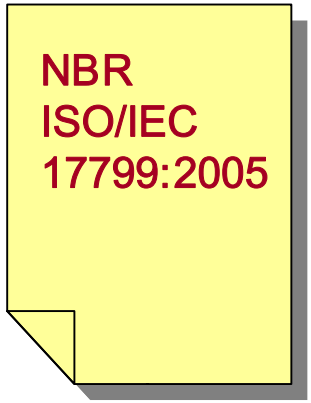
ISO/IEC 17799:2005 "Tecnologia da Informação – Técnicas de Segurança - Código de Prática para o Gestão da Segurança da Informação"

NBR ISO/IEC 17799:2005

- Baseada na BS 7799-1:1999
- Utilização como documento de referência
- Fornece um conjunto completo de controles de segurança
- Baseado nas melhores práticas de segurança da informação
- Consiste em 11 capítulos (mais um capítulo introdutório sobre avaliação e tratamento de risco), 39 objetivos de controle e 133 controles
- **Não pode ser usada em auditorias e certificações**

Situação atual e estrutura da ISO 17799

- Revisada em Junho de 2005
- Modificações estruturais
- Mesmo modelo de Objetivos de Controle/Controles
- Novo capítulo: Gestão de Incidentes de Segurança da Informação
- 17 controles novos
- Alguns controles antigos foram re-posicionados e/ou retirados
- 11 cláusulas de controle de segurança de A5 a A15 e 133 controles
- 1 cláusula introdutória: Introdução à avaliação e tratamento do risco



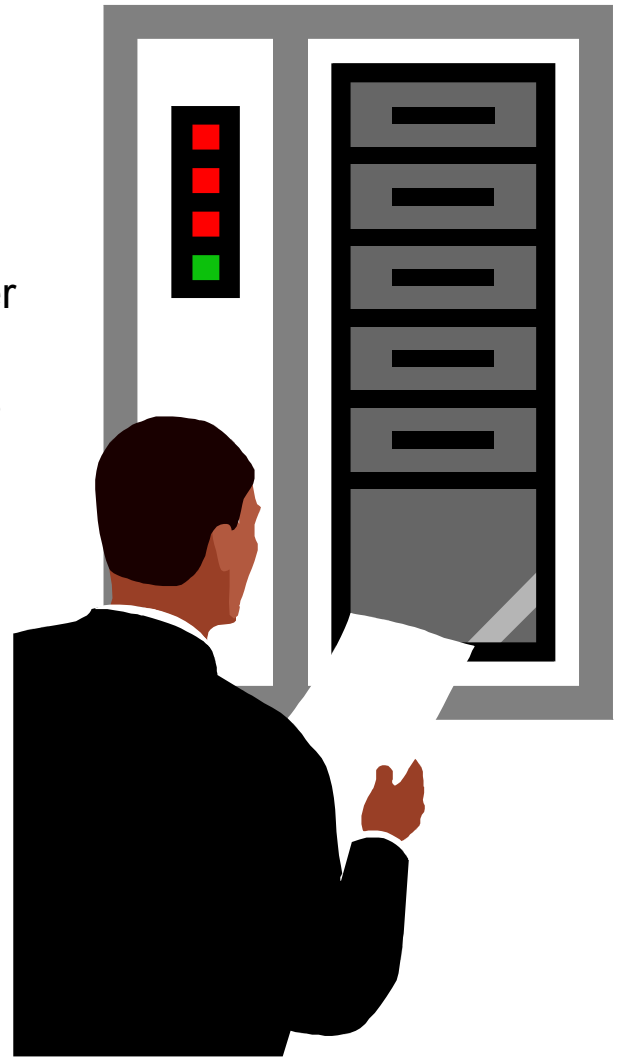
A ISO 17779 e a ISO 27001

São

- Uma metodologia estruturada reconhecida internacionalmente, dedicada a segurança da informação
- Um processo definido para avaliar, implementar, manter e gerenciar a segurança da informação
- Um grupo completo de controles contendo as melhores práticas para segurança da informação
- Desenvolvidas por empresas para empresas

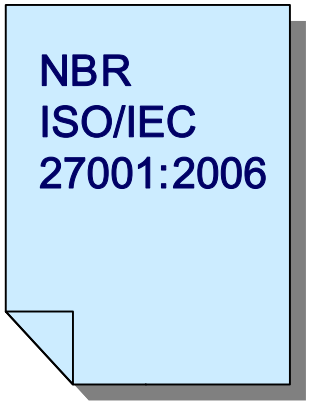
Não são

- Normas técnicas
- Dirigidas para produtos ou tecnologia
- Uma metodologia para avaliação de equipamentos



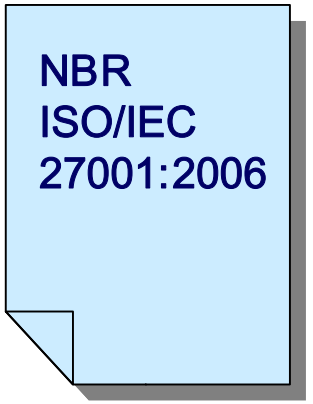
A ISO 17799 e a ISO 27001

- A ISO 17799 (atual ISO 27002) define as melhores práticas para a gestão da segurança da informação
- A ISO 27001 considera: **segurança física, técnica, procedimental e em pessoas**
- Sem um Sistema de Gestão da Segurança da Informação formal, existe um grande risco da segurança ser quebrada
- A segurança da informação é um processo de gestão, não é um processo tecnológico
- A ISO 27001 é a única norma internacional que pode ser auditada por uma terceira parte



Visão Geral da ISO 27001

- Incorpora um processo de escalonamento de risco e valorização de ativos
- O grau em que o sistema é formal e contém processos estruturados irá facilitar a replicação do sistema de um local para outro
- O investimento no compromisso da direção e em treinamento dos funcionários reduz a probabilidade de ameaças bem sucedidas
- A infra-estrutura (sistemas de gestão e processos) pode ser desenvolvida centralmente e então desdobrada globalmente
- Controles adicionais podem ser incorporados ao SGSI se assim for desejado



Razões para se adotar as ISO 17799 e 27001

- Governança Corporativa
- Melhoria da eficácia da Segurança da Informação
- Diferencial de mercado
- Atender os requisitos de partes interessadas e dos clientes
- Única norma com aceitação global
- Redução potencial no valor do seguro
- Focada nas responsabilidades dos funcionários
- A norma cobre TI bem como a organização, pessoal e instalações
- Conformidade com as legislações

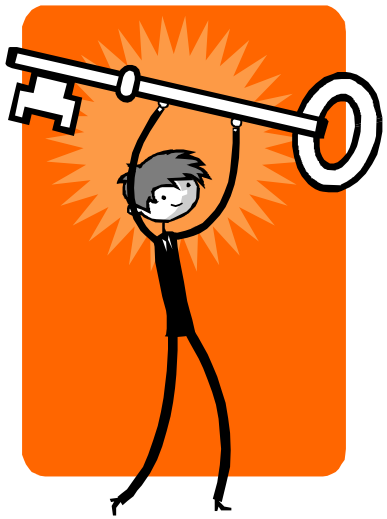
Dificuldades para Implementação de um SGSI

- Dificuldade na definição do escopo
- Dificuldade para desenvolver uma abordagem sistemática simples e clara para a Gestão de Risco
- Mesmo existindo Planos de Continuidade de Negócio, raramente eles são testados de alguma forma
- Designação da área de TI como responsável por desenvolver o projeto
- Falta de visão e “mente aberta” ao estabelecer os parâmetros dos controles identificados na norma
- Falta de ação para identificar e usar controles fora da norma
- Limitação de orçamento

Benefícios da Implementação da ISO 27001

- Reduz o risco de responsabilidade pela não implementação ou determinação de políticas e procedimentos
- Oportunidade de identificar e corrigir pontos fracos
- A alta direção assume a responsabilidade pela segurança da informação
- Permite revisão independente do sistema de gestão da segurança da informação
- Oferece confiança aos parceiros comerciais, partes interessadas, e clientes
- Melhor conscientização sobre segurança
- Combina recursos com outros Sistemas de Gestão
- Mecanismo para se medir o sucesso do sistema

A meta da NBR ISO/IEC 17799:2005 e da NBR ISO/IEC 27001:2006



Salvaguardar a *confidencialidade*, *integridade* e *disponibilidade* da informação escrita, falada e eletrônica.

Outros documentos

Série ISO/IEC 27000:

- ISO/IEC 27002
- ISO/IEC 27003
- ISO/IEC 27004
- ISO/IEC 27005
- ISO/IEC 27006

Você poderá consultar as normas disponíveis para aquisição no site www.abntnet.com.br

Outros Documentos

Publicações da BSI:

- PD 3001 – Preparação para a certificação ISO 27001
- PD 3002 – Guia para Avaliação de Risco
- PD 3003 – “Você está pronto para a auditoria ISO 27001?”
- PD 3004 – Guia para a implementação e auditoria ISO 27001
- PD 3005 – Guia para a seleção de controles da ISO 27001

Tecnologia da Informação – Diretrizes para a Gestão da Segurança em TI

- ISO/IEC 13335-1: Conceitos e modelos para a Segurança em TI
- ISO/IEC 13335-2: Gestão e planejamento da Segurança em TI
- ISO/IEC 13335-3: Avaliação de Risco
- ISO/IEC 13335-4: Seleção de Controles
- ISO/IEC 13335-5: Segurança em Redes

ISO/TR 13569 - Serviços bancários e financeiros - Diretrizes para a Segurança da Informação - 2ª edição 1997

BS 7858:1996 - Seleção de Segurança dos funcionários em um ambiente seguro

Consulte no site www.bsibrasil.com.br

Certificação ISO 27001- Alguns Dados Mundiais

Japan	1910*	Austria	11	Pakistan	2
UK	326	Saudi Arabia	9	Romania	2
India	279	Philippines	8	Slovak Republic	2
Taiwan	124	Spain	8	South Africa	2
Germany	74	Sweden	8	Sri Lanka	2
Hungary	57	Iceland	7	Armenia	1
Korea	49	UAE	7	Bulgaria	1
China	47	Greece	5	Gibraltar	1
USA	47	Kuwait	5	Egypt	1
Italy	42	Russian Federation	5	Lebanon	1
Netherlands	31	Thailand	4	Lithuania	1
Singapore	28	Argentina	3	Luxemburg	1

Certificação ISO 27001- Alguns Dados Mundiais

Hong Kong	25	Croatia	3	Macedonia	1
Australia	22	France	3	Moldova	1
Malaysia	19	Indonesia	3	Morocco	1
Ireland	17	Isle of Man	3	New Zealand	1
Poland	17	Macau	3	Peru	1
Brazil	15	Slovenia	3	Qatar	1
Czech Republic	15	Bahrain	2	Serbia and Montenegro	1
Switzerland	15	Belgium	2	Ukraine	1
Finland	14	Canada	2	Uruguay	1
Norway	14	Colombia	2	Vietnam	1
Turkey	13	Denmark	2	Relative Total	3363
Mexico	12	Oman	2	Absolute Total	3350*

Dados atualizados podem ser obtidos no site:
http://www.iso27001certificates.com

Exercício

Indique se é Verdadeiro ou Falso:

1-( ) A ISO 27001 combina recursos com outros Sistemas de Gestão, isto é, se a organização já é certificada na ISO 9001 o sistema de gestão de segurança da informação poderá utilizar processos já implantados pela ISO 9001.

2-( ) A disponibilidade de recursos é uma das dificuldades para implantação do SGSI.

3-( ) Atender os requisitos de partes interessadas e dos clientes pode ser uma das razões para se implantar um SGSI.

4-( ) A ISO 27001 não é uma metodologia estruturada reconhecida internacionalmente.

5-( ) Uma grande vantagem da ISO 27001 é ela considerar: segurança física, técnica, procedimental e em pessoas, normalmente os sistemas de gestão utilizados sem a orientação da ISO 27001 priorizam segurança técnica e física.

6-( ) Durante a identificação dos controles a serem utilizados no sistema basta considerar os controles especificados pela norma.

7-( ) A ISO 27001 não pode ser utilizada para certificação.

8-( ) A ISO 27001 apresenta requisitos de sistema e é utilizada como padrão para a realização de auditorias de certificação. A 17799 é um código de prática que deve ser utilizado para orientação durante o desenvolvimento e implantação do sistema de gestão de segurança da informação.

9-( ) A ISO 17799 apresenta 11 cláusulas de controle de segurança de A5 a A15 e 133 controles, os quais estão resumidos no anexo A da ISO 27001.

Respostas do exercício

Indique se é Verdadeiro ou Falso:

1-(V) A ISO 27001 combina recursos com outros Sistemas de Gestão, isto é, se a organização já é certificada na ISO 9001 o sistema de gestão de segurança da informação poderá utilizar processos já implantados pela ISO 9001. (por exemplo controle de documentos, registros, auditorias internas, ações corretivas e preventivas etc.)

2-(V) A disponibilidade de recursos é uma das dificuldades para implantação do SGSI.

3-(V) Atender os requisitos de partes interessadas e dos clientes pode ser uma das razões para se implantar um SGSI.

4-(F) A ISO 27001 não é uma metodologia estruturada reconhecida internacionalmente.

5-(V) Uma grande vantagem da ISO 27001 é ela considerar: segurança física, técnica, procedimental e em pessoas, normalmente os sistemas de gestão utilizados sem a orientação da ISO 27001 priorizam segurança técnica e física.

6-(F) Durante a identificação dos controles a serem utilizados no sistema basta considerar os controles especificados pela norma. (a norma orienta que os controles a serem implantados não devem se limitar aos controles apresentados)

7-(F) A ISO 27001 não pode ser utilizada para certificação. (a ISO 17799 é que não pode)

8-(V) A ISO 27001 apresenta requisitos de sistema e é utlizada como padrão para a realização de auditorias de certificação. A 17799 é um código de prática que deve ser utilizado para orientação durante o desenvolvimento e implantação do sistema de gestão de segurança da informação.

9-(V) A ISO 17799 apresenta 11 cláusulas de controle de segurança de A5 a A15 e 133 controles, os quais estão resumidos no anexo A da ISO 27001.

Fim do Módulo 1

Visão geral da organização ISO e
das normas NBR ISO/IEC 27001
e NBR ISO/IEC 17799