Descrição

A importância e a adoção de normas técnicas para o estabelecimento, implementação, manutenção e melhoria de um Sistema de Gestão da Segurança da Informação (SGSI) em uma organização, e a seleção de controles inserida no processo de implementação de um SGSI.

Propósito

Apresentar as normas reconhecidas internacionalmente como referências para o estabelecimento e a implementação de um Sistema de Gestão da Segurança da Informação.

Objetivos

Módulo 1

Finalidades e benefícios das normas ISO/IEC 27001 e 27002

Reconhecer as finalidades e os benefícios da adoção das normas ISO/IEC 27001 e 27002.

Acessar módulo

Módulo 2

Aplicações das normas ISO/IEC 27001 e ISO/IEC 27002

Identificar as aplicações das normas ISO/IEC 27001 e ISO/IEC 27002.

Acessar módulo

Introdução

O Sistema de Segurança da Informação (SGSI) é de extrema importância para a sustentabilidade e longevidade de uma organização, especialmente no contexto do mundo atual em que vivemos, que foca na digitalização das informações e na transformação digital.

Apesar de as organizações já terem uma consciência bem consolidada de importância de cuidar das seguranças das informações internas, bem como das externas por ela gerenciadas, há por vezes dúvidas com relação à melhor forma de se garantir a segurança dos dados. As normas de segurança da informação vêm justamente atender a essa lacuna, propondo padrões a serem seguidos que auxiliam a organização no estabelecimento, implantação, manutenção de um SGSI. Ao longo do material, detalhamos a finalidade, os benefícios e a aplicação da principal família de normas de segurança da informação: ISO/IEC 27000.

Finalidades e benefícios das normas ISO/IEC 27001 e 27002

Vídeos

Ao final deste módulo, você será capaz de reconhecer as finalidades e os benefícios da adoção das normas ISO/IEC 27

Conceito

Normas ISO e Segurança da Informação

A ISO - *International Organization for Standardization* (Organização Internacional de Padronização) é uma entidade fundada em 1947, sediada na Suíça e que congrega organismos de normalização nacionais.

> Sua principal atividade é elaborar padrões para especificações e métodos de trabalho nas mais diversas áreas da sociedade.

A ISO colabora estreitamente com a *International Electrotechnical Commission* (IEC) em todos os assuntos de padronização eletrotécnica. As normas internacionais para sistemas de gerenciamento fornecem um modelo a ser seguido para a configuração e operação de um sistema de gerenciamento.

Por meio do uso da família de padrões de um Sistema de Gestão da Segurança da Informação - SGSI (do inglês *Information Security Management System* – ISMS), torna-se possível o desenvolvimento e a implementação de uma estrutura visando à gerência da segurança dos ativos de informações.

Dentre outros documentos que eventualmente podem existir, a família ISO/IEC 27000 oferece um conjunto de normas relacionadas à Segurança da Informação.

Saiba mais

A Norma ISO/IEC 27000 traz os princípios e o vocabulário utilizados nas normas seguintes da família 27000. O download pode ser feito gratuitamente (em inglês) na página da ISO.

De acordo com a ABNT NBR ISO/IEC 27001:2013:

A Norma ISO/IEC 27001 (*Information Technology - Information Security Management Systems - Requirements* foi preparada para prover requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI).

> Cabe à alta direção de cada organização decidir pela adoção de um Sistema de Gestão da Segurança da Informação (SGSI).

A norma cita alguns fatores de influência para o seu estabelecimento e a sua implementação, como:

1. Necessidades;
2. Objetivos;
3. Requisitos de segurança;
4. Processos organizacionais;
5. Tamanho e estrutura da organização.

O SGSI **preserva a tríade CID** (confidencialidade, integridade e disponibilidade) da informação, aplicando um **processo de gestão de riscos**. Com isso, as partes interessadas (*stakeholders*) poderão ter uma maior confiança de que os riscos serão convenientemente gerenciados.

Segundo a ABNT (2013), é importante que um SGSI seja parte, e esteja integrado com os **processos da organização** e com a estrutura de **administração global**, e que a segurança da informação seja considerada no projeto dos processos, sistemas de informação e controles.

> **A Norma ISO/IEC 27001, em conjunto com a Norma ISO/IEC 27002 (Código de Boas Práticas da Gestão da Segurança da Informação), formam as principais referências, atualmente, para quem procura tratar a questão da segurança da informação de maneira eficiente e com eficácia.**

As normas técnicas nacionais são estabelecidas por um organismo nacional de normalização para aplicação em um dado país. No Brasil, as Normas Brasileiras (NBRs) são elaboradas pela ABNT (Associação Brasileira de Normas Técnicas).

Atenção!

A ABNT é reconhecida pelo Estado brasileiro como o Fórum Nacional de Normalização, e as NBRs são reconhecidas formalmente como as normas brasileiras.

As nomenclaturas das normas ISO/IEC 27001 e 27002 são, respectivamente, **ABNT NBR ISO/IEC 27001** e **ABNT NBR ISO/IEC 27002**.

Ao longo do texto, podem ser consideradas tanto as normas brasileiras quanto as normas ISO, mas as NBRs são idênticas às normas ISO, sendo possível fazer referência a ambas sem prejuízo no contexto do conteúdo e no entendimento. Observe, a seguir, sobre o que a Norma ISO/IEC 27001 é e não é.

A Norma ISO/IEC 27001 é: Vídeos

A Norma ISO/IEC 27001 não é:

A versão mais atual da norma (até a escrita desse texto) a ser considerada nesse texto é a ISO/IEC 27001: 2013, que sucede e substitui a versão de 2005.

Uma grande novidade dela é o alinhamento com as diretrizes do **Anexo L**, chamado até 2019 de Anexo SL (conhecido antigamente como ISO Guide 83).

> **O Anexo L é uma seção da ISO/IEC *Directives*, Part 1, *Consolidated ISO Supplement*, que padroniza definições e estruturas de diferentes sistemas de gestão ISO. Com isso, a norma está alinhada com outros padrões de sistemas de gestão, como ISO 9001, ISO 14000, ISO 20000, ISO 22000, ISO 22301.**

Na versão 2013 da Norma ISO/IEC 27001 houve o alinhamento com as diretrizes do Anexo L, que padroniza definições e estruturas de diferentes sistemas de gestão ISO. No Anexo L, todas as normas de sistema de gestão do futuro terão a **mesma estrutura de alto nível** (tabela 1), **texto principal idêntico**, bem como **termos e definições comuns**.

Atenção!

A estrutura de alto nível não pode ser modificada; por sua vez, podem ser acrescentadas subcláusulas e textos específicos para cada disciplina abordada.

Veja a tabela a seguir:

Cláusula 1:	Escopo
Cláusula 2:	Referência normativa
Cláusula 3:	Termos e definições
Cláusula 4:	Contexto da organização

Cláusula 5:	Liderança
Cláusula 6:	Planejamento
Cláusula 7:	Suporte
Cláusula 8:	Operação
Cláusula 9:	Avaliação de Desempenho
Cláusula 10:	Melhoria

Tabela 1: Estrutura geral de uma norma de gestão que segue as diretrizes do Anexo L.
Fabio Henrique Silva.

Cláusula 3 - Termos e definições

Confira agora sobre a Norma ABNT NBR ISO/IEC 27001:2013.

O ISO/IEC *Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO*, documento do qual o Anexo L faz parte, pode ser lido na página da ISO.

Requisitos

O que é a Norma ISO/IEC 27001

Estrutura geral da Norma ISO/IEC 27001

Conforme a ABNT NBR ISO/IEC 27001 (2013), o título da Norma **ABNT NBR ISO/IEC 27001:2013** é Sistemas de Gestão da Segurança da Informação – Requisitos.

> **Especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.**

Também inclui requisitos para a avaliação e o tratamento de riscos de segurança da informação voltados para a necessidade da organização.

A principal característica, ou palavra-chave, é: DEVE. O leitor observará que a norma sempre indicará o que o gestor deverá fazer em relação às cláusulas das disciplinas do SGSI. Por exemplo, em 4.3, a organização deve determinar os limites e a aplicabilidade do sistema de gestão da segurança da informação para estabelecer o seu escopo.

Para você que está começando a se familiarizar com a norma, uma boa maneira de ter uma noção geral dos conteúdos de normas é analisando o sumário e assimilando o que possuem as suas estruturas. A estrutura da Norma ABNT NBR ISO/IEC 27001:2013 pode ser conferida na tabela 2.

Algumas razões para adotar a norma incluem:

- Eficácia melhorada da Segurança da Informação.
- Diferenciação do mercado.
- Satisfazer exigências dos clientes.
- Único padrão com aceitação global.
- Responsabilidades focadas na equipe de trabalho.
- A Tecnologia da Informação cobre padrões tão bem quanto organização, pessoal e facilidades.
- Mandados e leis.

A Norma ISO/IEC 27001 é passível de certificação acreditada. Alguns **benefícios da certificação ISO/IEC 27001** incluem:

- Responsabilidade reduzida devido às políticas e aos procedimentos não implementados ou reforçados.
- Oportunidade de identificar e eliminar fraquezas.
- A gerência participa da Segurança da Informação.
- Revisão independente do seu SGSI.
- Fornece segurança a todas as partes interessadas.
- Melhor consciência da segurança.
- Une recursos com outros sistemas de gerenciamento.
- Mecanismo para medir o sucesso do sistema.

Certificados

Uma visão geral da situação dos certificados no mundo pode ser obtida através dos dados disponibilizados no *The ISO Survey of Certifications*.

Trata-se de uma pesquisa anual do número de certificados válidos para os padrões do sistema de gerenciamento ISO em todo o mundo. Os dados são fornecidos pelos organismos de certificação credenciados. Veja mais a seguir.

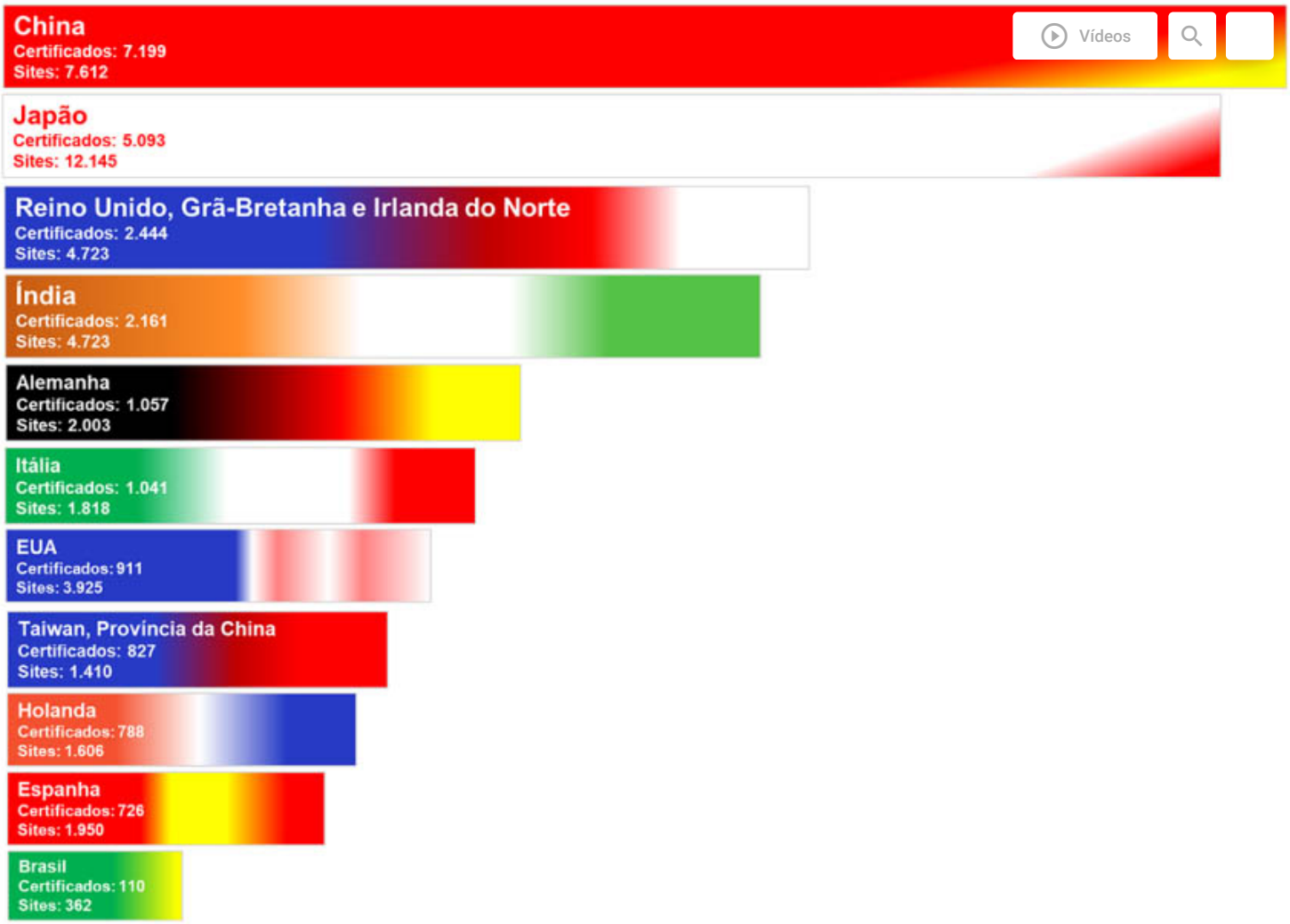
Certificado

É o documento emitido por um organismo de certificação.

Site

É um local permanente em que uma organização realiza trabalho ou serviço.

O conteúdo do gráfico, que você verá a seguir, foi extraído da planilha disponível na página da ISO. Ele exibe um trecho do **número total de certificados válidos** e o **número total de sites para o padrão ISO/IEC 27001:2013**.



Lista dos 10 países com maior número de certificados. O Brasil aparece na posição 39.

A **Norma ABNT NBR ISO/IEC 27002:2013** apresenta as **melhores práticas** a serem utilizadas na gestão da segurança da informação. Seu título é Código de Prática para a Gestão da Segurança da Informação. A sua principal característica, ou palavra-chave, como já foi explicado anteriormente, é: CONVÉM.

A versão mais atual da norma (até a escrita desse texto) a ser considerada neste tema é a ISO/IEC 27002:2013, que sucede e substitui a versão de 2005. No passado, era conhecida como ISO/IEC 17799.

Em comparação com a versão 2005, na versão 2013 o número de seções aumentou de **11** para 14.

> A versão 2013 recomenda 114 tipos de controles básicos.

Cada seção principal contém:

- Um objetivo do controle declarando o que se espera que seja alcançado.

- Um ou mais controles que podem ser aplicados para se alcançar o objetivo de controle.

As descrições do controle estão estruturadas da seguinte forma:

Controle

Diretrizes para implementação

Informações adicionais

A tabela 3 traz as principais seções da Norma ABNT NBR ISO/IEC 27002:2013. Note que os tópicos específicos abordados pela norma começam na seção 5.

Tendências

O estudo das normas técnicas não se limita apenas ao aprendizado dessas normas aqui apresentadas.

Um caminho que pode ser seguido é analisar também outras normas de sistemas de gestão, tais como: qualidade, meio ambiente, conhecimento, ativos, educação etc.

Vamos praticar alguns conceitos?

Vídeos

Questão 1

Qual palavra é citada frequentemente na Norma ISO/IEC 27001, que constitui sua característica marcante?

A Convém

B Recomenda

C Deve

D Espera

E Sugere

Responder

Questão 2

Marque a alternativa correta quanto à afirmação sobre a Norma ISO/IEC 27002.

A A palavra-chave que determina a sua principal característica é DEVE.

B A relevância de qualquer controle deve ser determinada segundo os riscos específicos a que uma organização está exposta.

C Todos os controles são importantes e devem ser considerados.

D Eventuais controles adicionais e recomendações que a comissão de segurança da organização deseja implementar, mas que não estejam incluídos na norma, devem ser desconsiderados.

E Controles são definidos por empresas especializadas.

Responder

★★★★★

2

Aplicações das normas ISO/IEC 27001 e ISO/IEC 27002

Ao final deste módulo, você será capaz de identificar as aplicações das normas ISO/IEC 27001 e ISO/IEC 27002.

Conceito

Requisitos da Norma ISO/IEC 27001

Benefícios da Norma ISO/IEC 27001

Como estamos supondo o início dos seus estudos nas normas, considere as seguintes **sugestões** e **premissas**:

- O enquadramento aos itens será realizado com fins didáticos, sem necessariamente levar em consideração ou conceituar termos que são utilizados no âmbito de um sistema de gestão.
- Leia cada descrição do estudo de caso como se estivesse ouvindo essas palavras diretamente da parte envolvida.
- Atenha-se apenas à descrição da cena, evite suposições sobre outros eventos que não estão descritos.
- Faça uso das estruturas das normas (tabelas 3 e 4) para facilitar a localização dos itens.
- Cada descrição do estudo de caso poderá ser enquadrada em mais de um item da norma e poderá haver outros itens não referenciados nesses exemplos.
- Faça suas análises somente com base nos itens da norma. Não utilize outros norteadores que não estejam escritos lá. Se a ocorrência descrita não se enquadrar em nada do que estiver escrito, considere que esta não precisa ser levada em consideração na análise.

O **segundo** exemplo é um estudo de caso para aplicação dos itens da Norma **ABNT NBR ISO/IEC 27002:2013**.

Leia, a seguir, uma notícia extraída de um site da web.

Notícia

- 9.4.1: Restrição de acesso à informação.
- 9.4.2: Procedimentos seguros de entrada no sistema (log-on).
- 9.4.3: Sistema de gerenciamento de senha.
- 9.4.4: Uso de programas utilitários privilegiados.
- 9.4.5: Controle de acesso ao código-fonte de programas.

Comentário

Como estamos trabalhando com a premissa de nos ater apenas à descrição da cena, e estamos analisando uma matéria jornalística (que carece de muitos detalhes), vamos considerar que o atacante poderá ter explorado qualquer uma das medidas de controle dos itens pertencentes ao item 9.4.

Exemplo de aplicação da Norma ISO/IEC 27001

Estudo de caso para aplicação dos itens da Norma ABNT NBR IS 27001:2013

Vídeos

Confira agora um estudo de caso para aplicação dos itens da Norma ABNT NBR ISO/IEC 27001:2013.

Falta pouco para atingir seus objetivos.

Vamos praticar alguns conceitos?

Questão 1

Continuando com o exemplo do estudo de caso para aplicação dos itens da Norma ABNT NBR ISO/IEC 27001:2013 da empresa de web hosting que busca a conformidade para o seu Sistema de Gestão de Segurança da Informação, e considerando as mesmas sugestões e premissas definidas no início dos conceitos deste módulo, veja a seguinte descrição da cena/ocorrência:

Cenas/Ocorrência	Registro de não conformidade (NC)		
	Req. ISO/IEC 27001	Existe NC?	Descrição da NC e da evidência objetiva ou indicação do que fazer a seguir
Um dos auditores internos é responsável pela administração do banco de dados em um setor. Como na auditoria metade da equipe da empresa viajou para treinamento do novo sistema, ele acabou auditando também a sua área, incluindo partes do seu trabalho.		( ) Sim ( ) Não ( ) Simples Obs. ( ) Falta informação	

Marque a alternativa que representa o parecer mais adequado do auditor para a descrição da cena.

A Existe não conformidade, os auditores não devem auditar seu próprio trabalho.

B A descrição é uma simples observação para uma descrição importante que ainda não foi feita.

C A prática está em conformidade com a norma, tendo em vista a possibilidade de a equipe ser pequena e o funcionário possuir competência para tal.

D Faltam as informações se esse fato estava previsto nos critérios dessa auditoria e se a imparcialidade foi assegurada.

E É preciso aprimorar a prática para se adequar à norma.

Vídeos

Responder

Questão 2

Leia a notícia a seguir extraída de um site da web, para aplicação dos itens da Norma ABNT NBR ISO/IEC 27002:2013:

Quando o Deutsche Bank perdeu seus escritórios nos ataques de 11 de setembro, os funcionários puderam acessar o e-mail corporativo no dia seguinte para que pudessem se conectar com clientes e colegas de trabalho em casa. "Tivemos acesso aos nossos arquivos, embora a TI estivesse na Torre Dois do World Trade Center", diz uma fonte. "Tivemos backup em Jersey City. Não perdemos nada. Tenho amigos que trabalham em empresas menores que não ficaram dois meses sem poder ir ao escritório. O escritório de advocacia de um amigo faliu" (DEUTSCHE BANK, 2009).

Este relato de adoção de medidas de proteção, nestes termos, poderá ser melhor enquadrado no item da Norma ISO/IEC 27002:2013.

A 7.1: Antes da contratação, dentro do item 7, *Segurança em Recursos Humanos*.

B 9.2: Gerenciamento de acesso do usuário, dentro do item 9, *Controle de Acesso*.

C 10.1: Controles criptográficos, dentro do item 10, *Criptografia*.

D 17.1: Continuidade da segurança da informação, dentro do item 17, *Aspectos da segurança da informação na Gestão da Continuidade do Negócio*.

E 9.4.1: Restrição de acesso à informação.

Responder

★★★★★

Considerações finais

As normas ISO/IEC 27001 e ISO/IEC 27002 fazem parte de um ecossistema de boas práticas em tecnologia da informação. Em um ambiente organizacional cada vez mais competitivo e alinhado com a conformidade em suas atividades, o processo para a adoção das normas, bem como de outros guias (por exemplo, ITIL, COBIT), está sendo uma estratégia necessária até para a própria sobrevivência, dependendo do contexto de suas atividades. E é nesse ambiente que o futuro profissional poderá continuamente se valorizar e se inserir.

Podcast

Ouça agora a importância e a aplicação das normas de Segurança da Informação.

00:00 05:27 1x

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT. **ABNT NBR ISO/IEC 27001:2013** – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. ABNT, 2013. Publicado em: 8 nov. 2013. Consultado na internet em: 5 maio 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT. **ABNT NBR ISO/IEC 27002:2013** – Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. ABNT, 2013. Publicado em: 8 nov. 2013. Consultado na internet em: 5 maio 2022.

DEUTSCHE BANK. **WetFeet Insider Guide Deutsche Bank**. Consultado na internet em: 5 maio 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIATION. ISO. **ISO/IEC 27000:2018**. Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO, 2018. Publicado em: fev. 2018. Consultado na internet em: 5 maio 2022.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a Internet** - Uma abordagem top-down. 5. ed. São Paulo: Pearson/Addison-Wesley, 2010.

LAUREANO, M. A. P. **Segurança da Informação**. Curitiba: Lt, 2012.

MACHADO, F. N. R. **Segurança da Informação** - Princípios e Controle de Ameaças - Série Eixos. São Paulo: Érica, 2014.

NAKAMURA, E. T.; GEUS, P. L. **Segurança de Redes em Ambientes Cooperativos**. Rio de Janeiro: Novatec, 2007.

SÊMULA, M. **Gestão da Segurança da Informação**: Uma Visão Executiva. São Paulo: ST, 2013.

STALLINGS, W. **Criptografia e segurança de redes** – Princípios e práticas. 4. ed. São Paulo: Pearson/Addison-Wesley, 2007.

ZMOGINSKI, F. **AT&T processa falsos clientes por roubo de dados**. Publicado em: 9 out. 2008. Consultado na internet em: 5 maio 2022.

Explore +

Para saber mais sobre os assuntos tratados neste conteúdo, procure na internet:

- Estudos de Caso ISO 27001 - *Segurança da Informação*, Intel.
- *ISO/IEC 27001 Information security management*, ISO.
- *ISO 27001 Information Security Management (ISMS)*, ISO.
- Tecnologia da informação — Técnicas de segurança — *Código de prática para controles de segurança da informação*, Norma Técnica ABNT NBR ISO/IEC 27001:2013, ABNT Catálogo.
- Tecnologia da informação — *Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos*, Norma Técnica ABNT NBR ISO/IEC 27001:2013, ABNT Catálogo.