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 implementação de um Sistema de Gestão da Segurança da Informação.

OBJETIVOS

MÓDULO 1

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

MÓDULO 2

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

MÓDULO 1

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

CONCEITO

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.

Foto: Shutterstock.com

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.

2

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).

★ IMPORTANTE

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, um comparativo sobre o que a norma ISO/IEC 27001 é e não é.

ISO/IEC 27001 É:

- Uma metodologia estruturada reconhecida internacionalmente dedicada à 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/IEC 27001 NÃO É:

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

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.

★ IMPORTANTE

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

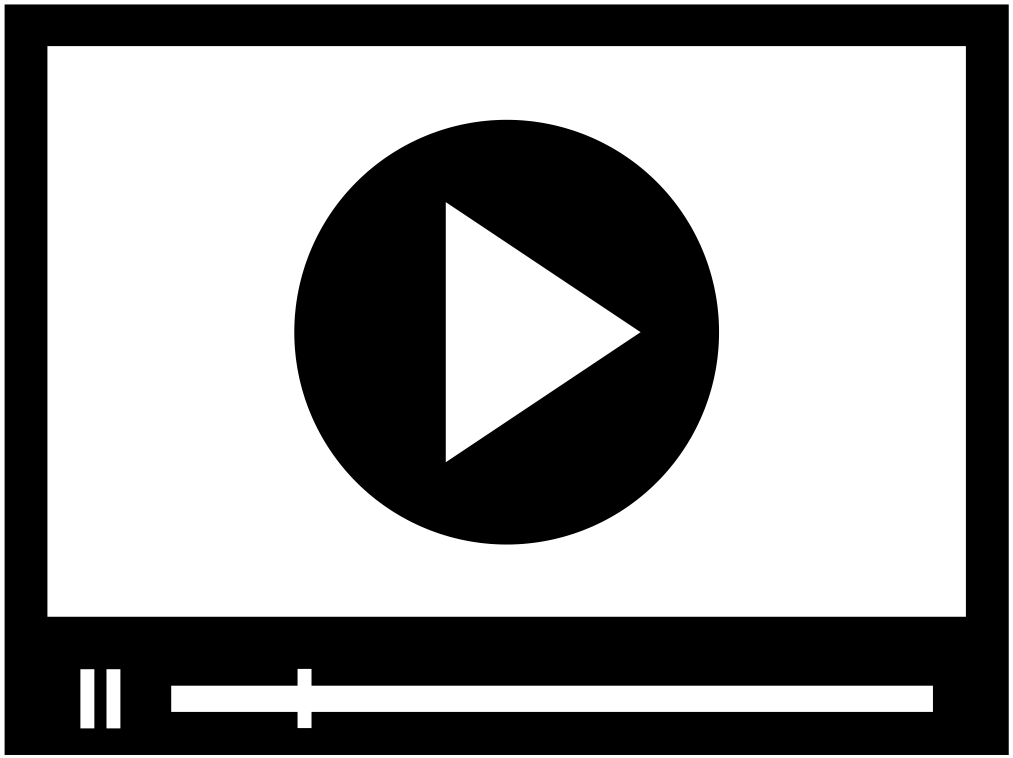
Cláusula 1:	Escopo
Cláusula 2:	**Referência normativa**
Cláusula 3:	**Termos e definições**
Cláusula 4:	**Contexto da organização**
Cláusula 5:	**Liderança**
Cláusula 6:	**Planejamento**

Cláusula 7:	**Suporte**
Cláusula 8:	**Operação**
Cláusula 9:	**Avaliação de Desempenho**
Cláusula 10:	**Melhoria**

Atenção! Para visualizaçãocompleta da tabela utilize a rolagem horizontal

Tabela 1 – Estrutura geral de uma norma de gestão que segue as diretrizes do Anexo L.

Elaborada por Fabio Henrique Silva.



Para entender mais sobre o assunto, assista ao vídeo abaixo.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.

SAIBA MAIS

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

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* .

1

Essa norma, então, 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.

2

3

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.

4

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 abaixo:

0	**Introdução**
0.1	**Geral**
0.2	**Compatibilidade com outras normas do sistema de gestão**

1	**Escopo**
2	**Referência normativa**
3	**Termos e definições**
4	**Contexto da organização**
4.1	**Entendendo a organização e seu contexto**
4.2	**Entendendo as necessidades e expectativas das partes interessadas**
4.3	**Determinando o escopo do sistema de gestão da segurança de informação**
4.4	**Sistema de Gestão da Segurança da Informação**
5	**Liderança**
5.1	**Liderança e comprometimento**

5.2	**Política**
5.3	**Autoridades, responsabilidades e papéis organizacionais**
6	**Planejamento**
6.1	**Ações para contemplar riscos e oportunidades**
6.1.1	**Geral**
6.1.2	**Avaliação de riscos de segurança da informação**
6.1.3	**Tratamento de riscos de segurança da informação**
6.2	**Objetivo de segurança da informação e planejamento para alcançá-los**
7	**Apoio**
7.1	**Recursos**
7.2	**Competência**

7.3	**Conscientização**
7.4	**Comunicação**
7.5	**Informação documentada**
7.5.1	**Geral**
7.5.2	**Criando e atualizando**
7.5.3	**Controle de informação documentada**
8	**Operação**
8.1	**Planejamento operacional e controle**
8.2	**Avaliação de riscos de segurança da informação**
8.3	**Tratamento de riscos de segurança da informação**

9	**Avaliação do desempenho**
9.1	**Monitoramento, medição, análise e avaliação**
9.2	**Auditoria interna**
9.3	**Análise crítica pela direção**
10	**Melhoria**
10.1	**Não conformidade e ação corretiva**
10.2	**Melhoria contínua**
Anexo A	**Referência aos controles e objetivos de controles**

Atenção! Para visualizaçãocompleta da tabela utilize a rolagem horizontal

Tabela: Estrutura da norma ABNT NBR ISO/IEC 27001:2013.

Elaborada por Fabio Henrique Silva.

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 a 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.

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.

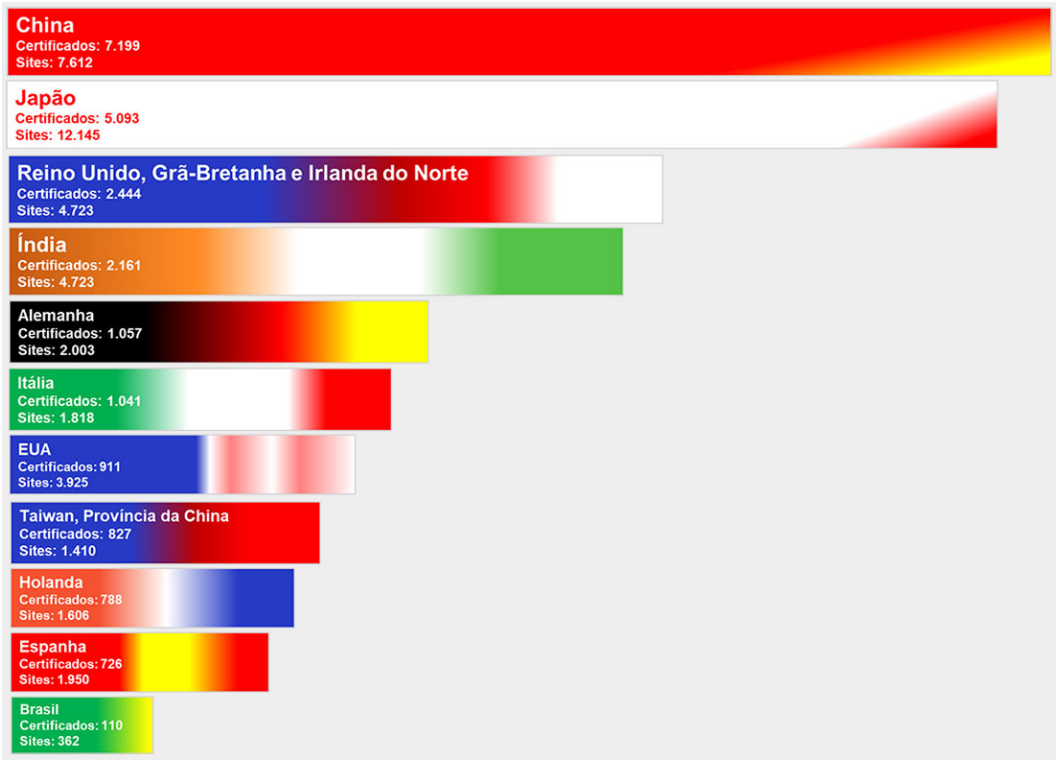


Imagem: The ISO Survey of Management System Standard Certifications 2018 – ISO/IEC 27001:2013. (ISO, 2020).

📷 **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

Define a declaração específica do controle, para atender ao objetivo de controle.

Segundo a ISO/IEC 27000 (2018), o controle é uma medida que pode modificar o risco, seja ele através de um processo, política, dispositivo, prática ou outras ações que modifiquem a ameaça e/ou a vulnerabilidade e, consequentemente, o risco.

DIRETRIZES PARA IMPLEMENTAÇÃO

Apresenta informações mais detalhadas para apoiar a implementação do controle e alcançar o objetivo do controle.

As diretrizes podem não ser totalmente adequadas ou suficientes em todas as situações e podem, portanto, não atender completamente aos requisitos de controle específicos de uma organização.

INFORMAÇÕES ADICIONAIS

Apresenta mais dados que podem ser considerados, como questões legais e referências normativas.

Se não existem informações adicionais, esta parte não é mostrada no controle.

A tabela abaixo traz as principais seções da norma ABNT NBR ISO/IEC 27002:2013.

Note que os tópicos específicos abordados pela norma começam na seção 5.

5	**Políticas de Segurança da Informação**
6	**Organização da Segurança da Informação**
7	**Segurança em Recursos Humanos**
8	**Gestão de Ativos**
9	**Controle de Acesso**
10	**Criptografia**
11	**Segurança Física e do Ambiente**
12	**Segurança nas Operações**
13	**Segurança nas Comunicações**
14	**Aquisição, desenvolvimento e manutenção de sistemas**

15	**Relacionamento na Cadeia de Suprimentos**
16	**Gestão de Incidentes de Segurança da Informação**
17	**Aspectos da Segurança da Informação na Gestão da Continuidade do Negócio**
18	**Conformidade**

Atenção! Para visualizaçãocompleta da tabela utilize a rolagem horizontal

Tabela: Principais seções da norma ABNT NBR ISO/IEC 27002:2013.

Elaborada por Fabio Henrique Silva.

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.

VEM QUE EU TE EXPLICO!

Os vídeos a seguir abordam os assuntos mais relevantes do conteúdo que você acabou de estudar.

Conceito Atividades da ISO e das entidades de normatização.

O que é a Norma ISO/IEC 27001 Explicar o que é e seu objetivos.

Clausulas da norma ISO/IEC 27001 Fazer uma visão geral das 10 clausulas.

VERIFICANDO O APRENDIZADO

1. QUAL PALAVRA É CITADA FREQUENTEMENTE NA NORMA ISO/IEC 27001, QUE CONSTITUI SUA CARACTERÍSTICA MARCANTE?

A) CONVÉM

B) RECOMENDA

C) DEVE

D) ESPERA

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.

GABARITO

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

A alternativa "C " está correta.

Orientações do que DEVE ser feito. Os requisitos definidos nesta norma são genéricos e é pretendido que sejam aplicáveis a todas as organizações, independentemente de tipo, tamanho e natureza. A exclusão de quaisquer dos requisitos especificados nas seções de 4 a 10 na versão 2013 não é aceitável quando uma organização reivindica conformidade com esta norma.

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

A alternativa "B " está correta.

A norma contém orientações do que CONVÉM ser feito. Embora todos os controles sejam importantes e devam ser considerados, a relevância de qualquer controle deve ser determinada segundo os riscos específicos a que uma organização está exposta. Nem todos os controles e diretrizes contidos na norma podem ser aplicados, e controles adicionais e recomendações não incluídos podem ser necessários. Ela possui 35 objetivos de controles e 114 controles básicos distribuídos em 14 seções.

MÓDULO 2

- **Identificar as aplicações das normas ISO/IEC 27001 e ISO/IEC 27002**

CONCEITOS

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.

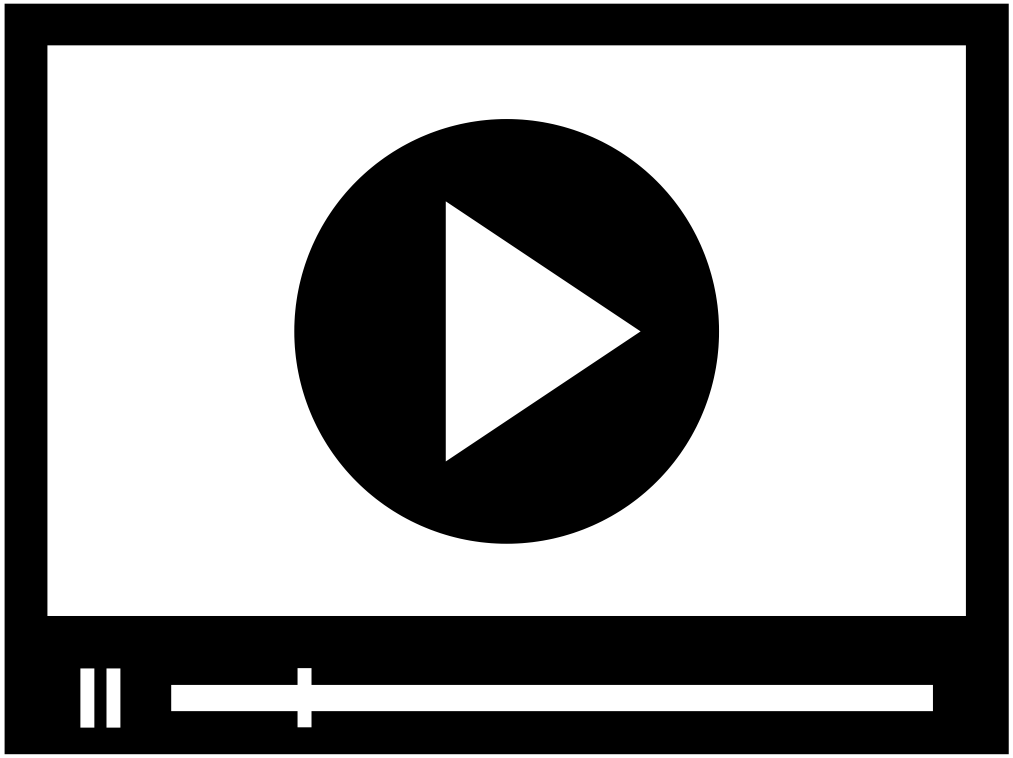
Faça uso das estruturas das normas (tabelas 3 e 4) para facilitar a localização dos itens.

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.

ATENÇÃO

Estudo de caso para aplicação dos itens da norma ABNT NBR ISO/IEC 27001:2013.



Para entender mais sobre o assunto, assista ao vídeo abaixo.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.

ATENÇÃO

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.

AT&T apresentou, esta semana, ação na Justiça do Texas contra 25 falsos clientes que contrataram serviços da companhia com o intuito de roubar informações de sua base de dados.

Os acusados criaram contas de clientes na AT&T que lhes permitiam armazenar gravações de voz no banco de dados da empresa. A intenção dos acusados, no entanto, era apenas ter acesso ao sistema da AT&T e, então, tentar ouvir gravações de outras companhias.

De acordo com a AT&T, o grupo conseguiu acessar gravações de 2.500 clientes da empresa. As informações seriam provavelmente usadas em disputas entre concorrentes ou para planejar estratégias de marketing.

A AT&T diz que gravações com dados sensíveis e informações financeiras são armazenadas em bancos especialmente seguros, que não foram acessados pelos falsos clientes.

Como os registros criados eram falsos, as 25 contas de clientes citadas no processo ainda precisam ser investigadas. O caso causou certa controvérsia ao ser apresentado à Justiça, já que o processo é movido contra falsos clientes, ou seja, pessoas que, em tese, não existem.

Assim que detectou o problema, a AT&T bloqueou o acesso às gravações dos 2.500 clientes envolvidos no caso e cancelou as contas de acesso dos acusados. Todos os clientes envolvidos foram notificados sobre o caso, diz a AT&T.

(ZMOGINSKI, 2008)

Estudo de caso para aplicação dos itens da norma ABNT NBR ISO/IEC 27002:2013.

O objetivo desse exemplo é, a partir da descrição do incidente, identificar o(s) item(ns) da norma que caracteriza(m) implementações inadequadas, ou ausências de implementações, dos controles e das diretrizes para implementação.

O enquadramento desse exemplo será feito no item 9.4, *Controle de acesso ao sistema e à informação* , que está dentro do item 9, *Controle de Acesso* .

O objetivo de controle do item 9.4 é "prevenir o acesso não autorizado aos sistemas e aplicações". O item 9.4 se desdobra nos seguintes itens:

- **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.**

Lembrando que cada um desses itens possui seu respectivo controle, diretrizes para implementação e informações adicionais.

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.

VEM QUE EU TE EXPLICO!

Os vídeos a seguir abordam os assuntos mais relevantes do conteúdo que você acabou de estudar.

Requisitos Norma ISO 27001, como é aplicada.

Benefícios da certificação ISO/IEC 27001 Falar sobre os 8 benefícios da certificação.

Conceitos Falar sobre o caso de 25 falsos clientes na AT&T

VERIFICANDO O APRENDIZADO

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, SEJA A SEGUINTE DESCRIÇÃO DA CENA/OCORRÊNCIA:

Cenas / Ocorrência	Registro da Não conformidade (NC)		
	Req.ISO/IEC 27001	Existe NC?	Descrição da NC e da Evidencia 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.

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* .

GABARITO

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, seja a seguinte descrição da cena/ocorrência:

Cenas / Ocorrência	Registro da Não conformidade (NC)		
	Req.ISO/IEC 27001	Existe NC?	Descrição da NC e da Evidencia 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 alternativa "D " está correta.

Na realidade, todas as respostas podem estar corretas, mas conforme já informado, iremos analisar com as sugestões e premissas estabelecidas no primeiro exemplo.

Essa cena será enquadrada no item 9.2, *Auditoria Interna* .

A letra A estaria correta se estivéssemos utilizando a norma ABNT NBR ISO/IEC 27001:2006, que cita exatamente que os auditores não devem auditar seu próprio trabalho. Essa frase deixou de existir na versão 2013, embora ainda seja uma boa prática.

Na letra B, pode até ser que venha uma descrição mais importante, mas iremos nos ater apenas à descrição, que já é suficiente para o auditor analisar na norma ou fazer questionamentos ao auditado.

A letra C não está correta, pois faltam informações sobre algumas frases do item da norma.

Enfim, na letra D, o auditor realizará exatamente as perguntas sobre as informações faltantes descritas, e ainda cabe mais uma, se esse acontecimento (auditar o próprio trabalho) está previsto no programa de auditoria.

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 alternativa "D " está correta.

Este é um relato jornalístico que carece de detalhes, mas usaremos para fins didáticos. Também faltam os subitens de cada uma das subseções citadas, mas a análise do exercício ficaria muito extensa. Para melhor enquadramento a um item da norma ISO/IEC 27002:2013, vamos analisar o objetivo de controle de cada item:

Letra a) 7.1: Antes da contratação. Objetivo: Assegurar que funcionários e partes externas entendem as suas responsabilidades e estão em conformidade com os papéis para os quais eles foram selecionados.

Letra b) 9.2: Gerenciamento de acesso do usuário. Objetivo: Assegurar acesso do usuário autorizado e prevenir acesso não autorizado a sistemas e serviços.

Letra c) 10.1: Controles criptográficos. Objetivo: Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou integridade da informação.

Letra d) 17.1: Continuidade da segurança da informação. Objetivo: Convém que a continuidade da segurança da informação seja contemplada nos sistemas de gestão da continuidade do negócio da organização.

CONCLUSÃO

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.

Para ouvir um *podcast* sobre o assunto, acesse a versão online deste conteúdo.

REFERÊNCIAS

ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. *In* : ABNT – Associação Brasileira de Normas Técnicas, 2013. Publicado em: 8 nov. 2013.

ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. *In* : ABNT - Associação Brasileira de Normas Técnicas, 2013. Publicado em: 8 nov. 2013.

DEUTSCHE BANK. WetFeet Insider Guide Deutsche Bank. Consultado em meio eletrônico em: 22 abr. 2020.

ISO/IEC 27000:2018. Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary. *In* : ISO - International Organization for Standardization, 2018. Publicado em: fev. 2018.

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, Marcos Aurélio Pchek. Segurança da Informação. Curitiba: Lt, 2012.

MACHADO, Felipe Nery Rodrigues. 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, Marcos. 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, Felipe. AT&T processa falsos clientes por roubo de dados. *In* : EXAME. Publicado em: 9 out. 2008.

EXPLORE+

Para saber mais sobre os assuntos tratados neste tema, 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.**

CONTEUDISTA

Fabio Henrique Silva

🔗 CURRÍCULO LATTES