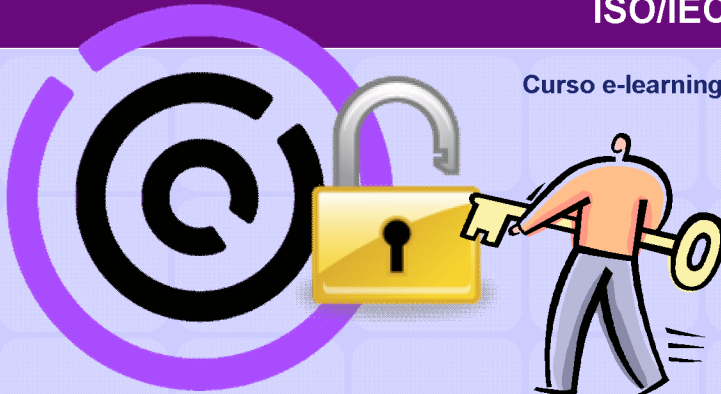


Fundamentos da Segurança da Informação com base na ISO/IEC 27002

Curso e-learning completo



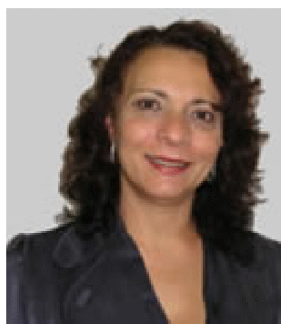
Preparatório para o exame EXIN ISO 27002 Foundation

Todos os direitos de cópia reservados. Não é permitida a distribuição física ou eletrônica deste material sem a permissão expressa do autor.

Apresentação da instrutora

Márcia Regina Guerra

- Graduada em Engenharia Elétrica pela Escola Politécnica, técnica eletrônica pela Escola Getúlio Vargas, pós-graduada em Engenharia de Segurança do Trabalho pela USP. Tem 35 anos de experiência profissional, sendo 27 deles dedicados a sistemas de gestão.
- Atuou nas seguintes empresas: Instituto de Pesquisas Tecnológicas, Asea Brown Boveri, Trevisan Consultores e Siemens. Há 15 anos fundou a ComExito Consultoria e Engenharia.
- Coordenou a primeira certificação ISO 9001 no Brasil, em 1989.
- Atualmente atua em consultoria, auditoria e treinamento em sistemas de gestão, como ISO 9001 (qualidade), ISO 14001 (meio ambiente), OHSAS 18001 (saúde e segurança ocupacional), SA8000 (responsabilidade social), ISO 20000-1 (gestão de TI), ISO 22000 (segurança alimentar), ISO 27001 (segurança da informação), COBIT, Seis Sigma e Governança de TI. Também realiza planejamento estratégico utilizando BSC, análise de riscos, etc.



© Todos os direitos reservados. Material exclusivo dos sites www.comexito.com.br e www.tiexames.com.br. Se você identificar que alguém está usando nosso material para outro fim, denuncie pelo telefone (11) 3522-6330.

Slide 2

Aviso de marcas registradas e direitos autorais

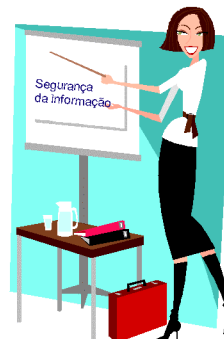
- Todos os direitos reservados. Nenhuma parte deste material poder ser reproduzida ou transmitida em qualquer ou por qualquer meio sem a permissão escrita do autor.
- Outras marcas registradas podem aparecer no decorrer deste curso. O uso destas marcas e logotipos é apenas para fins editoriais, em benefício exclusivo do dono da marca registrada, sem intenção de infringir as regras de sua utilização.

Objetivos do curso

Este curso é dirigido a todos os profissionais que querem conhecer os requisitos da norma NBR ISO/IEC 27002. Este curso fornece aos profissionais de TI um entendimento dos princípios básicos de gestão da segurança da informação.

Durante este você irá:

- Conhecer a organização ISO e as normas ISO/IEC 27001 e 27002
- Aprender o que é informação e quais os requisitos de qualidade da informação
- Entender os conceitos de ameaças e riscos à informação, medidas para redução de riscos e tipos de estratégias
- Aprender o que são ativos de informação para o negócio e como gerenciar estes ativos
- Conhecer medidas de controle físicas, técnicas e organizacionais
- Ter uma visão geral das legislações e regulamentações usuais
- Preparar-se para o exame ISO/IEC 27002 Foundation da EXIN



Conteúdo programático

- 1 Introdução**
Visão geral da organização ISO, visão geral das normas NBR ISO/IEC 27002 e NBR ISO/IEC 27001, apresentação do processo de exame do EXIN
- 2 Informação, objetivos do negócio e requisitos de qualidade**
Formas, sistemas, valor da informação, disponibilidade, integridade e confidencialidade, análise da informação, gestão da informação
- 3 Conceitos de riscos e ameaças para a segurança da informação**
Tipos de ameaças, danos e riscos, medidas para redução de risco, guia para implementação de medidas de segurança
- 4 Ativos da informação e incidentes de segurança**
O que são estes ativos e como gerenciá-los, sua classificação, papéis
- 5 Medidas físicas**
Segurança física, anéis de proteção, alarmes, proteção contra incêndio
- 6 Medidas técnicas**
Gerenciamento do acesso lógico, requisitos de segurança para sistemas de informação, criptografia, segurança de arquivos do sistema, vazamento de informação
- 7 Medidas organizacionais**
Política de segurança, pessoal, gestão de continuidade do negócio, gestão das comunicações e processos de operação
- 8 Legislação e regulamentações**
Observação de regulamentações, adequação, propriedade intelectual, proteção de documentos do negócio, de dados e confidencialidade de dados pessoais, prevenção contra abuso das instalações, cumprimento de política e padrões de segurança, medidas de monitoramento, auditorias, proteção de deficiências

© Todos os direitos reservados. Material exclusivo dos sites www.comexio.com.br e www.texamex.com.br e www.fim.com.br. Se você identificar que alguém está usando nosso material para outro fim, denuncie pelo telefone (11) 3522-6390.

Slide 5

Funcionamento do curso

Formato do curso



O treinamento é composto de slides com gravação em áudio realizada pela própria autora, e exercícios e quizzes para fixação do conteúdo.

Suporte

Para problemas técnicos utilize o canal Suporte Técnico.



Para enviar dúvidas e interagir com o instrutor, utilize o Fórum de Discussão.

Prazo



Você terá um prazo conforme indicado no site para concluir todos os módulos.

Você poderá repetir os módulos quantas vezes desejar dentro do período de validade da licença de uso.

Material



É disponibilizado o download em formato PDF dos slides apresentados durante este treinamento.

Referências para leitura complementar estão disponíveis no ambiente de ensino.

Não disponibilizamos para download o conteúdo gravado em áudio.

Certificado



O certificado pode ser solicitado pelo aluno ao final do treinamento, após a conclusão de todos os módulos.

Para este curso não aplicamos prova de avaliação.

© Todos os direitos reservados. Material exclusivo dos sites www.comexio.com.br e www.texamex.com.br e www.fim.com.br. Se você identificar que alguém está usando nosso material para outro fim, denuncie pelo telefone (11) 3522-6390.

Slide 6

Módulo 1



Introdução

Este módulo cobre:

1. Visão geral da organização ISO
2. Visão geral das normas NBR ISO/IEC 27002 e NBR ISO/IEC 27001
3. Apresentação do processo de exame
4. Exercícios

O que é a organização ISO?

- A ISO – International Organization for Standardization – é a maior organização para desenvolvimento e publicação de normas. Ela faz o relacionamento entre os órgãos nacionais de normatização de diferentes países. É uma organização não governamental, que forma uma ponte entre os setores público e privado. Sediada em Genebra, na Suíça, foi fundada em 1946.
- Mais de 160 países integram esta importante organização internacional, especializada em padronização e cujos membros são entidades normativas de âmbito nacional. O Brasil é representado pela Associação Brasileira de Normas Técnicas – ABNT.
- O propósito da ISO é desenvolver e promover normas que possam ser utilizadas igualmente por todos os países do mundo.
- A sigla ISO foi originada da palavra isonomia.



Para mais informações consulte o site:
<http://www.iso.org>



Situação no Brasil

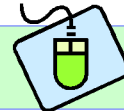
As normas para segurança da informação foram adotadas e traduzidas pela ABNT, recebendo a denominação de:

- **NBR ISO/IEC 27001:2006 – Tecnologia da Informação – Técnicas de Segurança – Sistema de Gestão de Segurança da Informação – Requisitos**
- **NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para Gestão de Segurança da Informação**

Neste treinamento, estas normas serão tratadas respectivamente por ISO 27001 e ISO 27002.

A norma ISO 27001 refere-se a quais requisitos de sistemas de gestão da informação devem ser implementados pela organização, e a ISO 27002 é um guia que orienta a utilização de controles de segurança da informação. Estas normas são genéricas por natureza.

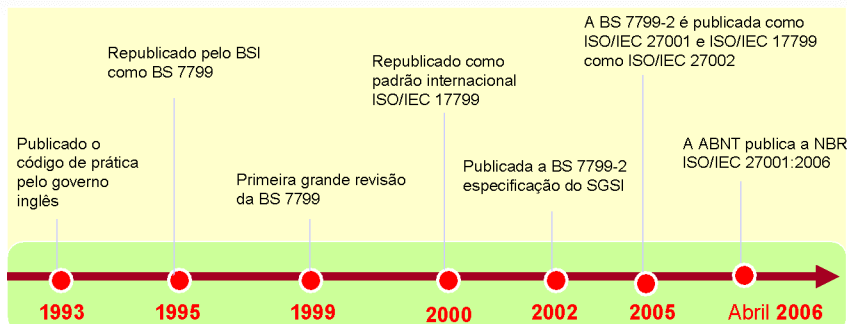
Para mais informações consulte o site:
<http://www.abntcolegao.com.br>



© Todos os direitos reservados. Material exclusivo dos sites www.comexio.com.br e www.texames.com.br. Se você identificar que alguém está usando nosso material para outro fim, denuncie pelo telefone (11) 3522-6390.

Slide 9

História das normas ISO 27001:2006 e da 27002:2005



Outras norma da família 27000 ainda não traduzidas pela ABNT:

- ISO/IEC 27000:2009 - Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
- ISO/IEC 27005:2008 - Information technology -- Security techniques -- Information security risk management
- ISO/IEC 27006:2007 - Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems

© Todos os direitos reservados. Material exclusivo dos sites www.comexio.com.br e www.texames.com.br. Se você identificar que alguém está usando nosso material para outro fim, denuncie pelo telefone (11) 3522-6390.

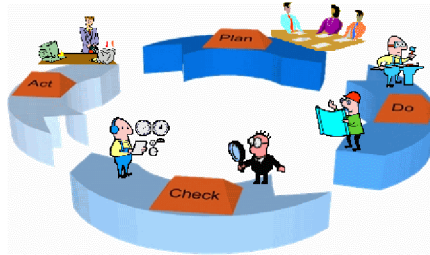
Slide 10

ISO/IEC 27002:2005 – Código de prática para SGSI

ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para Gestão da Segurança da Informação.

- Baseada na BS 7799-1:1999
- Utilização como documento de referência
- Fornece um conjunto completo de controles de segurança
- Baseada 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

**NBR
ISO/IEC
27002:2005**



© Todos os direitos reservados. Material exclusivo dos sites www.conexio.com.br e www.texames.com.br. Se você identificar que alguém está usando nosso material para outro fim, denuncie pelo telefone (11) 3522-6380.

Slide 11

Situação atual e estrutura da ISO 27002

- 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

**NBR
ISO/IEC
27002:2005**

© Todos os direitos reservados. Material exclusivo dos sites www.conexio.com.br e www.texames.com.br. Se você identificar que alguém está usando nosso material para outro fim, denuncie pelo telefone (11) 3522-6380.

Slide 12

A ISO 27002 e a ISO 27001

São

- Uma metodologia estruturada reconhecida internacionalmente, dedicada à 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



© Todos os direitos reservados. Material exclusivo dos sites www.conexto.com.br e www.texames.com.br. Se você identificar que alguém está usando nosso material para outro fim, denuncie pelo telefone (11) 3522-6390.

Slide 13

A ISO 27002 e a ISO 27001

- A 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 de a 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

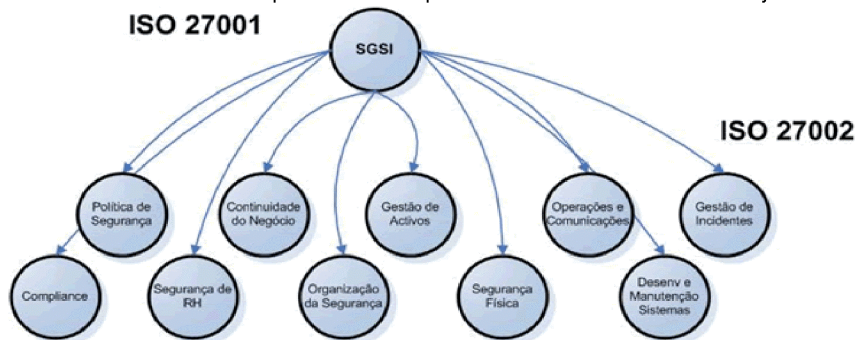


© Todos os direitos reservados. Material exclusivo dos sites www.conexto.com.br e www.texames.com.br. Se você identificar que alguém está usando nosso material para outro fim, denuncie pelo telefone (11) 3522-6390.

Slide 14

Visão geral das ISO 27001 e 27002

- Incorporam 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



© Todos os direitos reservados. Material exclusivo dos sites www.conexto.com.br e www.texames.com.br. Se você identificar que alguém está usando nosso material para outro fim, denuncie pelo telefone (11) 3522-6390.

Slide 15

Razões para se adotar as ISO 27002 e 27001



- Governança Corporativa
- Melhoria da eficácia da Segurança da Informação
- Diferencial de mercado
- Atender aos requisitos de partes interessadas e 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

© Todos os direitos reservados. Material exclusivo dos sites www.conexto.com.br e www.texames.com.br. Se você identificar que alguém está usando nosso material para outro fim, denuncie pelo telefone (11) 3522-6390.

Slide 16

Dificuldades para Implantação 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



© Todos os direitos reservados. Material exclusivo dos sites www.comexto.com.br e www.texames.com.br. Se você identificar que alguém está usando nosso material para outro fim, denuncie pelo telefone (11) 3522-6330.

Slide 17

Benefícios da Implementação das ISO 27001/2

- Reduz o risco de responsabilidade pela não implementação de um SGSI 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 medir o sucesso do sistema

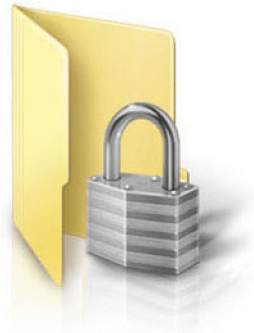


© Todos os direitos reservados. Material exclusivo dos sites www.comexto.com.br e www.texames.com.br. Se você identificar que alguém está usando nosso material para outro fim, denuncie pelo telefone (11) 3522-6330.

Slide 18

Meta das NBR ISO/IEC 27002 e 27001

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

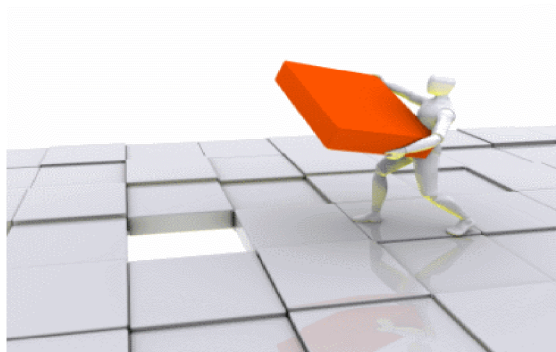


© Todos os direitos reservados. Material exclusivo dos sites www.conexio.com.br e www.texames.com.br. Se você identificar que alguém está usando nosso material para outro fim, denuncie pelo telefone (11) 3522-6380.

Slide 19

Série ISO/IEC 27000 em elaboração

- ISO 27003 – Esta norma deverá prover ajuda e orientação para implantação de um Sistema de Gestão de Segurança da Informação. Esta estrutura terá foco no PDCA para estabelecer, implementar e manter um Sistema de Segurança da informação.
- ISO 27004 – É o número oficial para planos de emergência e métricas para Sistemas de Segurança da Informação.



© Todos os direitos reservados. Material exclusivo dos sites www.conexio.com.br e www.texames.com.br. Se você identificar que alguém está usando nosso material para outro fim, denuncie pelo telefone (11) 3522-6380.

Slide 20

Certificação profissional para ISO 27002

- O EXIN é um instituto Holandês independente, com mais de 40 anos de atuação, sem fins lucrativos, que tem como principal objetivo a melhora da qualidade do setor de tecnologia da informação através da aplicação de testes e certificações.
- Desde 2009 o EXIN oferece duas certificações baseadas na ISO/IEC 27002:

Information Security Foundation based on ISO/IEC 27002

- Esta certificação é direcionada para qualquer profissional que lida com segurança da informação.
- Garante que o profissional tem um conhecimento básico sobre segurança da informação.
- Não exige um treinamento formal.
- O exame pode ser feito pela PROMETRIC.

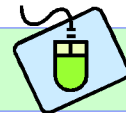


Information Security Management Advanced based on ISO/IEC 27002

- Esta certificação é direcionada para profissionais que se envolvem na implantação, avaliação e relatórios sobre segurança da informação, tais como Gerentes de Segurança Informação e Information Security Officer (ISO).
- É preciso passar por um treinamento oficial EXIN.
- O nível Foundation é obrigatório.

Para mais informações consulte o site

<http://www.exin-exams.com/exams/exam-program/iso-iec-27000/isfs.aspx>



© Todos os direitos reservados. Material exclusivo dos sites www.comexio.com.br e www.texamex.com.br. Se você identificar que alguém está usando nosso material para outro fim, denuncie pelo telefone (11) 3522-6390.

Slide 21

Orientações sobre o exame ISO 27002 *Foundation*

- É composto por 40 questões de múltipla escolha, sendo necessário acertar no mínimo 26 questões (65%).
- O exame pode ser realizado em centros de testes PROMETRIC, VUE e EXIN. É necessário ter um cartão de crédito internacional para efetuar o pagamento nos sites da PROMETRIC ou VUE.
- Disponível nos idiomas inglês, alemão e português.
- Sem consulta (a possibilidade de uso de dicionário deve ser verificada com o centro)
- Taxa: **US\$ 135,00** (PROMETRIC/VUE).
- Caso você precise de nota fiscal, poderá contratar a prova a partir de centros de testes EXIN aqui no Brasil. Sugerimos entrar em contato com a empresa IT Partners em SP para verificar esta possibilidade.

→ www.itpartners.com.br

Tutorial para agendar o exame na PROMETRIC



Inclui exame em português

© Todos os direitos reservados. Material exclusivo dos sites www.comexio.com.br e www.texamex.com.br. Se você identificar que alguém está usando nosso material para outro fim, denuncie pelo telefone (11) 3522-6390.

Slide 22

Certificação ISO 27002 Foundation

Requisitos do exame:

- 1. Informação e segurança - **10%**
 - 2. Ameaças e riscos - **30%**
 - 3. Abordagem e organização - **10%**
 - 4. Medição - **40%**
 - 5. Regulamentações e legislação - **10%**
-
- Nosso curso cobre todo o currículo para exame. Se o candidato quiser, também poderá ler uma apostila que o EXIN oferece gratuitamente.
 - No ambiente de ensino, na lista de material extra, você encontrará simulados online para praticar questões semelhantes às do exame. Para passar no exame é necessário realizar todo nosso curso e obter pelo menos 85% de acerto em nossos simulados.

Para mais informações consulte o site
<http://www.exin-exams.com/exams/exam-program/iso-iec-27000/isfs.aspx>



© Todos os direitos reservados. Material exclusivo dos sites www.comexto.com.br e www.texames.com.br e www.exin-exams.com. Se você identificar que alguém está usando nosso material para outro fim, denuncie pelo telefone (11) 3522-6330.

Slide 23

Sugestões para a data do exame

- Agende o exame antes de começar o curso. De preferência agende 15 dias antes.
- Escolha um dia da semana que você possa se ausentar no trabalho. Segunda ou sexta-feira são os melhores dias.
- Faça o exame no período da manhã.
- Chegue pelo menos 1 hora antes e revise o material de resumo.



© Todos os direitos reservados. Material exclusivo dos sites www.comexto.com.br e www.texames.com.br e www.exin-exams.com. Se você identificar que alguém está usando nosso material para outro fim, denuncie pelo telefone (11) 3522-6330.

Slide 24

Plano de estudos

- Tempo sugerido para estudos: 2 semanas (de 20 a 30 horas).
- Assista a dois módulos do curso e-learning a cada dia, e pratique as questões do simulado online correspondentes aos módulos assistidos. São 8 módulos que podem ser assistidos em 4 dias.
- No final do curso leia a apostila complementar. Tempo previsto para leitura: 2 dias
- Exercite os simulados online com 40 questões até obter mais de 85% de acerto. Evite decorar as questões dos simulados.
- Leia novamente a apostila ou assista ao módulo em que você está obtendo o menor acerto nos simulados. Tempo previsto: 3 dias.



© Todos os direitos reservados. Material exclusivo dos sites www.comexto.com.br e www.texamex.com.br e www.comexto.com.br. Se você identificar que alguém está usando nosso material para outro fim, denuncie pelo telefone (11) 3522-6390.

Slide 25

Certificação ISO 27002 Advanced

- A certificação *Advanced* em Gestão de Segurança da Informação também é baseada na ISO/IEC 27002
- Pré-requisito: ter a certificação *Foundation* em Segurança da Informação.

Requisitos do exame:

1. Política de segurança da informação e plano de segurança da informação - **20%**
2. Organização da segurança da informação - **30%**
3. Análise de risco - **15%**
4. Normas - **10%**
5. Adequação - **15%**
6. Avaliação - **10%**

- Este exame não pode ser realizado via PROMETRIC/VUE. Para agendá-lo é necessário que você contate um centro de treinamento EXIN.

Para mais informações consulte o site
<http://www.exin-exams.com/exams/exam-program/iso-iec-27000/isfs.aspx>



© Todos os direitos reservados. Material exclusivo dos sites www.comexto.com.br e www.texamex.com.br e www.comexto.com.br. Se você identificar que alguém está usando nosso material para outro fim, denuncie pelo telefone (11) 3522-6390.

Slide 26

Quiz - Módulo 1

19:59

Pergunta 1 De 6

Valor do Ponto: 10


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.


☐ Verdadeiro

☐ Falso

PROPERTIES
On passing, 'Finish' button:
On failing, 'Finish' button:
Allow user to leave quiz:
User may view slides after quiz:
User may attempt quiz:

[Goes to Next Slide](#)
[Goes to Next Slide](#)
[At any time](#)
[At any time](#)
[Unlimited times](#)

 Properties...

 Edit in Quizmaker

Ajude-nos a combater o uso indevido de nosso material

Para que possamos continuar desenvolvendo novos cursos com preços acessíveis, nós contamos com a sua colaboração. O conteúdo deste curso não pode ser reproduzido ou redistribuído de qualquer forma ou por qualquer meio.

Temos recebido constantemente avisos sobre alunos que estão:

- Compartilhando seus dados de acesso com outros colegas
- Distribuindo ilegalmente o conteúdo de nossos cursos em fóruns de discussão e outros meios
- Usando nosso material para ministrar treinamentos

Estas práticas indevidas, além de serem consideradas infrações de direitos autorais, prejudicam muito a continuidade do nosso trabalho. Se você identificar que alguém está usando indevidamente nosso conteúdo, ou distribuindo ilegalmente nosso material, por favor nos avise imediatamente pelo e-mail de contato do nosso site. Nós cuidaremos da investigação.

© Todos os direitos reservados. Material exclusivo dos sites www.conexito.com.br e www.texasjames.com.br e fm, denuncie pelo telefone (11) 3522-6300.

Slide 28