



Guia de preparação

Edição 201905

Copyright © EXIN Holding B.V. 2019. All rights reserved.
EXIN® is a registered trademark.

No part of this publication may be reproduced, stored, utilized or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written permission from EXIN.

Conteúdo

1. Visão geral	4
2. Requisitos do exame	7
3. Lista de conceitos básicos	11
4. Literatura do exame	14

1. Visão geral

EXIN Information Security Foundation based on ISO/IEC 27001 (ISFS.PR)

Escopo

EXIN Information Security Foundation baseado na ISO/IEC 27001 é uma certificação que valida o conhecimento de um profissional sobre:

- Informação e segurança: os conceitos, o valor da informação e da importância da confiabilidade.
- Ameaças e riscos: a relação entre as ameaças e confiabilidade.
- Abordagem e organização: a política de segurança e estabelecimento da Segurança da Informação.
- Medidas: física, técnica e organizacional.
- Legislação e regulamentação: a importância e funcionamento..

Resumo

A segurança da informação é a proteção das informações de uma grande variedade de ameaças com o objetivo de assegurar a continuidade do negócio, minimizar o risco do negócio e maximizar o retorno sobre os investimentos e as oportunidades de negócios.

A segurança das informações vem ganhando importância no mundo da Tecnologia da Informação (TI). A globalização da economia está gerando uma troca cada vez maior de informações entre as organizações (seus funcionários, clientes e fornecedores) bem como uma explosão no uso de computadores em rede e dispositivos de informática.

A norma internacional para Gerenciamento de Segurança da Informação ISO/IEC 27001, é uma norma amplamente respeitada e consultada e fornece uma estrutura para a organização e o gerenciamento de um programa de segurança das informações. A implementação de um programa com base nesta norma será muito útil para o objetivo de uma organização de atender a muitas das necessidades apresentadas no complexo ambiente operacional da atualidade. Uma compreensão categórica desta norma é importante para o desenvolvimento pessoal de todos os profissionais de segurança das informações.

Nos módulos de Segurança da Informação do EXIN, utiliza-se a seguinte definição: A Segurança da Informação lida com a definição, a implementação, a manutenção, a conformidade e a avaliação de um conjunto coerente de controles (medidas) que garantam a disponibilidade, a integridade e a confidencialidade da fonte de informações (manual e automática).

No EXIN Information Security Foundation baseado na ISO/IEC 27001 são testados os conceitos básicos de segurança da informação e suas relações. Um dos objetivos desse módulo é aumentar a conscientização de que as informações são valiosas e vulneráveis e aprender quais medidas são necessárias para protegê-las.

Contexto

O certificado em EXIN Information Security Foundation based on ISO/IEC 27001 faz parte do programa de qualificação em Segurança da Informação. O módulo é seguido pelos certificados de EXIN Information Security Management Professional based on ISO/IEC 27001 e EXIN Information Security Management Expert based on ISO/IEC 27001.



Grupo alvo

Qualquer pessoa na organização que manuseia informações. É também aplicável a proprietários de pequenas empresas a quem alguns conceitos básicos de Segurança da Informação são necessários. Este módulo pode ser um excelente ponto de partida para novos profissionais de segurança da informação.

Requisitos para a certificação

- Conclusão do exame EXIN Information Security Foundation based on ISO/IEC 27001 com sucesso.

Detalhes do exame

Tipo de exame:	Pergunta de múltipla escolha
Número de questões:	40
Mínimo para aprovação	65%
Com consulta	Não
Equipamentos eletrônicos permitidos:	Não
Tempo designado para o exame	60 minutos

As regras e Regulamentos dos exames EXIN aplicam se a este exame.



Bloom level

A certificação EXIN Information Security Foundation based on ISO/IEC 27001 testa candidatos no Bloom Nível 1 e Nível 2 de acordo com a Taxonomia Bloom Revisada:

- Bloom Level 1: Remembering (Lembrança) - depende da recuperação de informações. Os candidatos precisarão absorver, lembrar, reconhecer e recordar. Este é o elemento fundamental da aprendizagem antes que os candidatos possam avançar para níveis mais elevados.
- Bloom Level 2: Understanding (Compreensão) - um passo além da lembrança. O entendimento mostra que os candidatos compreendem o que é apresentado e podem avaliar como o material de aprendizagem pode ser aplicado em seu próprio ambiente.

Treinamento

Horas de contato

O número recomendado de horas presenciais para esse treinamento é de 14 horas. Isso inclui atribuições em grupo, preparação para o exame e paradas curtas (breaks). Este número de horas não inclui tarefas para casa, a logística (preparação) relacionada à sessão do exame, a sessão do exame e intervalos de almoço.

Carga de estudos indicada

60 horas, dependendo do conhecimento existente.

Provedores de treinamentos

Você encontrará uma lista de nossos provedores de treinamento credenciados em www.exin.com.

2. Requisitos do exame

Os requisitos do exame são definidos nas especificações do exame. A tabela a seguir lista os tópicos do módulo (requisitos do exame) e subtópicos (especificações do exame).

Requisito de exame	Especificação de exame	Peso
1. Informação e segurança		10%
	1.1 O conceito de informação	2.5%
	1.2 Valor da informação	2.5%
	1.3 Aspectos de confiabilidade	5%
2. Ameaças e riscos		30%
	2.1 Ameaças e riscos	15%
	2.2 Relacionamento entre ameaças, riscos e confiabilidade da informação	15%
3. Abordagem e organização		10%
	3.1 Política de segurança e organização de segurança	2.5%
	3.2 Componentes da organização da segurança	2.5%
	3.3 Gerenciamento de incidentes	5%
4. Medidas		40%
	4.1 Importância de medidas de segurança	10%
	4.2 Medidas físicas	10%
	4.3 Medidas técnicas	10%
	4.4 Medidas organizacionais	10%
5. Legislação e regulamentação		10%
	5.1 Legislação e regulamentação	10%
Total		100%

Especificações do exame

1 Informação e Segurança

- 1.1 O conceito de informação
O candidato é capaz de...
 - 1.1.1 explicar a diferença entre os dados e informações.
 - 1.1.2 descrever o meio de armazenamento que faz parte da infraestrutura básica.
- 1.2 Valor da informação
O candidato é capaz de...
 - 1.2.1 descrever o valor de dados / informação para as organizações.
 - 1.2.2 descrever como o valor de dados / informação pode influenciar as organizações.
 - 1.2.3 explicar como conceitos aplicados de segurança da informação protegem o valor de dados / informação.
- 1.3 Aspectos de confiabilidade
O candidato é capaz de...
 - 1.3.1 nome dos aspectos de confiabilidade da informação.
 - 1.3.2 descrever os aspectos de confiabilidade da informação.

2 Ameaças e riscos

- 2.1 Ameaça e risco
O candidato é capaz de...
 - 2.1.1 explicar os conceitos ameaça, de risco e análise de risco.
 - 2.1.2 explicar a relação entre uma ameaça e um risco.
 - 2.1.3 descreva os vários tipos de ameaças.
 - 2.1.4 descreva os vários tipos de danos.
 - 2.1.5 descrever diferentes estratégias de risco.
- 2.2 Relacionamento entre ameaças, riscos e confiabilidade das informações.
O candidato é capaz de...
 - 2.2.1 reconhecer exemplos dos diversos tipos de ameaças.
 - 2.2.2 descrever os efeitos que os vários tipos de ameaças têm sobre a informação e ao tratamento das informações.

3 Abordagem e Organização

- 3.1 Política de Segurança e organização de segurança
O candidato é capaz de...
 - 3.1.1 descrever os objetivos e o conteúdo de uma política de segurança.
 - 3.1.2 descrever os objetivos e o conteúdo de uma organização de segurança.
- 3.2 Componentes da organização da segurança
O candidato é capaz de...
 - 3.2.1 explicar a importância de um código de conduta.
 - 3.2.2 explicar a importância da propriedade.
 - 3.2.3 nomear os mais importantes papéis na organização da segurança da informação.

3.3 Gerenciamento de Incidentes

O candidato é capaz de...

- 3.3.1 resumir como incidentes de segurança são comunicados e as informações que são necessárias.
- 3.3.2 dar exemplos de incidentes de segurança.
- 3.3.3 explicar as consequências da não notificação de incidentes de segurança.
- 3.3.4 explicar o que implica uma escalção (funcional e hierárquico).
- 3.3.5 descrever os efeitos de uma escalção dentro da organização.
- 3.3.6 explicar o ciclo do incidente.

4 Medidas

4.1 Importância das medidas de segurança

O candidato é capaz de...

- 4.1.1 descrever as maneiras pelas quais as medidas de segurança podem ser estruturadas ou organizadas.
- 4.1.2 dar exemplos de cada tipo de medida de segurança.
- 4.1.3 explicar a relação entre os riscos e medidas de segurança.
- 4.1.4 explicar o objetivo da classificação das informações.
- 4.1.5 descrever o efeito da classificação.

4.2 Medidas de segurança física

O candidato é capaz de...

- 4.2.1 dar exemplos de medidas de segurança física.
- 4.2.2 descrever os riscos relacionados a medidas inadequadas de segurança física.

4.3 Medidas de ordem técnica

O candidato é capaz de...

- 4.3.1 dar exemplos de medidas de segurança técnica.
- 4.3.2 descrever os riscos relacionados a medidas inadequadas de segurança técnica.
- 4.3.3 compreender os conceitos de criptografia, assinatura digital e certificado.
- 4.3.4 nome das três etapas para internet banking (PC, web site, pagamento).
- 4.3.5 nomear vários tipos de software malicioso.
- 4.3.6 descrever as medidas que podem ser usadas contra software malicioso.

4.4 Medidas organizacionais

O candidato é capaz de...

- 4.4.1 dar exemplos de medidas de segurança organizacional.
- 4.4.2 descrever os perigos e riscos relacionados a medidas inadequadas de segurança organizacional.
- 4.4.3 descrever as medidas de segurança de acesso, tais como a segregação de funções e do uso de senhas.
- 4.4.4 descrever os princípios de gestão de acesso.
- 4.4.5 descrever os conceitos de identificação, autenticação e autorização.
- 4.4.6 explicar a importância para uma organização de um bem montado Gerenciamento da Continuidade de Negócios.
- 4.4.7 tornar clara a importância da realização de exercícios.

5 Legislação e regulamentos

5.1 Legislação e regulamentos

O candidato é capaz de...

- 5.1.1 explicar porque a legislação e as regulamentações são importantes para a confiabilidade da informação.
- 5.1.2 dar exemplos de legislação relacionada à segurança da informação.
- 5.1.3 dar exemplos de regulamentações relacionadas à segurança da informação.
- 5.1.4 indicar as medidas possíveis que podem ser tomadas para cumprir as exigências da legislação e regulamentação.

3. Lista de conceitos básicos

Este capítulo contém os termos com que os candidatos devem se familiarizar. Os termos estão listados em ordem alfabética.

Por favor, note que o conhecimento destes termos de maneira independente não é suficiente para o exame; O candidato deve compreender os conceitos e estar apto a fornecer exemplos.

Inglês

Access Control
Asset
Audit
Authentication
Authenticity
Authorization
Availability
Backup
Big Data
Biometrics
Botnet
Business Assets
Business Continuity Management (BCM)

Business Continuity Plan (BCP)
BYOD (Bring your own device)
Category
Certificate
Change Management
Classification
Clear desk policy
Cloud
Code of conduct
Code of practice for information security (ISO/IEC 27002)
Completeness
Compliance
Computer criminality legislation
Confidentiality
Continuity
Controls
Copyright legislation
Corrective
Correctness
Damage
Data
Detective
Digital Signature
Direct damage

Português

Controle de Acesso
Ativo
Auditoria
Autenticação
Autenticidade
Autorização
Disponibilidade
Backup (Cópia de segurança)
Big Data (Grandes dados)
Biometria
Botnet
Ativos de Negócios
Gerenciamento da Continuidade de Negócios (GCN)
Plano de Continuidade de Negócios (PCN)
BYOD
Categoria
Certificado
Gerenciamento da Mudança
Classificação
Política de mesa limpa
Nuvem
Código de conduta
Código de boas práticas de segurança da informação (ISO/IEC 27002)
Completeza
Conformidade
Legislação sobre Crimes de Informática
Confidencialidade
Continuidade
Medidas
Legislação de direitos autorais
Corretiva
Exatidão
Danos
Dados
Detectivo
Assinatura Digital
Danos diretos

Disaster	Desastre
Disaster Recovery Plan (DRP)	Plano de Recuperação de Desastre (PRD)
Encryption	Criptografia
Escalation	Escalação
- Functional escalation - Hierarchical escalation	- Escalação funcional - Escalação hierárquica
Exclusivity	Exclusividade
Hacking	Hacking
Hoax	Hoax
Identification	Identificação
Impact	Impacto
Incident Cycle	Ciclo de Incidentes
Indirect damage	Danos indiretos
Information	Informação
Information analysis	Análise da Informação
Information Architecture	Arquitetura da Informação
Information management	Gerenciamento da Informação
Information security review	Revisão da segurança da informação
Information system	Sistema de Informação
Infrastructure	Infraestrutura
Integrity	Integridade
Interference	Interferência
Intrusion Detection System (IDS)	Sistema de Detecção de Intrusos (IDS)
ISO/IEC 27001	ISO/IEC 27001
ISO/IEC 27002	ISO/IEC 27002
Key	Chave
Logical Access Management	Gerenciamento de acesso lógico
Maintenance door	Porta de Manutenção
Malware	Malware
Managing business assets	Gerenciamento de ativos de negócios
Non-disclosure agreement	Acordo de confidencialidade
Non-repudiation	Não-repúdio
Opportunity	Oportunidade
OWASP	Projeto Aberto de Segurança de Aplicativos da Web (OWASP)
Patch	Patch
Personal data protection legislation	Legislação sobre proteção de dados pessoais
Personal Firewall	Firewall pessoal
Phishing	Phishing
Precision	Precisão
Preventive	Preventiva
Priority	Prioridade
Privacy policy	Política de Privacidade
Production factor	Fator de produção
Public Key Infrastructure (PKI)	Infraestrutura de chave pública (ICP)
Public records legislation	Legislação sobre registros públicos
Qualitative risk analysis	Análise de risco qualitativa
Quantitative risk analysis	Análise quantitativa de risco
Reductive	Redutiva

Redundancy	Redundância
Reliability of information	Confiabilidade das informações
Repressive	Repressiva
Risk	Risco
Risk Analysis	Análise de Risco
Risk Assessment (Dependency & Vulnerability analysis)	Avaliação de Riscos (análise de dependência e vulnerabilidade)
Risk avoiding	Evitar riscos
Risk bearing	Reter riscos
Risk Management	Gerenciamento de riscos
Risk reduction	Redução de riscos
Risk Strategy	Estratégia de Risco
Robustness	Robustez
Rootkit	Rootkit
Secret authentication information	Informações secretas de autenticação
Security event	Evento de segurança
Security in development	Segurança em desenvolvimento
Security incident	Incidente de Segurança
Security measure	Medida de segurança
Security organization	Organização de Segurança
Security policy	Política de Segurança
Security regulations for special information for the government	Regulamentação de segurança para informações especiais p/ o governo
Security regulations for the government	Regulamentação de Segurança para o governo
Segregation of duties	Segregação de funções
Social Engineering	Engenharia Social
Spyware	Spyware
Stand-by arrangement	Stand-by
Storage Medium	Meio de armazenamento
System acceptance testing	Teste de aceitação do sistema
Teleworking	Trabalho remoto/à distância
Threat	Ameaça
Trojan	Trojan
Uninterruptible power supply(UPS)	Fornecedor Ininterrupto de Energia (UPS- Uninterruptible Power Supply)
Urgency	Urgência
User access provisioning	Provisionamento de acesso do usuário
Validation	Validação
Verification	Verificação
Virtual Private Network (VPN)	Rede privada virtual (RPV)
Virus	Vírus
Vulnerability	Vulnerabilidade
Worm	Worm

4. Literatura do exame

Literatura do exame

- A. Hintzbergen, J., Hintzbergen, K., Smulders, A. e Baars, H.
Fundamentos de Segurança da Informação: com base na ISO 27001 e ISO 27002
 Brasport, 1ª edição, 2018
 ISBN 9788574528601

Referência da literatura

Requisito de exame	Especificação de exame	Literatura
1. Informação e segurança		
	1.1 O conceito de informação	Capítulo 3 e §4.10
	1.2 Valor da informação	Capítulo 3 e 4
	1.3 Aspectos de confiabilidade	Capítulo 3 e 4
2. Ameaças e riscos		
	2.1 Ameaças e riscos	Capítulo 3
	2.2 Relacionamento entre ameaças, riscos e confiabilidade da informação	Capítulo 3 e 11
3. Abordagem e organização		
	3.1 Política de segurança e organização de segurança	Capítulo 3, 5 e 6
	3.2 Componentes da organização da segurança	Capítulo 6, 7, 8 e 13
	3.3 Gerenciamento de incidentes	Capítulo 3, 15 e 16
4. Medidas		
	4.1 Importância de medidas de segurança	Capítulo 3, 8 e 16
	4.2 Medidas físicas	Capítulo 3 e 11
	4.3 Medidas técnicas	Capítulo 6, 10, 11 e 12
	4.4 Medidas organizacionais	Capítulo 3, 6, 9, 17 e 18
5. Legislação e regulamentação		
	5.1 Legislação e regulamentação	Capítulo 18

Contato EXIN

www.exin.com

