Guia de Elaboração de Documentos

Fundamentos da Segurança da Informação baseado na norma ISO/IEC 27002

Edição Junho 2011

EXIN INFORMATION SECURITY

Conteúdo

1 Visão Geral

Fundamentos da Segurança da Informação baseado na norma ISO/IEC 27002 (ISFS.PR)

Resumo
Os Guias de Elaboração de Documentos são desenhados para auxiliar provedores de treinamentos a desenvolver cursos e materiais didáticos que atendam aos requisitos do EXIN.

O principal objetivo do Guia é identificar os assuntos tratados no exame, os requisitos e especificações do exame e o público alvo para apoiar o desenvolvimento de novos cursos de alta qualidade.

Segurança da Informação tem se tornado cada vez mais importante. A globalização da economia conduz a um crescente intercâmbio de informações entre as organizações (seus funcionários, clientes e fornecedores) e uma utilização crescente de redes, tais como a rede interna da empresa, a conexão com as redes de outras empresas e da Internet.

No módulo de Fundamentos da Segurança da Informação baseados na norma ISO/IEC 27002 (ISFS), os conceitos básicos de segurança da informação e sua coerência são testados. O público alvo são os colaboradores em geral. O conhecimento básico que é testado neste módulo contribui para o entendimento de que as informações são vulneráveis e que medidas são necessárias para proteger essas informações.

Os tópicos para este módulo são:
- 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.

e
- Legislação e regulamentação: a importância e funcionamento.

Contexto

O Certificado de Gerenciamento Avançado de Segurança da Informação baseado na ISO/IEC 27002 segue o Certificado de Fundamentos da Segurança da Informação baseados na ISO/IEC 27002.

Público 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.

Pré-requisitos

Nenhum

Formato do exame

Exame com questões de múltipla escolha

Estimativa de Tempo de Estudo

60 horas

Exercício prático

Não aplicável

Tempo destinado ao exame

60 minutos

Detalhes do exame

Número de questões:	40
Mínimo para aprovação:	65 % (26 de 40)
Com consulta:	não
Equipamentos eletrônicos permitidos:	não

Exemplos de questões

Você pode fazer o download do simulado e se preparar melhor para o exame acessando http://www.exin-exams.com

Curso

Quantidade de alunos em classe

O número máximo de alunos em sala é 25.
(Isso não é aplicável nos casos de ensino à distância / CBT - computer based training/e-learning)

Horas de contato

O número mínimo de horas de contato durante o curso é de 7 horas. Isso inclui as atividades em grupo, preparação para o exame, e coffee breaks, mas não inclui tarefas de casa, preparação da logística de exame e horário de almoço.

Provedores de Treinamento

A lista das empresas credenciadas para ministrar este e outros treinamentos do Exin encontra-se no nosso site: http://www.exin-exams.com.

2 Requisitos do exame

Os requisitos do exame são os principais temas de um módulo. O candidato deve ter o domínio completo sobre estes temas. Os requisitos do exame são elaborados na especificação do exame.

Requisitos 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
	4.5 Importância de medidas de segurança	
5 Legislação e regulamentação		**10**
	5.1 Legislação e regulamentação	10
Total		**100**

Requisitos e especificações do exame

1. Informação e Segurança (10%)

1.1 O conceito de informação (2,5%)

O candidato entende 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 infra-estrutura básica

1.2 Valor da informação (2,5%)

O candidato entende o valor da informação para as organizações.
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 / informações pode influenciar as organizações
1.2.3 Explicar como conceitos aplicados de segurança de informações protegem o valor de dados / informações

1.3 Aspectos de confiabilidade (5%)

O candidato conhece os aspectos de confiabilidade (confidencialidade, integridade, disponibilidade) da informação.
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 (30%)

2.1 Ameaça e risco (15%)

O candidato compreende os conceitos de ameaça e risco.
O candidato é capaz de:
2.1.1 Explicar os conceitos de 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. (15%)

O candidato compreende a relação entre as 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 (10%)

3.1 Política de Segurança e organização de segurança (2,5%)

O candidato tem conhecimento da política de segurança e conceitos de organização de segurança.
O candidato é capaz de:
3.1.1 enunciar os objetivos e o conteúdo de uma política de segurança
3.1.2 enunciar os objetivos e o conteúdo de uma organização de segurança

3.2 Componentes da organização da segurança (2,5%)

O candidato conhece as várias 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 na organização da segurança da informação

3.3 Gerenciamento de Incidentes (5%)

O candidato compreende a importância da gestão de incidentes e escaladas.
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 conseqüências da não notificação de incidentes de segurança
3.3.4 Explicar o que implica uma escalada (funcional e hierárquico)
3.3.5 Descrever os efeitos da escalada dentro da organização
3.3.6 Explicar o ciclo do incidente

4. Medidas (40%)

4.1 Importância das medidas de segurança (10%)

O candidato entende a importância de 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 (10%)

O candidato tem conhecimento tanto da criação e execução de 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 envolvidos com insuficientes medidas de segurança física

4.3 Medidas de ordem técnica (10%)

O candidato tem conhecimento tanto da criação quanto da execução de medidas de segurança técnica.
O candidato é capaz de:
4.3.1 Dar exemplos de medidas de segurança técnica
4.3.2 Descrever os riscos envolvidos com insuficientes medidas de segurança técnica
4.3.3 Compreender os conceitos de criptografia, assinatura digital e certificado
4.3.4 Nome das três etapas para a banca online (PC, web site, pagamento)
4.3.5 Nomear vários tipos de software malicioso
4.3.6 Descrever as medidas que podem ser usados contra software malicioso

4.4 Medidas organizacionais (10%)

O candidato tem conhecimento tanto da criação quanto da execução de medidas de segurança organizacional.
O candidato é capaz de:
4.4.1 Dar exemplos de medidas de segurança organizacional
4.4.2 Descrever os perigos e riscos envolvidos com insuficientes medidas 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 regulamentação (10%)

5.1 Legislação e regulamentos (10%)

O candidato entende a importância e os efeitos da legislação e regulamentações.

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 regulamentos relacionados à segurança da informação

5.1.4 Indicar as medidas possíveis que podem ser tomadas para cumprir as exigências da legislação e regulamentação

Justificativa de escolhas

Requisitos para o exame: justificativa da distribuição de peso.
As medidas de segurança são, para a maioria do pessoal, os primeiros aspectos de Segurança da Informação que essas pessoas encontram. Conseqüentemente, as medidas são fundamentais para o módulo e têm o maior peso. A seguir, ameaças e riscos em termos de peso. Finalmente, a percepção da política, organização e legislação e regulamentação na área de Segurança da Informação são necessárias para compreender a importância das medidas de Segurança da Informação.

3 Lista de conceitos básicos

Este capítulo contém os termos com os quais os candidatos devem mostrar familiaridade.

Os termos estão listados em ordem alfabética.

• Ameaça	• Threat
• Análise da Informação	• Information analysis
• Análise de Risco	• Risk Analysis
• Análise de risco qualitativa	• Qualitative risk analysis
• Análise quantitativa de risco	• Quantitative risk analysis
• Arquitetura da Informação	• Information Architecture
• Assinatura Digital	• Digital Signature
• Ativo	• Asset
• Auditoria	• Audit
• Autenticação	• Authentication
• Autenticidade	• Authenticity
• Autorização	• Authorization
• Avaliação de Riscos (análise de dependência e vulnerabilidade)	• Risk Assessment (Dependency & Vulnerability analysis)
• Backup (Cópia de segurança)	• Backup
• Biometria	• Biometrics
• Botnet	• Botnet
• Categoria	• Category
• Certificado	• Certificate
• Chave	• Key
• Ciclo de Incidentes	• Incident Cycle
• Classificação	• Classification
• Código de boas práticas de segurança da informação (ISO/IEC 27002:2005)	• Code of practice for information security (ISO/IEC 27002:2005)
• Código de conduta	• Code of conduct
• Completeza	• Completeness
• Confiabilidade das informações	• Reliability of information
• Confidencialidade	• Confidentiality
• Conformidade	• Compliance
• Continuidade	• Continuity
• Controle de Acesso	• Access Control
• Corretiva	• Corrective
• Criptografia	• Encryption
• Dados	• Data
• Danos	• Damage
Danos diretos	Direct damage
Danos indiretos	Indirect damage
• Desastre	• Disaster
• Detectiva	• Detective
• Disponibilidade	• Availability

• Engenharia Social	• Social Engineering
• Escalação	• Escalation
Escalação funcional	Functional escalation
Escalação hierárquica	Hierarchical escalation
• Estratégia de Risco	• Risk Strategy
Reter riscos	Risk bearing
Evitar riscos	Risk avoiding
Redução de riscos	Risk reduction
• Exatidão	• Correctness
• Exclusividade	• Exclusivity
• Fator de produção	• Production factor
• Firewall pessoal	• Personal Firewall
• Fornecedor Ininterrupto de Energia (UPS-Uninterruptible Power Supply)	• Uninterruptible power supply (UPS)
• Gerenciamento da Continuidade de Negócios (GCN)	• Business Continuity Management (BCM)
• Gerenciamento da Informação	• Information management
• Gerenciamento da Mudança	• Change Management
• Gerenciamento de acesso lógico	• Logical Access Management
• Gerenciamento de riscos	• Risk Management
• Hacking	• Hacking
• Hoax	• Hoax
• Identificação	• Identification
• Impacto	• Impact
• Incidente de Segurança	• Security incident
• Informação	• Information
• Infra-estrutura	• Infrastructure
• Infra-estrutura de chave pública (ICP)	• Public Key Infrastructure (PKI)
• Integridade	• Integrity
• Interferência	• Interference
• ISO/IEC 27001:2005	• ISO/IEC 27001:2005
• ISO/IEC 27002:2005	• ISO/IEC 27002:2005
• Legislação de direitos autorais	• Copyright legislation
• Legislação sobre Crimes de Informática	• Computer criminality legislation
• Legislação sobre proteção de dados pessoais	• Personal data protection legislation
• Legislação sobre registros públicos	• Public records legislation
• Malware	• Malware
• Medida de segurança	• Security measure
• Meio de armazenamento	• Storage Medium
• Não-repúdio	• Non-repudiation
• Oportunidade	• Opportunity
• Organização de Segurança	• Security organization
• Patch	• Patch
• Phishing	• Phishing
• Plano de Continuidade de Negócios (PCN)	• Business Continuity Plan (BCP)

• Plano de Recuperação de Desastre (PRD)	• Disaster Recovery Plan (DRP)
• Política de mesa limpa	• Clear desk policy
• Política de Privacidade	• Privacy policy
• Política de Segurança	• Security policy
• Porta de Manutenção	• Maintenance door
• Precisão	• Precision
• Preventiva	• Preventive
• Prioridade	• Priority
• Rede privada virtual (RPV)	• Virtual Private Network (VPN)
• Redutiva	• Reductive
• Regulamentação de segurança para informações especiais p/ o governo	• Security regulations for special information for the government
• Regulamentação de Segurança para o governo	• Security regulations for the government
• Repressiva	• Repressive
• Risco	• Risk
• Robustez	• Robustness
• Rootkit	• Rootkit
• Segregação de funções	• Segregation of duties
• Sistema de Informação	• Information system
• Spam	• Spam
• Spyware	• Spyware
• Stand-by	• Stand-by arrangement
• Trojan	• Trojan
• Urgência	• Urgency
• Validação	• Validation
• Verificação	• Verification
• Vírus	• Virus
• Vulnerabilidade	• Vulnerability
• Worm	• Worm

4 Literatura

Literatura de Suporte para o Exame

A Hintzbergen, J., Hintzbergen, K., Smulders, A. and Baars, H.
Foundations of Information Security – Based on ISO27001 and ISO27002
Van Haren Publishing, 2010
ISBN 978 90 8753 568 1

Visão geral da literatura

Especificação do exame	Literatura	
1.1	**A:**	Capítulo 4
1.2	**A:**	Capítulo 4
1.3	**A:**	Capítulo 4
2.1	**A:**	Capítulo 5
2.2	**A:**	Capítulo 5
3.1	**A:**	Capítulo 9
3.2	**A:**	§6.2, §6.4, Capítulo 9
3.3	**A:**	Capítulo 6
4.1	**A:**	Capítulo 5, Capítulo 6
4.2	**A:**	Capítulo 7
4.3	**A:**	Capítulo 8, 10
4.4	**A:**	Capítulo 9, 10
5.1	**A:**	Capítulo 11

Contato EXIN

www.exin-exams.com

We turn skills into reputation