Documento de Serviço ISFS
Fundamentos da Segurança da Informação
baseados na ISO/IEC 27002
edição Fevereiro 2010

CONTEÚDO

Data: 3 fevereiro 2010

1. Introdução

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

O principal objetivo do Documento de Serviço 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.

2. Descrição do módulo

Nome do módulo

Fundamentos da Segurança da Informação baseados na ISO/IEC 27002 (ISFS.PR[1])

Descrição do módulo

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.

Outras tendências relevantes incluem:
- normas (internacionais) e certificação no domínio da Segurança da Informação;
- a informatização do gerenciamento;
- o desenvolvimento de ferramentas automatizadas de segurança;
- controle remoto
- a terceirização de tarefas de gestão conformidade

Além disso, as atividades de muitas companhias se baseiam em TI e a informação tornou-se um ativo valioso. Proteção da informação é crucial para a continuidade e o bom funcionamento da organização: a informação deve ser confiável.

A norma internacional, o Código de Boas Práticas de Segurança da Informação ISO/IEC 27002:2005, estrutura a Segurança da Informação da organização. Por essa razão, é um importante ponto de partida para este módulo.
No módulo sobre Segurança da Informação, será utilizada a definição do PvIB (Plataforma Holandesa de Especialistas em Segurança da Informação): Segurança da Informação lida com a definição, implementação, manutenção, conformidade e avaliação de um conjunto coerente de medidas que salvaguardem a disponibilidade, integridade e confidencialidade do fornecimento (manual e automático)de informações.

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. A população alvo são os empregados em toda organização. 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.
O módulo avançado de Gerenciamento de Segurança da Informação baseado na ISO/IEC 27002

[1] O “S” no código do modulo é indicação de: baseado em padrão

(ISMAS) testa aspectos organizacionais e de gestão da Segurança da Informação. O público alvo são pessoas que estão profissionalmente envolvidas com a implementação e avaliação de Segurança da Informação.
O módulo Segurança da Informação baseada na norma ISO/IEC 27002 (ISMES.EN) testa conhecimentos específicos, compreensão e habilidades na estruturação, manutenção e otimização da informação dentro de uma organização.

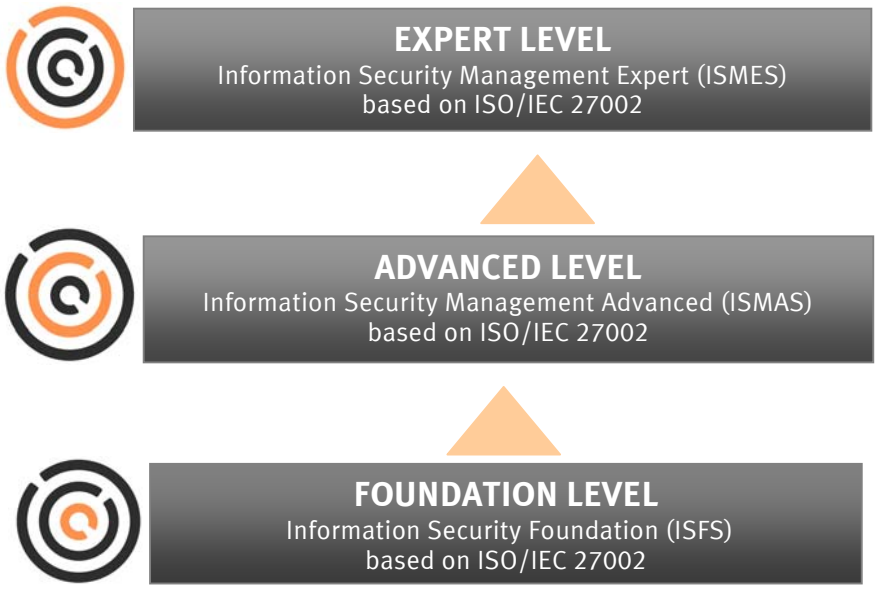
Requisitos do exame

- 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.

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.

Esquema de qualificação dos certificados disponíveis



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

Requerimentos de entrada para o exame: Nenhum.
A realização do curso de Fundamentos da Segurança da Informação baseados na ISO/IEC 27002 em um provedor de treinamento acreditado pelo EXIN é recomendado.

Formato do exame

Exame com questões de múltipla escolha

3. Requisitos e especificações do exame

Os requisitos do exame são os principais temas de um módulo. O candidato deve ter o comando completo sobre estes temas. Os requisitos do exame são elaborados na especificação do exame. O EXIN aplica especificações do exame em seis níveis de domínio baseado na Taxonomia Revisada de Bloom (Anderson & Krathwohl, 2001).

As especificações do exame são estruturadas em dois níveis: nível de maestria e nível dos testes:

O nível de maestria
Dependendo da dificuldade requerida, o nível de maestria (1.1) define:

1 Lembrança: a capacidade de recordar, reproduzir e reafirmar informações aprendidas
2 Compreensão: a capacidade de apreender o significado da informação, ao interpretar e traduzir o que foi aprendido
3 Aplicação: a capacidade de fazer uso da informação em um contexto diferente daquele que foi aprendido
4 Análise: a capacidade de romper com as informações obtidas em suas partes para compreendê-la
5 Avaliação: a capacidade de tomar decisões com base na reflexão aprofundada, crítica e avaliada
6 Criação: a capacidade de criar novas idéias e informações com o que foi aprendido

O nível de teste
O nível de teste (1.1.1) define:
- O que será testado (indicação específica do conteúdo)
- Como este será testado (por exemplo: pedindo para nomear ou descrever algo, ou dar exemplos)

Esta tabela lista os principais tópicos do módulo de requisitos (exame). A importância dos temas principais em relação ao exame é expressa como uma percentagem do total (ver segunda coluna).

Requisitos do exame	**Peso**
1. Informação e Segurança	10%
2. Ameaças e riscos	30%
3. Abordagem e organização	10%
4. Medidas	40%
5. Legislação e regulamentação	10%

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.

4. Matriz do exame

Formato do exame

Tipo de exame: múltipla escolha
Número de questões: 40
Duração do exame: 60 minutos
Taxa para aprovação: 65%

Matriz do exame

A matriz do exame especifica o número e o peso das questões no exame, baseados nos requisitos do exame e as especificações do nível de maestria.

Requisito de exame	Especificação de exame ao nível de maestria		Peso (%)	Número de questões
1 Informação e segurança				
O conceito de informação	1.1	Entendimento	2.5	1
Valor da informação	1.2	Entendimento	2.5	1
Aspectos de confiabilidade	1.3	Lembrança	5	2
Subtotal			**10**	**4**
2 Ameaças e riscos				
Ameaças e riscos	2.1	Entendimento	15	6
Relacionamento entre ameaças, riscos e confiabilidade da informação	2.2	Entendimento	15	6
Subtotal			**30**	**12**
3 Abordagem e organização				
Política de segurança e organização de segurança	3.1	Lembrança	2.5	1
Componentes da organização da segurança	3.2	Lembrança	2.5	1
Gerenciamento de incidentes	3.3	Entendimento	5	2
Subtotal			**10**	**4**

4 Medidas				
Importância de medidas de segurança	4.1	Entendimento	10	4
Medidas físicas	4.2	Lembrança	10	4
Medidas técnicas	4.3	Lembrança	10	4
Medidas organizacionais	4.4	Lembrança	10	4
Subtotal			**40**	**16**

5 Legislação e regulamentação				
Legislação e regulamentação	5.1	Entendimento	10	4
Subtotal			**10**	**4**
Total			**100**	**40**

5. Lista de conceitos básicos

Este capítulo contém os termos com os quais os candidatos devem mostrar familiaridade. Esses termos estão listados em ordem alfabética. Estão incluídos tanto as abreviaturas quanto o nome completo do termo a ser estudado.

Por favor, note que o conhecimento destes termos isoladamente não é suficiente para o exame; o candidato deve entender e estar apto a aplicar a teoria.

Lista de conceitos básicos

- Ameaça
- Análise da Informação
- Análise de Risco
- Análise de risco qualitativa
- Análise quantitativa de risco
- Arquitetura da Informação
- Assinatura Digital
- Ativo
- Auditoria
- Autenticação
- Autenticidade
- Autorização
- Avaliação de Riscos (análise de dependência e vulnerabilidade)
- Backup (Cópia de segurança)
- Biometria
- Botnet
- Categoria
- Certificado
- Chave
- Ciclo de Incidentes
- Classificação
- Código de boas práticas de segurança da informação (ISO/IEC 27002:2005)
- Código de conduta
- Completeza
- Confiabilidade das informações
- Confidencialidade
- Conformidade
- Continuidade
- Controle de Acesso
- Corretiva
- Criptografia
- Dados
- Danos
- Danos indiretos
- Desastre
- Detectiva
- Disponibilidade
- Engenharia Social
- Escalação
    - Escalação funcional
    - Escalação hierárquica
- Estratégia de Risco

    - Evitar riscos
    - Reter riscos
    - Reduzir riscos
- Exatidão
- Exclusividade
- Fator de produção
- Firewall pessoal
- Fornecedor Ininterrupto de Energia (UPS-Uninterruptible Power Supply)
- Gerenciamento da Continuidade de Negócios (GCN)
- Gerenciamento da Informação
- Gerenciamento de acesso lógico
- Gerenciamento de Mudança
- Gerenciamento de riscos
- Hacking
- Hoax
- Identificação
- Impacto
- Incidente de Segurança
- Informação
- Infra-estrutura
- Infra-estrutura de chave pública (ICP)
- Integridade
- Interferência
- ISO / IEC 27001:2005
- ISO / IEC 27002:2005
- Legislação de direitos autorais
- Legislação sobre Crimes de Informática
- Legislação sobre proteção de dados pessoais
- Legislação sobre registros públicos
- Malware
- Medida de segurança
- Não-repúdio
- Oportunidade
- Organização de Segurança
- Patch
- Phishing
- Plano de Continuidade de Negócios (PCN)
- Plano de Recuperação de Desastre (PRD)
- Política de mesa limpa
- Política de Privacidade
- Política de Segurança
- Porta de Manutenção
- Precisão
- Prejuízos diretos
- Preventiva
- Prioridade
- Rede privada virtual (RPV)
- Redutiva
- Regulamentação de segurança para informações especiais p/ o governo
- Regulamentação de Segurança para o governo
- Repressiva
- Risco
- Robustez
- Rootkit
- Segregação de funções

- Sistema de Informação
- Spam
- Spyware
- Stand-by
- Suporte de armazenamento
- Trojan
- Urgência
- Validação
- Verificação
- Vírus
- Vulnerabilidade
- Worm

6. Literatura

Recomenda-se aos candidatos a leitura do livro abaixo listado para preparação para o exame.

Livro

A Hintzbergen, J., Baars, H., Hintzbergen, K. and Smulders, A.
The Basics of Information Security - A practical handbook
The Netherlands, 2009

Explanação e justificativa

Esta publicação está disponível gratuitamente, no formato PDF (em inglês), no sítio internet do EXIN:
http://www.exin-exams.com/exams/exam-program/iso-iec-27000/isfs.aspx

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:** §6.1, §6.3, Capítulo 9
3.3	**A:** Capítulo 6
4.1	**A:** Capítulo 5, Capítulo 6
4.2	**A:** Capítulo 7
4.3	**A:** Capítulos 8 e 9
4.4	**A:** Capítulos 8 e 9
5.1	**A:** Capítulo 10

7. Requisitos de acreditação

A despeito dos requisitos gerais declarados no Guia de Acreditação do EXIN, há certo número de critérios para a entrega de cursos acreditados para o módulo de Fundamentos da Segurança da Informação baseados na ISO/IEC 27002 que devem atender:

Quantidade de alunos em classe

O número máximo de alunos em sala é **16**.
(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.

Ensino à distância

- A extensão da formação deve ser comparável ao número de horas de contacto para uma interação pessoal, com no mínimo 7 horas.
- Um treinamento por computador (CBT-Computer Based Training*/e-learning*) pode ser definido em quatro níveis: textos, gráficos, animação e multimídia. Treinamentos só em texto não podem ser acreditados. O treinamento deve conter, pelo menos gráficos.
- O treinamento por computador (CBT-Computer Based Training*/e-learning*) tem um alto nível de usabilidade (facilidade de navegação, uso racional de cores, disponibilidade de mensagens de ajuda, etc.)
- O treinamento por computador deve ser mais do que apenas um curso seqüencial. O treinamento baseado em computador tem a facilidade de lidar com os assuntos de forma interativa.
- A ferramenta de treinamento por computados apóia os instrutores na monitoração das atividades dos alunos.
- Ao aluno é dada a facilidade de contato com um instrutor. O tempo de interação com os alunos não deve ser maior do que um dia de trabalho.
- Há uma explicação sobre a estrutura do treinamento baseado em computador e uma visão clara dos assuntos.

Requisitos de competência do instrutor

- O instrutor deve ter obtido o certificado em Fundamentos da Segurança da Informação baseados na ISO/IEC 27002.

Material de curso

Curso aprovado deve conter:

- Uma explicação sobre a estrutura do treinamento baseado em computado uma visão clara dos assuntos. (aplicável apenas a ensino à distância / treinamento baseado em computador)
- Conter informações sobre o tema do curso e publicações relevantes.
- Conter atividades, em conformidade com os requisitos do exame. Quaisquer novas orientações fornecidas pelo Documento de Serviço aplicável também são levados em conta. Estas atividades poderiam ser realizadas sob a forma de discussão em grupo, simulação, etc.

Para mais informações, verifique o Guia de Acreditação na Extranet ou contate o departamento de acreditação do EXIN (accreditation@exin-exams.com).

8. Plano de curso

O programa do curso indica a possível estrutura do mesmo. Trata-se de uma simples indicação que de nenhuma maneira dita como a formação deve ser conduzida. No entanto, prevê uma ordem lógica para os tópicos do exame e exemplos de exercícios e questões para discutir com os participantes.

Tópicos a serem abordados no curso	Método de instrução
1. Protegendo a informação • O que é informação? • O que faz a informação valiosa? • O que faz a informação menos valiosa? • O que fazemos sobre isso?	*Perguntar aos alunos as 4 questões listadas no item 1. Protegendo a informação.* *Explicar:* • *Definição de informação de acordo com o dicionário Webster:* ***'A comunicação ou recepção de conhecimento ou inteligência'.*** • *Diferença entre dado e informação* • *Valioso = dinheiro* • *Requisitos de confiabilidade: CDI* • *Ameaças à CDI* • *Averiguando riscos e tomando medidas*
2. Segurança da Informação • O que é Segurança da Informação?	*Explicar a definição de segurança da informação* ***Definição:*** *Segurança da Informação tem a ver com a definição, implementação, manutenção, compatibilidade e avaliação de um conjunto coerente de medidas que salvaguardem a disponibilidade, integridade e confidencialidade do (manual e automatizado) fornecimento de informação.* **Exercício A** • *Qual informação é valiosa em sua organização e por quê?* o *Deixe os alunos prepararem (em pares) e então apresentar suas respostas.*
3. Exemplos de informação valiosa • Empregados (seu conhecimento e experiência) • Os produtos ou serviços que vendemos • Dados pessoas de fornecedores, clientes, empregados • Nossos processos • Manuais/receitas	**Exercício B** • *Como a informação da sua organização pode ser ameaçada?* o *Deixa os alunos, em dois grupos, escreverem o maior número de exemplos práticos de ameaças, como eles as vêm, em dois quadros brancos.* *Certifique-se que os exemplos são*

• Informações financeiras	*práticos, e específicos para sua organização, não genéricas. Por exemplo: **NÃO**: informação pode ser roubada; **MAS** eu posso ter uma chamada telefônica profissional enquanto eu estou no trem e tenho que falar sobre um novo projeto, enquanto a pessoa ao meu lado fica escutando a conversa.*
4. Ameaças • Ameaças humanas e não humanas • Intencional e não intencional • Ameaça humana intencional: engenharia social • Interrupções na infra-estrutura básica • Interrupções no ambiente físico	*Explicar a diferença entre ameaças humanas e não humanas e entre ameaças intencionais e não intencionais.* **Exercício C** • *Junto com os alunos atribua as categorias de ameaças para as ameaças listadas no quadro branco.*

5. Dano
• Dano direto
• Dano indireto
• Expectativa Anual de Perda
• Expectativa de Perda Única
	Exercício D
	• *Pedir aos alunos para dar exemplos para cada tipo de dano:*
	  o *<u>Direto:</u> por exemplo, roubo*
	  o *<u>Indireto: por exemplo, perda de reputação</u>*

6. Risco • O que podemos fazer com as ameaças e os danos que esperamos quando as ameaças se materializam? • Análise de risco • Estratégia de risco: suportar, neutralizar, evitar	*Explicar a diferença entre ameaça e risco. Discuta o relacionamento entre ameaças, riscos e confiabilidade da informação.*

7. Medidas de segurança durante o ciclo de incidente
• Quando e o que podemos fazer para prevenir ou reduzir danos?
• Ciclo de incidente
• Tipos de medidas:
  o Redutiva
  o Preventiva
  o Detectiva
  o Repressiva
  o Corretiva
	Exercício E
	• *Deixe que os alunos pensem em uma medida para cada uma das ameaças que foram listadas no quadro e, se a medida for muito cara, deixe-os decidir sobre aceitar os riscos inerentes.*
	
	Exercício F
	• *Junto com os alunos atribua as categorias de medidas (redutiva, preventiva, detectiva, repressiva e corretiva) para as medidas no quadro*

	branco.
8. Medidas físicas • Cabeamento, equipamento e anéis de proteção	*Questões a discutir com os alunos:* o *O que são ativos em sua organização? (prédios, facilidades, equipamentos, documentos, pessoas, reputação)* o *Classificação: Que tipo de informação você quer registrar sobre seus ativos se você não quer dar a eles o mesmo nível de segurança (proprietário, tipo, localização, nível de confidencialidade)* o *Exemplos de desastres?* o *Que tipo de medida você pode tomar? Exemplos de medidas redutiva, preventiva, detectiva, repressiva e corretiva.*
9. Medidas técnicas • Gerenciamento de acessos • Validação de dados de entrada e de saída • Criptografia e PKI *Explicar os conceitos sem entrar em detalhes técnicos. Os candidatos somente precisam entender os conceitos de criptografia, assinatura digital e certificado sem conhecer tecnicamente como eles funcionam.*	
10. Medidas organizacionais Por exemplo • Gerenciamento de ativos • Classificação • Política • Relato de incidentes • ISO/IEC 27002 (padrão) • Pessoal • Conscientização • Desastres e continuidade de negócios • Gerenciamento de mudanças • Testes • Segregação de funções • Terceirização • Proteção contra malware e phishing • Manuseio de mídias, equipamentos móveis e troca de informações • Política de mesa limpa	
11. Legislação e regulamentações • Compatibilidade com a legislação nacional antes das regulamentações da companhia • ISO/IEC 27002 • Propriedade intelectual	*Dar exemplos de atos legislativos relacionados à segurança da informação específicos para o local (país). Explicar a diferença entre uma norma e um ato legislativo.*

• Proteção de dados pessoais • Prevenção de abuso das facilidades de TI • Crime computacional • Lei Sarbanes-Oxley • Responsabilidade da gerência • Auditoria	