information security

# exame simulado

**ISFS.PR**

**Fundamentos da Segurança da Informação**
**baseados na norma ISO/IEC 27002**
**Edição 2010**

**conteúdo**




**EXIN International B.V.**
**Examination Institute for Information Science**
Janssoenborch, Hoog Catharijne
Godebaldkwartier 365, 3511 DT Utrecht
P.O. Box 19147, 3501 DC Utrecht
The Netherlands
Telephone +31 30 234 48 25
Fax +31 30 231 59 86
E-mail info@exin.nl
Internet www.exin-exams.com


ISO 9001 BUREAU VERITAS Certification

## Introdução

Este é um exemplo de exame de Fundamentos da Segurança da Informação baseados na norma ISO/IEC 27002.

Este exemplo de exame consiste de 40 questões de múltipla escolha. Cada questão tem um número de possíveis respostas, das quais somente uma resposta é a correta.

O número máximo de pontos que podem ser obtidos nesse exame é 40. Cada resposta correta tem o valor de um ponto. Se você obtiver 26 pontos ou mais será considerado aprovado.

O tempo permitido para o exame é de 60 minutos.

Nenhum direito será derivado desta informação.

Boa sorte!

## Exame simulado

**1 de 40**

Você recebeu do seu contador uma cópia da sua declaração fiscal e deve verificar se os dados estão corretos.

Qual característica de confiabilidade da informação que você está verificando?

**A**. Disponibilidade
**B**. Exclusividade
**C**. Integridade
**D**. Confidencialidade

**2 de 40**

A fim de ter uma apólice de seguro de incêndio, o departamento administrativo deve determinar o valor dos dados que ele gerencia.

Qual fator não é importante para determinar o valor de dados para uma organização?

**A**. O conteúdo dos dados.
**B**. O grau em que a falta, dados incompletos ou incorretos podem ser recuperados.
**C**. A indispensabilidade dos dados para os processos de negócio.
**D**. importância dos processos de negócios que fazem uso dos dados.

**3 de 40**

Nosso acesso à informação é cada vez mais fácil. Ainda assim, a informação tem de ser confiável, a fim de ser utilizável.

O que não é um aspecto de confiabilidade da informação?

**A**. Disponibilidade
**B**. Integridade
**C**. Quantidade
**D**. Confidencialidade

**4 de 40**

"Completeza" faz parte de qual aspecto de confiabilidade da informação?

**A**. Disponibilidade
**B**. Exclusividade
**C**. Integridade
**D**. Confidencialidade

**5 de 40**

Um departamento administrativo vai determinar os perigos aos quais está exposto.

O que chamamos de um possível evento que pode ter um efeito perturbador sobre a confiabilidade da informação?

**A**. Dependência
**B**. Ameaça
**C**. Vulnerabilidade
**D**. Risco

**6 de 40**

Qual é o propósito do gerenciamento de risco?

**A**. Determinar a probabilidade de que um certo risco ocorrerá.
**B**. Determinar os danos causados por possíveis incidentes de segurança.
**C**. Delinear as ameaças a que estão expostos os recursos de TI.
**D**. Utilizar medidas para reduzir os riscos para um nível aceitável.

**7 de 40**

Qual das afirmações sobre a análise de risco é a correta?

1. Riscos que são apresentados em uma análise de risco podem ser classificados.
2. Numa análise de risco todos os detalhes têm que ser considerados.
3. A análise de risco limita-se à disponibilidade.
4. A análise de risco é simples de efetuar através do preenchimento de um pequeno questionário padrão com perguntas padrão.

**A**. 1
**B**. 2
**C**. 3
**D**. 4

**8 de 40**

Qual dos exemplos abaixo pode ser classificado como fraude?

1. Infectar um computador com um vírus.
2. Realização de uma operação não autorizada.
3. Divulgação de linhas de comunicação e redes.
4. Utilização da Internet no trabalho para fins privados.

**A**. 1
**B**. 2
**C**. 3
**D**. 4

**9 de 40**

Um risco possível para uma empresa é dano por incêndio. Se essa ameaça ocorre, isto é, se um incêndio na verdade eclode, danos diretos e indiretos podem ocorrer.

O que é um exemplo de prejuízo direto?

**A**. Um banco de dados é destruído
**B**. Perda de imagem
**C**. Perda de confiança do cliente
**D**. Obrigações legais não podem mais ser satisfeitas

**10 de 40**

A fim de reduzir os riscos, uma empresa decide optar por uma estratégia de um conjunto de medidas. Uma das medidas é que um acordo stand-by é organizado para a empresa.

A que tipo de medidas um acordo stand-by pertence?

**A**. Medidas corretivas
**B**. Medidas detectivas
**C**. Medidas preventivas
**D**. Medidas repressivas

**11 de 40**

O que é um exemplo de uma ameaça humana?

**A**. Um pen drive que passa vírus para a rede.
**B**. Muito pó na sala do servidor.
**C**. Um vazamento que causa uma falha no fornecimento de eletricidade.

**12 de 40**

O que é um exemplo de uma ameaça humana?

**A**. Um apagão
**B**. Fogo
**C**. Phishing

**13 de 40**

A confiabilidade é constantemente ameaçada. Exemplos de ameaças são: um cabo se soltar, a informação que alguém altera por acidente, dados que são usados para fins particulares ou falsificados.

Qual destes exemplos é uma ameaça à confidencialidade?

**A**. Um cabo solto
**B**. Exclusão acidental de dados
**C**. Utilização privada de dados
**D**. Falsificação de dados

**14 de 40**

Um empregado nega o envio de uma mensagem específica.

Qual o aspecto de confiabilidade da informação está em perigo aqui?

**A**. Disponibilidade
**B**. Exatidão
**C**. Integridade
**D**. Confidencialidade

**15 de 40**

No ciclo de incidente há quatro etapas sucessivas.

Qual é a ordem dessas etapas?

**A**. Ameaça, Dano, Incidente, Recuperação
**B**. Ameaça, Incidente, Dano, Recuperação
**C**. Incidente, Ameaça, Dano, Recuperação
**D**. Incidente, Recuperação, Dano, Ameaça

**16 de 40**

Um incêndio interrompe os trabalhos da filial de uma empresa de seguros de saúde. Os funcionários são transferidos para escritórios vizinhos para continuar seu trabalho.

No ciclo de vida do incidente, onde são encontrados os arranjos de continuidade?

**A**. Entre a ameaça e o incidente
**B**. Entre a recuperação e a ameaça
**C**. Entre o dano e a recuperação
**D**. Entre o incidente e os danos

**17 de 40**

Como é melhor descrito o objetivo da política de segurança da informação?

**A**. A política documenta a análise de riscos e a busca de medidas de contorno.
**B**. A política fornece orientação e apoio à gestão em matéria de segurança da informação.
**C**. A política torna o plano de segurança concreto, fornecendo-lhe os detalhes necessários.
**D**. A política fornece percepções sobre as ameaças e as possíveis consequências.

**18 de 40**

O código de conduta para os negócios eletrônicos (e-business) é baseado em uma série de princípios.

Quais dos seguintes princípios não pertencem?

**A**. Confiabilidade
**B**. Registro
**C**. Confidencialidade e privacidade

**19 de 40**

Um trabalhador da companhia de seguros Euregio descobre que a data de validade de uma política foi alterada sem seu conhecimento. Ela é a única pessoa autorizada a fazer isso. Ela relata este incidente de segurança ao Helpdesk. O atendente do help desk registra as seguintes informações sobre este incidente:

data e hora
descrição do incidente
possíveis conseqüências do incidente

Que informação importante sobre o incidente está faltando aqui?

**A**. O nome da pessoa que denunciou o incidente
**B**. O nome do pacote de software
**C**. O número do PC
**D**. Uma lista de pessoas que foram informadas sobre o incidente

**20 de 40**

Uma empresa experimenta os seguintes incidentes:

1. Um alarme de incêndio não funciona.
2. A rede é invadida.
3. Alguém finge ser um membro do quadro de pessoal.
4. Um arquivo no computador não pode ser convertido em um arquivo PDF.

Qual destes incidentes não é um incidente de segurança?

**A**. 1
**B**. 2
**C**. 3
**D**. 4

**21 de 40**

As medidas de segurança podem ser agrupadas de várias maneiras.

Qual das seguintes é correta?

**A**. Física, lógica, preventiva
**B**. Lógica repressiva, preventiva
**C**. Organizacional, preventiva, corretiva, física
**D**. Preventiva, detectiva, repressiva, corretiva

**22 de 40**

Um alarme de fumaça é colocado em uma sala de computadores.

Sob qual categoria de medidas de segurança este item se enquadra?

**A**. Corretiva
**B**. Detectiva
**C**. Organizacional
**D**. Preventiva

**23 de 40**

O Security Officer (ISO-Information Security Officer)), da companhia de seguros Euregio deseja ter uma lista de medidas de segurança em conjunto.

O que ele tem que fazer, primeiramente, antes de selecionar as medidas de segurança a serem implementadas?

**A**. Implantar o monitoramento.
**B**. Realizar uma avaliação.
**C**. Formular uma política de segurança da informação.
**D**. Realizar uma análise de risco.

**24 de 40**

Qual é a finalidade da classificação das informações?

**A**. Determinar quais tipos de informações podem requerer diferentes níveis de proteção.
**B**. Atribuir informações a um proprietário.
**C**. Reduzir os riscos de erro humano.
**D**. Impedir o acesso não autorizado a informações.

**25 de 40**

A autenticação forte é necessária para acessar áreas altamente protegidas. Em caso de autenticação forte a identidade de uma pessoa é verificada através de três fatores.

Qual fator é verificado quando é preciso digitar um número de identificação pessoal (PIN)?

**A**. Algo que você é
**B**. Algo que você tem
**C**. Algo que você sabe

**26 de 40**

O acesso à sala de computadores está fechado usando um leitor de crachás. Somente o Departamento de Sistemas de Gestão tem um crachá.

Que tipo de medida de segurança é essa?

**A**. Uma medida de segurança de correção
**B**. Uma medida de segurança física
**C**. Uma medida de segurança lógica
**D**. Uma medida de segurança repressiva

**27 de 40**

Quatro membros do pessoal do departamento de TI compartilham um mesmo crachá.

A que risco este fato pode levar?

**A**. Se a energia falhar, os computadores vão ficar fora.
**B**. Se houver fogo os extintores de incêndio não podem ser usados.
**C**. Se alguma coisa desaparecer da sala de informática, não vai ficar claro quem é responsável.
**D**. Pessoas não autorizadas podem ter acesso à sala de computadores sem serem vistas.

**28 de 40**

No salão de recepção de um escritório da administração, há uma impressora que todos os funcionários podem usar em caso de emergência. O arranjo é que as impressões devem ser recolhidas imediatamente, para que elas não possam ser levadas por um visitante.

Qual outro risco para a informação da empresa que esta situação traz?

**A**. Os arquivos podem permanecer na memória da impressora.
**B**. Visitantes seriam capazes de copiar e imprimir as informações confidenciais da rede.
**C**. A impressora pode tornar-se deficiente através do uso excessivo, de modo que já não estará disponível para uso.

**29 de 40**

Qual das seguintes medidas de segurança é uma medida técnica?

1. Atribuição de Informações a um dono
2. Criptografia de arquivos
3. Criação de uma política de definição do que é e não é permitido no e-mail
4. Senhas do sistema de gestão armazenadas em um cofre

**A**. 1
**B**. 2
**C**. 3
**D**. 4

**30 de 40**

As cópias de segurança (backup) do servidor central são mantidas na mesma sala fechada como o servidor. Que risco a organização enfrenta?

**A**. Se o servidor falhar, levará um longo tempo antes que o servidor esteja novamente operacional.
**B**. Em caso de incêndio, é impossível obter o sistema de volta ao seu estado anterior.
**C**. Ninguém é responsável pelos backups.
**D**. Pessoas não autorizadas têm acesso fácil para os backups.

**31 de 40**

Qual das tecnologias abaixo é maliciosa?

**A**. Criptografia
**B**. Hash
**C**. Virtual Private Network (VPN)
**D**. Vírus, worms e spyware

**32 de 40**

Que medida não ajuda contra software mal-intencionado?

**A**. Uma política ativa de correções
**B**. Um programa anti-spyware
**C**. Um filtro anti-spam
**D**. Uma senha

**33 de 40**

O que é um exemplo de medida organizacional?

**A**. Cópia de segurança (backup) de dados
**B**. Criptografia
**C**. Segregação de funções
**D**. Manutenção de equipamentos de rede e caixas de junção em uma sala trancada

**34 de 40**

A identificação é determinar se a identidade de alguém é correta.

Esta declaração é correta?

**A**. sim
**B**. não

**35 de 40**

Por que é necessário manter um plano de recuperação de desastres atualizados e testá-lo regularmente?

**A**. A fim de sempre ter acesso às cópias de segurança (backups) recentes, que estão localizadas fora do escritório.
**B**. Para ser capaz de lidar com as falhas que ocorrem diariamente.
**C**. Porque de outra forma, na eventualidade de uma ruptura muito grande, as medidas tomadas e os procedimentos previstos podem não ser adequados ou podem estar desatualizados.
**D**. Porque esta é exigida pela Lei de Proteção de Dados Pessoais.

**36 de 40**

O que é a autorização?

**A**. A determinação da identidade de uma pessoa.
**B**. O registro das ações realizadas.
**C**. A verificação da identidade de uma pessoa.
**D**. A concessão de direitos específicos, tais como o acesso seletivo para uma pessoa.

**37 de 40**

Qual norma legal importante na área de segurança da informação que o governo tem que cumprir?

**A**. Análise de dependência e vulnerabilidade
**B**. ISO / IEC 20000
**C**. ISO / IEC 27002
**D**. Leislação nacional de segurança de informação ou regulamentos.

**38 de 40**

Com base em qual legislação alguém pode pedir para inspecionar os dados que tenham sido registrados?

**A**. A Lei de Registros Públicos
**B**. A Lei de Proteção de Dados Pessoais
**C**. A Lei de Crimes de Informática
**D**. A Lei de Acesso Público a Informações do Governo

**39 de 40**

O Código de Prática de Segurança da Informação (ISO / IEC 27002) é uma descrição de um método de análise de risco.

Esta declaração é correta?

**A**. Sim
**B**. Não

**40 de 40**

O Código de Prática de Segurança da Informação (ISO / IEC 27002) só se aplica às grandes empresas.

Esta declaração é correta?

**A**. Sim
**B**. Não

## Gabarito de respostas

**1 de 40**

Você recebeu do seu contador uma cópia da sua declaração fiscal e deve verificar se os dados estão corretos.

Qual característica de confiabilidade da informação que você está verificando?

**A**. Disponibilidade
**B**. Exclusividade
**C**. Integridade
**D**. Confidencialidade

A. Incorreto. A disponibilidade é o grau em que a informação está disponível para os usuários nos momentos necessários.
B. Incorreto. A exclusividade é uma característica de sigilo.
C. Correto. Esta é uma preocupação da integridade. Consulte a seção 4.5 *"Os princípios de segurança da informação"*.
D. Incorreto. Trata-se do grau em que o acesso à informação é restrito a apenas aqueles que são autorizados.

**2 de 40**

A fim de ter uma apólice de seguro de incêndio, o departamento administrativo deve determinar o valor dos dados que ele gerencia.

Qual fator não é importante para determinar o valor de dados para uma organização?

**A**. O conteúdo dos dados.
**B**. O grau em que a falta, dados incompletos ou incorretos podem ser recuperados.
**C**. A indispensabilidade dos dados para os processos de negócio.
**D**. importância dos processos de negócios que fazem uso dos dados.

A. Correto. O conteúdo dos dados não determina o seu valor. Ver ponto 4.3 do *"Os princípios de segurança da informação"*.
B. Incorreto. Dados ausentes, incompletos ou incorretos podem ser facilmente recuperados são menos valiosos do que os dados que são difíceis ou impossíveis de recuperar.
C. Incorreto. A indispensabilidade dos dados para os processos de negócios, em parte, determina o valor.
D. Incorreto. Dados críticos para os processos importantes de negócio são, consequentemente, valiosos.

**3 de 40**

Nosso acesso à informação é cada vez mais fácil. Ainda assim, a informação tem de ser confiável, a fim de ser utilizável.

O que não é um aspecto de confiabilidade da informação?

**A**. Disponibilidade
**B**. Integridade
**C**. Quantidade
**D**. Confidencialidade

A. Incorreto. A disponibilidade é um aspecto de confiabilidade da informação
B. Incorreto. A integridade é um aspecto de confiabilidade da informação
C. Correto. Quantidade não é um aspecto de confiabilidade das informações. Consulte a seção de 4.5 *"Os princípios de segurança da informação"*.
D. Incorreto. A confidencialidade é um aspecto de confiabilidade da informação

**4 de 40**

"Completeza" faz parte de qual aspecto de confiabilidade da informação?

**A**. Disponibilidade
**B**. Exclusividade
**C**. Integridade
**D**. Confidencialidade

A. Incorreto. As informações podem estar disponíveis sem ter que ser completas
B. Incorreto. A exclusividade é uma característica de sigilo.
C. Correto. Integridade é parte do aspecto de confiabilidade. Consulte a seção de 4.5 *"Os princípios de segurança da informação"*.
D. Incorreto. As informações confidenciais não têm que ser completas

**5 de 40**

Um departamento administrativo vai determinar os perigos aos quais está exposto.

O que chamamos de um possível evento que pode ter um efeito perturbador sobre a confiabilidade da informação?

**A**. Dependência
**B**. Ameaça
**C**. Vulnerabilidade
**D**. Risco

A. Incorreto. A dependência não é um evento.
B. Correto. A ameaça é um evento possível que pode ter um efeito perturbador sobre a confiabilidade da informação. Veja a seção 5 de *"Os princípios de segurança da informação"*.
C. Incorreto. A vulnerabilidade é o grau em que um objeto está suscetível a uma ameaça.
D. Incorreto. Um risco é o prejuízo médio esperado durante um período de tempo como resultado de uma ou mais ameaças levando à ruptura

**6 de 40**

Qual é o propósito do gerenciamento de risco?

**A**. Determinar a probabilidade de que um certo risco ocorrerá.
**B**. Determinar os danos causados por possíveis incidentes de segurança.
**C**. Delinear as ameaças a que estão expostos os recursos de TI.
**D**. Utilizar medidas para reduzir os riscos para um nível aceitável.

A. Incorreto. Isso faz parte da análise de risco.
B. Incorreto. Isso faz parte da análise de risco.
C. Incorreto. Isso faz parte da análise de risco.
D. Correto. O objetivo do gerenciamento de risco é o de reduzir os riscos para um nível aceitável. Veja a seção 5 de *"Os princípios de segurança da informação"*.

**7 de 40**

Qual das afirmações sobre a análise de risco é a correta?

1. Riscos que são apresentados em uma análise de risco podem ser classificados.
2. Numa análise de risco todos os detalhes têm que ser considerados.
3. A análise de risco limita-se à disponibilidade.
4. A análise de risco é simples de efetuar através do preenchimento de um pequeno questionário padrão com perguntas padrão.

**A**. 1
**B**. 2
**C**. 3
**D**. 4

A. Correto. Nem todos os riscos são iguais. Como regra os maiores riscos são abordados em primeiro lugar. Veja a seção 5 de *"Os princípios de segurança da informação"*.
B. Incorreto. É impossível em uma análise de risco examinar todos os detalhes.
C. Incorreto. A análise de risco considera todos os aspectos de confiabilidade, incluindo a integridade e confidencialidade, juntamente com a disponibilidade.
D. Incorreto. Em uma análise de riscos, questões raramente são aplicáveis a cada situação.

**8 de 40**

Qual dos exemplos abaixo pode ser classificado como fraude?

1. Infectar um computador com um vírus.
2. Realização de uma operação não autorizada
3. Divulgação de linhas de comunicação e redes.
4. Utilização da Internet no trabalho para fins privados.

**A**. 1
**B**. 2
**C**. 3
**D**. 4

A. Incorreto. A infecção por vírus é classificada como a "ameaça de alteração não autorizada".
B. Correto. Uma transação não autorizada é classificada como "fraude". Consulte a seção 10.6 de *"Os princípios de segurança da informação"*.
C. Incorreto. A divulgação de linhas de comunicação e redes é classificada como "ameaça" de divulgação.
D. Incorreto. A utilização privada é classificada como a ameaça de "abuso".

**9 de 40**

Um risco possível para uma empresa é dano por incêndio. Se essa ameaça ocorre, isto é, se um incêndio na verdade eclode, danos diretos e indiretos podem ocorrer.

O que é um exemplo de prejuízo direto?

**A**. Um banco de dados é destruído
**B**. Perda de imagem
**C**. Perda de confiança do cliente
**D**. Obrigações legais não podem mais ser satisfeitas

A. Correto. Um banco de dados destruído é um exemplo de prejuízos direto. Ver ponto 5.5 do *"Os princípios de segurança da informação"*.
B. Incorreto. Danos de imagem é um prejuízo indireto.
C. Incorreto. Perda de confiança do cliente é indireto.
D. Incorreto. Ser incapaz de cumprir as obrigações legais é dano indireto.

**10 de 40**

A fim de reduzir os riscos, uma empresa decide optar por uma estratégia de um conjunto de medidas. Uma das medidas é que um acordo stand-by é organizado para a empresa.

A que tipo de medidas um acordo stand-by pertence?

**A**. Medidas corretivas
**B**. Medidas detectivas
**C**. Medidas preventivas
**D**. Medidas repressivas

A. Incorreto. Medidas corretivas são tomadas após evento
B. Incorreto. Medidas detectivas são tomadas depois de um sinal de detecção.
C. Incorreto. As medidas preventivas são destinadas a evitar incidentes.
D. Correto. Medidas repressivas, tais como um acordo stand-by, visam minimizar os danos.
Consulte a seção 5.3.4 de *"Os princípios de segurança da informação"*.

**11 de 40**

O que é um exemplo de uma ameaça humana?

**A**. Um pen drive que passa vírus para a rede.
**B**. Muito pó na sala do servidor.
**C**. Um vazamento que causa uma falha no fornecimento de eletricidade.

A. Correto. Um pen drive que passa vírus para a rede sempre é inserido por uma pessoa. Desta forma, um vírus que entra na rede é, então, uma ameaça humana. Veja a seção 5.4.1 de *"Os princípios de segurança da informação"*.
B. Incorreto. Poeira não é uma ameaça humana.
C. Incorreto. A falha de energia elétrica não é uma ameaça humana.

**12 de 40**

O que é um exemplo de uma ameaça humana?

**A**. Um apagão
**B**. Fogo
**C**. Phishing

A. Incorreto. Um relâmpago é um exemplo de uma ameaça não humana
B. Incorreto. O fogo é um exemplo de uma ameaça não humana
C. Correto. Phishing (atraem usuários para sites falsos) é uma forma de ameaça humana. Veja a seção 5.4.1 e 9.4.6 de *"Os princípios de segurança da informação"*.

**13 de 40**

A confiabilidade é constantemente ameaçada. Exemplos de ameaças são: um cabo se soltar, a informação que alguém altera por acidente, dados que são usados para fins particulares ou falsificados.

Qual destes exemplos é uma ameaça à confidencialidade?

**A**. Um cabo solto
**B**. Exclusão acidental de dados
**C**. Utilização privada de dados
**D**. Falsificação de dados

A. Incorreto. Um cabo solto é uma ameaça para a disponibilidade de informações.
B. Incorreto. A alteração não intencional de dados é uma ameaça à sua integridade.
C. Correto. A utilização de dados para fins privados é uma forma de abuso e é uma ameaça à confidencialidade. Consulte a seção de 4.5 *"Os princípios de segurança da informação"*.
D. Incorreto. A falsificação de dados é uma ameaça à sua integridade.

**14 de 40**

Um empregado nega o envio de uma mensagem específica.

Qual o aspecto de confiabilidade da informação está em perigo aqui?

**A**. Disponibilidade
**B**. Exatidão
**C**. Integridade
**D**. Confidencialidade

A. Incorreto. Sobrecarregar a infra-estrutura é um exemplo de uma ameaça à disponibilidade.
B. Incorreto. Exatidão não é um aspecto de confiabilidade. É uma característica de integridade.
C. correto. A negação do envio de uma mensagem tem a ver com o não-repúdio, uma ameaça à integridade. Consulte a seção de 4.5 *"Os princípios de segurança da informação"*.
D. Incorreto. O uso indevido e / ou divulgação de dados são ameaças à confidencialidade.

**15 de 40**

No ciclo de incidente há quatro etapas sucessivas.

Qual é a ordem dessas etapas?

**A**. Ameaça, Dano, Incidente, Recuperação
**B**. Ameaça, Incidente, Dano, Recuperação
**C**. Incidente, Ameaça, Dano, Recuperação
**D**. Incidente, Recuperação, Dano, Ameaça

A. Incorreto. Os danos se seguem após o incidente.
B. Correto. A ordem das etapas do ciclo do incidente é: ameaça, incidente, dano e recuperação. Veja a seção 6.4.4 de *"Os princípios de segurança da informação"*.
C. Incorreto. O incidente segue a ameaça.
D. Incorreto. A recuperação é a última etapa.

**16 de 40**

Um incêndio interrompe os trabalhos da filial de uma empresa de seguros de saúde. Os funcionários são transferidos para escritórios vizinhos para continuar seu trabalho.

No ciclo de vida do incidente, onde são encontrados os arranjos de continuidade?

**A**. Entre a ameaça e o incidente
**B**. Entre a recuperação e a ameaça
**C**. Entre o dano e a recuperação
**D**. Entre o incidente e os danos

A. Incorreto. Realização de um acordo stand-by, sem que primeiro haja um incidente é muito caro.
B. Incorreto. A recuperação ocorre após a colocação do acordo de stand-by em funcionamento.
C. Incorreto. Danos e recuperação são realmente limitados pelo acordo stand-by.
D. Correto. Um stand-by é uma medida repressiva que é iniciada, a fim de limitar os danos. Veja a seção 6.4.4 e 9.3 de *"Os princípios de segurança da informação"*.

**17 de 40**

Como é melhor descrito o objetivo da política de segurança da informação?

**A**. A política documenta a análise de riscos e a busca de medidas de contorno.
**B**. A política fornece orientação e apoio à gestão em matéria de segurança da informação.
**C**. A política torna o plano de segurança concreto, fornecendo-lhe os detalhes necessários.
**D**. A política fornece percepções sobre as ameaças e as possíveis consequências.

A. Incorreto. Este é o propósito da análise e gerenciamento de riscos.
B. Correto. A política de segurança fornece orientação e apoio à gestão em matéria de segurança da informação. Veja a seção 9.1 de *"Os princípios de segurança da informação"*.
C. Incorreto. O plano de segurança faz com que a política de segurança da informação seja concret
A. O plano inclui medidas que tenham sido escolhidas, quem é responsável pelo que, as orientações para a implementação de medidas, etc.
D. Incorreto. Este é o propósito de uma análise de ameaça.

**18 de 40**

O código de conduta para os negócios eletrônicos (e-business) é baseado em uma série de princípios.

Quais dos seguintes princípios não pertencem?

**A**. Confiabilidade
**B**. Registro
**C**. Confidencialidade e privacidade

A. Incorreto. Confiabilidade forma uma das bases do código de conduta.
B. Correto. O código de conduta é baseado nos princípios de confiabilidade, transparência, confidencialidade e privacidade. Consulte a 9.4.12 seção de *"Os princípios de segurança da informação"*.
C. Incorreto. O código de conduta se baseia em matéria de confidencialidade e privacidade, entre outras coisas.

**19 de 40**

Um trabalhador da companhia de seguros Euregio descobre que a data de validade de uma política foi alterada sem seu conhecimento. Ela é a única pessoa autorizada a fazer isso. Ela relata este incidente de segurança ao Helpdesk. O atendente do help desk registra as seguintes informações sobre este incidente:

data e hora
descrição do incidente
possíveis conseqüências do incidente

Que informação importante sobre o incidente está faltando aqui?

**A**. O nome da pessoa que denunciou o incidente
**B**. O nome do pacote de software
**C**. O número do PC
**D**. Uma lista de pessoas que foram informadas sobre o incidente

A. Correto. Ao relatar um incidente, o nome do usuário deve ser registrado no mínimo. Veja a seção 6.4.1 de *"Os princípios de segurança da informação"*.
B. Incorreto. Esta informação adicional pode ser adicionada posteriormente
C. Incorreto. Esta informação adicional pode ser adicionada posteriormente
D. Incorreto. Esta informação adicional pode ser adicionada posteriormente

**20 de 40**

Uma empresa experimenta os seguintes incidentes:

1. Um alarme de incêndio não funciona.
2. A rede é invadida.
3. Alguém finge ser um membro do quadro de pessoal.
4. Um arquivo no computador não pode ser convertido em um arquivo PDF.

Qual destes incidentes não é um incidente de segurança?

**A**. 1
**B**. 2
**C**. 3
**D**. 4

A. Incorreto. Um alarme de incêndio defeituoso é um incidente que pode ameaçar a disponibilidade de dados.
B. Incorreto. Hacking é um incidente que pode ameaçar a disponibilidade, integridade e confidencialidade dos dados.
C. Incorreto. Desvio de identidade é um incidente que pode ameaçar o aspecto da disponibilidade, integridade e confidencialidade dos dados.
D. Correto. Um incidente de segurança é um incidente que ameaça a confidencialidade, confiabilidade e disponibilidade dos dados. Esta não é uma ameaça para a disponibilidade, integridade e confidencialidade dos dados. Consulte a seção de 6.4 *"Os princípios de segurança da informação"*.

**21 de 40**

As medidas de segurança podem ser agrupadas de várias maneiras.

Qual das seguintes é correta?

**A**. Física, lógica, preventiva
**B**. Lógica repressiva, preventiva
**C**. Organizacional, preventiva, corretiva, física
**D**. Preventiva, detectiva, repressiva, corretiva

A. Incorreto. Organizacional / lógico / físico é um grupo apropriado, como é preventiva / detectiva / repressiva / corretivas.
B. Incorreto. Organizacional / lógico / físico é um grupo apropriado, como é preventiva / detectiva / repressiva / corretivas.
C. Incorreto. Organizacional / lógico / físico é um grupo apropriado, como é preventiva / detectiva / repressiva / corretivas.
D. Correto. Preventiva / detectiva / repressiva / corretiva é um grupo apropriado, como é organizacional / lógico / físico. Consulte a seção de 5.3 *"Os princípios de segurança da informação"*.

**22 de 40**

Um alarme de fumaça é colocado em uma sala de computadores.

Sob qual categoria de medidas de segurança este item se enquadra?

**A**. Corretiva
**B**. Detectiva
**C**. Organizacional
**D**. Preventiva

A. Incorreto. Um alarme detecta fumaça e, em seguida, envia um alarme, mas não tomar qualquer ação corretiva.
B. Correto. Um alarme de incêndio só tem uma função de sinalização, após o alarme dado, a ação ainda é necessária. Consulte a seção de 5.3 *"Os princípios de segurança da informação"*.
C. Incorreto. Só as medidas que seguem um sinal de alarme de incêndio são organizacionais; a colocação de um alarme de fumaça não é organizacional.
D. Incorreto. Um alarme de fumaça não impede o fogo e não é, portanto, uma medida preventiva.

**23 de 40**

O Security Officer (ISO-Information Security Officer), da companhia de seguros Euregio deseja ter uma lista de medidas de segurança em conjunto.

O que ele tem que fazer, primeiramente, antes de selecionar as medidas de segurança a serem implementadas?

**A**. Implantar o monitoramento.
**B**. Realizar uma avaliação.
**C**. Formular uma política de segurança da informação.
**D**. Realizar uma análise de risco.

A. Incorreto. O monitoramento é uma medida possível.
B. Incorreto. A avaliação acontece depois que a lista de medidas é montada.
C. Incorreto. Uma política de segurança da informação é importante, mas não é necessária a fim de selecionar medidas.
D. Correto. Antes das medidas de segurança serem selecionadas, Euregio deve conhecer os seus riscos para determinar quais os riscos requerem uma medida de segurança. Veja a seção 5 de *"Os princípios de segurança da informação"*.

**24 de 40**

Qual é a finalidade da classificação das informações?

**A**. Determinar quais tipos de informações podem requerer diferentes níveis de proteção.
**B**. Atribuir informações a um proprietário.
**C**. Reduzir os riscos de erro humano.
**D**. Impedir o acesso não autorizado a informações.

A. Correto. O objetivo da classificação das informações é de manter uma proteção adequada. Consulte a seção de 6.3 *"Os princípios de segurança da informação"*.
B. Incorreto. Alocação de informações para um proprietário é o meio de classificação e não o fim.
C. Incorreto. Reduzir os riscos de erro humano é parte dos requisitos de segurança dos funcionários.
D. Incorreto. Impedir o acesso não autorizado a informações é parte de segurança de acesso.

**25 de 40**

A autenticação forte é necessária para acessar áreas altamente protegidas. Em caso de autenticação forte a identidade de uma pessoa é verificada através de três fatores.

Qual fator é verificado quando é preciso digitar um número de identificação pessoal (PIN)?

**A**. Algo que você é
**B**. Algo que você tem
**C**. Algo que você sabe

A. Incorreto. Um código PIN não é um exemplo de algo que você é.
B. Incorreto. Um código PIN não é algo que você tem.
C. Correto. Um código PIN é algo que você sabe. Consulte a seção 7.2.2.1 de *"Os princípios de segurança da informação"*.

**26 de 40**

O acesso à sala de computadores está fechado usando um leitor de crachás. Somente o Departamento de Sistemas de Gestão tem um crachá.

Que tipo de medida de segurança é essa?

**A**. Uma medida de segurança de correção
**B**. Uma medida de segurança física
**C**. Uma medida de segurança lógica
**D**. Uma medida de segurança repressiva

A. Incorreto. A medida de segurança de correção é uma medida de recuperação.
B. Correto. Esta é uma medida de segurança física. Consulte a seção 7 do *"Os princípios de segurança da informação"*.
C. Incorreto. Uma medida de segurança lógica controla o acesso ao software e informação, e não o acesso físico às salas
D. Incorreto. A medida de segurança repressiva visa minimizar as conseqüências de um rompimento.

**27 de 40**

Quatro membros do pessoal do departamento de TI compartilham um mesmo crachá.

A que risco este fato pode levar?

**A**. Se a energia falhar, os computadores vão ficar fora.
**B**. Se houver fogo os extintores de incêndio não podem ser usados.
**C**. Se alguma coisa desaparecer da sala de informática, não vai ficar claro quem é responsável.
**D**. Pessoas não autorizadas podem ter acesso à sala de computadores sem serem vistas.

A. Incorreto. Computadores fora do ar como resultado de uma falha de energia não têm nada a ver com a gestão de acesso.
B. Incorreto. Mesmo com um crachá, a equipe de TI pode apagar um incêndio com um extintor de incêndio.
C. Correto. Embora fosse claro que alguém do departamento de TI entrou na sala, não é certo que isso tenha acontecido. Consulte a seção de 7.2 *"Os princípios de segurança da informação"*.
D. Incorreto. Ninguém tem acesso à sala de computadores sem um crachá.

**28 de 40**

No salão de recepção de um escritório da administração, há uma impressora que todos os funcionários podem usar em caso de emergência. O arranjo é que as impressões devem ser recolhidas imediatamente, para que elas não possam ser levadas por um visitante.

Qual outro risco para a informação da empresa que esta situação traz?

**A**. Os arquivos podem permanecer na memória da impressora.
**B**. Visitantes seriam capazes de copiar e imprimir as informações confidenciais da rede.
**C**. A impressora pode tornar-se deficiente através do uso excessivo, de modo que já não estará disponível para uso.

A. Correto. Se os arquivos permanecem na memória podem ser impressos e levados por qualquer transeunte. 9.4.11 consulte a seção de *"Os princípios de segurança da informação"*.
B. Incorreto. Não é possível usar uma impressora para copiar as informações da rede.
C. Incorreto. A indisponibilidade de uma impressora não forma um risco para a informação da companhia.

**29 de 40**

Qual das seguintes medidas de segurança é uma medida técnica?

1. Atribuição de Informações a um dono
2. Criptografia de arquivos
3. Criação de uma política de definição do que é e não é permitido no e-mail
4. Senhas do sistema de gestão armazenadas em um cofre

**A**. 1
**B**. 2
**C**. 3
**D**. 4

A. Incorreto. Alocação de informações para um proprietário é a classificação, que é uma medida organizacional.
B. Correto. Esta é uma medida técnica que impede que pessoas não autorizadas leiam as informações. Ver ponto 8.3 do *"Os princípios de segurança da informação"*.
C. Incorreto. Esta é uma medida organizacional, um código de conduta que está escrito no contrato de trabalho.
D. Incorreto. Esta é uma medida organizacional.

**30 de 40**

As cópias de segurança (backup) do servidor central são mantidas na mesma sala fechada como o servidor. Que risco a organização enfrenta?

**A**. Se o servidor falhar, levará um longo tempo antes que o servidor esteja novamente operacional.
**B**. Em caso de incêndio, é impossível obter o sistema de volta ao seu estado anterior.
**C**. Ninguém é responsável pelos backups.
**D**. Pessoas não autorizadas têm acesso fácil para os backups.

A. Incorreto. Pelo contrário, isso ajudaria a recuperar o sistema operacional mais rapidamente.
B. Correto. A chance de que as cópias de segurança também podem ser destruídas em um incêndio é muito grande. Veja a seção 9.4.7 de *"Os princípios de segurança da informação"*.
C. Incorreto. A responsabilidade não tem nada a ver com o local de armazenamento.
D. Incorreto. A sala de informática está bloqueada.

**31 de 40**

Qual das tecnologias abaixo é maliciosa?

**A**. Criptografia
**B**. Hash
**C**. Virtual Private Network (VPN)
**D**. Vírus, worms e spyware

A. Incorreto. Criptografia torna a informação impossível de ser lida por qualquer pessoa, exceto aquela que possue conhecimento especial, usualmente feito por uma chave
B. Incorreto. Hash é um método de criptografia da informação
C. Incorreto. VPN é uma conexão segura feita para acesso à internet
D. Correto. Todas essas são formas de tecnologias maliciosas que estabelecem pedidos a um computador para fins maliciosos. Veja a seção 9.4.6 de *"Os princípios de segurança da informação"*.

**32 de 40**

Que medida não ajuda contra software mal-intencionado?

**A**. Uma política ativa de correções
**B**. Um programa anti-spyware
**C**. Um filtro anti-spam
**D**. Uma senha

A. Incorreto. Software mal intencionado freqüentemente usa falhas de programação em programas populares. Correções reparam brechas de segurança nesses programas, reduzindo a chance de infecções por software mal intencionado.
B. Incorreto. Spyware é um programa malicioso que coleta informações confidenciais e então as distribui. Um programa anti-spyware pode detectar esse tipo de programa no computador
C. Incorreto. Spam é um e-mail não pedido. É freqüentemente uma simples propaganda, mas pode também ter programas maliciosos anexados ou um link para um site na internet com software malicioso. Um filtro remove spam.
D. Correto. Uma senha é um meio de autenticação. Ela não bloqueia qualquer tipo de software malicioso. Veja seção 8.1.2.1 de *"Os princípios de segurança da informação"*.

**33 de 40**

O que é um exemplo de medida organizacional?

**A**. Cópia de segurança (backup) de dados
**B**. Criptografia
**C**. Segregação de funções
**D**. Manutenção de equipamentos de rede e caixas de junção em uma sala trancada

A. Incorreto. Cópia de segurança (backup) é uma medida técnica
B. Incorreto. Criptografia de dados é uma medida técnica
C. Correto. Segregação de funções é uma medida organizacional. A iniciação, execução e controle de funções são alocados a diferentes pessoas. Por exemplos, a transferência de um grande volume de dinheiro é preparada por um escriturário, o diretor financeiro executa o pagamento e um contador audita a transação. Veja seção 9.4.3 de *"Os princípios de segurança da informação"*.
D. Incorreto. Trancar as salas é uma medida de segurança física.

**34 de 40**

A identificação é determinar se a identidade de alguém é correta.

Esta declaração é correta?

**A**. sim
**B**. não

A. Incorreto. Identificação é o processo de tornar uma identidade conhecida.
B. Correto. Estabelecer se a identidade de alguém é correta é chamado de autenticação. Veja a seção 8.1 de *"Os princípios de segurança da informação"*.

**35 de 40**

Por que é necessário manter um plano de recuperação de desastres atualizados e testá-lo regularmente?

**A**. A fim de sempre ter acesso às cópias de segurança (backups) recentes, que estão localizadas fora do escritório.
**B**. Para ser capaz de lidar com as falhas que ocorrem diariamente.
**C**. Porque de outra forma, na eventualidade de uma ruptura muito grande, as medidas tomadas e os procedimentos previstos podem não ser adequados ou podem estar desatualizados.
**D**. Porque esta é exigida pela Lei de Proteção de Dados Pessoais.

A. Incorreto. Esta é uma das medidas técnicas utilizadas para recuperar um sistema.
B. Incorreto. Para rupturas normais, as medidas usualmente executadas e os procedimentos de incidentes são suficientes.
C. Correto. Uma ruptura maior requer planos atualizados e testados. Veja seção 9.3 de *"Os princípios de segurança da informação"*.
D. Incorreto. A Lei de Proteção de Dados Pessoais envolve a privacidade dos dados pessoais.

**36 de 40**

O que é a autorização?

**A**. A determinação da identidade de uma pessoa.
**B**. O registro das ações realizadas.
**C**. A verificação da identidade de uma pessoa.
**D**. A concessão de direitos específicos, tais como o acesso seletivo para uma pessoa.

A. Incorreto. A determinação da identidade de uma pessoa é chamada de identificação
B. Incorreto. O registro das ações realizadas é chamado diário
C. Incorreto. A verificação da identidade da pessoa é chamada de autenticação
D. Correto. A permissão de direitos específicos, tal como acesso seletivo para uma pessoa, é chamada de autorização. Veja seção 8.1 de *"Os princípios de segurança da informação"*.

**37 de 40**

Qual norma legal importante na área de segurança da informação que o governo tem que cumprir?

**A**. Análise de dependência e vulnerabilidade
**B**. ISO / IEC 20000
**C**. ISO / IEC 27002
**D**. Leislação nacional de segurança de informação ou regulamentos.

A. Incorreto.  Dependência & Análise de Risco é um método de análise de risco.
B. Incorreto. ISO/IEC 20000 é um padrão para organizar o gerenciamento de serviços de TI e não é compulsório.
C. Incorreto. ISO/IEC 27002 é o Código de Segurança da Informação. É um guia para organizar a Segurança de Informação e não é compulsório.
D. Correto. Legislação nacional de segurança da informação ou regulamentos são intencionados para todos os governos e são obrigatórios. Veja seção 10 de *"Os princípios de segurança da informação"*.

**38 de 40**

Com base em qual legislação alguém pode pedir para inspecionar os dados que tenham sido registrados?

**A**. A Lei de Registros Públicos
**B**. A Lei de Proteção de Dados Pessoais
**C**. A Lei de Crimes de Informática
**D**. A Lei de Acesso Público a Informações do Governo

A. Incorreto. A Lei de Registros Públicos regula o armazenamento e a destruição de documentos arquivados.
B. Correto. O direito de inspeção é regulado na Lei de Proteção de Dados Pessoais. Veja seção 10.5 de *"Os princípios de segurança da informação"*.
C. Incorreto. A Lei de Crimes de Informática é uma mudança do Código Penal e do Código de Processo Criminal de forma a tornar mais fácil lidar com ofensas praticadas por meio de tecnologia da informação avançada. Um exemplo de uma nova ofensa é o hacking.
D. Incorreto. A Lei de Acesso Público a Informações do Governo regula a inspeção de documentos oficiais escritos. Dados pessoais não são documentos oficiais.

**39 de 40**

O Código de Prática de Segurança da Informação (ISO / IEC 27002) é uma descrição de um método de análise de risco.

Esta declaração é correta?

**A**. Sim
**B**. Não

A. Incorreto. O Código de Segurança da Informação é uma coleção de medidas.
B. Correto. O Código de Segurança da Informação pode ser usado em uma análise de risco mas não é um método. Veja seção 9.1 de *"Os princípios de segurança da informação"*.

**40 de 40**

O Código de Prática de Segurança da Informação (ISO / IEC 27002) só se aplica às grandes empresas.

Esta declaração é correta?

**A**. Sim
**B**. Não

A. Incorreto. O Código de Segurança da Informação é aplicável a todos os tipos de organização, grandes e pequenas.
B. Correto. O Código de Segurança da Informação é aplicável a todos os tipos de organização, grandes e pequenas. Veja seção 9.1 de *"Os princípios de segurança da informação"*.

## Avaliação

A tabela abaixo mostra as respostas corretas às questões deste exemplo de exame.

| número | resposta | pontos |
|---|---|---|
| 1 | **C** | 1 |
| 2 | **A** | 1 |
| 3 | **C** | 1 |
| 4 | **C** | 1 |
| 5 | **B** | 1 |
| 6 | **D** | 1 |
| 7 | **A** | 1 |
| 8 | **B** | 1 |
| 9 | **A** | 1 |
| 10 | **D** | 1 |
| 11 | **A** | 1 |
| 12 | **C** | 1 |
| 13 | **C** | 1 |
| 14 | **C** | 1 |
| 15 | **B** | 1 |
| 16 | **D** | 1 |
| 17 | **B** | 1 |
| 18 | **B** | 1 |
| 19 | **A** | 1 |
| 20 | **D** | 1 |

| número | resposta | pontos |
|---|---|---|
| 21 | **D** | 1 |
| 22 | **B** | 1 |
| 23 | **D** | 1 |
| 24 | **A** | 1 |
| 25 | **C** | 1 |
| 26 | **B** | 1 |
| 27 | **C** | 1 |
| 28 | **A** | 1 |
| 29 | **B** | 1 |
| 30 | **B** | 1 |
| 31 | **D** | 1 |
| 32 | **D** | 1 |
| 33 | **C** | 1 |
| 34 | **B** | 1 |
| 35 | **C** | 1 |
| 36 | **D** | 1 |
| 37 | **D** | 1 |
| 38 | **B** | 1 |
| 39 | **B** | 1 |
| 40 | **B** | 1 |