Exame simulado

Edição 201804

Conteúdo

Introdução

Este é o exame simulado de EXIN Information Security Foundation baseado na ISO/IEC 27001. As regras e regulamentos do exame do EXIN se aplicam a este exame.

Este exame simulado consiste de 40 questões de múltipla escolha. Cada questão de múltipla escolha possui um certo número de alternativas de resposta, entre as quais apenas uma resposta é a correta.

O número máximo de pontos que pode ser obtido neste exame é 40. Cada resposta correta vale um ponto. Para passar você deve obter 26 pontos ou mais.

O tempo permitido para este exame é de 60 minutos.

Boa Sorte!

Exame simulado

1 / 40

Qual a relação entre dados e informações?

A. Dados são informações estruturadas
B. Informações são o significado e o valor atribuídos a uma coleção de dados

2 / 40
A fim de ter uma apólice de seguro de incêndio, o departamento administrativo deve determinar o valor dos dados que gerencia.

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

A. O conteúdo dos dados.
B. O grau em que, dados ausentes 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 / 40
Um hacker obtém acesso a um servidor Web e pode exibir um arquivo no servidor que contém números de cartão de crédito.

Quais princípios de confidencialidade, integridade e disponibilidade (CIA) do arquivo de cartão de crédito são violados?

A. Disponibilidade
B. Confidencialidade
C. Integridade

4 / 40
Existe uma impressora de rede no corredor da empresa onde você trabalha. Muitos funcionários não vão pegar suas impressões imediatamente e deixam o material na impressora.

Quais são as consequências disto com relação à confiabilidade das informações?

A. A integridade das informações não pode mais ser garantida
B. A disponibilidade das informações não pode mais ser garantida
C. A confidencialidade das informações não pode mais ser garantida

5 / 40
Uma análise de risco bem executada oferece uma grande quantidade de informações úteis. A análise de risco tem quatro principais objetivos.

Qual das opções abaixo **não** é um dos quatro principais objetivos da análise de risco?

A. Identificação dos ativos e seus valores
B. Implementação de contramedidas
C. Estabelecimento do equilíbrio entre os custos de um incidente e os custos de medidas de segurança
D Determinação de vulnerabilidades e ameaças relevantes

6 / 40
Um departamento administrativo vai determinar os riscos aos quais está exposto.

Como denominamos um possível evento que possa comprometer a confiabilidade da informação?

A. Dependência
B. Ameaça
C. Vulnerabilidade
D Risco

7 / 40
Qual é o propósito do gerenciamento de risco?

A. Determinar a probabilidade de ocorrência de um certo risco.
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.

8 / 40
Há alguns anos você começou sua empresa, que já cresceu de 1 para 20 empregados. As informações de sua empresa valem mais e mais e já passaram os dias em que você podia manter tudo em suas próprias mãos. Você está ciente de que precisa tomar medidas, mas quais? Você contrata um consultor, que o aconselha a começar com uma análise de risco qualitativa.

O que é uma análise de risco qualitativa?

A. Esta análise segue um cálculo preciso de probabilidade estatística a fim de calcular a exata perda causada pelo dano
B. Esta análise é baseada em cenários e situações e produz uma visão subjetiva de possíveis ameaças

9 / 40
Houve um incêndio em uma filial da companhia Midwest Insurance. Os bombeiros chegaram rapidamente ao local e puderam apagar o fogo antes que se espalhasse e queimasse toda a instalação. O servidor, entretanto, foi destruído pelo fogo. As fitas de segurança (backup) mantidas em outra sala derreteram e muitos outros documentos foram perdidos definitivamente.

Qual é um exemplo de dano indireto causado pelo incêndio?

A. Fitas de segurança (backup) derretidas
B. Sistemas de computação queimados
C. Documentos queimados
D. Danos provocados pela água dos extintores de incêndio

10 / 40
Você é o proprietário de uma companhia de correio (courier), SpeeDelivery. Você realizou uma análise de risco e agora quer determinar sua estratégia de risco. Você decide tomar medidas contra os grandes riscos, mas não contra os pequenos riscos.

Como é chamada a estratégia de risco adotada neste caso?

A. Retenção de risco
B. Prevenção de risco
C. Redução de risco

11 / 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. Uma fuga de energia que causa uma falha no fornecimento de eletricidade.

12 / 40
O que é um exemplo de uma ameaça humana?

A. Um relâmpago
B. Fogo
C. Phishing

13 / 40

Você trabalha no escritório de uma grande companhia. Você recebe um telefonema de uma pessoa dizendo ser do helpdesk. Ela pede para que você lhe diga sua senha.

Que tipo de ameaça é esta?

A. Ameaça natural
B. Ameaça organizacional
C. Engenharia social

14 / 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 acordos stand-by (plano de contingência)?

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

15 / 40
Informações envolvem inúmeros aspectos de confiabilidade, a qual é constantemente ameaçada. Exemplos de ameaças são: um cabo se soltar, informações alteradas por acidente, dados que são usados para fins particulares ou falsificados.

Qual destes exemplos é uma ameaça à integridade?

A. Um cabo solto
B. Alteração acidental de dados
C. Utilização privada de dados

16 / 40
Um funcionário nega o envio de uma mensagem específica.

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

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

17 / 40
Qual a **melhor** maneira de descrever o objetivo da política de segurança da informação?

A. A política documenta a análise de riscos e a busca de contramedidas.
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 / 40
Um incidente de segurança relacionado com um servidor Web é relatado a um funcionário do helpdesk. Sua colega tem mais experiência em servidores Web; então, ele transfere o caso para ela.

Qual termo descreve essa transferência?

A. Escalonamento funcional
B. Escalonamento hierárquico

19 / 40
Uma funcionária trabalhador de uma companhia de seguros 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 helpdesk registra as seguintes informações sobre este incidente:

- data e hora
- descrição do incidente
- possíveis consequências do incidente

Qual a informação mais 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 / 40
No ciclo de incidente há quatro etapas sucessivas.

Qual é a etapa que sucede o incidente?

A. Ameaça
B. Dano
C. Recuperação

21 / 40
Qual das seguintes medidas é uma medida preventiva?

A. Instalação de um sistema de registro de eventos (log) que permite que mudanças em um sistema sejam reconhecidas
B. Desativação de todo tráfego internet depois que um hacker ganhou acesso aos sistemas da companhia
C. Armazenamento de informações sigilosas em um cofre

22 / 40
Qual das opções abaixo é uma medida repressiva em caso de incêndio?

A. Fazer um seguro contra incêndio
B. Apagar o fogo depois que o incêndio for detectado pelo detector de incêndio
C. Reparar os danos causados pelo incêndio

23 / 40
Qual é o objetivo da classificação da informação?

A. Criar um manual sobre como manusear dispositivos móveis
B. Aplicar identificações que facilitem o reconhecimento das informações
C. Estruturar as informações de acordo com sua confidencialidade

24 / 40
Quem é autorizado a mudar a classificação de um documento?

A. O autor do documento
B. O administrador do documento
C. O proprietário do documento
D. O gerente do proprietário do documento

25 / 40
O acesso à sala de computadores está bloqueado por um leitor de crachás. Somente o Departamento de Gerenciamento de Sistemas tem um crachá.

Que tipo de medida de segurança é essa?

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

26 / 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 mostrar um crachá de acesso?

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

27 / 40
Na segurança física, múltiplas zonas em expansão (anéis de proteção) podem ser aplicadas, nas quais diferentes medidas podem ser adotadas.

O que não é um anel de proteção?

A. Edifício
B. Anel médio
C. Objeto
D. Anel externo

28 / 40
Qual das ameaças listadas abaixo pode ocorrer como resultado da ausência de uma medida de segurança física?

A. Um usuário pode ver os arquivos pertencentes a outro
B. Um servidor é desligado por causa de superaquecimento
C. Um documento confidencial é deixado na impressora
D. Hackers podem entrar livremente na rede de computadores

29 / 40
Qual das seguintes medidas de segurança é uma medida técnica?

A. Atribuição de informações a um proprietário
B. Criptografia de arquivos
C. Criação de uma política que define o que é e não é permitido no e-mail
D. Armazenamento de senhas de gerenciamento do sistema em um cofre

30 / 40
As cópias de segurança (backup) do servidor central são mantidas na mesma sala fechada que o servidor.

Que risco a organização enfrenta?

A. Se o servidor falhar, levará um longo tempo antes que o servidor esteja novamente em funcionamento.
B. Em caso de incêndio, é impossível recuperar o sistema ao seu estado anterior.
C. Ninguém é responsável pelos backups.
D. Pessoas não autorizadas têm acesso fácil aos backups.

31 / 40
Que tipo de malware cria uma rede de computadores contaminados?

A. Bomba Lógica
B. Storm Worm ou Botnet
C. Cavalo de Troia
D. Spyware

32 / 40
Em uma organização, o agente de segurança detecta que a estação de trabalho de um funcionário está infectada com software malicioso. O software malicioso foi instalado como resultado de um ataque direcionado de phishing.

Qual ação é a mais benéfica para evitar esses incidentes no futuro?

A. Implementar a tecnologia MAC
B. Iniciar um programa de conscientização de segurança
C. Atualizar as regras do firewall
D. Atualizar as assinaturas do filtro de spam

33 / 40
Você trabalha no departamento de TI de uma empresa de tamanho médio. Informações confidenciais têm caído em mãos erradas por várias vezes. Isso tem prejudicado a imagem da companhia. Você foi solicitado a propor medidas de segurança organizacional em laptops para sua companhia.

Qual o **primeiro** passo que você deveria dar?

A. Formular uma política para tratar da segurança de dispositivos móveis (PDAs, laptops, smartphones, pen drive)
B. Designar uma equipe de segurança
C. Criptografar os discos rígidos dos laptops e mídias de armazenamento externo, como pen drives
D. Estabelecer uma política de controle de acesso

34 / 40
Qual é o nome do sistema que garante a coerência da segurança da informação na organização?

A. Sistema de Gestão de Segurança da Informação (SGSI)
B. Rootkit
C. Regulamentos de segurança para informações especiais do governo.

35 / 40
Como se chama o processo de “definir se a identidade de alguém é correta”?

A. Autenticação
B. Autorização
C. Identificação

36 / 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 grande interrupção, as medidas tomadas e os procedimentos previstos podem não ser adequados ou podem estar desatualizados.
D. Porque isso é exigido pela Lei de Proteção de Dados Pessoais

37 / 40
Com base em qual legislação alguém pode pedir para inspecionar seus dados pessoais que tenham sido registrados (em países onde a lei é aplicável)?

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

38 / 40
Qual é a legislação ou ato regulatório relacionado à segurança da informação que pode ser imposto a todas as organizações (em países onde a lei é aplicável)?

A. Direito de Propriedade Intelectual
B. ISO/IEC 27001
C. ISO/IEC 27002
D. Legislação de proteção de dados pessoais

39 / 40
Você é o proprietário de uma companhia de correio (courier), SpeeDelivery. Você emprega algumas pessoas que, enquanto esperam para fazer as entregas, podem realizar outras tarefas. Você percebe, no entanto, que eles usam esse tempo para enviar e ler seus e-mails particulares e navegar na Internet.

Em termos legais, de que forma o uso da internet e do e-mail pode ser melhor regulado?

A. Instalando um aplicativo que impeça o acesso a certos sites da Internet e que realizem filtragem em arquivos anexados a e-mails
B. Elaborando um código de conduta para o uso da internet e do e-mail, no qual os direitos e obrigações tanto do empregador quanto dos empregados estejam claramente declarados
C. Implementando normas de privacidade
D. Instalando rastreadores de vírus

40 / 40
Em quais condições é permitido a um empregador verificar se os serviços de Internet e e-mail no ambiente de trabalho estão sendo utilizados para finalidades pessoais?

A. O empregador poderá fazer essa verificação, se o funcionário for informado depois de cada sessão de verificação
B. O empregador poderá fazer essa verificação se os funcionários forem informados que isso pode acontecer
C. O empregador poderá fazer essa verificação se um firewall também estiver instalado

Gabarito de respostas

1 / 40
Qual a relação entre dados e informações?

A. Dados são informações estruturadas
B. Informações são o significado e o valor atribuídos a uma coleção de dados

A. Incorreto. Informações são dados estruturados.
B. Correto. Informações são dados que têm um significado em algum contexto para seu receptor. (Capítulo 3)

2 / 40
A fim de ter uma apólice de seguro de incêndio, o departamento administrativo deve determinar o valor dos dados que gerencia.

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

A. O conteúdo dos dados.
B. O grau em que, dados ausentes 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. (Capítulo 4)
B. Incorreto. Dados ausentes, incompletos ou incorretos que 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 / 40
Um hacker obtém acesso a um servidor Web e pode exibir um arquivo no servidor que contém números de cartão de crédito.

Quais princípios de confidencialidade, integridade e disponibilidade (CIA) do arquivo de cartão de crédito são violados?

A. Disponibilidade
B. Confidencialidade
C. Integridade

A. Incorreto. O hacker não excluiu o arquivo nem negou acesso a entidades autorizadas, de forma alguma; portanto, a disponibilidade não foi prejudicada.
B. Correto. O hacker conseguiu ler o arquivo (confidencialidade). (Capítulo 3)
C. Incorreto. Não houve nenhuma informação alterada no arquivo de cartão de crédito; portanto, a integridade do arquivo não foi violada.

4 / 40
Existe uma impressora de rede no corredor da empresa onde você trabalha. Muitos funcionários não vão pegar suas impressões imediatamente e deixam o material na impressora.

Quais são as consequências disto com relação à confiabilidade das informações?

A. A integridade das informações não pode mais ser garantida
B. A disponibilidade das informações não pode mais ser garantida
C. A confidencialidade das informações não pode mais ser garantida

A. Incorreto. A integridade das informações continua garantida, pois o material está impresso em papel.
B. Incorreto. As informações continuam disponíveis no sistema utilizado para criar e imprimi-las.
C. Correto. As informações podem acabar sendo lidas por pessoas que não deveriam ter acesso a elas. (Capítulo 3)

5 / 40
Uma análise de risco bem executada oferece uma grande quantidade de informações úteis. A análise de risco tem quatro principais objetivos.

Qual das opções abaixo **não** é um dos quatro principais objetivos da análise de risco?

A. Identificação dos ativos e seus valores
B. Implementação de contramedidas
C. Estabelecimento do equilíbrio entre os custos de um incidente e os custos de medidas de segurança
D Determinação de vulnerabilidades e ameaças relevantes

A. Incorreto. Este é um dos principais objetivos de uma análise de risco.
B. Correto. Este não é um objetivo de uma análise de risco. É possível selecionar medidas quando em uma análise de risco se determina quais riscos exigem uma medida de segurança. Capítulo 3)
C. Incorreto. Este é um dos principais objetivos de uma análise de risco.
D. Incorreto. Este é um dos principais objetivos de uma análise de risco.

6 / 40
Um departamento administrativo vai determinar os riscos aos quais está exposto.

Como denominamos um possível evento que possa comprometer 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 comprometer a confiabilidade da informação. (Capítulo 3)
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 que levam a um comprometimento.

7 / 40
Qual é o propósito do gerenciamento de risco?

A. Determinar a probabilidade de ocorrência de um certo risco.
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. (Capítulo 3)

8 / 40
Há alguns anos você começou sua empresa, que já cresceu de 1 para 20 empregados. As informações de sua empresa valem mais e mais e já passaram os dias em que você podia manter tudo em suas próprias mãos. Você está ciente de que precisa tomar medidas, mas quais? Você contrata um consultor, que o aconselha a começar com uma análise de risco qualitativa.

O que é uma análise de risco qualitativa?

A. Esta análise segue um cálculo preciso de probabilidade estatística a fim de calcular a exata perda causada pelo dano
B. Esta análise é baseada em cenários e situações e produz uma visão subjetiva de possíveis ameaças

A. Incorreto. Em uma análise de risco quantitativa, realiza-se uma tentativa de determinar numericamente as probabilidades de vários eventos e a extensão provável das perdas se determinado evento ocorrer.
B. Correto. Uma análise de risco qualitativa envolve a definição de diversas ameaças, determinando a extensão das vulnerabilidades e elaborando contramedidas, caso ocorra um ataque. (Capítulo 3)

9 / 40
Houve um incêndio em uma filial da companhia Midwest Insurance. Os bombeiros chegaram rapidamente ao local e puderam apagar o fogo antes que se espalhasse e queimasse toda a instalação. O servidor, entretanto, foi destruído pelo fogo. As fitas de segurança (backup) mantidas em outra sala derreteram e muitos outros documentos foram perdidos definitivamente.

Qual é um exemplo de dano indireto causado pelo incêndio?

A. Fitas de segurança (backup) derretidas
B. Sistemas de computação queimados
C. Documentos queimados
D. Danos provocados pela água dos extintores de incêndio

A. Incorreto. Fitas derretidas de backup são danos diretos causados pelo fogo.
B. Incorreto. Sistemas de computador queimados são danos diretos causados pelo fogo.
C. Incorreto. Documentos queimados são danos diretos causados pelo fogo.
D. Correto. Danos provocados pela água em função dos extintores de incêndio são danos indiretos causados pelo fogo. Este é um efeito colateral de apagar o fogo, que visa minimizar os danos causados pelo fogo. (Capítulo 3)

10 / 40
Você é o proprietário de uma companhia de correio (courier), SpeeDelivery. Você realizou uma análise de risco e agora quer determinar sua estratégia de risco. Você decide tomar medidas contra os grandes riscos, mas não contra os pequenos riscos.

Como é chamada a estratégia de risco adotada neste caso?

A. Retenção de risco
B. Prevenção de risco
C. Redução de risco

A. Correto. Isso significa que certos riscos são aceitos (Capítulo 3)
B. Incorreto. Isso significa que medidas são adotadas para que a ameaça seja neutralizada a tal ponto que já não provoque um incidente
C. Incorreto. Isso significa que medidas de segurança são adotadas para que as ameaças já não se manifestem ou, se isso acontecer, os danos resultantes sejam minimizados.

11 / 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. Uma fuga de energia 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, por esse meio é uma ameaça human. (Capítulo 3)
B. Incorreto. A poeira não é uma ameaça humana.
C. Incorreto. A falha de energia elétrica não é uma ameaça humana.

12 / 40
O que é um exemplo de uma ameaça humana?

A. Um relâmpago
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 (atrair usuários para sites falsos) é uma forma de ameaça humana. (Capítulo 3)

13 / 40
Você trabalha no escritório de uma grande companhia. Você recebe um telefonema de uma pessoa dizendo ser do helpdesk. Ela pede para que você lhe diga sua senha.

Que tipo de ameaça é esta?

A. Ameaça natural
B. Ameaça organizacional
C. Engenharia social

A. Incorreto. Uma chamada telefônica é uma ação humana; portanto, não é uma ameaça natural.
B. Incorreto. O termo ”ameaça organizacional” não é um termo comum para um tipo de ameaça.
C. Correto. O uso de expressões ou nomes corretos de pessoas conhecidas e seus departamentos dá a impressão de que é um colega tentando obter segredos da empresa e segredos comerciais. Você deve verificar se está realmente falando com o helpdesk. Um funcionário do helpdesk jamais solicitará sua senha. (Capítulo 3)

14 / 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 acordos stand-by (plano de contingência)?

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

A. Incorreto. A realização de um acordo stand-by sem que primeiro haja um incidente é muito cara.
B. Incorreto. A recuperação ocorre após o acordo stand-by entrar em vigor.
C. Incorreto. Os danos e a recuperação são realmente limitados pelo acordo stand-by.
D. Correto. Um acordo stand-by é uma medida corretiva iniciada a fim de limitar os danos. (Capítulo 3)

15 / 40
Informações envolvem inúmeros aspectos de confiabilidade, a qual é constantemente ameaçada. Exemplos de ameaças são: um cabo se soltar, informações alteradas por acidente, dados que são usados para fins particulares ou falsificados.

Qual destes exemplos é uma ameaça à integridade?

A. Um cabo solto
B. Alteração acidental de dados
C. Utilização privada de dados

A. Incorreto. Um cabo solto é uma ameaça para a disponibilidade de informações.
B. Correto. A alteração não intencional de dados é uma ameaça à sua integridade. (Capítulo 3)
C. Incorreto. O uso de dados para fins particulares é uma forma de uso indevido e é uma ameaça para a confidencialidade.

16 / 40
Um funcionário nega o envio de uma mensagem específica.

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

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

A. Incorreto. Sobrecarregar a infraestrutura 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 está relacionadada à irretratabilidade, uma ameaça à integridade. (Capítulo 3)
D. Incorreto. O uso indevido e/ou divulgação de dados são ameaças à confidencialidade.

17 / 40
Qual a **melhor** maneira de descrever o objetivo da política de segurança da informação?

A. A política documenta a análise de riscos e a busca de contramedidas.
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. (Capítulo 5)
C. Incorreto. O plano de segurança faz com que a política de segurança da informação seja concreta. O plano inclui as medidas 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 / 40
Um incidente de segurança relacionado com um servidor Web é relatado a um funcionário do helpdesk. Sua colega tem mais experiência em servidores Web; então, ele transfere o caso para ela.

Qual termo descreve essa transferência?

A. Escalonamento funcional
B. Escalonamento hierárquico

A. Correto. Se o funcionário do helpdesk não conseguir lidar com o incidente pessoalmente, o incidente pode ser relatado a alguém com mais experiência, que possa ser capaz de resolver o problema. Isso se chama escalonamento funcional (horizontal). (Capítulo 16)
B. Incorreto. Isso se chama escalonamento funcional (horizontal). O escalonamento hierárquico ocorre quando uma tarefa é transferida para alguém com mais autoridade.

19 / 40
Uma funcionária trabalhador de uma companhia de seguros 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 helpdesk registra as seguintes informações sobre este incidente:

- data e hora
- descrição do incidente
- possíveis consequências do incidente

Qual a informação mais 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, no mínimo o nome do usuário deve ser registrado. (Capítulo 16)
B. Incorreto. Esta é uma informação adicional que pode ser acrescentada posteriormente.
C. Incorreto. Esta é uma informação adicional que pode ser acrescentada posteriormente.
D. Incorreto. Esta é uma informação adicional que pode ser acrescentada posteriormente.

20 / 40
No ciclo de incidente há quatro etapas sucessivas.

Qual é a etapa que sucede o incidente?

A. Ameaça
B. Dano
C. Recuperação

A. Incorreto. O dano se segue após o incidente. A ordem correta das etapas é ameaça, incidente, dano e recuperação.
B. Correto. A ordem das etapas do ciclo do incidente é: ameaça, incidente, dano e recuperação. (Capítulo 16)
C. Incorreto. O dano sucede o incidente. A ordem correta das etapas é ameaça, incidente, dano e recuperação.

21 / 40
Qual das seguintes medidas é uma medida preventiva?

A. Instalação de um sistema de registro de eventos (log) que permite que mudanças em um sistema sejam reconhecidas
B. Desativação de todo tráfego internet depois que um hacker ganhou acesso aos sistemas da companhia
C. Armazenamento de informações sigilosas em um cofre

A. Incorreto. Por meio de um sistema de registro, somente depois que o incidente ocorreu é possível pesquisar sobre o que aconteceu. Esta é uma medida de detecção, que visa detectar os incidentes.
B. Incorreto. A desativação de todo o tráfego de Internet é uma medida repressiva, que visa a limitar um incidente.
C. Correto. O armazenamento em cofre é uma medida preventiva que evita danos às informações sigilosas. (Capítulo 3)

22 / 40
Qual das opções abaixo é uma medida repressiva em caso de incêndio?

A. Fazer um seguro contra incêndio
B. Apagar o fogo depois que o incêndio for detectado pelo detector de incêndio
C. Reparar os danos causados pelo incêndio

A. Incorreto. Um seguro protege contra as consequências financeiras de um incêndio.
B. Correto. Esta medida repressiva minimiza os danos causados pelo fogo. (Capítulo 3)
C. Incorreto. Esta não é uma medida repressiva, pois não minimiza os danos causados pelo incêndio.

23 / 40

Qual é o objetivo da classificação da informação?

A. Criar um manual sobre como manusear dispositivos móveis
B. Aplicar identificações que facilitem o reconhecimento das informações
C. Estruturar as informações de acordo com sua confidencialidade

A. Incorreto. A criação de um manual está relacionada com as diretrizes do usuário e não com a classificação das informações.
B. Incorreto. A identificação das informações é uma designação, uma forma especial de categorizar as informações, o que ocorre após a classificação.
C. Correto. A classificação de informações é utilizada para definir os diferentes níveis de confidencialidade nos quais as informações podem ser estruturadas. (Capítulo 3 e 8)

24 / 40
Quem é autorizado a mudar a classificação de um documento?

A. O autor do documento
B. O administrador do documento
C. O proprietário do documento
D. O gerente do proprietário do documento

A. Incorreto. O autor pode alterar o conteúdo, mas não a classificação de um documento.
B. Incorreto. O administrador não pode alterar a classificação de um documento.
C. Correto. O proprietário deve assegurar que o ativo seja classificado ou reclassificado, se necessário; portanto, está autorizado a alterar a classificação de um documento. (Capítulo 3 e 8)
D. Incorreto. O gerente do proprietário não tem autoridade sobre nisso.

25 / 40
O acesso à sala de computadores está bloqueado por um leitor de crachás. Somente o Departamento de Gerenciamento de Sistemas tem um crachá.

Que tipo de medida de segurança é essa?

A. Uma medida de segurança corretiva
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 corretiva é uma medida de recuperação.
B. Correto. Esta é uma medida de segurança físic. (Capítulo 3 e 11)
C. Incorreto. Uma medida de segurança lógica controla o acesso ao software e à informação, e não o acesso físico às salas.
D. Incorreto. A medida de segurança repressiva visa minimizar as consequências de uma interrupção.

26 / 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 mostrar um crachá de acesso?

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

A. Incorreto. Um crachá de acesso não é um exemplo de algo que você é.
B. Correto. Um crachá de acesso é um exemplo de algo que você tem. (Capítulo 11)
C. Incorreto. Um crachá de acesso não é algo que você sabe.

27 / 40
Na segurança física, múltiplas zonas em expansão (anéis de proteção) podem ser aplicadas, nas quais diferentes medidas podem ser adotadas.

O que não é um anel de proteção?

A. Edifício
B. Anel médio
C. Objeto
D. Anel externo

A. Incorreto. Um edifício é uma zona válida e trata do acesso às instalações.
B. Correto. Anéis de proteção: anel externo (área ao redor das instalações), edifício (acesso às instalações), espaço de trabalho (as salas das instalações, também conhecidas como "anel interno"), objeto (o ativo que deve ser protegido). Não existe um anel médio. (Capítulo 11)
C. Incorreto. Um objeto é uma área válida e trata do ativo que precisa ser protegido.
D. Incorreto. Um anel externo é uma zona válida e trata da área ao redor das instalações.

28 / 40
Qual das ameaças listadas abaixo pode ocorrer como resultado da ausência de uma medida de segurança física?

A. Um usuário pode ver os arquivos pertencentes a outro
B. Um servidor é desligado por causa de superaquecimento
C. Um documento confidencial é deixado na impressora
D. Hackers podem entrar livremente na rede de computadores

A. Incorreto. O controle lógico de acesso é uma medida técnica que impede o acesso não autorizado aos documentos de outro usuário.
B. Correto. A segurança física inclui a proteção de equipamentos por meio do controle de temperatura (ar-condicionado, umidade do ar). (Capítulo 11)
C. Incorreto. Uma política de segurança deve abranger as regras de como lidar com documentos confidenciais. Todos os funcionários devem estar cientes dessa política e praticar as regras. É uma medida organizacional.
D. Incorreto. Impedir que hackers entrem no computador ou na rede é uma medida técnica.

29 / 40
Qual das seguintes medidas de segurança é uma medida técnica?

A. Atribuição de informações a um proprietário
B. Criptografia de arquivos
C. Criação de uma política que define o que é e não é permitido no e-mail
D. Armazenamento de senhas de gerenciamento do sistema em um cofre

A. Incorreto. A atribuição de informações a 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. (Capítulo 6)
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 / 40
As cópias de segurança (backup) do servidor central são mantidas na mesma sala fechada que o servidor.

Que risco a organização enfrenta?

A. Se o servidor falhar, levará um longo tempo antes que o servidor esteja novamente em funcionamento.
B. Em caso de incêndio, é impossível recuperar o sistema ao seu estado anterior.
C. Ninguém é responsável pelos backups.
D. Pessoas não autorizadas têm acesso fácil aos 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 possam ser destruídas em um incêndio é muito grande. (Capítulo 11)
C. Incorreto. A responsabilidade não tem nada a ver com o local de armazenamento.
D. Incorreto. A sala de informática está trancada.

31 / 40
Que tipo de malware cria uma rede de computadores contaminados?

A. Bomba Lógica
B. Storm Worm ou Botnet
C. Cavalo de Troia
D. Spyware

A. Incorreto. Uma bomba lógica nem sempre é um malware. É parte de código incorporada a um sistema de software.
B. Correto. Um worm é um pequeno programa de computador que se reproduz propositadamente e cópias do original são distribuídas através da rede de seu host. (Capítulo 12)
C. Incorreto. Um cavalo de Troia é um programa que, além de realizar a função para a qual foi criado, realiza propositadamente atividades secundárias, sem que o usuário perceba.
D. Incorreto. Um spyware é um programa de computador que coleta informações sobre o usuário do computador e as envia a terceiros.

32 / 40
Em uma organização, o agente de segurança detecta que a estação de trabalho de um funcionário está infectada com software malicioso. O software malicioso foi instalado como resultado de um ataque direcionado de phishing.

Qual ação é a mais benéfica para evitar esses incidentes no futuro?

A. Implementar a tecnologia MAC
B. Iniciar um programa de conscientização de segurança
C. Atualizar as regras do firewall
D. Atualizar as assinaturas do filtro de spam

A. Incorreto. O MAC está relacionado com o controle de acesso, o que não impede que um usuário seja convencido a executar algumas ações como resultado do ataque direcionado.
B. Correto. A vulnerabilidade inerente a essa ameaça é a falta de consciência do usuário. Os usuários são convencidos, nesses tipos de ataques, a executar algum código que viola a política (por exemplo, instalar software suspeito). Combater esse tipo de ataques com um programa de conscientização de segurança reduzirá a possibilidade de recorrência no futuro. (Capítulo 12)
C. Incorreto. Embora o firewall possa, por exemplo, bloquear o tráfego que resultou da instalação de software malicioso, não será útil para evitar a recorrência da ameaça.
D. Incorreto. O ataque direcionado não precisa usar e-mail. O indivíduo que realiza o ataque pode usar sites de relacionamento ou até mesmo o telefone para fazer contato com a vítima

33 / 40
Você trabalha no departamento de TI de uma empresa de tamanho médio. Informações confidenciais têm caído em mãos erradas por várias vezes. Isso tem prejudicado a imagem da companhia. Você foi solicitado a propor medidas de segurança organizacional em laptops para sua companhia.

Qual o **primeiro** passo que você deveria dar?

A. Formular uma política para tratar da segurança de dispositivos móveis (PDAs, laptops, smartphones, pen drive)
B. Designar uma equipe de segurança
C. Criptografar os discos rígidos dos laptops e mídias de armazenamento externo, como pen drives
D. Estabelecer uma política de controle de acesso

A. Correto. A política sobre como usar dispositivos móveis é uma medida organizacional, e medidas de segurança para laptops podem ser obrigatórias. (Capítulo 6)
B. Incorreto. Designar uma equipe de segurança é uma medida técnica. Quando alguém leva um laptop para fora do escritório, o risco de vazamento de informações permanece.
C. Incorreto. Criptografar os discos rígidos de laptops e pen drives é uma medida técnica. Isso pode ser realizado com base em uma medida organizacional.
D. Incorreto. A política de controle de acesso é uma medida organizacional, que abrange apenas o acesso a edifícios ou sistemas de TI.

34 / 40
Qual é o nome do sistema que garante a coerência da segurança da informação na organização?

A. Sistema de Gestão de Segurança da Informação (SGSI)
B. Rootkit
C. Regulamentos de segurança para informações especiais do governo.

A. Correto. O SGSI é descrito na norma ISO/IEC 27001. (Capítulo 3)
B. Incorreto. Um rootkit é um conjunto malicioso de ferramentas de software frequentemente usado por terceiros (geralmente um hacker).
C. Incorreto. Isso é um conjunto de regras governamentais sobre como lidar com informações especiais.

35 / 40
Como se chama o processo de “definir se a identidade de alguém é correta”?

A. Autenticação
B. Autorização
C. Identificação

A. Correto. Definir se a identidade de alguém é correta chama-se autenticação. (Capítulo 9)
B. Incorreto. Quando alguém recebe os direitos de acesso a um computador ou rede, isso se chama autorização.
C. Incorreto. A identificação é o processo de tornar uma identidade conhecida.

36 / 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 grande interrupção, as medidas tomadas e os procedimentos previstos podem não ser adequados ou podem estar desatualizados.
D. Porque isso é exigido pela Lei de Proteção de Dados Pessoais

A. Incorreto. Esta é uma das medidas técnicas utilizadas para recuperar um sistema.
B. Incorreto. Para interrupção normais, as medidas usualmente executadas e os procedimentos de incidentes são suficientes.
C. Correto. Uma grande interrupção requer planos atualizados e testados. (Capítulo 17)
D. Incorreto. A Lei de Proteção de Dados Pessoais envolve a privacidade dos dados pessoais.

37 / 40
Com base em qual legislação alguém pode pedir para inspecionar seus dados pessoais que tenham sido registrados (em países onde a lei é aplicável)?

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 pela Lei de Proteção de Dados Pessoais. (Capítulo 18)
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 crimes praticados por meio de tecnologia da informação avançada. Um exemplo de um novo crime 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.

38 / 40
Qual é a legislação ou ato regulatório relacionado à segurança da informação que pode ser imposto a todas as organizações (em países onde a lei é aplicável)?

A. Direito de Propriedade Intelectual
B. ISO/IEC 27001
C. ISO/IEC 27002
D. Legislação de proteção de dados pessoais

A. Incorreto. Essa regulamentação não está relacionada com a segurança de informações para as organizações.
B. Incorreto. Esta é uma norma com orientações para as organizações sobre como lidar com a definição de um processo de segurança de informações.
C. Incorreto. Esta norma, também conhecida como “Código de boas práticas para segurança de informações”, contém orientações sobre a política e as medidas de segurança de informações.
D. Correto. Todas as organizações devem ter uma política e procedimentos para proteção de dados pessoais, que devem ser conhecidos por todos que processam dados pessoais. (Capítulo 18)

39 / 40
Você é o proprietário de uma companhia de correio (courier), SpeeDelivery. Você emprega algumas pessoas que, enquanto esperam para fazer as entregas, podem realizar outras tarefas. Você percebe, no entanto, que eles usam esse tempo para enviar e ler seus e-mails particulares e navegar na Internet.

Em termos legais, de que forma o uso da internet e do e-mail pode ser melhor regulado?

A. Instalando um aplicativo que impeça o acesso a certos sites da Internet e que realizem filtragem em arquivos anexados a e-mails
B. Elaborando um código de conduta para o uso da internet e do e-mail, no qual os direitos e obrigações tanto do empregador quanto dos empregados estejam claramente declarados
C. Implementando normas de privacidade
D. Instalando rastreadores de vírus

A. Incorreto. Instalar esse tipo de software regulamenta parcialmente o uso da Internet e do e-mail, mas não o tempo gasto em uso privativo. Esta é uma medida técnica.
B. Correto. Em um código de conduta, a utilização da Internet e do e-mail pode ser documentada, quais sites podem ou não ser visitados e até que ponto o uso privativo é permitido. Estas são normas internas.(Capítulo 18)
C. Incorreto. Normas de privacidade somente regulamentam o uso de dados pessoais de funcionários e clientes, e não o uso da Internet e do e-mail.
D. Incorreto. Um mecanismo de varredura de vírus verifica os e-mails que chegam e softwares maliciosos nas conexões com a Internet. Ele não regulamenta o uso da Internet e do e-mail. É uma medida técnica.

40 / 40
Em quais condições é permitido a um empregador verificar se os serviços de Internet e e-mail no ambiente de trabalho estão sendo utilizados para finalidades pessoais?

A. O empregador poderá fazer essa verificação, se o funcionário for informado depois de cada sessão de verificação
B. O empregador poderá fazer essa verificação se os funcionários forem informados que isso pode acontecer
C. O empregador poderá fazer essa verificação se um firewall também estiver instalado

A. Incorreto. O funcionário não precisa ser informado após cada verificação.
B. Correto. Os funcionários devem saber que o empregador tem o direito de monitorar o uso dos serviços de TI. (Capítulo 3 e 18)
C. Incorreto. Um firewall protege contra invasores externos. Isso não influencia o direito de o empregador monitorar a utilização dos serviços de TI.

Avaliação

A tabela a seguir mostra as respostas corretas às questões apresentadas neste exame simulado.

Número	Resposta	Número	Resposta
1	B	21	C
2	A	22	B
3	B	23	C
4	C	24	C
5	B	25	B
6	B	26	B
7	D	27	B
8	B	28	B
9	D	29	B
10	A	30	B
11	A	31	B
12	C	32	B
13	C	33	A
14	D	34	A
15	B	35	A
16	C	36	C
17	B	37	B
18	A	38	D
19	A	39	B
20	B	40	B

Contato EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER