Exame simulado

Edição 202404

Conteúdo

Introdução

Este é o exame simulado EXIN Information Security Foundation based on ISO/IEC 27001 (ISFS.PR). As regras e regulamentos do exame do EXIN se aplicam a este exame.

Este exame contém 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 1 ponto. Você precisa de 26 pontos ou mais para passar no exame.

O tempo permitido para este exame é de 60 minutos.

Boa Sorte!

Exame simulado

1 / 40
Um banco de dados contém alguns milhões de transações de uma empresa telefônica. Uma fatura foi gerada e enviada a um cliente.

O que essa fatura contém para esse cliente?

A) Dados
B) Informação
C) Dados e informação

2 / 40
Qual é a diferença entre dados e informação?

A) Dados podem ser quaisquer fatos ou números. Informação são dados que têm significado.
B) Dados são compostos por números não estruturados. Informação consiste em números estruturados.
C) Dados não exigem segurança. Informação exige segurança.
D) Dados não têm valor. Informação, que são dados processados, tem valor.

3 / 40
Qual é o foco do gerenciamento da informação?

A) Permitir que atividades e processos de negócios continuem sem interrupção
B) Assegurar que o valor da informação seja identificado e aproveitado
C) Evitar que pessoas não autorizadas tenham acesso a sistemas automatizados
D) Entender como a informação flui através de uma organização

4 / 40
Uma organização precisa entender os riscos que enfrenta antes que possa tomar medidas apropriadas.

O que deve ser conhecido para determinar o risco?

A) A probabilidade de algo acontecer e suas consequências para a organização.
B) Os perigos mais comuns e como mitigá-los, conforme definido nas melhores práticas.
C) As ameaças que a organização enfrenta e o quão vulnerável a organização é a elas.
D) Os eventos não planejados que uma organização enfrenta e o que fazer em caso de tais eventos.

5 / 40
Além de integridade e confidencialidade, qual é o terceiro aspecto da confiabilidade da informação?

A) Exatidão
B) Disponibilidade
C) Completude
D) Valor

6 / 40
Uma organização tem, em sua recepção, uma impressora ligada à rede. Muitos funcionários não recuperam suas impressões de imediato, deixando-as na impressora.

Qual é a consequência disso para a confiabilidade da informação?

A) Não se pode garantir a disponibilidade da informação.
B) Não se pode garantir a confidencialidade da informação.
C) Não se pode garantir a integridade da informação.

7 / 40
Qual é a diferença entre responsabilização e auditabilidade?

A) Responsabilização significa que uma organização tem suas contas financeiras bem administradas. Auditabilidade significa que uma organização foi aprovada em uma auditoria.
B) Responsabilização significa ser responsável pelos resultados das atividades de uma organização. Auditabilidade se refere à prontidão de uma organização para ser submetida a uma avaliação independentemente.
C) Responsabilização significa ter responsabilidade pelas ações de uma pessoa. Auditabilidade significa ter responsabilidade pelas ações de uma organização.
D) Responsabilização significa que a organização está em conformidade com a Sarbanes-Oxley (SOX). Auditabilidade se refere a uma organização estar em conformidade com a ISO/IEC 27001.

8 / 40
Como **melhor** se descreve a finalidade de uma política de segurança da informação?

A) Uma política de segurança da informação documenta a análise dos riscos e a busca por controles apropriados.
B) Uma política de segurança da informação dá orientação e suporte à organização com relação à segurança da informação.
C) Uma política de segurança da informação concretiza o plano de segurança ao lhe fornecer os detalhes necessários.
D) Uma política de segurança da informação fornece uma visão sobre as ameaças e suas eventuais consequências.

9 / 40
Sara ficou encarregada de assegurar que a organização cumpra com a legislação de proteção de dados pessoais.

Qual é a **primeira** medida que ela deve tomar?

A) Nomear uma pessoa responsável por apoiar os gerentes na adesão à política
B) Proibir a coleta e o armazenamento de informações pessoais
C) Tornar os funcionários responsáveis pelo envio de seus dados pessoais
D) Converter a legislação de proteção de dados pessoais em uma política de privacidade

10 / 40
Uma organização decide terceirizar parte de sua TI.

Qual a **melhor** forma de garantir segurança da informação quando se trabalha com um fornecedor?

A) Nomear um novo information security officer (ISO) na organização do fornecedor
B) Formalizar os requisitos de segurança da informação para o fornecedor em um acordo
C) Manter as duas organizações totalmente separadas para tornar todos responsáveis por seus dados
D) Exigir que o fornecedor siga os processos e os procedimentos da organização do cliente

11 / 40
Quem é responsável por converter a estratégia e os objetivos de negócio em estratégia e objetivos de segurança?

A) Chief information security officer (CISO)
B) Gestão geral
C) Information security officer (ISO)
D) Information security policy officer

12 / 40
Qual é o **melhor** exemplo de uma ameaça humana?

A) Um vazamento que provoca uma falha no fornecimento de energia.
B) Um pen drive que transmite um vírus para a rede.
C) Há muito pó na sala dos servidores.

13 / 40
Um sistema de banco de dados não possui os patches de segurança mais recentes e foi hackeado. Os hackers conseguiram acessar os dados e eliminá-los.

Que conceito de segurança da informação descreve a falta de patches de segurança?

A) Impacto
B) Risco
C) Ameaça
D) Vulnerabilidade

14 / 40
Houve um incêndio em uma empresa. Os bombeiros chegaram rapidamente ao local e conseguiram apagar o fogo antes que ele se espalhasse e atingisse todas as instalações da empresa. Entretanto, o incêndio destruiu o servidor. As fitas de backup (cópia de segurança) que ficavam em outra sala derreteram e muitos outros documentos foram perdidos.

Que dano **indireto** foi causado por esse incêndio?

A) Sistemas de computadores queimados
B) Documentos queimados
C) Fitas de backup derretidas
D) Danos causados pela água

15 / 40
Empresas podem ter diferentes estratégias de risco dependendo do tipo de negócio.

Que estratégia de risco é **mais** adequada para um hospital?

A) Aceitar o risco
B) Evitar o risco
C) Suportar o risco
D) Reduzir o risco

16 / 40
Uma análise de risco bem realizada fornece muita informação útil. Uma análise de risco tem diferentes objetivos principais.

O que **não** é um objetivo principal de uma análise de risco?

A) Balancear os custos de um incidente e os custos de um controle
B) Determinar vulnerabilidades e ameaças importantes
C) Identificar os ativos e seu valor
D) Implementar medidas e controles

17 / 40
Em caso de incêndio, qual é um controle repressivo?

A) Extinção do incêndio após sua detecção
B) Reparação dos danos causados pelo incêndio
C) Contratação de um seguro contra incêndio

18 / 40
Qual é o objetivo da classificação da informação?

A) Rotular a informação para facilitar seu reconhecimento
B) Criar um manual sobre como lidar com dispositivos móveis
C) Estruturar a informação de acordo com sua sensibilidade

19 / 40
Qual é a razão **mais** importante para pôr em prática a segregação de funções?

A) Assegurar que os funcionários não realizem o mesmo trabalho ao mesmo tempo
B) Responsabilizar conjuntamente todos os funcionários pelos erros que cometem
C) Tornar claro quem é responsável por quais tarefas e atividades
D) Minimizar a possibilidade de alterações não autorizadas ou não intencionais

20 / 40
Qual é a **melhor** forma de assegurar um acesso apropriado à informação?

A) Automatizar fluxos de trabalho
B) Definir procedimentos operacionais
C) Desenvolver instruções de trabalho para todas as tarefas
D) Fornecer treinamento

21 / 40
Houve um incêndio em uma filial de uma organização. Os funcionários foram transferidos para filiais próximas para continuar seu trabalho.

No ciclo de vida de um incidente, onde se localiza a mudança para um stand-by arrangement?

A) Entre as etapas de dano e de recuperação
B) Entre as etapas de incidente e de dano
C) Entre as etapas de recuperação e de ameaças
D) Entre as etapas de ameaças e de incidente

22 / 40
Uma funcionária descobre que a data de validade de uma política foi alterada sem seu conhecimento. Ela é a única pessoa autorizada a fazer essa alteração e notifica esse incidente de segurança ao help desk.

O funcionário do help desk registra as seguintes informações sobre esse incidente:
- data e hora
- descrição do incidente
- eventuais consequências do incidente

Que informação importante sobre o incidente não foi registrada?

A) O nome da pessoa que notifica o incidente
B) O nome do pacote de software
C) O número do computador

23 / 40
Por que é importante auditar regularmente o sistema de gestão de segurança da informação (SGSI) da organização?

A) Auditorias são um requisito comum em contratos de clientes para garantir segurança da informação.
B) Auditorias são um elemento necessário para estar em conformidade com requisitos legais ou regulatórios.
C) Auditorias detectam problemas relacionados à capacidade de cumprir os objetivos financeiros da organização.
D) Auditorias detectam fragilidades na implementação de controles de segurança da informação.

24 / 40
Que documento contém uma regra que proíbe o uso do e-mail da empresa para fins pessoais?

A) Certificado de boa índole
B) Código de conduta
C) Regulamento Geral sobre a Proteção de Dados (GDPR)
D) Acordo de não divulgação (NDA)

25 / 40
Quando um funcionário detecta um incidente, normalmente quem ele deve notificar **primeiro**?

A) Help desk
B) Information security manager (ISM)
C) Information security officer (ISO)
D) Gerente

26 / 40
Qual é a forma **mais** eficaz de criar conscientização sobre segurança da informação entre os funcionários?

A) Ter como foco treinamento sobre conscientização para o time de gestão
B) Enviar todos os funcionários para um treinamento externo sobre segurança da informação
C) Criar um programa de conscientização específico para a organização
D) Utilizar um curso de treinamento genérico online sobre segurança da informação

27 / 40
Que controle físico gerencia o acesso às informações de uma organização?

A) Instalação de ar-condicionado
B) Proibição do uso de pen drives
C) Exigência de nome de usuário e senha
D) Uso de vidro inquebrável

28 / 40
Um centro de dados usa bancos de baterias, mas não tem gerador de energia.

Qual é o risco associado a essa situação para a disponibilidade do centro de dados?

A) A energia principal pode não voltar automaticamente quando a energia for restabelecida, pois é preciso ter um gerador de energia para isso.
B) O corte da energia principal pode durar mais do que alguns minutos ou horas, o que causará falta de energia.
C) A vida útil dos bancos de baterias é limitada, então eles podem ficar sem diesel e parar de funcionar após alguns dias.
D) Após algumas horas, os bancos de baterias devem ser alimentados pelo gerador de energia, logo eles oferecem apenas proteção limitada.

29 / 40
Por que há ar-condicionado na sala dos servidores?

A) As fitas de backup (cópia de segurança) são feitas de um plástico fino que não resiste a altas temperaturas. Portanto, se fizer calor demais na sala dos servidores, elas podem ser danificadas.
B) Os funcionários que trabalham na sala dos servidores não devem trabalhar no calor. O calor aumenta a probabilidade de eles cometerem erros.
C) Na sala dos servidores, o ar deve ser refrigerado e o calor produzido pelos equipamentos deve ser removido. O ar-condicionado também desumidifica e filtra o ar da sala.
D) A sala dos servidores é a melhor forma de refrigerar o ar do escritório. Nenhuma área do escritório deve ser perdida com um equipamento tão grande.

30 / 40
Na segurança física, diversos anéis de proteção podem ser usados, nos quais diferentes medidas podem ser tomadas.

O que **não** é um anel de proteção?

A) Prédio
B) Área intermediária
C) Área segura
D) Anel externo

31 / 40
O controle para proteger um ativo depende do tipo de ativo.

Qual é a forma **mais** apropriada de proteger o ativo?

A) Proteger um formulário preenchendo-o e assinando-o
B) Proteger um laptop alocando-o a um único usuário
C) Proteger um pen drive com criptografia
D) Proteger uma conexão de internet com um backup (cópia de segurança)

32 / 40
Que controle de segurança da informação ajuda a desenvolver sistemas tendo em conta a segurança da informação?

A) Garantir redundância dos servidores
B) Implementar controles físicos nas entradas
C) Verificar os antecedentes dos funcionários
D) Utilizar classificação de dados nos ativos de informação

33 / 40
Uma organização muda sua política. A partir de agora, os funcionários estão autorizados a trabalhar remotamente.

Que controle deve ser implementado agora?

A) Criar V-LANs para segmentar a rede corporativa
B) Criptografar as informações da rede corporativa
C) Instalar firewalls na rede corporativa
D) Usar uma VPN para se conectar à rede corporativa

34 / 40
Os funcionários de uma organização trabalham com laptops protegidos por criptografia assimétrica. Todos os consultores usam o mesmo par de chaves para manter barato o gerenciamento das chaves.

Se alguma informação for comprometida, novas chaves devem ser fornecidas.

Em que caso novas chaves devem ser fornecidas?

A) Quando a chave privada se torna conhecida
B) Quando a chave pública se torna conhecida
C) Quando a infraestrutura de chave pública (ICP) se torna conhecida

35 / 40
Que tipo de segurança uma infraestrutura de chave pública (ICP) oferece?

A) Uma ICP garante que os backups (cópias de segurança) dos dados da empresa sejam feitos regularmente.
B) Uma ICP mostra aos clientes que um negócio na internet é seguro.
C) Uma ICP verifica qual pessoa ou sistema pertence a uma chave pública específica.

36 / 40
Que tipo de malware é um programa que, além da função que aparentemente desempenha, realiza propositalmente atividades secundárias?

A) Bomba lógica
B) Spyware
C) Trojan
D) Worm

37 / 40
Que tipo de malware cria uma rede de computadores contaminados ao se replicar?

A) Bomba lógica
B) Spyware
C) Trojan
D) Worm

38 / 40
Qual é o ato legislativo ou regulatório relacionado à segurança da informação que pode ser imposto a todas as organizações?

A) Regulamento Geral sobre a Proteção de Dados (GDPR)
B) Direitos de propriedade intelectual (PI)
C) ISO/IEC 27001
D) ISO/IEC 27002

39 / 40
Que norma ISO tem como foco a implementação de controles de segurança da informação?

A) ISO/IEC 27000
B) ISO/IEC 27001
C) ISO/IEC 27002
D) ISO/IEC 27005

40 / 40
Que organização tem as normas **mais** comumente usadas na Europa?

A) Instituto Nacional Americano de Padrões (ANSI)
B) Organização Internacional de Padronização (ISO)
C) Instituto Nacional de Padrões e Tecnologia (NIST)

Gabarito de respostas

1 / 40
Um banco de dados contém alguns milhões de transações de uma empresa telefônica. Uma fatura foi gerada e enviada a um cliente.

O que essa fatura contém para esse cliente?

A) Dados
B) Informação
C) Dados e informação

A) Incorreto. O banco de dados contém dados. No entanto, quando uma fatura é gerada e enviada a um destinatário, isso é informação para o destinatário.
B) Correto. O valor da informação é determinado pelo destinatário. A fatura contém dados valiosos para o destinatário, e, portanto, isso é informação. (Literatura: A, Capítulo 4.8.5)
C) Incorreto. A fatura contém apenas informação para o destinatário.

2 / 40
Qual é a diferença entre dados e informação?

A) Dados podem ser quaisquer fatos ou números. Informação são dados que têm significado.
B) Dados são compostos por números não estruturados. Informação consiste em números estruturados.
C) Dados não exigem segurança. Informação exige segurança.
D) Dados não têm valor. Informação, que são dados processados, tem valor.

A) Correto. Informação se origina de dados quando se dá a eles um significado em um certo contexto. (Literatura: A, Capítulo 3.1)
B) Incorreto. Dados podem ser estruturados ou não estruturados. Informação normalmente é estruturada.
C) Incorreto. Tanto dados quanto informação exigem segurança.
D) Incorreto. Tanto dados quanto informação têm valor.

3 / 40
Qual é o foco do gerenciamento da informação?

A) Permitir que atividades e processos de negócios continuem sem interrupção
B) Assegurar que o valor da informação seja identificado e aproveitado
C) Evitar que pessoas não autorizadas tenham acesso a sistemas automatizados
D) Entender como a informação flui através de uma organização

A) Incorreto. Esse é o foco do gerenciamento da continuidade de negócios (BCM). A finalidade do BCM é evitar que as atividades de negócios sejam perturbadas, proteger os processos críticos das consequências de perturbações de longo alcance nos sistemas de informação e possibilitar uma recuperação rápida.
B) Correto. O gerenciamento da informação descreve o modo como uma organização planeja, coleta, organiza, utiliza, controla, dissemina e elimina eficientemente sua informação, e pelo qual assegura que o valor dessa informação seja identificado e aproveitado ao máximo. (Literatura: A, Capítulo 4.9)
C) Incorreto. Esse é foco do gerenciamento de acesso, que garante que pessoas ou processos não autorizados não tenham acesso a sistemas automatizados, bancos de dados e programas.
D) Incorreto. Esse é o foco da análise da informação, que fornece uma visão clara de como uma organização lida com a informação e de como a informação flui através de uma organização.

4 / 40
Uma organização precisa entender os riscos que enfrenta antes que possa tomar medidas apropriadas.

O que deve ser conhecido para determinar o risco?

A) A probabilidade de algo acontecer e suas consequências para a organização.
B) Os perigos mais comuns e como mitigá-los, conforme definido nas melhores práticas.
C) As ameaças que a organização enfrenta e o quão vulnerável a organização é a elas.
D) Os eventos não planejados que uma organização enfrenta e o que fazer em caso de tais eventos.

A) Correto. Dois fatores de alto nível determinam o risco: a probabilidade de algo acontecer e seu impacto no negócio. (Literatura: A, Capítulo 3.1)
B) Incorreto. É insensato ter isso como ponto de partida quando uma organização define seus riscos. Fazer o que outras organizações fazem não torna essa organização segura.
C) Incorreto. Essa é uma descrição do termo probabilidade. Embora seja importante conhecer a probabilidade, um aspecto importante está faltando: como isso vai afetar o negócio.
D) Incorreto. Eventualmente, será necessário fazer a correspondência entre riscos e controles, porém isso é mais uma resposta ao risco do que uma forma de primeiro entender o risco.

5 / 40
Além de integridade e confidencialidade, qual é o terceiro aspecto da confiabilidade da informação?

A) Exatidão
B) Disponibilidade
C) Completude
D) Valor

A) Incorreto. Os três aspectos da confiabilidade da informação são disponibilidade, integridade e confidencialidade. Exatidão faz parte de integridade.
B) Correto. Os três aspectos da confiabilidade da informação são disponibilidade, integridade e confidencialidade. (Literatura: A, Capítulo 3.4.3)
C) Incorreto. Os três aspectos da confiabilidade da informação são disponibilidade, integridade e confidencialidade. Completude faz parte de integridade.
D) Incorreto. Os três aspectos da confiabilidade da informação são disponibilidade, integridade e confidencialidade.

6 / 40
Uma organização tem, em sua recepção, uma impressora ligada à rede. Muitos funcionários não recuperam suas impressões de imediato, deixando-as na impressora.

Qual é a consequência disso para a confiabilidade da informação?

A) Não se pode garantir a disponibilidade da informação.
B) Não se pode garantir a confidencialidade da informação.
C) Não se pode garantir a integridade da informação.

A) Incorreto. A informação ainda está disponível no sistema que foi utilizado para criá-la e imprimi-la.
B) Correto. A informação pode acabar nas mãos de, ou ser lida por, pessoas que não devem ter acesso a essa informação. (Literatura: A, Capítulo 3.4.1)
C) Incorreto. A integridade da informação das impressões ainda está garantida, já que está no papel.

7 / 40
Qual é a diferença entre responsabilização e auditabilidade?

A) Responsabilização significa que uma organização tem suas contas financeiras bem administradas. Auditabilidade significa que uma organização foi aprovada em uma auditoria.
B) Responsabilização significa ser responsável pelos resultados das atividades de uma organização. Auditabilidade se refere à prontidão de uma organização para ser submetida a uma avaliação independentemente.
C) Responsabilização significa ter responsabilidade pelas ações de uma pessoa. Auditabilidade significa ter responsabilidade pelas ações de uma organização.
D) Responsabilização significa que a organização está em conformidade com a Sarbanes-Oxley (SOX). Auditabilidade se refere a uma organização estar em conformidade com a ISO/IEC 27001.

A) Incorreto. Responsabilização não tem relação direta com contabilidade financeira. Auditabilidade não tem relação com ser aprovado em uma auditoria.
B) Correto. Essas são as definições corretas de responsabilização e auditabilidade. (Literatura: A, Capítulo 3.4.4)
C) Incorreto. A definição de responsabilização está correta, mas a definição de auditabilidade não está. Auditabilidade não tem nada a ver com responsabilidade pelas ações da organização.
D) Incorreto. Nem responsabilização nem auditabilidade se referem à conformidade com a SOX ou com normas ISO/IEC.

8 / 40
Como **melhor** se descreve a finalidade de uma política de segurança da informação?

A) Uma política de segurança da informação documenta a análise dos riscos e a busca por controles apropriados.
B) Uma política de segurança da informação dá orientação e suporte à organização com relação à segurança da informação.
C) Uma política de segurança da informação concretiza o plano de segurança ao lhe fornecer os detalhes necessários.
D) Uma política de segurança da informação fornece uma visão sobre as ameaças e suas eventuais consequências.

A) Incorreto. A análise dos riscos e a busca por controles são a finalidade da análise de risco e do gerenciamento de riscos.
B) Correto. Com a política de segurança, a gerência dá orientação e suporte com relação à segurança da informação. (Literatura: A, Capítulo 4.2.1)
C) Incorreto. O plano de segurança concretiza a política de segurança da informação. O plano inclui os controles que foram escolhidos, quem é responsável por quê, as diretrizes para a implementação dos controles etc.
D) Incorreto. A finalidade da análise de ameaças é fornecer uma visão sobre as ameaças e suas eventuais consequências.

9 / 40
Sara ficou encarregada de assegurar que a organização cumpra com a legislação de proteção de dados pessoais.

Qual é a **primeira** medida que ela deve tomar?

A) Nomear uma pessoa responsável por apoiar os gerentes na adesão à política
B) Proibir a coleta e o armazenamento de informações pessoais
C) Tornar os funcionários responsáveis pelo envio de seus dados pessoais
D) Converter a legislação de proteção de dados pessoais em uma política de privacidade

A) Incorreto. Uma pessoa para apoiar os gerentes não é um requisito para cumprir com a legislação de proteção de dados pessoais. Além disso, a política deve primeiro se alinhar com a legislação.
B) Incorreto. Essa não é a melhor forma de cumprir com a legislação de proteção de dados pessoais.
C) Incorreto. Essa não é uma forma de cumprir com a legislação de proteção de dados pessoais.
D) Correto. O primeiro passo para o cumprimento é criar uma política interna para a organização. (Literatura: A, Capítulo 5.1)

10 / 40
Uma organização decide terceirizar parte de sua TI.

Qual a **melhor** forma de garantir segurança da informação quando se trabalha com um fornecedor?

A) Nomear um novo information security officer (ISO) na organização do fornecedor
B) Formalizar os requisitos de segurança da informação para o fornecedor em um acordo
C) Manter as duas organizações totalmente separadas para tornar todos responsáveis por seus dados
D) Exigir que o fornecedor siga os processos e os procedimentos da organização do cliente

A) Incorreto. Não é necessário nomear um novo ISO na organização do fornecedor se essa organização já o possui.
B) Correto. Embora realizar um acordo não seja um mecanismo infalível para gerenciar o risco do fornecedor, é a forma mais eficaz de fazê-lo. (Literatura: A, Capítulo 5.20)
C) Incorreto. A organização do cliente continua responsável por todas as informações. Manter as organizações totalmente separadas geralmente pressupõe que a organização do cliente não sabe como garantir ou influenciar a segurança da informação na organização do fornecedor.
D) Incorreto. Essa não é a melhor forma, pois um fornecedor deve poder ter seu próprio processo de segurança da informação.

11 / 40
Quem é responsável por converter a estratégia e os objetivos de negócio em estratégia e objetivos de segurança?

A) Chief information security officer (CISO)
B) Gestão geral
C) Information security officer (ISO)
D) Information security policy officer

A) Correto. O CISO ocupa o nível de gestão mais alto da organização e desenvolve a estratégia de segurança geral para toda a empresa. (Literatura: A, Capítulo 5.2)
B) Incorreto. A gestão geral define a estratégia que serve de entrada para que o CISO defina a estratégia de segurança geral.
C) Incorreto. O ISO desenvolve a política de segurança da informação de uma unidade de negócios baseado na política da empresa e assegura que a mesma seja cumprida.
D) Incorreto. O information security policy officer é responsável por manter a política que deriva da estratégia de segurança.

12 / 40
Qual é o **melhor** exemplo de uma ameaça humana?

A) Um vazamento que provoca uma falha no fornecimento de energia.
B) Um pen drive que transmite um vírus para a rede.
C) Há muito pó na sala dos servidores.

A) Incorreto. Um vazamento não é uma ameaça humana, e sim uma ameaça não humana.
B) Correto. Um pen drive é sempre inserido por alguém. Se essa ação fizer um vírus entrar na rede, é uma ameaça humana. (Literatura: A, Capítulo 3.9.1)
C) Incorreto. Pó não é uma ameaça humana, e sim uma ameaça não humana.

13 / 40
Um sistema de banco de dados não possui os patches de segurança mais recentes e foi hackeado. Os hackers conseguiram acessar os dados e eliminá-los.

Que conceito de segurança da informação descreve a falta de patches de segurança?

A) Impacto
B) Risco
C) Ameaça
D) Vulnerabilidade

A) Incorreto. Impacto é o efeito que um evento produz na organização ou na sua informação.
B) Incorreto. Risco é a combinação da probabilidade de ocorrência de um evento e com seu impacto.
C) Incorreto. Um exemplo de ameaça é uma entidade externa tentando explorar uma vulnerabilidade. Nesse caso, os hackers são a ameaça.
D) Correto. Um exemplo de vulnerabilidade é uma falta de proteção. (Literatura: A, Capítulo 3.5.3)

14 / 40
Houve um incêndio em uma empresa. Os bombeiros chegaram rapidamente ao local e conseguiram apagar o fogo antes que ele se espalhasse e atingisse todas as instalações da empresa. Entretanto, o incêndio destruiu o servidor. As fitas de backup (cópia de segurança) que ficavam em outra sala derreteram e muitos outros documentos foram perdidos.

Que dano **indireto** foi causado por esse incêndio?

A) Sistemas de computadores queimados
B) Documentos queimados
C) Fitas de backup derretidas
D) Danos causados pela água

A) Incorreto. Sistemas de computadores queimados são danos diretos causados pelo incêndio.
B) Incorreto. Documentos queimados são danos diretos causados pelo incêndio.
C) Incorreto. Fitas de backup derretidas são danos diretos causados pelo incêndio.
D) Correto. Danos causados pela água dos extintores de incêndio são danos indiretos causados pelo incêndio. Esse é um efeito colateral da extinção do fogo, que tem por objetivo minimizar os danos causados pelo incêndio. (Literatura: A, Capítulo 3.10)

15 / 40
Empresas podem ter diferentes estratégias de risco dependendo do tipo de negócio.

Que estratégia de risco é **mais** adequada para um hospital?

A) Aceitar o risco
B) Evitar o risco
C) Suportar o risco
D) Reduzir o risco

A) Incorreto. Um hospital não pode aceitar facilmente riscos devido a perdas financeiras ou morte de pacientes.
B) Correto. Hospitais devem tentar evitar qualquer risco. (Literatura: A, Capítulo 3.11)
C) Incorreto. Suportar o risco significa que certos riscos são aceitos. Isso pode acontecer porque o custo dos controles excede os possíveis danos. Em um hospital, essa não é a melhor forma de lidar com riscos.
D) Incorreto. Reduzir o risco significa que medidas de segurança são tomadas, de forma que já não surjam ameaças ou, caso ocorram, os danos resultantes sejam minimizados. Danos para os clientes nunca são uma boa ideia, então hospitais devem evitar o risco.

16 / 40
Uma análise de risco bem realizada fornece muita informação útil. Uma análise de risco tem diferentes objetivos principais.

O que **não** é um objetivo principal de uma análise de risco?

A) Balancear os custos de um incidente e os custos de um controle
B) Determinar vulnerabilidades e ameaças importantes
C) Identificar os ativos e seu valor
D) Implementar medidas e controles

A) Incorreto. Esse é um dos principais objetivos de uma análise de risco.
B) Incorreto. Esse é um dos principais objetivos de uma análise de risco.
C) Incorreto. Esse é um dos principais objetivos de uma análise de risco.
D) Correto. Esse não é um objetivo de uma análise de risco. (Literatura: A, Capítulo 3.7)

17 / 40
Em caso de incêndio, qual é um controle repressivo?

A) Extinção do incêndio após sua detecção
B) Reparação dos danos causados pelo incêndio
C) Contratação de um seguro contra incêndio

A) Correto. Esse controle repressivo minimiza os danos causados pelo incêndio. (Literatura: A, Capítulo 3.8)
B) Incorreto. Esse não é um controle repressivo, pois não minimiza os danos causados pelo incêndio.
C) Incorreto. A contratação de um seguro protege contra as consequências financeiras de um incêndio e é um seguro contra riscos.

18 / 40
Qual é o objetivo da classificação da informação?

A) Rotular a informação para facilitar seu reconhecimento
B) Criar um manual sobre como lidar com dispositivos móveis
C) Estruturar a informação de acordo com sua sensibilidade

A) Incorreto. Rotular a informação é fazer designação, que é uma forma especial de categorizar a informação de acordo com sua classificação.
B) Incorreto. Criar um manual está relacionado com orientações para os usuários, e não com a classificação da informação.
C) Correto. A classificação da informação é utilizada para definir os diferentes níveis de sensibilidade em que a informação pode ser estruturada. (Literatura: A, Capítulo 5.12)

19 / 40
Qual é a razão **mais** importante para pôr em prática a segregação de funções?

A) Assegurar que os funcionários não realizem o mesmo trabalho ao mesmo tempo
B) Responsabilizar conjuntamente todos os funcionários pelos erros que cometem
C) Tornar claro quem é responsável por quais tarefas e atividades
D) Minimizar a possibilidade de alterações não autorizadas ou não intencionais

A) Incorreto. A segregação de funções é usada para evitar a possibilidade de modificações não autorizadas ou não intencionais, ou o uso indevido dos ativos da organização. Ela não determina quando as atividades devem ser realizadas.
B) Incorreto. A segregação de funções separa as atividades e as responsabilidades, mas não responsabiliza conjuntamente um grupo de pessoas.
C) Incorreto. A segregação de funções é usada para evitar a possibilidade de modificações não autorizadas ou não intencionais, ou o uso indevido dos ativos da organização. Seu objetivo não é tornar claro quem é responsável pelo quê.
D) Correto. As funções devem ser segregadas para evitar a possibilidade de modificações não autorizadas ou não intencionais, ou o uso indevido dos ativos da organização. (Literatura: A, Capítulo 5.3)

20 / 40
Qual é a **melhor** forma de assegurar um acesso apropriado à informação?

A) Automatizar fluxos de trabalho
B) Definir procedimentos operacionais
C) Desenvolver instruções de trabalho para todas as tarefas
D) Fornecer treinamento

A) Incorreto. Automatizar fluxos de trabalho certamente contribuirá para a segurança da informação, mas não facilita um acesso apropriado.
B) Correto. O uso de procedimentos para orientar como o trabalho é realizado de maneira apropriada, segura e responsável é uma forma eficaz de se obter uma segurança da informação eficiente. (Literatura: A, Capítulo 5.36.1)
C) Incorreto. Isso é muito detalhado e prescritivo e, portanto, não é a melhor forma.
D) Incorreto. Treinamento é importante, mas não assegura acesso apropriado à informação.

21 / 40
Houve um incêndio em uma filial de uma organização. Os funcionários foram transferidos para filiais próximas para continuar seu trabalho.

No ciclo de vida de um incidente, onde se localiza a mudança para um stand-by arrangement?

A) Entre as etapas de dano e de recuperação
B) Entre as etapas de incidente e de dano
C) Entre as etapas de recuperação e de ameaças
D) Entre as etapas de ameaças e de incidente

A) Incorreto. Dano e recuperação são limitados pelo stand-by arrangement.
B) Correto. Um stand-by arrangement é uma medida repressiva que é acionada para limitar os danos. (Literatura: A, Capítulo 3.8.4)
C) Incorreto. A etapa de recuperação ocorre após se colocar um stand-by arrangement em operação.
D) Incorreto. É muito caro realizar um stand-by arrangement sem que haja um incidente.

22 / 40
Uma funcionária descobre que a data de validade de uma política foi alterada sem seu conhecimento. Ela é a única pessoa autorizada a fazer essa alteração e notifica esse incidente de segurança ao help desk.

O funcionário do help desk registra as seguintes informações sobre esse incidente:
- data e hora
- descrição do incidente
- eventuais consequências do incidente

Que informação importante sobre o incidente não foi registrada?

A) O nome da pessoa que notifica o incidente
B) O nome do pacote de software
C) O número do computador

A) Correto. Ao se notificar um incidente, deve-se registrar pelo menos o nome da pessoa que o notifica. (Literatura: A, Capítulo 5.25)
B) Incorreto. Essa informação adicional pode ser incluída posteriormente.
C) Incorreto. Essa informação adicional pode ser incluída posteriormente.

23 / 40
Por que é importante auditar regularmente o sistema de gestão de segurança da informação (SGSI) da organização?

A) Auditorias são um requisito comum em contratos de clientes para garantir segurança da informação.
B) Auditorias são um elemento necessário para estar em conformidade com requisitos legais ou regulatórios.
C) Auditorias detectam problemas relacionados à capacidade de cumprir os objetivos financeiros da organização.
D) Auditorias detectam fragilidades na implementação de controles de segurança da informação.

A) Incorreto. Contratos de clientes raramente contêm requisitos de auditoria.
B) Incorreto. Requisitos legais ou regulatórios geralmente não exigem a realização de auditorias.
C) Incorreto. Auditorias não são normalmente utilizadas para verificar o desempenho financeiro.
D) Correto. A finalidade das auditorias é encontrar fragilidades nos controles implementados. (Literatura: A, Capítulo 5.35)

24 / 40
Que documento contém uma regra que proíbe o uso do e-mail da empresa para fins pessoais?

A) Certificado de boa índole
B) Código de conduta
C) Regulamento Geral sobre a Proteção de Dados (GDPR)
D) Acordo de não divulgação (NDA)

A) Incorreto. Um certificado de boa índole é emitido por uma organização como a Secretaria da Justiça e indica que o indivíduo não cometeu nenhuma infração penal.
B) Correto. O código de conduta é um documento (muitas vezes parte do manual do funcionário) que descreve as políticas da empresa que são aplicáveis aos funcionários. (Literatura: A, Capítulo 6.2)
C) Incorreto. O GDPR trata da proteção de informações pessoais.
D) Incorreto. Um NDA é um contrato que proíbe a divulgação de certas informações. O uso do e-mail da empresa para fins pessoais não é controlado por tal documento.

25 / 40
Quando um funcionário detecta um incidente, normalmente quem ele deve notificar **primeiro**?

A) Help desk
B) Information security manager (ISM)
C) Information security officer (ISO)
D) Gerente

A) Correto. Normalmente, incidentes devem ser notificados ao help desk para avaliação, aplicação de procedimentos iniciais e escalação, se necessário. Eles não devem ser escalados verticalmente de imediato. (Literatura: A, Capítulo 6.8)
B) Incorreto. De imediato, incidentes não devem ser escalados verticalmente. Além disso, nem todo incidente é de segurança, então o incidente deve ser primeiramente avaliado pelo help desk para determinar se há um incidente de segurança.
C) Incorreto. De imediato, incidentes não devem ser escalados verticalmente. Além disso, nem todo incidente é de segurança, então o incidente deve ser primeiramente avaliado pelo help desk para determinar se há um incidente de segurança.
D) Incorreto. De imediato, incidentes não devem ser escalados verticalmente.

26 / 40
Qual é a forma **mais** eficaz de criar conscientização sobre segurança da informação entre os funcionários?

A) Ter como foco treinamento sobre conscientização para o time de gestão
B) Enviar todos os funcionários para um treinamento externo sobre segurança da informação
C) Criar um programa de conscientização específico para a organização
D) Utilizar um curso de treinamento genérico online sobre segurança da informação

A) Incorreto. Todos os funcionários precisam de conscientização sobre segurança da informação, não apenas os gerentes.
B) Incorreto. Treinamento externo pode não ser totalmente aplicável às necessidades específicas de uma organização.
C) Correto. Adaptar um programa de conscientização sobre segurança para as necessidades organizacionais específicas é o mais eficaz. (Literatura: A, Capítulo 6.3)
D) Incorreto. Treinamento genérico sobre segurança da informação pode não ser totalmente aplicável às necessidades específicas de uma organização.

27 / 40
Que controle físico gerencia o acesso às informações de uma organização?

A) Instalação de ar-condicionado
B) Proibição do uso de pen drives
C) Exigência de nome de usuário e senha
D) Uso de vidro inquebrável

A) Incorreto. Ar-condicionado não gerencia o acesso às informações de uma organização.
B) Incorreto. Esse é um controle organizacional.
C) Incorreto. Esse é um controle técnico.
D) Correto. O uso de vidro inquebrável é um exemplo de controle físico para evitar que pessoas não autorizadas entrem no edifício. (Literatura: A, Capítulo 7.4)

28 / 40
Um centro de dados usa bancos de baterias, mas não tem gerador de energia.

Qual é o risco associado a essa situação para a disponibilidade do centro de dados?

A) A energia principal pode não voltar automaticamente quando a energia for restabelecida, pois é preciso ter um gerador de energia para isso.
B) O corte da energia principal pode durar mais do que alguns minutos ou horas, o que causará falta de energia.
C) A vida útil dos bancos de baterias é limitada, então eles podem ficar sem diesel e parar de funcionar após alguns dias.
D) Após algumas horas, os bancos de baterias devem ser alimentados pelo gerador de energia, logo eles oferecem apenas proteção limitada.

A) Incorreto. Um gerador de energia não é usado para acionar o fornecimento principal de energia.
B) Correto. Bancos de baterias apenas protegem contra cortes e picos de energia temporários, enquanto o gerador de energia protege contra cortes de maior duração. (Literatura: A, Capítulo 7.11.1)
C) Incorreto. O gerador funciona a diesel, enquanto um banco de baterias é alimentado por baterias.
D) Incorreto. Os bancos de baterias apenas funcionarão por um curto período, mas não são alimentados pelo gerador. O gerador simplesmente substitui o banco de baterias.

29 / 40
Por que há ar-condicionado na sala dos servidores?

A) As fitas de backup (cópia de segurança) são feitas de um plástico fino que não resiste a altas temperaturas. Portanto, se fizer calor demais na sala dos servidores, elas podem ser danificadas.
B) Os funcionários que trabalham na sala dos servidores não devem trabalhar no calor. O calor aumenta a probabilidade de eles cometerem erros.
C) Na sala dos servidores, o ar deve ser refrigerado e o calor produzido pelos equipamentos deve ser removido. O ar-condicionado também desumidifica e filtra o ar da sala.
D) A sala dos servidores é a melhor forma de refrigerar o ar do escritório. Nenhuma área do escritório deve ser perdida com um equipamento tão grande.

A) Incorreto. Fitas de backup não devem ser armazenadas na sala dos servidores. Um incêndio destruiria tanto a informação em uso quanto o backup.
B) Incorreto. Esse não é o motivo para se instalar ar-condicionado na sala dos servidores.
C) Correto. As salas de servidores devem ser consideradas à parte quando se pensa em segurança física. As salas de servidores contêm equipamentos sensíveis que produzem calor e são vulneráveis à umidade e ao calor. (Literatura: A, Capítulo 7.11.2)
D) Incorreto. A sala dos servidores não é o lugar para refrigerar o ar de todo o escritório.

30 / 40
Na segurança física, diversos anéis de proteção podem ser usados, nos quais diferentes medidas podem ser tomadas.

O que **não** é um anel de proteção?

A) Prédio
B) Área intermediária
C) Área segura
D) Anel externo

A) Incorreto. O prédio é um anel que dá acesso às instalações.
B) Correto. Há quatro anéis de proteção: anel externo, prédio, espaço de trabalho e área segura. (Literatura: A, Capítulo 7.0.1)
C) Incorreto. A área segura é uma área válida onde se lida com o ativo que deve ser protegido.
D) Incorreto. O anel externo é uma área válida que corresponde à área ao redor das instalações.

31 / 40
O controle para proteger um ativo depende do tipo de ativo.

Qual é a forma **mais** apropriada de proteger o ativo?

A) Proteger um formulário preenchendo-o e assinando-o
B) Proteger um laptop alocando-o a um único usuário
C) Proteger um pen drive com criptografia
D) Proteger uma conexão de internet com um backup (cópia de segurança)

A) Incorreto. Preencher um pedaço de papel com informações não é um controle apropriado.
B) Incorreto. É obviamente melhor que uma única pessoa use um único laptop, mas essa não é a opção mais apropriada. O gerenciamento de contas do usuário e o controle de senha são controles melhores.
C) Correto. Criptografia é um controle válido para proteger um pen drive. Muitas organizações empregam esse controle independentemente da classificação da informação armazenada no pen drive. (Literatura: A, Capítulo 8.12)
D) Incorreto. Usar um backup não é a melhor forma direta de proteger uma conexão de internet.

32 / 40
Que controle de segurança da informação ajuda a desenvolver sistemas tendo em conta a segurança da informação?

A) Garantir redundância dos servidores
B) Implementar controles físicos nas entradas
C) Verificar os antecedentes dos funcionários
D) Utilizar classificação de dados nos ativos de informação

A) Correto. Redundância de servidores é um controle que deve ser considerado durante o desenvolvimento de sistemas. (Literatura: A, Capítulo 8.14)
B) Incorreto. Esse é um controle válido para melhorar a segurança da informação, mas não está relacionado com o desenvolvimento de sistemas.
C) Incorreto. Esse é um controle válido para melhorar a segurança da informação, mas não está relacionado com o desenvolvimento de sistemas.
D) Incorreto. Esse é um controle válido para melhorar a segurança da informação, mas não está relacionado com o desenvolvimento de sistemas.

33 / 40
Uma organização muda sua política. A partir de agora, os funcionários estão autorizados a trabalhar remotamente.

Que controle deve ser implementado agora?

A) Criar V-LANs para segmentar a rede corporativa
B) Criptografar as informações da rede corporativa
C) Instalar firewalls na rede corporativa
D) Usar uma VPN para se conectar à rede corporativa

A) Incorreto. Segmentar redes para garantir confidencialidade e divisão de funções já deveria ter sido implementado. Estas não se aplicam especificamente à mudança da política de trabalho remoto.
B) Incorreto. Criptografia é uma ferramenta vital a ser utilizada para proteger a informação, porém ela não se aplica especificamente para permitir que funcionários trabalhem remotamente.
C) Incorreto. Firewalls entre a rede corporativa e o mundo externo são importantes, mas eles já deveriam ter sido implementados. Além disso, firewalls não protegem diretamente conexões remotas.
D) Correto. O uso de VPNs é um controle que deve ser implementado quando os funcionários são autorizados a trabalhar remotamente. (Literatura: A, Capítulo 8.2)

34 / 40
Os funcionários de uma organização trabalham com laptops protegidos por criptografia assimétrica. Todos os consultores usam o mesmo par de chaves para manter barato o gerenciamento das chaves.

Se alguma informação for comprometida, novas chaves devem ser fornecidas.

Em que caso novas chaves devem ser fornecidas?

A) Quando a chave privada se torna conhecida
B) Quando a chave pública se torna conhecida
C) Quando a infraestrutura de chave pública (ICP) se torna conhecida

A) Correto. Na criptografia assimétrica, é importante manter privada a chave privada. A chave pública pode ser conhecida. (Literatura: A, Capítulo 8.24.5)
B) Incorreto. A chave pública pode ser aberta para todo o mundo. A chave privada deve ser mantida em segredo para assegurar integridade e disponibilidade.
C) Incorreto. A PCI é utilizada para a troca de chaves em sistemas de criptografia assimétrica.

35 / 40
Que tipo de segurança uma infraestrutura de chave pública (ICP) oferece?

A) Uma ICP garante que os backups (cópias de segurança) dos dados da empresa sejam feitos regularmente.
B) Uma ICP mostra aos clientes que um negócio na internet é seguro.
C) Uma ICP verifica qual pessoa ou sistema pertence a uma chave pública específica.

A) Incorreto. Uma ICP não garante a realização de backups.
B) Incorreto. Uma ICP fornece garantia sobre qual pessoa ou sistema pertence a uma chave pública específica.
C) Correto. Uma característica de uma ICP é fornecer garantia, por meio de acordos, procedimentos e uma estrutura organizacional, sobre qual pessoa ou sistema pertence a uma chave pública específica. (Literatura: A, Capítulo 8.24.6)

36 / 40
Que tipo de malware é um programa que, além da função que aparentemente desempenha, realiza propositalmente atividades secundárias?

A) Bomba lógica
B) Spyware
C) Trojan
D) Worm

A) Incorreto. Uma bomba lógica é uma parte de código que está incluído em um sistema de software. Esse código irá executar uma função quando condições específicas forem atendidas. Ele nem sempre é usado para fins maliciosos e nem sempre realiza atividades secundárias.
B) Incorreto. Spyware é um programa de computador que coleta informações do computador do usuário e as envia para terceiros.
C) Correto. Um trojan é um programa que, além da função que aparentemente desempenha, realiza propositalmente atividades secundárias, despercebidas pelo usuário do computador, que podem danificar a integridade do sistema infectado. (Literatura: A, Capítulo 8.7.2)
D) Incorreto. Um worm cria uma rede de computadores contaminados ao se replicar.

37 / 40
Que tipo de malware cria uma rede de computadores contaminados ao se replicar?

A) Bomba lógica
B) Spyware
C) Trojan
D) Worm

A) Incorreto. Uma bomba lógica é uma parte de código que está incluído em um sistema de software. Esse código irá executar uma função quando condições específicas forem atendidas. Ele nem sempre é usado para fins maliciosos.
B) Incorreto. Spyware é um programa de computador que coleta informações sobre o usuário do computador e as envia para terceiros.
C) Incorreto. Um trojan é um programa que, além da função que aparentemente desempenha, realiza propositalmente atividades secundárias, despercebidas pelo usuário do computador, que podem danificar a integridade do sistema infectado.
D) Correto. Isso é o que um worm faz. (Literatura: A, Capítulo 8.7)

38 / 40
Qual é o ato legislativo ou regulatório relacionado à segurança da informação que pode ser imposto a todas as organizações?

A) Regulamento Geral sobre a Proteção de Dados (GDPR)
B) Direitos de propriedade intelectual (PI)
C) ISO/IEC 27001
D) ISO/IEC 27002

A) Correto. Todas as organizações devem ter uma política e procedimentos para a proteção de dados pessoais, que devem ser do conhecimento de todos que processam dados pessoais. (Literatura: A, Capítulo 5.33)
B) Incorreto. Esse regulamento não está relacionado à segurança da informação para as organizações.
C) Incorreto. Essa é uma norma com diretrizes para as organizações sobre como lidar com a implantação de um processo de segurança da informação.
D) Incorreto. Essa norma, também conhecida como "segurança da informação, segurança cibernética e proteção da privacidade - controles de segurança da informação", contém diretrizes sobre política e controles de segurança da informação.

39 / 40
Que norma ISO tem como foco a implementação de controles de segurança da informação?

A) ISO/IEC 27000
B) ISO/IEC 27001
C) ISO/IEC 27002
D) ISO/IEC 27005

A) Incorreto. Essa é a introdução geral à série de normas ISO/IEC 27000.
B) Incorreto. Essa é a norma com requisitos para um sistema de gestão de segurança da informação (SGSI).
C) Correto. Essa é a norma que especifica os controles de segurança da informação, com orientação para sua implementação. (Literatura: A, Capítulo 4.12)
D) Incorreto. A ISO/IEC 27005 foca na gestão de riscos de segurança da informação.

40 / 40
Que organização tem as normas **mais** comumente usadas na Europa?

A) Instituto Nacional Americano de Padrões (ANSI)
B) Organização Internacional de Padronização (ISO)
C) Instituto Nacional de Padrões e Tecnologia (NIST)

A) Incorreto. As normas ANSI são mais comuns nos Estados Unidos da América.
B) Correto. Na Europa, as normas ISO são as mais comuns. (Literatura: A, Capítulo 5.36)
C) Incorreto. As normas NIST são mais comuns nos Estados Unidos da América.

Avaliação

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

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

Contato EXIN

www.exin.com