Exame simulado

Edição 202309

Conteúdo

Introdução

Este é o exame simulado EXIN Information Security Management Professional based on ISO/IEC 27001 (ISMP.PR). As regras e regulamentos do exame do EXIN se aplicam a esse exame.

Esse exame contém 30 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, exceto se especificado o contrário.

O número máximo de pontos que pode ser obtido nesse exame é 30. Cada resposta correta vale 1 ponto. Você precisa de 20 pontos ou mais para passar no exame.

O tempo permitido para esse exame é de 90 minutos.

Boa Sorte!

Exame simulado

1 / 30
Qual é um elemento **chave** no desenvolvimento da estratégia de segurança?

A) Descrição de como os serviços são suportados
B) Política que não entra em conflito com a legislação do país da organização
C) Objetivos de controle relevantes
D) Retorno sobre o Investimento (ROI)

2 / 30
Uma organização tem diversos fornecedores que contribuem para a entrega e suporte de serviços de ponta a ponta.

Em que capacidade a organização deve investir **principalmente** para minimizar os problemas de segurança da informação oriundos de seus fornecedores?

A) Auditorias
B) Governança
C) Gerenciamento de riscos
D) Treinamento

3 / 30
O gerente de segurança é responsável por definir os controles de segurança de uma empresa. A empresa está selecionando um fornecedor para hospedar o sistema de pedidos na web.

Qual é o aspecto **mais** importante que o gerente de segurança deve buscar?

A) Um padrão para due care (devido cuidado)
B) Um padrão para due diligence (devida diligência)
C) Benchmarking
D) Melhores práticas de segurança

4 / 30
Controles de segurança são definidos com base na classificação de segurança de um elemento de dados.

Quem é responsável pela classificação de um elemento de dados?

A) O conselho de administração, que dirige a empresa
B) O custodiante de dados, que gerencia o uso dos dados
C) O proprietário do processo (process owner), que governa o processo
D) O proprietário do sistema (system owner), que protege o sistema de informação

5 / 30
Solicita-se a um gerente de riscos que realize uma avaliação de riscos completa para uma empresa.

Qual é o **melhor** método para identificar a **maioria** das ameaças à empresa?

A) Fazer um brainstorm com representantes de todas as partes interessadas
B) Entrevistar a alta gestão
C) Enviar uma lista de verificação para identificação de ameaças a todos os funcionários envolvidos com segurança da informação

6 / 30
Uma empresa que vende livros está implementando atualmente uma gestão de segurança da informação. A líder do projeto de segurança da informação entende que o processo de identificação de riscos necessita que ela liste os ativos da organização por ordem de importância. Para desenvolver essa lista, ela trabalha com o gerente financeiro. A importância é ponderada pelos seguintes critérios: impacto no faturamento (30%), impacto na rentabilidade (40%) e impacto na imagem pública (30%).

O gerente financeiro encontrou quatro ativos de informação importantes:

- Pedidos aos fornecedores (saída)
- Pedidos dos clientes via SSL (entrada)
- Aconselhamento dos fornecedores quanto ao fulfillment (entrada)
- Solicitação de serviço do cliente por e-mail (entrada)

Qual ativo tem a maior importância com base nos critérios de impacto?

A) Pedidos aos fornecedores (saída)
B) Pedidos dos clientes via SSL (entrada)
C) Aconselhamento dos fornecedores quanto ao fulfillment (entrada)
D) Solicitação de serviço do cliente por e-mail (entrada)

7 / 30
Um gerente de operações busca orientação sobre como abrir um segundo centro de dados como local de hot standby.

O que o information security officer (ISO) recomendaria ao gerente de operações?

A) Garantir que a rede e o fornecimento de energia sejam redundantes e de diferentes fornecedores
B) Garantir que o acesso físico seja permitido apenas a operadores específicos
C) Garantir que a empresa não seja vítima da legislação do Ato Patriota (Patriot Act)
D) Garantir que o local tenha um perfil de risco físico diferente daquele do local principal

8 / 30
Uma grande empresa transportadora adotou a norma de segurança da informação e necessita estabelecer controles para seu departamento de desenvolvimento de software, que será terceirizado. Um consultor externo foi nomeado para assegurar que controles de segurança consistentes com o código de prática sejam implementados em toda a cadeia de suprimentos para o desenvolvimento de software na nova situação de terceirização.

Que controle deve ser implementado para garantir disponibilidade do código fonte caso algum dos parceiros na cadeia de suprimentos encerre suas atividades?

A) Testes de aceitação
B) Documentação eficaz
C) Acordos judiciais
D) Contratos de licenciamento

9 / 30
O escopo do gerenciamento de riscos não se limita apenas aos processos organizacionais, devendo também ser integrado à metodologia de gerenciamento de projetos. Por exemplo, deve-se realizar uma avaliação de riscos de segurança da informação na fase inicial de cada projeto. Ao implementar o gerenciamento de riscos do projeto, é necessário considerar o escopo desse projeto.

O que deve ser incluído no escopo do gerenciamento de riscos do projeto para projetos padrão?

A) É necessário se preparar para o nível de risco máximo e, consequentemente, implementar subprocessos importantes relacionados ao risco, como identificação, quantificação, desenvolvimento de respostas e controle de respostas.
B) É necessário somente incluir uma simples identificação e mecanismo de classificação para ameaças e riscos especificamente relacionados ao projeto, pois uma organização de projeto é apenas uma pequena parte da organização.
C) Devem-se incluir os processos necessários para avaliar, gerenciar e reduzir o impacto de ocorrências, como seria o caso em um projeto de segurança da informação.

10 / 30
Qual é a **melhor** estratégia a ser implementada quando a avaliação de riscos aponta que uma vulnerabilidade específica pode ser explorada?

A) Implementação de uma estrutura de gerenciamento de riscos
B) Implementação de um controle de segurança da informação
C) Implementação de um software antivírus

11 / 30
Uma organização convenceu sua liderança sênior da necessidade de uma abordagem formal no gerenciamento de riscos. A liderança sênior demonstrou preocupação quanto ao custo dos controles de riscos propostos.

Que afirmação deve ser incluída no caso de negócio para a implementação de controles de riscos?

A) Controles são a principal forma de melhorar o perfil de risco da organização.
B) Controles determinam as opções de mitigação de riscos da organização.
C) Controles ajudam a organização a identificar seus ativos mais críticos.
D) Controles fornecem informações à organização sobre vulnerabilidades de ativos.

12 / 30
Um funcionário trabalha na avaliação de riscos organizacionais. O objetivo da avaliação não é zerar os riscos residuais, mas alinhar os riscos residuais com o apetite de riscos da organização.

Quando o programa de avaliação de riscos cumpre seu objetivo **principal**?

A) Quando os controles são implementados
B) Quando a transferência do risco é concluída
C) Quando os tomadores de decisão são informados sobre os riscos não controlados e grupos de autoridade competentes decidem manter os riscos
D) Quando a análise de riscos é concluída

13 / 30
A manutenção de um programa de segurança da informação exige um processo contínuo. Isso requer dados de entrada de vários fatores diferentes que influenciarão seu sucesso.

Qual é uma influência de entrada que exigiria uma mudança no processo?

A) Política
B) Avaliação de riscos
C) Plano de segurança

14 / 30
O information security officer (ISO) de uma empresa global acaba de receber uma revisão de gerenciamento da política de segurança da informação.

O que esses resultados devem incluir?

A) Feedback das partes interessadas
B) Melhorias dos objetivos de controle e dos controles
C) Status das medidas preventivas e corretivas

15 / 30
Uma organização está implementando a gestão de incidentes de segurança da informação. Ela já possui um mecanismo para os colaboradores relatarem eventos observados ou suspeitos de segurança da informação, mas esses eventos não são bem administrados depois de relatados.

A organização implementou processos, funções e responsabilidades relevantes.

Agora, ela está avançando na implementação de outras atividades necessárias para a gestão de incidentes de segurança da informação.

O que **não** é uma atividade para implementar a gestão de incidentes de segurança da informação?

A) Chegar a um acordo sobre como evitar incidentes de segurança da informação usando conhecimento adquirido com incidentes para fortalecer e melhorar os controles de segurança da informação
B) Definir e comunicar procedimentos sobre resposta a incidentes de segurança da informação que devem ser realizados por pessoal competente
C) Elaborar um esquema de categorização e priorização que possa ser usado para categorizar eventos de segurança da informação como incidentes de segurança da informação
D) Implementar procedimentos para coletar e preservar evidência relacionada a eventos de segurança da informação para uso em qualquer ação disciplinar ou judicial necessária
E) Estabelecer regras para controlar o acesso físico e lógico à informação e a outros ativos associados para evitar incidentes de segurança da informação

16 / 30
A gestão de incidentes de segurança é feita pelo processo de gerenciamento de incidentes segundo diretrizes da gestão de segurança da informação. Essas diretrizes exigem diversos tipos de planos de mitigação.

Qual plano de mitigação abrange a recuperação a curto prazo após a ocorrência de um incidente de segurança?

A) O plano de continuidade de negócios (BCP)
B) O plano de recuperação de desastres
C) O plano de resposta a incidentes
D) O plano de tratamento de riscos

17 / 30
Quem é responsável por coordenar o programa de conscientização sobre segurança de uma organização?

A) Todos na organização
B) A gestão de segurança da informação
C) O departamento de TI
D) O assessor do CIO

18 / 30
No ano passado, uma organização se tornou mais rigorosa com relação aos controles de segurança de seus funcionários. Antes de implementar controles adicionais, o information security officer (ISO) deseja conhecer a mentalidade dos funcionários quanto aos controles de segurança da informação.

Como o ISO obtém rapidamente uma ideia sobre isso?

A) Ao checar o fluxo de dados da Internet
B) Ao determinar se há vírus na rede
C) Ao percorrer o escritório após o horário normal de trabalho

19 / 30
O gerente de continuidade de negócios pede contribuições para um plano de contingência.

Qual deve ser a **primeira** atividade do gerente de continuidade de negócios?

A) Definir o escopo
B) Identificar funções de negócios críticas
C) Testar o plano

20 / 30
Um arquiteto de segurança discute com o time interno de prevenção de incêndios sobre a afirmação na política de segurança da informação de que as portas das áreas confidenciais devem estar sempre trancadas. O time de resposta a emergências quer ter acesso a essas áreas em caso de incêndio.

Qual é a **melhor** solução para esse dilema?

A) As portas devem permanecer fechadas em caso de incêndio para evitar acesso às áreas confidenciais.
B) As portas devem abrir automaticamente em caso de incêndio.
C) O arquiteto de segurança deve ser informado quando houver incêndio.

21 / 30
Qual é a **maior** vantagem de usar designs abertos de arquitetura de segurança?

A) Designs abertos são fáceis de configurar.
B) Designs abertos são muito testados.
C) Designs abertos têm muitas funcionalidades adicionais.

22 / 30
Que afirmação sobre arquitetura de segurança é a **mais** correta?

A) A arquitetura de segurança define completamente as regras de implementação.
B) A arquitetura de segurança segue a estratégia.
C) A arquitetura de segurança é secundária.

23 / 30
Por que é importante definir quais serviços de segurança serão prestados?

A) Para melhor alinhar os requisitos de segurança da informação e o serviço ao cliente
B) Para determinar a estratégia de segurança da informação de uma organização
C) Para garantir que uma organização esteja em conformidade com os requisitos da ISO/IEC 27001
D) Para compreender o escopo do sistema de gestão de segurança da informação (SGSI)

24 / 30
Que item de segurança é concebido para receber um grande volume de tráfego relacionado à rede que pode indicar um ataque de negação de serviço?

A) Firewall
B) Sistema de detecção e prevenção de intrusão baseado no host (IDPS de host)
C) Sistema de detecção e prevenção de intrusão baseado na rede (IDPS de rede)
D) Rede privada virtual (VPN)

25 / 30
A CEO de uma empresa começou a usar seu tablet PC e deseja que o gerente de segurança possibilite que ela use e-mail profissional e agenda no tablet. O gerente de segurança entende essa vontade de permitir a possibilidade de uso de dispositivos pessoais (Bring Your Own Device, BYOD) e organiza um treinamento de conscientização sobre BYOD.

Que outro controle o gerente de segurança deve propor para evitar perda de dados em caso de furto ou perda do dispositivo pessoal?

A) Não atender ao desejo até que seja possível uma integração estável das funções de negócios em dispositivos pessoais
B) Criptografar o armazenamento local e as conexões de rede
C) Implementar autentificação forte usando tokens com senhas de uso único
D) Instalar um antimalware e um firewall para evitar infecção

26 / 30
Por que os elementos de segurança na infraestrutura de TI são importantes?

A) Para possibilitar a continuidade de negócios da infraestrutura de TI
B) Para gerenciar incidentes de segurança da informação que impactam a infraestrutura de TI
C) Para evitar acesso físico não autorizado à infraestrutura de TI
D) Para proteger os ativos de informação que estão na infraestrutura de TI

27 / 30
Zoneamento é um controle de segurança para separar áreas físicas com diferentes níveis de segurança. Zonas com maiores níveis de segurança podem ser protegidas com mais controles. O gerente de segurança de um hotel, responsável pela segurança, está considerando diferentes zonas para o hotel.

Que funções de negócios devem ser combinadas em uma zona de segurança?

A) Sala de reunião do conselho e espaço geral do escritório
B) Academia e depósito
C) Quartos do hotel e bar aberto ao público
D) Restaurante aberto ao público e lobby

28 / 30
Um gerente de segurança de uma grande empresa tem a tarefa de obter proteção física para o armazenamento de dados corporativos.

A proteção física pode ser obtida através de qual controle?

A) Fazer com que os visitantes façam login e logoff ao acessar o centro de dados corporativos
B) Instalar um firewall para evitar acesso à infraestrutura de rede
C) Usar controles de cartão-chave de acesso para os funcionários que necessitam de acesso
D) Elaborar uma política que defina quem pode ter acesso à empresa

29 / 30
Sabendo que controles de segurança físicos são uma parte importante de um programa de segurança da informação, solicitou-se ao time de segurança da informação que projetasse e implementasse um perímetro de segurança para um departamento que está configurando alguns novos sistemas de dados.

Segundo a ISO/IEC 27001, qual é a recomendação **mais** importante que deve ser considerada ao se estabelecer esse perímetro?

A) Um modelo de suporte de duas pessoas
B) Instalação de câmeras e alarmes
C) Registro de sistemas e monitoração
D) A extensão do perímetro deve ser alinhada com o valor dos dados

30 / 30
A gerente de recursos humanos de uma organização perguntou o que poderia fazer para obter resultados rápidos na área de emprego e contratação para ajudar a fortalecer o programa de segurança de dados da organização conforme a ISO/IEC 27001.

Qual deve ser o conselho?

A) Verificar antecedentes
B) Implementar uma política de segurança
C) Instalar portões giratórios na entrada

Gabarito de respostas

1 / 30
Qual é um elemento **chave** no desenvolvimento da estratégia de segurança?

A) Descrição de como os serviços são suportados
B) Política que não entra em conflito com a legislação do país da organização
C) Objetivos de controle relevantes
D) Retorno sobre o Investimento (ROI)

A) Incorreto. Essa resposta não diz respeito à definição de uma estratégia de segurança global e está mais focada no acordo de nível de serviço (SLA).
B) Incorreto. Essa resposta não diz respeito à definição de uma estratégia de segurança global e está mais relacionada à política de desenvolvimento.
C) Correto. Possuir objetivos de controle relevantes é um elemento chave no desenvolvimento da estratégia de segurança. (Literatura: A, Slide 013)
D) Incorreto. Essa resposta não diz respeito à definição de uma estratégia de segurança global e está mais relacionada à previsão financeira e à orçamentação.

2 / 30
Uma organização tem diversos fornecedores que contribuem para a entrega e suporte de serviços de ponta a ponta.

Em que capacidade a organização deve investir **principalmente** para minimizar os problemas de segurança da informação oriundos de seus fornecedores?

A) Auditorias
B) Governança
C) Gerenciamento de riscos
D) Treinamento

A) Incorreto. Auditorias são essenciais para assegurar que as atividades acordadas estejam sendo realizadas. Seria melhor, porém, investir em capacidades de governança para assegurar que haja políticas que direcionem o comportamento de todas as partes envolvidas na prestação de serviços.
B) Correto. Governança é a capacidade sobrejacente que direciona as políticas e processos da organização, incluindo o envolvimento dos fornecedores. A governança lida com a avaliação, o direcionamento e a monitoração da organização em tópicos como segurança da informação. A governança trabalha com o desenvolvimento de políticas, o recebimento de informações de monitoração, a avaliação dessas informações com base nas políticas da organização e a provisão de direcionamento à diretoria para fazer mudanças quando necessário. (Literatura: A, Slide 018)
C) Incorreto. O gerenciamento de riscos tem diversas atividades que seriam úteis nesse cenário, mas fortalecer as capacidades de governança da organização aumentará a probabilidade de um controle geral mais rigoroso das atividades de todas as partes envolvidas na prestação de serviços.
D) Incorreto. É importante investir em treinamento, mas uma capacidade de governança robusta ajudará a organização a desenvolver políticas que direcionarão o comportamento de todas as partes envolvidas na prestação de serviços.

3 / 30
O gerente de segurança é responsável por definir os controles de segurança de uma empresa. A empresa está selecionando um fornecedor para hospedar o sistema de pedidos na web.

Qual é o aspecto **mais** importante que o gerente de segurança deve buscar?

A) Um padrão para due care (devido cuidado)
B) Um padrão para due diligence (devida diligência)
C) Benchmarking
D) Melhores práticas de segurança

A) Incorreto. Um padrão para due care simboliza um nível mínimo de segurança.
B) Incorreto. Due diligence significa que o fornecedor cumpre um requisito padrão. Isso não é necessariamente o padrão.
C) Incorreto. Benchmarking é uma técnica utilizada para comparar organizações com negócios, maturidade e mercados semelhantes.
D) Correto. Melhores práticas de segurança são o que há de melhor para uma dada indústria ou linha de trabalho. É isso que o gerente de segurança buscará em um fornecedor. (Literatura: A, Slide 024)

4 / 30
Controles de segurança são definidos com base na classificação de segurança de um elemento de dados.

Quem é responsável pela classificação de um elemento de dados?

A) O conselho de administração, que dirige a empresa
B) O custodiante de dados, que gerencia o uso dos dados
C) O proprietário do processo (process owner), que governa o processo
D) O proprietário do sistema (system owner), que protege o sistema de informação

A) Incorreto. O conselho de administração é o prestador de contas geral de qualquer processo de negócios, mas a responsabilidade de exercer todas as funções é delegada.
B) Incorreto. Um custodiante é responsável por definir e gerenciar os requisitos para qualquer elemento de dados no que diz respeito ao cumprimento de leis e regulações. Ele também é responsável pela utilização de dados por diferentes partes e processos na forma de contratos de dados.
C) Correto. Qualquer elemento de dados é objeto de controle de um processo de negócios. O proprietário do processo é a única pessoa que pode identificar se um elemento de dados é crítico na organização. (Literatura: A, Slide 045)
D) Incorreto. O proprietário do sistema é responsável por implementar o controle como exigido pela classificação de confidencialidade, integridade e disponibilidade (CIA).

5 / 30
Solicita-se a um gerente de riscos que realize uma avaliação de riscos completa para uma empresa.

Qual é o **melhor** método para identificar a **maioria** das ameaças à empresa?

A) Fazer um brainstorm com representantes de todas as partes interessadas
B) Entrevistar a alta gestão
C) Enviar uma lista de verificação para identificação de ameaças a todos os funcionários envolvidos com segurança da informação

A) Correto. Um brainstorm com todas as partes interessadas garante que todas as perspectivas sejam representadas. (Literatura: A, Slide 030)
B) Incorreto. A alta gestão pode monitorar várias ameaças, mas não todas. Há uma maneira melhor de identificar mais ameaças.
C) Incorreto. Os funcionários envolvidos com segurança da informação não conseguem enxergar todas as ameaças. Há uma maneira melhor de identificar mais ameaças.

6 / 30
Uma empresa que vende livros está implementando atualmente uma gestão de segurança da informação. A líder do projeto de segurança da informação entende que o processo de identificação de riscos necessita que ela liste os ativos da organização por ordem de importância. Para desenvolver essa lista, ela trabalha com o gerente financeiro. A importância é ponderada pelos seguintes critérios: impacto no faturamento (30%), impacto na rentabilidade (40%) e impacto na imagem pública (30%).

O gerente financeiro encontrou quatro ativos de informação importantes:

- Pedidos aos fornecedores (saída)
- Pedidos dos clientes via SSL (entrada)
- Aconselhamento dos fornecedores quanto ao fulfillment (entrada)
- Solicitação de serviço do cliente por e-mail (entrada)

Qual ativo tem a maior importância com base nos critérios de impacto?

A) Pedidos aos fornecedores (saída)
B) Pedidos dos clientes via SSL (entrada)
C) Aconselhamento dos fornecedores quanto ao fulfillment (entrada)
D) Solicitação de serviço do cliente por e-mail (entrada)

A) Incorreto. Quando os pedidos para os fornecedores não podem ser emitidos, há um grande impacto na possibilidade de gerar faturamento e ter lucro. Geralmente isso atrasa os pedidos dos clientes. Alguns clientes podem transferir suas compras para um concorrente. Isso também impacta a rentabilidade e a imagem pública. Entretanto, ainda poderá haver faturamento e lucro.
B) Correto. Quando um cliente não consegue fazer um pedido online, ele fará o pedido imediatamente com outro fornecedor. O impacto no faturamento, na rentabilidade e na imagem pública será máximo. (Literatura: A, Slide 037)
C) Incorreto. Quando o fornecedor não consegue enviar as entregas, há um grande impacto na possibilidade de gerar faturamento e ter lucro. Ademais, isso atrasa os pedidos dos clientes. Alguns clientes podem transferir suas compras para um concorrente. Isso impacta a rentabilidade e a imagem pública. Eventualmente, poderá haver faturamento e lucro.
D) Incorreto. Quando as solicitações de serviço dos clientes não podem ser atendidas, há um grande impacto na imagem pública. O impacto no faturamento e na rentabilidade será significantemente menor do que em comparação a falhas em elementos do processo de logística.

7 / 30
Um gerente de operações busca orientação sobre como abrir um segundo centro de dados como local de hot standby.

O que o information security officer (ISO) recomendaria ao gerente de operações?

A) Garantir que a rede e o fornecimento de energia sejam redundantes e de diferentes fornecedores
B) Garantir que o acesso físico seja permitido apenas a operadores específicos
C) Garantir que a empresa não seja vítima da legislação do Ato Patriota (Patriot Act)
D) Garantir que o local tenha um perfil de risco físico diferente daquele do local principal

A) Incorreto. Isso é apenas parte do perfil de risco.
B) Incorreto. Esse é um controle geral de segurança.
C) Incorreto. Isso não é um risco de segurança físico, mas um problema de legislação.
D) Correto. Como se trata de um local de backup, é aconselhável certificar-se de que tenha um perfil de risco diferente. (Literatura: A, Slide 050)

8 / 30
Uma grande empresa transportadora adotou a norma de segurança da informação e necessita estabelecer controles para seu departamento de desenvolvimento de software, que será terceirizado. Um consultor externo foi nomeado para assegurar que controles de segurança consistentes com o código de prática sejam implementados em toda a cadeia de suprimentos para o desenvolvimento de software na nova situação de terceirização.

Que controle deve ser implementado para garantir disponibilidade do código fonte caso algum dos parceiros na cadeia de suprimentos encerre suas atividades?

A) Testes de aceitação
B) Documentação eficaz
C) Acordos judiciais
D) Contratos de licenciamento

A) Incorreto. Testes de aceitação são um mecanismo para assegurar que as entregas do processo de desenvolvimento atendam aos critérios de qualidade do cliente. O cliente não obtém acesso ao código fonte.
B) Incorreto. Documentação eficaz é um requisito geral para todos os controles. O código fonte não faz parte da documentação acessível ao cliente.
C) Correto. Acordos judiciais assegurarão que o código fonte seja armazenado em um local neutro. O código fonte estará acessível ao cliente quando certos critérios forem atendidos, por exemplo, se o fornecedor for à falência. (Literatura: A, Slide 050)
D) Incorreto. Contratos de licenciamento apenas asseguram a propriedade do código e direitos de propriedade intelectual. Eles não garantem acesso ao código fonte pelo cliente se o fornecedor encerrar suas atividades.

9 / 30
O escopo do gerenciamento de riscos não se limita apenas aos processos organizacionais, devendo também ser integrado à metodologia de gerenciamento de projetos. Por exemplo, deve-se realizar uma avaliação de riscos de segurança da informação na fase inicial de cada projeto. Ao implementar o gerenciamento de riscos do projeto, é necessário considerar o escopo desse projeto.

O que deve ser incluído no escopo do gerenciamento de riscos do projeto para projetos padrão?

A) É necessário se preparar para o nível de risco máximo e, consequentemente, implementar subprocessos importantes relacionados ao risco, como identificação, quantificação, desenvolvimento de respostas e controle de respostas.
B) É necessário somente incluir uma simples identificação e mecanismo de classificação para ameaças e riscos especificamente relacionados ao projeto, pois uma organização de projeto é apenas uma pequena parte da organização.
C) Devem-se incluir os processos necessários para avaliar, gerenciar e reduzir o impacto de ocorrências, como seria o caso em um projeto de segurança da informação.

A) Incorreto. Implementação de todos os subprocessos possíveis apenas é aplicável em cenários de projetos de alto risco, como projetos de segurança ou em ambientes de missão crítica. A abordagem deve ser genérica apenas em tais ambientes.
B) Correto. Geralmente, esse escopo deve ser suficiente para a maioria dos projetos. Dito isso, é necessário permitir projetos maiores e mais críticos, então deve haver também um processo para escalar para processos mais detalhados de gerenciamento de riscos para projetos corporativos maiores/mais abrangentes. Assim, é necessário implementar um escopo genérico, como se faz para a organização como um todo. (Literatura: A, Slide 047)
C) Incorreto. O gerenciamento de riscos de projeto é muito semelhante ao gerenciamento de riscos normal. Consequentemente, o escopo genérico deve ser semelhante. Em muitas ocasiões, apenas será necessária uma abordagem simples, identificando e classificando apenas as ameaças especificamente enfrentadas pelo projeto.

10 / 30
Qual é a **melhor** estratégia a ser implementada quando a avaliação de riscos aponta que uma vulnerabilidade específica pode ser explorada?

A) Implementação de uma estrutura de gerenciamento de riscos
B) Implementação de um controle de segurança da informação
C) Implementação de um software antivírus

A) Incorreto. Uma estrutura de gerenciamento de riscos é uma metodologia de riscos, não uma estratégia.
B) Correto. Controles devem ser implementados para minimizar os riscos organizacionais. (Literatura: A, Slide 033)
C) Incorreto. Embora o software antivírus ajude as organizações a se protegerem contra vírus e malwares, essa não é a solução para todos os riscos.

11 / 30
Uma organização convenceu sua liderança sênior da necessidade de uma abordagem formal no gerenciamento de riscos. A liderança sênior demonstrou preocupação quanto ao custo dos controles de riscos propostos.

Que afirmação deve ser incluída no caso de negócio para a implementação de controles de riscos?

A) Controles são a principal forma de melhorar o perfil de risco da organização.
B) Controles determinam as opções de mitigação de riscos da organização.
C) Controles ajudam a organização a identificar seus ativos mais críticos.
D) Controles fornecem informações à organização sobre vulnerabilidades de ativos.

A) Correto. A segurança da informação pode ser melhorada principalmente pela implementação de controles. (Literatura: A, Slide 050 e 051)
B) Incorreto. Esse é um benefício da avaliação de riscos, não da implementação de controles.
C) Incorreto. Esse é um benefício da avaliação de riscos, não da implementação de controles.
D) Incorreto. Esse é um benefício da identificação de ameaças, não da implementação de controles.

12 / 30
Um funcionário trabalha na avaliação de riscos organizacionais. O objetivo da avaliação não é zerar os riscos residuais, mas alinhar os riscos residuais com o apetite de riscos da organização.

Quando o programa de avaliação de riscos cumpre seu objetivo **principal**?

A) Quando os controles são implementados
B) Quando a transferência do risco é concluída
C) Quando os tomadores de decisão são informados sobre os riscos não controlados e grupos de autoridade competentes decidem manter os riscos
D) Quando a análise de riscos é concluída

A) Incorreto. Se não houver monitoração contínua dos controles, eles se deteriorarão com o tempo e o risco ultrapassará o apetite de riscos da organização.
B) Incorreto. Transferência de riscos é apenas um dos métodos usados para controlar riscos. Essa questão refere-se à totalidade da estrutura de controle.
C) Correto. É importante que profissionais de segurança da informação se certifiquem de que os riscos restantes sejam mantidos dentro dos limites do apetite de riscos da organização. (Literatura: A, Slide 030)
D) Incorreto. Quando a análise de riscos é concluída, o verdadeiro trabalho do gerenciamento de riscos está apenas começando.

13 / 30
A manutenção de um programa de segurança da informação exige um processo contínuo. Isso requer dados de entrada de vários fatores diferentes que influenciarão seu sucesso.

Qual é uma influência de entrada que exigiria uma mudança no processo?

A) Política
B) Avaliação de riscos
C) Plano de segurança

A) Incorreto. Política é um resultado do programa, e não um dado de entrada.
B) Correto. Avaliação de riscos é uma mudança de entrada que requer adaptação do processo. (Literatura: A, Slide 033)
C) Incorreto. Plano de segurança é um resultado do programa, e não um dado de entrada.

14 / 30
O information security officer (ISO) de uma empresa global acaba de receber uma revisão de gerenciamento da política de segurança da informação.

O que esses resultados devem incluir?

A) Feedback das partes interessadas
B) Melhorias dos objetivos de controle e dos controles
C) Status das medidas preventivas e corretivas

A) Incorreto. Isso é dado de entrada para uma revisão de gerenciamento da política de segurança da informação.
B) Correto. Isso deve estar incluído nos resultados. (Literatura: A, Slide 060)
C) Incorreto. Isso é dado de entrada para uma revisão de gerenciamento da política de segurança da informação.

15 / 30
Uma organização está implementando a gestão de incidentes de segurança da informação. Ela já possui um mecanismo para os colaboradores relatarem eventos observados ou suspeitos de segurança da informação, mas esses eventos não são bem administrados depois de relatados.

A organização implementou processos, funções e responsabilidades relevantes.

Agora, ela está avançando na implementação de outras atividades necessárias para a gestão de incidentes de segurança da informação.

O que **não** é uma atividade para implementar a gestão de incidentes de segurança da informação?

A) Chegar a um acordo sobre como evitar incidentes de segurança da informação usando conhecimento adquirido com incidentes para fortalecer e melhorar os controles de segurança da informação
B) Definir e comunicar procedimentos sobre resposta a incidentes de segurança da informação que devem ser realizados por pessoal competente
C) Elaborar um esquema de categorização e priorização que possa ser usado para categorizar eventos de segurança da informação como incidentes de segurança da informação
D) Implementar procedimentos para coletar e preservar evidência relacionada a eventos de segurança da informação para uso em qualquer ação disciplinar ou judicial necessária
E) Estabelecer regras para controlar o acesso físico e lógico à informação e a outros ativos associados para evitar incidentes de segurança da informação

A) Incorreto. Isso é parte da implementação da gestão de incidentes de segurança da informação.
B) Incorreto. Isso é parte da implementação da gestão de incidentes de segurança da informação.
C) Incorreto. Isso é parte da implementação da gestão de incidentes de segurança da informação.
D) Incorreto. Isso é parte da implementação da gestão de incidentes de segurança da informação.
E) Correto. Implementar controle de acesso pode reforçar a prevenção de incidentes, mas não é parte da implementação da gestão de incidentes de segurança da informação. (Literatura: A, Slides 085 e 094)

16 / 30
A gestão de incidentes de segurança é feita pelo processo de gerenciamento de incidentes segundo diretrizes da gestão de segurança da informação. Essas diretrizes exigem diversos tipos de planos de mitigação.

Qual plano de mitigação abrange a recuperação a curto prazo após a ocorrência de um incidente de segurança?

A) O plano de continuidade de negócios (BCP)
B) O plano de recuperação de desastres
C) O plano de resposta a incidentes
D) O plano de tratamento de riscos

A) Incorreto. O BCP é implantado após se determinar que o desastre afeta a operação dos negócios. Seu objetivo é assegurar uma organização a longo prazo de medidas apropriadas para garantir a continuidade dos processos de negócios.
B) Correto. O plano de recuperação de desastres abrange a recuperação a curto prazo e é executado imediatamente após o incidente ser rotulado como desastre. (Literatura: A, Slide 081)
C) Incorreto. O prazo para o plano de resposta a incidentes é imediato/em tempo real. Ele é executado quando o incidente de segurança acontece.
D) Incorreto. O plano de tratamento de riscos é um tipo de plano de melhoria da segurança da informação. Planos de melhoria geralmente são executados anualmente.

17 / 30
Quem é responsável por coordenar o programa de conscientização sobre segurança de uma organização?

A) Todos na organização
B) A gestão de segurança da informação
C) O departamento de TI
D) O assessor do CIO

A) Incorreto. Todos na organização são responsáveis pela segurança organizacional, porém não são responsáveis por coordenar o programa de conscientização sobre segurança da organização.
B) Correto. A gestão de segurança da informação é responsável por coordenar a campanha de conscientização sobre segurança. (Literatura: A, Slide 095)
C) Incorreto. O departamento de TI deve promover questões e preocupações de segurança e estar ciente das mesmas, porém ele não é responsável por coordenar a campanha de conscientização sobre segurança da organização.
D) Incorreto. O assessor do CIO pode ser responsável por promover e defender a conscientização, mas não é diretamente responsável por coordenar a campanha de conscientização sobre segurança da organização.

18 / 30
No ano passado, uma organização se tornou mais rigorosa com relação aos controles de segurança de seus funcionários. Antes de implementar controles adicionais, o information security officer (ISO) deseja conhecer a mentalidade dos funcionários quanto aos controles de segurança da informação.

Como o ISO obtém rapidamente uma ideia sobre isso?

A) Ao checar o fluxo de dados da Internet
B) Ao determinar se há vírus na rede
C) Ao percorrer o escritório após o horário normal de trabalho

A) Incorreto. Isso apenas fornece informações sobre como a Internet é usada, não sobre a mentalidade geral dos funcionários.
B) Incorreto. Essa é uma medida técnica e não fornece nenhuma informação sobre a mentalidade dos funcionários.
C) Correto. Quando o ISO percorre o escritório após o horário normal de trabalho, é possível ver como os funcionários lidam com informação sensível. (Literatura: A, Slide 095)

19 / 30
O gerente de continuidade de negócios pede contribuições para um plano de contingência.

Qual deve ser a **primeira** atividade do gerente de continuidade de negócios?

A) Definir o escopo
B) Identificar funções de negócios críticas
C) Testar o plano

A) Incorreto. O escopo é um pilar do gerenciamento de projeto e não um alicerce para o planejamento de contingência, pois o escopo é orientado pelos resultados da análise de impacto no negócio (BIA).
B) Correto. O principal aspecto que deve ser concluído para que se tenha um plano de contingência é a empresa definir suas funções de negócios e sistemas críticos e documentá-los. (Literatura: A, Slide 080)
C) Incorreto. O teste do plano de contingência é extremamente importante e deve ocorrer pelo menos anualmente, porém não é a primeira atividade.

20 / 30
Um arquiteto de segurança discute com o time interno de prevenção de incêndios sobre a afirmação na política de segurança da informação de que as portas das áreas confidenciais devem estar sempre trancadas. O time de resposta a emergências quer ter acesso a essas áreas em caso de incêndio.

Qual é a **melhor** solução para esse dilema?

A) As portas devem permanecer fechadas em caso de incêndio para evitar acesso às áreas confidenciais.
B) As portas devem abrir automaticamente em caso de incêndio.
C) O arquiteto de segurança deve ser informado quando houver incêndio.

A) Incorreto. A segurança vem antes da proteção.
B) Correto. A segurança vem antes da proteção. (Literatura: A, Slide 091)
C) Incorreto. Embora estar informado seja bom, o time de resposta a emergências não pode esperar até que o arquiteto de segurança chegue ao local.

21 / 30
Qual é a **maior** vantagem de usar designs abertos de arquitetura de segurança?

A) Designs abertos são fáceis de configurar.
B) Designs abertos são muito testados.
C) Designs abertos têm muitas funcionalidades adicionais.

A) Incorreto. Designs abertos não são mais fáceis de configurar do que designs secretos.
B) Correto. Designs abertos são testados exaustivamente. Além disso, designs secretos nunca permanecem secretos. (Literatura: A, Slide 114)
C) Incorreto. Designs abertos não têm necessariamente mais funcionalidades do que designs secretos.

22 / 30
Que afirmação sobre arquitetura de segurança é a **mais** correta?

A) A arquitetura de segurança define completamente as regras de implementação.
B) A arquitetura de segurança segue a estratégia.
C) A arquitetura de segurança é secundária.

A) Incorreto. A arquitetura de segurança é um design de mais alto nível do que isso e não define completamente as regras de implementação.
B) Correto. A arquitetura de segurança segue a estratégia de segurança da informação. (Literatura: A, Slide 112)
C) Incorreto. A arquitetura de segurança é estratégica e, portanto, não é secundária.

23 / 30
Por que é importante definir quais serviços de segurança serão prestados?

A) Para melhor alinhar os requisitos de segurança da informação e o serviço ao cliente
B) Para determinar a estratégia de segurança da informação de uma organização
C) Para garantir que uma organização esteja em conformidade com os requisitos da ISO/IEC 27001
D) Para compreender o escopo do sistema de gestão de segurança da informação (SGSI)

A) Correto. A definição de quais serviços de segurança serão prestados, e em qual arquitetura, deve ser realizada para melhor alinhar os requisitos de segurança da informação e o serviço aos clientes. (Literatura: A, Slide 113)
B) Incorreto. A estratégia de segurança da informação é determinada antes que seja definida a arquitetura de segurança da informação, que inclui serviços de segurança.
C) Incorreto. Isso não é um requisito da ISO/IEC 27001.
D) Incorreto. O escopo do SGSI deve ser compreendido antes que os serviços de segurança sejam definidos.

24 / 30
Que item de segurança é concebido para receber um grande volume de tráfego relacionado à rede que pode indicar um ataque de negação de serviço?

A) Firewall
B) Sistema de detecção e prevenção de intrusão baseado no host (IDPS de host)
C) Sistema de detecção e prevenção de intrusão baseado na rede (IDPS de rede)
D) Rede privada virtual (VPN)

A) Incorreto. Essa é uma ferramenta de segurança, mas não recebe grande volume de tráfego de rede.
B) Incorreto. Essa ferramenta tem como foco o volume de tráfego de dados baseado no host, e não o volume de tráfego de dados baseado na rede.
C) Correto. O IDPS de rede é utilizado para recolher e coletar fluxos de dados em toda a rede de uma organização a fim de verificar se eventos anormais são um indicativo de um ataque ativo, como seria um de negação de serviço. (Literatura: A, Slide 108)
D) Incorreto. Esse é um dispositivo de acesso à infraestrutura de rede.

25 / 30
A CEO de uma empresa começou a usar seu tablet PC e deseja que o gerente de segurança possibilite que ela use e-mail profissional e agenda no tablet. O gerente de segurança entende essa vontade de permitir a possibilidade de uso de dispositivos pessoais (Bring Your Own Device, BYOD) e organiza um treinamento de conscientização sobre BYOD.

Que outro controle o gerente de segurança deve propor para evitar perda de dados em caso de furto ou perda do dispositivo pessoal?

A) Não atender ao desejo até que seja possível uma integração estável das funções de negócios em dispositivos pessoais
B) Criptografar o armazenamento local e as conexões de rede
C) Implementar autentificação forte usando tokens com senhas de uso único
D) Instalar um antimalware e um firewall para evitar infecção

A) Incorreto. Isso pode ser sensato, mas a CEO não pode ser ignorada.
B) Correto. Em caso de furto ou perda, pelo menos os dados corporativos estarão seguros. (Literatura: A, Slide 061)
C) Incorreto. Isso apenas possibilita um login seguro à rede corporativa.
D) Incorreto. Em caso de furto ou perda, os dados ainda estarão acessíveis a terceiros.

26 / 30
Por que os elementos de segurança na infraestrutura de TI são importantes?

A) Para possibilitar a continuidade de negócios da infraestrutura de TI
B) Para gerenciar incidentes de segurança da informação que impactam a infraestrutura de TI
C) Para evitar acesso físico não autorizado à infraestrutura de TI
D) Para proteger os ativos de informação que estão na infraestrutura de TI

A) Incorreto. Possibilitar a continuidade de negócios da infraestrutura de TI é importante, mas o propósito desse elemento de segurança é proteger os ativos de informação.
B) Incorreto. Gerenciar incidentes de segurança da informação que impactam a infraestrutura de TI é importante, mas o propósito desse elemento de segurança é proteger os ativos de informação.
C) Incorreto. Evitar acesso físico não autorizado à infraestrutura de TI é importante, mas o propósito desse elemento de segurança é proteger os ativos de informação.
D) Correto. Todos os elementos de segurança da informação existem para proteger a informação. A maior parte da informação está localizada na infraestrutura de TI, que precisa ser protegida. (Literatura: A, Slide 018)

27 / 30
Zoneamento é um controle de segurança para separar áreas físicas com diferentes níveis de segurança. Zonas com maiores níveis de segurança podem ser protegidas com mais controles. O gerente de segurança de um hotel, responsável pela segurança, está considerando diferentes zonas para o hotel.

Que funções de negócios devem ser combinadas em uma zona de segurança?

A) Sala de reunião do conselho e espaço geral do escritório
B) Academia e depósito
C) Quartos do hotel e bar aberto ao público
D) Restaurante aberto ao público e lobby

A) Incorreto. A sala de reunião do conselho pode conter informação estratégica valiosa e, portanto, confidencial, que não deve estar acessível aos funcionários comuns.
B) Incorreto. O depósito deve estar disponível apenas para (alguns) funcionários, enquanto a academia deve ser acessível a todos os hóspedes e funcionários.
C) Incorreto. Os quartos do hotel e o bar devem ser separados. O bar aberto ao público pode ser usado por todos e os quartos do hotel se destinam apenas aos hóspedes pagantes.
D) Correto. Ambos os locais podem ser usados por qualquer pessoa. (Literatura: A, Slide 091)

28 / 30
Um gerente de segurança de uma grande empresa tem a tarefa de obter proteção física para o armazenamento de dados corporativos.

A proteção física pode ser obtida através de qual controle?

A) Fazer com que os visitantes façam login e logoff ao acessar o centro de dados corporativos
B) Instalar um firewall para evitar acesso à infraestrutura de rede
C) Usar controles de cartão-chave de acesso para os funcionários que necessitam de acesso
D) Elaborar uma política que defina quem pode ter acesso à empresa

A) Incorreto. Isso não fornece diretamente uma barreira física ou proteção física. Isso é um bom controle passivo/detectivo e ponto de auditoria.
B) Incorreto. Isso não é um controle de proteção física. Isso é um controle de proteção lógica.
C) Correto. Cartões-chave são uma boa forma de controle de acesso físico, especialmente quando combinados com algum tipo de câmera / procedimento de reconhecimento facial para verificar a identidade de alguém entrando no centro de dados. (Literatura: A, Slide 090)
D) Incorreto. Isso é um controle organizacional.

29 / 30
Sabendo que controles de segurança físicos são uma parte importante de um programa de segurança da informação, solicitou-se ao time de segurança da informação que projetasse e implementasse um perímetro de segurança para um departamento que está configurando alguns novos sistemas de dados.

Segundo a ISO/IEC 27001, qual é a recomendação **mais** importante que deve ser considerada ao se estabelecer esse perímetro?

A) Um modelo de suporte de duas pessoas
B) Instalação de câmeras e alarmes
C) Registro de sistemas e monitoração
D) A extensão do perímetro deve ser alinhada com o valor dos dados

A) Incorreto. Esse é um bom controle físico, mas não é o controle mais importante e nem uma recomendação.
B) Incorreto. Esse é um bom controle físico, mas não é o controle mais importante e nem uma recomendação.
C) Incorreto. Esse é um bom controle, mas não é o controle mais importante e nem um controle de perímetro.
D) Correto. Todas as decisões que um time de segurança da informação toma devem ser centradas em dados e baseadas na classificação dos dados envolvidos. (Literatura: A, Slide 087)

30 / 30
A gerente de recursos humanos de uma organização perguntou o que poderia fazer para obter resultados rápidos na área de emprego e contratação para ajudar a fortalecer o programa de segurança de dados da organização conforme a ISO/IEC 27001.

Qual deve ser o conselho?

A) Verificar antecedentes
B) Implementar uma política de segurança
C) Instalar portões giratórios na entrada

A) Correto. Uma melhor prática é realizar verificação de antecedentes de potenciais funcionários. Essa simples etapa aumenta consideravelmente a segurança global dos dados organizacionais. (Literatura: A, Slides 094 e 097)
B) Incorreto. Essa é uma boa ideia, mas não produz resultados rápidos. Essa seria uma estratégia de longo prazo.
C) Incorreto. Esse é um controle físico e não ajuda na área de emprego e contratação.

Avaliação

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

Questão	Resposta	Questão	Resposta
1	C	16	B
2	B	17	B
3	D	18	C
4	C	19	B
5	A	20	B
6	B	21	B
7	D	22	B
8	C	23	A
9	B	24	C
10	B	25	B
11	A	26	D
12	C	27	D
13	B	28	C
14	B	29	D
15	E	30	A

Contato EXIN

www.exin.com