Exame simulado

Edição 202001

Conteúdo

Introdução

Este é o exame simulado EXIN Privacy & Data Protection Practitioner (PDPP.PR). As regras e regulamentos do exame do EXIN se aplicam a este exame.

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

O número máximo de pontos que pode ser obtido neste exame é 40. Cada resposta correta vale 1 ponto. Você precisa de 26 pontos ou mais para passar no exame.

O tempo permitido para este exame é de 120 minutos.

Você é autorizado a utilizar o GDPR do exame durante todo este exame.

Boa Sorte!

Exame simulado

1 / 40
Uma empresa implementa uma política de privacidade, que ajuda a demonstrar a conformidade com o GDPR. É recomendável que essa política seja publicamente acessível por várias razões.

Qual é a **principal** razão para disponibilizar publicamente a política de privacidade?

A) Permitir que clientes e parceiros verifiquem quais dados pessoais a organização deve processar
B) Permitir que clientes, parceiros e a autoridade supervisora avaliem como os dados pessoais são tratados
C) Comunicar o resultado das Avaliações de Impacto sobre a Proteção de Dados (DPIAs) realizadas na organização
D) Informar a autoridade supervisora sobre o modo como a organização responderá após uma violação de dados pessoais

2 / 40
De acordo com o GDPR, qual informação **não** constitui uma parte obrigatória de uma política de privacidade?

A) Informações sobre transferências internacionais de dados pessoais a um país terceiro
B) Informações sobre a identidade e detalhes de contato do controlador
C) Informações relativas às medidas para segurança dos dados na organização
D) Informações relativas aos períodos de retenção e direitos do titular dos dados

3 / 40
O GDPR adota os princípios de privacidade desde a concepção (by design) e por padrão (by default). A aplicação desses princípios inclui a implementação de medidas técnicas e organizacionais.

Por que as medidas organizacionais são necessárias?

A) Porque a privacidade desde a concepção e por padrão requer que a organização limite o acesso a dados pessoais apenas aos controladores
B) Porque a proteção dos direitos dos titulares dos dados requer processos organizacionais que as medidas técnicas não conseguem cobrir
C) Porque a designação de um Data Protection Officer (DPO), quando obrigatória, é considerada uma medida organizacional

4 / 40
Uma empresa está elaborando um projeto para criar um novo serviço gratuito para os consumidores.

De acordo com a privacidade desde a concepção (by design), qual é o momento **mais** desejável para a discussão da proteção de dados?

A) No início do projeto
B) Durante a fase de implementação
C) Quando o projeto está quase completo

5 / 40
A montagem de um Sistema de Gestão de Proteção de Dados (SGPD) é realizada em fases. A primeira fase do desenvolvimento de um SGPD é chamada de Preparação para Proteção de Dados e Privacidade. Uma etapa desta fase consiste em realizar auditorias e avaliações de dados iniciais.

Por que essas auditorias e avaliações de dados devem ser realizadas na fase de Preparação para Proteção de Dados e Privacidade da montagem de um SGPD?

A) As auditorias e avaliações de dados analisam a conscientização e a prontidão do pessoal em relação à proteção de dados e privacidade.
B) As auditorias e avaliações de dados identificam riscos relativos à conformidade, aos indivíduos e outros riscos relacionados para a organização.
C) As auditorias e avaliações de dados fornecem uma visão geral clara dos fluxos de dados pessoais atuais, dentro e fora da organização.
D) As auditorias e avaliações de dados fornecem um inventário indicando onde os diferentes tipos de dados pessoais ficam localizados na organização.

6 / 40
Uma organização deseja se adequar ao GDPR. Ela está desenvolvendo um Sistema de Gestão de Proteção de Dados (SGPD). A construção do SGPD está na primeira fase: Preparação para Proteção de Dados e Privacidade.

O Data Protection Officer (DPO) esboçou uma estrutura de governança, estabeleceu fluxos de dados, criou um inventário de dados pessoais e estabeleceu todos os três elementos do programa de proteção de dados e privacidade (etapa 7).

Qual é a **última** etapa da primeira fase da montagem de um SGPD?

A) Realizar uma análise dos aspectos de comunicação e treinamento em relação à proteção de dados e privacidade necessários para o quadro de funcionários de sua empresa
B) Definir funções e responsabilidades claras nas descrições dos cargos e documentos relacionados, como os contratos de trabalho, dos gerentes de privacidade e de um Data Protection Officer
C) Esboçar uma orientação abrangente para todos os membros responsáveis pela proteção de dados e privacidade para obter a conformidade com a legislação relevante
D) Esboçar e enviar à diretoria da organização um relatório sobre as etapas realizadas até o momento, recomendando planos de ação e um orçamento.

7 / 40
Uma empresa deseja desenvolver um Sistema de Gestão de Proteção de Dados (SGPD). A primeira fase do desenvolvimento de um SGPD consiste na Preparação para Proteção de Dados e Privacidade.

Que etapa **não** pertence a essa primeira fase?

A) Desenvolver minutas de planos de ação para implementação
B) Estabelecer uma organização de governança dos dados
C) Manter a documentação da privacidade dos dados
D) Realizar auditorias e avaliações de dados iniciais

8 / 40
Uma empresa deseja montar um Sistema de Gestão de Proteção de Dados (SGPD). A segunda fase do desenvolvimento de um SGPD é chamada Organização da Proteção de Dados e Privacidade. Uma das etapas da fase 2 tem o seguinte objetivo:

integrar o pensamento sobre a proteção de dados e privacidade a toda a empresa e a todas as suas funções.

Qual etapa da fase 2 tem este objetivo?

A) Conduzir uma auditoria das medidas e controles para privacidade e proteção de dados com o objetivo de identificar lacunas e erros
B) Implementar e operar sistemas computadorizados de proteção de dados e privacidade
C) Informar os funcionários sobre o estado do programa de privacidade e proteção de dados
D) Manter uma comunicação mútua regular para questões de proteção de dados e privacidade

9 / 40
Um Data Protection Officer (DPO) percebe a importância de manter uma comunicação regular com todos os outros indivíduos indicados que sejam responsáveis pela proteção de dados e privacidade. Esse grupo de indivíduos deve trabalhar no sentido de um resultado para toda a organização, em relação à proteção de dados e privacidade.

Que resultado beneficia **mais** a organização?

A) A criação de um sistema no qual todas as questões de proteção de dados e privacidade devem ser encaminhadas para o DPO e subsequentemente resolvidas por ele
B) O desenvolvimento de perspectivas divergentes sobre a proteção de dados e a privacidade durante a terceirização ou transferência de dados na organização
C) A introdução de uma abordagem colaborativa e proativa para incluir a proteção de dados e a privacidade em todas as partes da organização
D) A conscientização de que a terceirização da proteção de dados e privacidade cria uma responsabilidade solidária pela conformidade

10 / 40
Se uma organização quiser desenvolver, implementar e gerenciar um Sistema de Gestão de Proteção de Dados (SGPD), isso é feito em várias fases. A implementação do SGPD tem cinco fases, a saber: preparação, organização, implementação do desenvolvimento, governança e avaliação e melhoria.

As fases de implementação de um SGPD podem ser comparadas a quê?

A) Um processo de melhorias contínuas comparável ao ciclo PDCA (PEVA)
B) Um guia para a implementação da governança de privacidade
C) Um inventário das regulamentações de dados como preparação para o SGPD
D) O impacto das regulamentações, regras e normas de privacidade

11 / 40
Um elemento central do GDPR é o fato de que uma organização deve demonstrar a conformidade. A implementação de um Sistema de Gestão de Proteção de Dados (SGPD) pode ajudar a demonstrar a conformidade.

Qual fase da implementação de um SGPD demonstra **melhor** a conformidade com o GDPR?

A) Fase 1: a organização se prepara para a implementação da privacidade e proteção de dados.
B) Fase 2: as estruturas e os mecanismos organizacionais para a privacidade são estabelecidos.
C) Fase 3: as medidas de proteção de dados e privacidade são desenvolvidas e implementadas.
D) Fase 4: os mecanismos de governança de privacidade para a organização são estabelecidos.

12 / 40
Um Data Protection Officer (DPO) desenvolve e implementa um Sistema de Gestão de Proteção de Dados e Privacidade (SGPD). A implementação está na fase 3: Desenvolvimento e Implementação da Proteção de Dados e Privacidade.

O que deve ser realizado **primeiro** na fase 3?

A) Analisar e definir as necessidades e os requisitos da empresa em relação à proteção de dados e privacidade
B) Investigar o conhecimento e a compreensão dos funcionários sobre os conceitos de proteção de dados e privacidade
C) Pesquisar as melhores práticas do setor e adaptá-las às necessidades e requisitos da empresa
D) Compreender a legislação de proteção de dados e privacidade global e determinar a relevância dessa informação

13 / 40
Um plano de resposta à violação de dados pessoais descreve as seguintes ações:

- Um **provedor externo** responde à violação, fornece serviços de relações públicas e auxilia na minimização do dano.
- O **Data Protection Officer (DPO)** solicita suporte da autoridade supervisora.
- O **processador** notifica os parceiros de negócios e os titulares dos dados sobre a violação de dados e solicita seu suporte.

Quem tem a **maior** probabilidade de minimizar o impacto para terceiros e os titulares dos dados?

A) O provedor externo
B) O DPO
C) O processador

14 / 40
Três instituições de saúde estão trabalhando em conjunto no desenvolvimento de um aplicativo de celular para monitoramento de pacientes. O time médico insere seus dados pessoais e qualificações no aplicativo e os pacientes adicionam seus dados pessoais, incluindo dados médicos.

As instituições de saúde indicam um único Data Protection Officer (DPO). Para executar uma versão piloto, eles precisam colocar o aplicativo nas lojas de aplicativos. Após sua introdução nas lojas de aplicativos, a segurança do novo aplicativo é testada. Como precaução de segurança, a descrição declara que o aplicativo está na fase piloto. Apenas alguns poucos titulares dos dados baixam o aplicativo para testar, mas eles o utilizam de verdade e inserem dados reais.

O teste mostra que o aplicativo não é nem um pouco seguro. Ele pode ser facilmente atacado por hackers. Um hacker poderia alterar os dados de saúde dos pacientes, além de coletar e usar os dados de modos não autorizados.

De acordo com o GDPR, o que o DPO deve fazer?

A) O DPO não precisa tomar nenhuma medida, porque o aplicativo está na fase piloto e apenas um pequeno número de pacientes está participando.
B) O DPO não precisa tomar nenhuma medida porque o impacto das vulnerabilidades não pode ser qualificado como alto durante uma fase piloto.
C) O DPO deve informar os pacientes e a autoridade supervisora porque o aplicativo acarreta um alto risco aos direitos e liberdades dos pacientes.
D) O DPO deve notificar a autoridade supervisora e garantir que as medidas de segurança do aplicativo sejam ajustadas às normas de segurança exigidas.

15 / 40
A conformidade com o GDPR pode ser auxiliada pela implementação de um regime de gerenciamento de incidentes sistemático.

Qual seria uma descrição de um processo de gerenciamento de incidentes eficaz?

A) Reconhecer a ocorrência de um incidente, responder às preocupações imediatas e de longo prazo, e acompanhar o incidente para garantir que as medidas adotadas foram eficazes
B) Reconhecer a ocorrência de um incidente e relatar o incidente ao Data Protection Officer (DPO) para análise dos fluxos de dados e melhoria das políticas de segurança
C) Acompanhar todos os incidentes que envolverem dados pessoais, realizar uma Avaliação de Impacto sobre a Proteção de Dados (DPIA) para analisar os riscos e estabelecer um plano de melhoria
D) Acompanhar todos os casos de processamento de dados pessoais para recuperar os dados após um incidente com mais facilidade e garantir que as atividades de resposta possam ser reduzidas para minimizar os custos

16 / 40
O CEO pediu que o time de privacidade avalie a organização em termos de desempenho de proteção de dados e privacidade. Um benchmark (referência comparativa) seria um modo adequado de determinar objetivamente como está o desempenho da organização.

O que o benchmark de privacidade **não** cobre?

A) Uma pesquisa que enfoca a satisfação dos clientes da organização em relação à privacidade
B) Comparações entre unidades de negócios ou departamentos em relação à conformidade com a privacidade
C) O desempenho atual da organização em relação à privacidade, em comparação a um ano atrás
D) O desempenho da organização em relação à privacidade comparado com o de entidades semelhantes na indústria

17 / 40
Uma organização deseja usar inteligência artificial (IA) e algoritmos de aprendizagem profunda no departamento de recursos humanos (RH) para examinar as relações de emprego, criar perfis de qualificações de funcionários e definir bônus para objetivos individuais.

O que deve ser feito **inicialmente** e antes da implementação deste novo tipo de processamento de dados pessoais?

A) Conduzir uma Avaliação de Impacto sobre a Proteção de Dados (DPIA)
B) Conduzir uma avaliação de privacidade do departamento de RH
C) Relatar o processamento à autoridade supervisora

18 / 40
De acordo com o GDPR, qual atividade é sempre uma responsabilidade do controlador?

A) Ser responsável pela realização de uma Avaliação de Impacto sobre a Proteção de Dados (DPIA)
B) Contratar uma empresa de segurança para a proteção de dados pessoais em trânsito
C) Implementar um novo método para coleta de dados pessoais dos clientes
D) Manter registros das atividades de processamento realizadas pelo processador

19 / 40
Um hospital terceiriza a impressão das faturas dos pacientes a uma gráfica. A gráfica também imprime faturas para outras organizações.

Devido a um erro, os nomes e endereços foram misturados durante a separação na gráfica e algumas faturas foram enviadas aos pacientes errados.

O hospital tinha analisado cuidadosamente seus próprios processos. O hospital tinha um processo de verificação robusto em vigor e acordos contratuais com a gráfica.

Por que o hospital será **responsabilizado** pela autoridade supervisora?

A) Porque o contrato determina assim
B) Porque o hospital é o controlador
C) Porque a mistura ocorreu entre pacientes
D) Porque a verificação não funcionou

20 / 40
Quando um controlador e um processador assinam um contrato para o processamento de dados pessoais, ambos têm responsabilidades específicas. Algumas dessas responsabilidades são estipuladas pelo GDPR e outras podem ser dispostas no contrato.

De acordo com o GDPR, quando o processador sempre precisa de uma autorização por escrito do controlador?

A) Quando o processador contrata uma empresa para proteger os dados durante transferências
B) Quando o processador contrata um terceiro para processar dados pessoais
C) Quando o processador implementa um novo método para coleta de dados pessoais
D) Quando o processador implementa um novo método para exclusão de dados pessoais

21 / 40
Quem tem a obrigação legal de manter os registros das atividades de processamento?

A) O Diretor de Informações (CIO)
B) O Chief Privacy Officer
C) O controlador e o processador
D) O Data Protection Officer (DPO)

22 / 40
Uma organização norte-americana situada na Área Econômica Europeia (AEE) processa dados pessoais de pessoas físicas. Ela processa dados étnicos em larga escala.

De acordo com o GDPR, uma organização deve indicar um Data Protection Officer (DPO) em três casos específicos.

Neste caso, por qual motivo é obrigatório que a organização indique um DPO?

A) Os dados pessoais de estrangeiros são processados.
B) Os dados pessoais são processados por um país terceiro.
C) Os dados pessoais de minorias são processados.
D) As categorias especiais de dados pessoais são processadas.

23 / 40
Um Data Protection Officer (DPO) trabalha para o Ministério dos Transportes, que é um departamento nacional.

Um novo projeto é anunciado para monitorar o comportamento das pessoas ao dirigir nas rodovias nacionais. O Ministério deseja usar um sistema inteligente de análise de vídeo para discriminar os carros e automaticamente reconhecer os números das placas.

O secretário de Estado tem pressa para iniciar o projeto e expressa a preocupação de que as questões de privacidade possam provocar atrasos indesejáveis.

O que o DPO deve fazer?

A) Pedir que o secretário de Estado entre em contato com a autoridade supervisora porque claramente isso está fora do escopo do DPO
B) Garantir ao secretário de Estado que uma DPIA é desnecessária se os titulares dos dados forem informados sobre o processamento dos dados
C) Informar o secretário de Estado que uma DPIA é obrigatória para o monitoramento em larga escala de um espaço público
D) Solicitar que o secretário de Estado reconsidere o projeto porque o processamento de dados de vigilância em massa é proibido

24 / 40
Os Data Protection Officers (DPOs) são limitados por sigilo ou confidencialidade em relação ao desempenho de suas tarefas.

Em relação a qual parte o DPO está **isento** desse sigilo ou confidencialidade para buscar orientação?

A) A diretoria da empresa
B) Os membros de uma rede de proteção de dados e privacidade
C) O Diretor de Segurança de Informações (ISO)
D) A autoridade supervisora

25 / 40
Uma Avaliação de Impacto sobre a Proteção de Dados (DPIA) é uma ferramenta para identificar riscos à proteção de dados, em especial aqueles que provavelmente terão um grande efeito sobre os direitos e as liberdades de pessoas físicas.

Por que a DPIA pode ser vista como parte do gerenciamento de riscos mais amplo de uma organização?

A) Porque a DPIA avalia todos os riscos de segurança da organização examinada e substitui outras avaliações de risco ou gerenciamento de riscos
B) Porque a DPIA avalia os riscos pela probabilidade e gravidade do risco, de um modo semelhante a outros componentes bem definidos do gerenciamento de riscos
C) Porque a DPIA é obrigatória para cada projeto, de acordo com o GDPR, o que reduz todos os outros requisitos legais para gerenciamento de riscos

26 / 40
De acordo com o GDPR, o que deve sempre fazer parte de uma DPIA?

A) Desenvolver um procedimento de solicitação de acesso pelos indivíduos para garantir a conformidade com os direitos dos titulares dos dados
B) Identificar os dados pessoais que são processados e os objetivos buscados com o processamento
C) Notificar os titulares dos dados sobre a ocorrência de uma avaliação e solicitar seu consentimento explícito
D) Estabelecer um plano de resposta a incidentes e definir salvaguardas apropriadas para evitar violações de dados

27 / 40
Uma organização desenvolve um novo produto para detectar funcionários com desempenho inferior. Ela pesquisa seu histórico na internet e analisa seu comportamento no trabalho usando inteligência artificial (IA).

Embora os engenheiros de software não compreendam totalmente o algoritmo, a gerência decide demitir os funcionários incluídos na faixa de 10% mais inferior.

O Data Protection Officer (DPO) está preocupado com o impacto desse produto e informa a diretoria que é necessária uma Avaliação de Impacto sobre a Proteção de Dados (DPIA).

Qual opção **não** faz parte do motivo pelo qual uma DPIA é obrigatória?

A) A automatização do processamento de dados pessoais
B) A avaliação que pode afetar os titulares dos dados de modo considerável
C) O processamento de categorias especiais de dados pessoais
D) A avaliação sistemática de aspectos pessoais de pessoas físicas

28 / 40
O que **não** é considerado um resultado de uma Avaliação de Impacto sobre a Proteção de Dados (DPIA)?

A) Um registro de acesso a dados confidenciais, com uma verificação de autorização automatizada
B) Um registro das opiniões dos titulares dos dados sobre as operações de processamento pretendidas
C) Uma descrição sistemática das operações de processamento pretendidas
D) Uma avaliação dos riscos aos direitos e liberdades dos titulares dos dados

29 / 40
O GDPR detalha o que deve estar contido no resultado de uma Avaliação de Impacto sobre a Proteção de Dados (DPIA), no mínimo.

O que **não** é obrigatório em uma DPIA?

A) Uma descrição do processamento e seus objetivos
B) Uma avaliação da necessidade e da proporcionalidade das operações de processamento em relação às finalidades
C) Uma avaliação dos riscos aos direitos e liberdades dos titulares dos dados
D) A orientação da autoridade supervisora

30 / 40
Uma Avaliação de Impacto sobre a Proteção de Dados (DPIA) mostra que o processamento pretendido envolve a coleta de mais dados sobre clientes individuais que o necessário para obter o objetivo desejado.

De acordo com o GDPR, qual é a resposta **mais** apropriada?

A) Anonimizar os dados o mais rápido possível
B) Introduzir um programa de treinamento e conscientização
C) Limitar o período de tempo no qual os dados serão armazenados
D) Reduzir a quantidade de dados coletados

31 / 40
O que é melhor fazer **primeiro**, antes de iniciar uma Avaliação de Impacto sobre a Proteção de Dados (DPIA)?

A) Determinar medidas para abordar os riscos identificados
B) Determinar se há necessidade de uma DPIA
C) Identificar os riscos aos direitos e liberdades dos titulares dos dados

32 / 40
Uma empresa realiza uma Avaliação de Impacto sobre a Proteção de Dados (DPIA).

Por que o mapeamento dos dados é útil em uma DPIA?

A) Ele avalia todos os riscos organizacionais à privacidade.
B) Ele ajuda a ter uma visão geral dos dados pessoais em uso.
C) Ele ajuda a informar todas as partes relevantes.

33 / 40
Um especialista em privacidade é contratado por uma organização. Ela deseja terceirizar parte de suas atividades de processamento dos dados. O especialista realiza uma Avaliação de Impacto sobre a Proteção de Dados (DPIA) do processamento que envolve um processador de dados.

Uma das principais etapas de uma DPIA requer que o controlador forneça todas as informações e não requer o envolvimento do processador.

Que etapa é essa?

A) Avaliação da necessidade e da proporcionalidade do processamento
B) Avaliação dos riscos aos direitos e liberdades dos titulares dos dados
C) Medidas de mitigação para abordar os riscos, incluindo salvaguardas
D) Descrições sistemáticas das operações de processamento pretendidas

34 / 40
Uma grande empresa está tendo dificuldades financeiras. A diretoria quer que os funcionários trabalhem com mais eficiência.

A diretoria inicia uma experiência, na qual as atividades dos funcionários na internet são monitoradas. Os dados são analisados para verificar onde é possível obter maior eficiência. As pessoas classificadas como *ineficientes* poderão ser demitidas.

Por que uma Avaliação de Impacto sobre a Proteção de Dados (DPIA) deve ser realizada antes de utilizar o novo procedimento?

A) Porque uma grande empresa tem muitos funcionários. Portanto, o processamento será realizado em larga escala.
B) Porque isso constitui um experimento. Uma DPIA é exigida para atividades de processamento novas e experimentais.
C) Porque isso constitui um processamento sistemático. As decisões podem afetar os funcionários de modo considerável.

35 / 40
Uma organização pretende tomar decisões automatizadas sobre seus clientes, com base na definição de perfis.

Que parte da Avaliação de Impacto sobre a Proteção de Dados (DPIA) requer uma atenção extra?

A) A avaliação da necessidade de realizar uma DPIA em relação a essa atividade de processamento
B) As medidas que serão implementadas para proteger os direitos do titular dos dados
C) As medidas para proteger os dados pessoais, evitando que sejam solicitados pelos titulares dos dados
D) Os procedimentos para apagamento dos dados após um titular dos dados solicitar que seus dados sejam removidos

36 / 40
O GDPR declara que as organizações devem buscar modos de prevenir violações de dados pessoais. Portanto, é importante reconhecer rapidamente incidentes que possam ser classificados como violações de dados pessoais.

De acordo com o GDPR, que incidente **não** constitui uma violação de dados pessoais?

A) Um paciente está esperando um pacote contendo equipamento médico, mas ele é entregue no endereço errado.
B) Um funcionário de uma clínica de saúde mental não lembra onde colocou algumas pastas de pacientes que não podem ser rastreadas.
C) A destruição acidental de dados pessoais por um incêndio ou terremoto em um depósito de dados.
D) A divulgação não autorizada de dados financeiros confidenciais de uma empresa relativos a uma aquisição planejada.

37 / 40
Em que situação o relato de uma violação de dados pessoais à autoridade supervisora é necessário?

A) Se a organização não conseguir resolver o incidente dentro de um prazo de 72 horas após sua ocorrência
B) Em qualquer situação na qual exista uma ameaça de segurança aos direitos e liberdades de pessoas físicas
C) Apenas se o incidente for reconhecido como uma violação de dados pessoais dentro de um prazo de 72 horas
D) Quando uma violação de dados pessoais acarretar um risco aos direitos e liberdades de pessoas físicas

38 / 40
O chefe do departamento de Recursos Humanos (RH) perdeu um pendrive contendo as informações pessoais de 35 funcionários. O pendrive é protegido por criptografia robusta. O departamento de RH também tem essas informações pessoais armazenadas em um dispositivo de cópia de segurança.

De acordo com o GDPR, é obrigatório relatar essa violação de dados pessoais à autoridade supervisora?

A) Sim, porque todos os incidentes de segurança devem ser relatados à autoridade supervisora.
B) Sim, porque o relato permite que a autoridade supervisora informe os funcionários.
C) Não, porque o relato de violações de dados não constitui um interesse legítimo da empresa.
D) Não, porque esta violação de dados pessoais não produz riscos aos direitos dos titulares dos dados.

39 / 40
De acordo com o GDPR, em que situação uma violação de dados pessoais deve ser relatada aos titulares dos dados afetados?

A) Quando for provável que a violação de dados pessoais provoque um alto risco aos direitos e liberdades do titular dos dados
B) Quando a autoridade supervisora determinar que o consentimento constituiu a única base legal para o processamento
C) Quando houver um incidente de segurança rotulado como violação de dados pessoais dentro de 72 horas
D) Quando os dados pessoais forem comprometidos por fatores externos, como hackers ou outros cibercriminosos

40 / 40
No processo de resposta a incidentes para melhor prática, são definidas as fases de Preparação, Resposta e Acompanhamento. Em cada fase, a documentação é essencial.

Na fase de Resposta, é importante reunir e preservar as evidências para mostrar por que um incidente ocorreu e por que a organização não foi capaz de prevenir o incidente.

O que deve ser reunido e preservado?

A) Planos de controle de auditoria
B) Avaliações de Impacto sobre a Proteção de Dados (DPIAs)
C) Evidências para proporcionar um quadro claro
D) Planos de recuperação do sistema

Gabarito de respostas

1 / 40
Uma empresa implementa uma política de privacidade, que ajuda a demonstrar a conformidade com o GDPR. É recomendável que essa política seja publicamente acessível por várias razões.

Qual é a **principal** razão para disponibilizar publicamente a política de privacidade?

A) Permitir que clientes e parceiros verifiquem quais dados pessoais a organização deve processar
B) Permitir que clientes, parceiros e a autoridade supervisora avaliem como os dados pessoais são tratados
C) Comunicar o resultado das Avaliações de Impacto sobre a Proteção de Dados (DPIAs) realizadas na organização
D) Informar a autoridade supervisora sobre o modo como a organização responderá após uma violação de dados pessoais

A) Incorreto. As políticas de privacidade disponibilizadas publicamente não estabelecem quais dados pessoais devem ser processados pela organização. Elas fornecem transparência ao processamento de dados pessoais.
B) Correto. Uma política de privacidade disponibilizada publicamente favorece a transparência, permite sua avaliação por clientes e parceiros e fornece uma declaração clara a partir da qual as autoridades supervisoras e outros reguladores podem avaliar a organização. (Literatura A, Capítulo 16)
C) Incorreto. O resultado das DPIAs deve ser documentado para consulta interna e não deve ser incluído na política de privacidade.
D) Incorreto. O modo como a organização responde à violação de dados faz parte do plano de resposta a violações de dados, que constitui um documento interno e não precisa estar publicamente disponível.

2 / 40
De acordo com o GDPR, qual informação **não** constitui uma parte obrigatória de uma política de privacidade?

A) Informações sobre transferências internacionais de dados pessoais a um país terceiro
B) Informações sobre a identidade e detalhes de contato do controlador
C) Informações relativas às medidas para segurança dos dados na organização
D) Informações relativas aos períodos de retenção e direitos do titular dos dados

A) Incorreto. Isso é obrigatório.
B) Incorreto. Isso é obrigatório.
C) Correto. Isto faz parte de uma política de segurança da informação. (Literatura A, Capítulo 16; Artigo 13 do GDPR)
D) Incorreto. Isso é obrigatório.

3 / 40
O GDPR adota os princípios de privacidade desde a concepção (by design) e por padrão (by default). A aplicação desses princípios inclui a implementação de medidas técnicas e organizacionais.

Por que as medidas organizacionais são necessárias?

A) Porque a privacidade desde a concepção e por padrão requer que a organização limite o acesso a dados pessoais apenas aos controladores
B) Porque a proteção dos direitos dos titulares dos dados requer processos organizacionais que as medidas técnicas não conseguem cobrir
C) Porque a designação de um Data Protection Officer (DPO), quando obrigatória, é considerada uma medida organizacional

A) Incorreto. As medidas organizacionais têm o objetivo de proteger os direitos dos titulares dos dados e consistem em procedimentos para um processamento honesto e transparente.
B) Correto. Alguns processos e procedimentos internos devem ser abordados por medidas organizacionais para garantir que os direitos dos titulares dos dados possam ser plenamente exercidos em conformidade com o GDPR. Ferramentas técnicas e sistemas complementam as medidas organizacionais, mas não as substituem. (Literatura: A, Capítulo 9)
C) Incorreto. As medidas organizacionais têm o objetivo de proteger os direitos dos titulares dos dados e consistem em procedimentos para um processamento honesto e transparente.

4 / 40
Uma empresa está elaborando um projeto para criar um novo serviço gratuito para os consumidores.

De acordo com a privacidade desde a concepção (by design), qual é o momento **mais** desejável para a discussão da proteção de dados?

A) No início do projeto
B) Durante a fase de implementação
C) Quando o projeto está quase completo

A) Correto. A privacidade e a proteção de dados devem ser promovidas desde o início do projeto, de acordo com o princípio de privacidade desde a concepção. (Literatura: A, Capítulo 5; F)
B) Incorreto. A discussão da proteção de dados na fase de implementação é muito tardia.
C) Incorreto. A discussão da proteção de dados na fase de conclusão do projeto é muito tardia.

5 / 40
A montagem de um Sistema de Gestão de Proteção de Dados (SGPD) é realizada em fases. A primeira fase do desenvolvimento de um SGPD é chamada de Preparação para Proteção de Dados e Privacidade. Uma etapa desta fase consiste em realizar auditorias e avaliações de dados iniciais.

Por que essas auditorias e avaliações de dados devem ser realizadas na fase de Preparação para Proteção de Dados e Privacidade da montagem de um SGPD?

A) As auditorias e avaliações de dados analisam a conscientização e a prontidão do pessoal em relação à proteção de dados e privacidade.
B) As auditorias e avaliações de dados identificam riscos relativos à conformidade, aos indivíduos e outros riscos relacionados para a organização.
C) As auditorias e avaliações de dados fornecem uma visão geral clara dos fluxos de dados pessoais atuais, dentro e fora da organização.
D) As auditorias e avaliações de dados fornecem um inventário indicando onde os diferentes tipos de dados pessoais ficam localizados na organização.

A) Incorreto. As auditorias e avaliações de dados não pretendem fornecer uma análise da conscientização e prontidão do pessoal em relação à proteção de dados e privacidade.
B) Correto. As auditorias e avaliações de dados nessa fase identificam riscos relativos à conformidade, aos indivíduos e outros riscos relacionados. O resultado proporciona uma primeira noção sobre o que deve ser coberto pelo SGPD. (Literatura: B, Capítulo 2.2.1)
C) Incorreto. Auditorias e avaliações de dados não são usadas para fornecer informações sobre os fluxos de dados dentro e fora da organização.
D) Incorreto. Auditorias e avaliações de dados não são usadas para fornecer um inventário que indique onde os tipos de dados ficam localizados na organização, e sim para identificar riscos.

6 / 40
Uma organização deseja se adequar ao GDPR. Ela está desenvolvendo um Sistema de Gestão de Proteção de Dados (SGPD). A construção do SGPD está na primeira fase: Preparação para Proteção de Dados e Privacidade.

O Data Protection Officer (DPO) esboçou uma estrutura de governança, estabeleceu fluxos de dados, criou um inventário de dados pessoais e estabeleceu todos os três elementos do programa de proteção de dados e privacidade (etapa 7).

Qual é a **última** etapa da primeira fase da montagem de um SGPD?

A) Realizar uma análise dos aspectos de comunicação e treinamento em relação à proteção de dados e privacidade necessários para o quadro de funcionários de sua empresa
B) Definir funções e responsabilidades claras nas descrições dos cargos e documentos relacionados, como os contratos de trabalho, dos gerentes de privacidade e de um Data Protection Officer
C) Esboçar uma orientação abrangente para todos os membros responsáveis pela proteção de dados e privacidade para obter a conformidade com a legislação relevante
D) Esboçar e enviar à diretoria da organização um relatório sobre as etapas realizadas até o momento, recomendando planos de ação e um orçamento.

A) Incorreto. Este é um dos três elementos do programa de proteção de dados e privacidade que já foi estabelecido na etapa 7.
B) Incorreto. Esta etapa é realizada muito mais tarde na fase 2, etapa 4.
C) Incorreto. Esta é a primeira etapa que deve ser realizada na fase 2.
D) Correto. Esta é a última etapa que deve ser realizada na primeira fase. (Literatura: B, Capítulo 2.2.1)

7 / 40
Uma empresa deseja desenvolver um Sistema de Gestão de Proteção de Dados (SGPD). A primeira fase do desenvolvimento de um SGPD consiste na Preparação para Proteção de Dados e Privacidade.

Que etapa **não** pertence a essa primeira fase?

A) Desenvolver minutas de planos de ação para implementação
B) Estabelecer uma organização de governança dos dados
C) Manter a documentação da privacidade dos dados
D) Realizar auditorias e avaliações de dados iniciais

A) Incorreto. Esta etapa pertence à primeira fase.
B) Incorreto. Esta etapa pertence à primeira fase.
C) Correto. Esta etapa pertence à fase 4: Proteção de Dados e Privacidade: Governança. A primeira fase consiste nas seguintes etapas: condução de análise de privacidade, coleta de leis de privacidade, análise do impacto à privacidade, realização de auditorias e avaliações de dados iniciais, estabelecimento de uma organização de governança dos dados, estabelecimento de fluxos de dados e inventário de dados pessoais, estabelecimento de um programa de proteção de dados e privacidade, desenvolvimento de planos de ação para implementação da proteção de dados e privacidade. (Literatura: B, Capítulo 2.2)
D) Incorreto. Esta etapa pertence à primeira fase.

8 / 40
Uma empresa deseja montar um Sistema de Gestão de Proteção de Dados (SGPD). A segunda fase do desenvolvimento de um SGPD é chamada Organização da Proteção de Dados e Privacidade. Uma das etapas da fase 2 tem o seguinte objetivo:

integrar o pensamento sobre a proteção de dados e privacidade a toda a empresa e a todas as suas funções.

Qual etapa da fase 2 tem este objetivo?

A) Conduzir uma auditoria das medidas e controles para privacidade e proteção de dados com o objetivo de identificar lacunas e erros
B) Implementar e operar sistemas computadorizados de proteção de dados e privacidade
C) Informar os funcionários sobre o estado do programa de privacidade e proteção de dados
D) Manter uma comunicação mútua regular para questões de proteção de dados e privacidade

A) Incorreto. Esta auditoria só pode ocorrer após a implementação completa. Ela é o resultado da fase 5.
B) Incorreto. Esta é uma medida técnica para garantir a integridade dos dados, não uma medida cultural para integrar o pensamento sobre a proteção de dados e privacidade a toda a empresa e a todas as suas funções.
C) Incorreto. Embora seja importante que os funcionários conheçam o estado do programa, esse tipo de comunicação não é suficiente para envolver a todos e integrar de modo eficaz o pensamento sobre a proteção de dados e privacidade a toda a empresa e a todas as suas funções.
D) Correto. A comunicação regular e constante é obrigatória para a implementação eficaz da estratégia de proteção de dados e privacidade da empresa a todas as suas operações. (Literatura: B, Capítulo 2.2.2.)

9 / 40
Um Data Protection Officer (DPO) percebe a importância de manter uma comunicação regular com todos os outros indivíduos indicados que sejam responsáveis pela proteção de dados e privacidade. Esse grupo de indivíduos deve trabalhar no sentido de um resultado para toda a organização, em relação à proteção de dados e privacidade.

Que resultado beneficia **mais** a organização?

A) A criação de um sistema no qual todas as questões de proteção de dados e privacidade devem ser encaminhadas para o DPO e subsequentemente resolvidas por ele
B) O desenvolvimento de perspectivas divergentes sobre a proteção de dados e a privacidade durante a terceirização ou transferência de dados na organização
C) A introdução de uma abordagem colaborativa e proativa para incluir a proteção de dados e a privacidade em todas as partes da organização
D) A conscientização de que a terceirização da proteção de dados e privacidade cria uma responsabilidade solidária pela conformidade

A) Incorreto. A empresa teria mais benefícios se a comunicação regular inspirasse uma mudança de cultura em relação à proteção de dados e privacidade entre todos os funcionários, em vez de deixar todos os problemas de proteção de dados e privacidade unicamente para o DPO.
B) Incorreto. A empresa teria mais benefícios se a comunicação regular criasse uma perspectiva comum, alinhada à declaração da missão de privacidade, em vez de perspectivas divergentes sobre a proteção de dados e privacidade na empresa.
C) Correto. A comunicação regular com todos os indivíduos responsáveis pela privacidade e proteção de dados na organização permite que compreendam melhor o panorama e os desafios de cada departamento e troquem ideias e sugestões sobre modos de incluir a privacidade e proteção de dados em todos os sistemas, serviços, produtos e projetos em andamento. (Literatura: B, Capítulo 2.2.2)
D) Incorreto. A empresa teria mais benefícios se a comunicação regular levasse todos os funcionários a compreender que têm obrigações e responsabilidade pela proteção de dados e privacidade das informações sob seus cuidados, mesmo quando as atividades ou tarefas forem terceirizadas.

10 / 40
Se uma organização quiser desenvolver, implementar e gerenciar um Sistema de Gestão de Proteção de Dados (SGPD), isso é feito em várias fases. A implementação do SGPD tem cinco fases, a saber: preparação, organização, implementação do desenvolvimento, governança e avaliação e melhoria.

As fases de implementação de um SGPD podem ser comparadas a quê?

A) Um processo de melhorias contínuas comparável ao ciclo PDCA (PEVA)
B) Um guia para a implementação da governança de privacidade
C) Um inventário das regulamentações de dados como preparação para o SGPD
D) O impacto das regulamentações, regras e normas de privacidade

A) Correto. As fases de implementação de um SGPD descrevem um processo de melhoria contínua muito próximo ao ciclo PDCA. (Literatura A, Capítulo 1; B, Capítulo 2)
B) Incorreto. Isso se refere à fase 4 da montagem de um SGPD.
C) Incorreto. Isso descreve apenas uma parte da segunda etapa da fase 1 (a fase de preparação).
D) Incorreto. Isso descreve apenas a etapa 3 da fase 1.

11 / 40
Um elemento central do GDPR é o fato de que uma organização deve demonstrar a conformidade. A implementação de um Sistema de Gestão de Proteção de Dados (SGPD) pode ajudar a demonstrar a conformidade.

Qual fase da implementação de um SGPD demonstra **melhor** a conformidade com o GDPR?

A) Fase 1: a organização se prepara para a implementação da privacidade e proteção de dados.
B) Fase 2: as estruturas e os mecanismos organizacionais para a privacidade são estabelecidos.
C) Fase 3: as medidas de proteção de dados e privacidade são desenvolvidas e implementadas.
D) Fase 4: os mecanismos de governança de privacidade para a organização são estabelecidos.

A) Incorreto. Esta fase prepara para a implementação, mas ainda não inclui nenhuma forma de conformidade.
B) Incorreto. Esta fase constitui a base para a implementação dos requisitos de privacidade, mas não demonstra conformidade por si só.
C) Correto. A implementação de procedimentos, políticas e controles demonstra a conformidade. (Literatura B, Capítulo 2.2; Artigo 24(1) do GDPR)
D) Incorreto. Esta fase é importante para manter a conformidade, mas requer a implementação antes.

12 / 40
Um Data Protection Officer (DPO) desenvolve e implementa um Sistema de Gestão de Proteção de Dados e Privacidade (SGPD). A implementação está na fase 3: Desenvolvimento e Implementação da Proteção de Dados e Privacidade.

O que deve ser realizado **primeiro** na fase 3?

A) Analisar e definir as necessidades e os requisitos da empresa em relação à proteção de dados e privacidade
B) Investigar o conhecimento e a compreensão dos funcionários sobre os conceitos de proteção de dados e privacidade
C) Pesquisar as melhores práticas do setor e adaptá-las às necessidades e requisitos da empresa
D) Compreender a legislação de proteção de dados e privacidade global e determinar a relevância dessa informação

A) Correto. A primeira medida consiste em compreender e definir as necessidades e os requisitos da empresa, para estabelecer as metas e os objetivos para as estratégias, planos e políticas de proteção de dados e privacidade. (Literatura: B, Capítulo 2.2)
B) Incorreto. Esta investigação deve ser realizada após a análise e a definição das necessidades e requisitos da corporação.
C) Incorreto. As melhores práticas do setor só podem ser adaptadas para a corporação após a análise e a definição das necessidades e requisitos da organização.
D) Incorreto. A relevância das informações só pode ser determinada após a análise e a definição das necessidades e requisitos da organização.

13 / 40
Um plano de resposta à violação de dados pessoais descreve as seguintes ações:

- Um **provedor externo** responde à violação, fornece serviços de relações públicas e auxilia na minimização do dano.
- O **Data Protection Officer (DPO)** solicita suporte da autoridade supervisora.
- O **processador** notifica os parceiros de negócios e os titulares dos dados sobre a violação de dados e solicita seu suporte.

Quem tem a **maior** probabilidade de minimizar o impacto para terceiros e os titulares dos dados?

A) O provedor externo
B) O DPO
C) O processador

A) Correto. A parte externa fornece serviços que auxiliam a responder com rapidez a uma violação de dados pessoais e ajudam a minimizar o impacto para terceiros e titulares dos dados. (Literatura: B, Capítulo 2)
B) Incorreto. O DPO deve fornecer informações e oferecer assistência à autoridade supervisora, não o contrário.
C) Incorreto. Não existe uma obrigação legal para que os processadores notifiquem os parceiros de negócios sobre uma violação de dados. Além disso, a notificação aos titulares dos dados deve ser realizada apenas (1) quando for provável que a violação de dados pessoais provoque um alto risco aos direitos e liberdades de pessoas físicas e (2) pelo controlador, não pelo processador.

14 / 40
Três instituições de saúde estão trabalhando em conjunto no desenvolvimento de um aplicativo de celular para monitoramento de pacientes. O time médico insere seus dados pessoais e qualificações no aplicativo e os pacientes adicionam seus dados pessoais, incluindo dados médicos.

As instituições de saúde indicam um único Data Protection Officer (DPO). Para executar uma versão piloto, eles precisam colocar o aplicativo nas lojas de aplicativos. Após sua introdução nas lojas de aplicativos, a segurança do novo aplicativo é testada. Como precaução de segurança, a descrição declara que o aplicativo está na fase piloto. Apenas alguns poucos titulares dos dados baixam o aplicativo para testar, mas eles o utilizam de verdade e inserem dados reais.

O teste mostra que o aplicativo não é nem um pouco seguro. Ele pode ser facilmente atacado por hackers. Um hacker poderia alterar os dados de saúde dos pacientes, além de coletar e usar os dados de modos não autorizados.

De acordo com o GDPR, o que o DPO deve fazer?

A) O DPO não precisa tomar nenhuma medida, porque o aplicativo está na fase piloto e apenas um pequeno número de pacientes está participando.
B) O DPO não precisa tomar nenhuma medida porque o impacto das vulnerabilidades não pode ser qualificado como alto durante uma fase piloto.
C) O DPO deve informar os pacientes e a autoridade supervisora porque o aplicativo acarreta um alto risco aos direitos e liberdades dos pacientes.
D) O DPO deve notificar a autoridade supervisora e garantir que as medidas de segurança do aplicativo sejam ajustadas às normas de segurança exigidas.

A) Incorreto. O número de titulares dos dados é irrelevante. A qualificação de alto risco aos direitos e liberdades de pessoas físicas determina as medidas que devem ser tomadas.
B) Incorreto. Uma fase piloto não serve como desculpa para permitir que os dados corram risco.
C) Correto. O controlador adotou medidas insuficientes para garantir a segurança dos dados. O risco refere-se a dados pessoais de categoria especial. Portanto, tanto a autoridade supervisora quanto os titulares dos dados devem ser notificados. (Literatura: A, Capítulo 14; Artigos 33(1) e 34(1) do GDPR)
D) Incorreto. É prudente adotar estas duas medidas. Contudo, o GDPR especifica a notificação dos titulares dos dados e não especifica que as medidas de segurança devam ser ajustadas.

15 / 40
A conformidade com o GDPR pode ser auxiliada pela implementação de um regime de gerenciamento de incidentes sistemático.

Qual seria uma descrição de um processo de gerenciamento de incidentes eficaz?

A) Reconhecer a ocorrência de um incidente, responder às preocupações imediatas e de longo prazo, e acompanhar o incidente para garantir que as medidas adotadas foram eficazes
B) Reconhecer a ocorrência de um incidente e relatar o incidente ao Data Protection Officer (DPO) para análise dos fluxos de dados e melhoria das políticas de segurança
C) Acompanhar todos os incidentes que envolverem dados pessoais, realizar uma Avaliação de Impacto sobre a Proteção de Dados (DPIA) para analisar os riscos e estabelecer um plano de melhoria
D) Acompanhar todos os casos de processamento de dados pessoais para recuperar os dados após um incidente com mais facilidade e garantir que as atividades de resposta possam ser reduzidas para minimizar os custos

A) Correto. Esta é uma descrição de um processo de gerenciamento de incidentes. (Literatura A, Capítulo 14)
B) Incorreto. Os incidentes devem ser relatados ao pessoal responsável. O DPO não precisa analisar os fluxos de dados após cada incidente.
C) Incorreto. DPIAs não precisam ser realizadas após cada incidente.
D) Incorreto. O acompanhamento de todos os casos de processamento de dados pessoais é ineficaz. Esta opção também ignora as etapas de resposta a um incidente e de garantia de que as medidas adotadas foram eficazes.

16 / 40
O CEO pediu que o time de privacidade avalie a organização em termos de desempenho de proteção de dados e privacidade. Um benchmark (referência comparativa) seria um modo adequado de determinar objetivamente como está o desempenho da organização.

O que o benchmark de privacidade **não** cobre?

A) Uma pesquisa que enfoca a satisfação dos clientes da organização em relação à privacidade
B) Comparações entre unidades de negócios ou departamentos em relação à conformidade com a privacidade
C) O desempenho atual da organização em relação à privacidade, em comparação a um ano atrás
D) O desempenho da organização em relação à privacidade comparado com o de entidades semelhantes na indústria

A) Correto. Um benchmark compara a situação atual da empresa com a de períodos anteriores ou com o setor. Neste caso, nenhuma comparação é efetuada. Além disso, nem todos os clientes conhecem as melhores práticas de privacidade ou foram expostos às diferentes práticas de privacidade da sua organização. (Literatura: B, Capítulo 2.2.5)
B) Incorreto. O benchmark de privacidade ajuda a fazer comparações entre unidades de negócios ou departamentos em relação à conformidade com a privacidade.
C) Incorreto. O benchmark de privacidade também pode ser usado como um tipo de autoavaliação para comparar os resultados com avaliações anteriores, com o objetivo de identificar melhorias ou áreas que possam apresentar deterioração.
D) Incorreto. O benchmarking é uma metodologia objetiva para comparar o desempenho de privacidade da organização com entidades semelhantes no setor e com as melhores práticas.

17 / 40
Uma organização deseja usar inteligência artificial (IA) e algoritmos de aprendizagem profunda no departamento de recursos humanos (RH) para examinar as relações de emprego, criar perfis de qualificações de funcionários e definir bônus para objetivos individuais.

O que deve ser feito **inicialmente** e antes da implementação deste novo tipo de processamento de dados pessoais?

A) Conduzir uma Avaliação de Impacto sobre a Proteção de Dados (DPIA)
B) Conduzir uma avaliação de privacidade do departamento de RH
C) Relatar o processamento à autoridade supervisora

A) Correto. O processamento envolve uma nova tecnologia para definição de perfis e tem a probabilidade de produzir um alto risco aos direitos e liberdades de pessoas físicas, pois pode afetar de modo considerável seu comportamento, atividades e recompensas no trabalho. (Literatura: A, Capítulo 5; Artigo 35 do GDPR)
B) Incorreto. A avaliação da conformidade de uma unidade de negócios com as políticas de privacidade é realizada em caráter periódico, sem aviso prévio, não durante a implementação de um novo tipo de processamento.
C) Incorreto. Isto é realizado após a condução da DPIA e apenas em determinadas condições.

18 / 40
De acordo com o GDPR, qual atividade é sempre uma responsabilidade do controlador?

A) Ser responsável pela realização de uma Avaliação de Impacto sobre a Proteção de Dados (DPIA)
B) Contratar uma empresa de segurança para a proteção de dados pessoais em trânsito
C) Implementar um novo método para coleta de dados pessoais dos clientes
D) Manter registros das atividades de processamento realizadas pelo processador

A) Correto. A responsabilidade pelas DPIAs é do controlador e não deve ser terceirizada para um processador de dados. (Literatura A, Capítulo 12; Artigo 35 do GDPR)
B) Incorreto. Isso pode ser responsabilidade do processador, se houver uma autorização prévia por escrito.
C) Incorreto. Isso pode ser responsabilidade do processador, se houver uma autorização prévia por escrito.
D) Incorreto. Esse elemento é uma responsabilidade do processador. O controlador mantém um registro das atividades de processamento que ele controla.

19 / 40
Um hospital terceiriza a impressão das faturas dos pacientes a uma gráfica. A gráfica também imprime faturas para outras organizações.

Devido a um erro, os nomes e endereços foram misturados durante a separação na gráfica e algumas faturas foram enviadas aos pacientes errados.

O hospital tinha analisado cuidadosamente seus próprios processos. O hospital tinha um processo de verificação robusto em vigor e acordos contratuais com a gráfica.

Por que o hospital será **responsabilizado** pela autoridade supervisora?

A) Porque o contrato determina assim
B) Porque o hospital é o controlador
C) Porque a mistura ocorreu entre pacientes
D) Porque a verificação não funcionou

A) Incorreto. O hospital é responsável porque, como controlador, está sujeito ao princípio da responsabilidade, determinado pelo GDPR.
B) Correto. O GDPR afirma que “O controlador deve ser responsável […], parágrafo 1 (“responsabilidade”)” pela legalidade do processamento. O controlador será considerado responsável pela autoridade supervisora, independentemente do contrato firmado entre o controlador e o processador. O controlador deve empregar somente processadores que forneçam garantias suficientes de que implementam medidas técnicas e organizacionais apropriadas. (Literatura A, Capítulo 12; Artigo 5(2) do GDPR)
C) Incorreto. Não há diferença se todos os titulares dos dados pertencem ao mesmo controlador. Quem é o controlador é o que importa aqui.
D) Incorreto. Não há indicação de que a verificação não tenha funcionado. A autoridade supervisora sempre responsabilizará o controlador.

20 / 40
Quando um controlador e um processador assinam um contrato para o processamento de dados pessoais, ambos têm responsabilidades específicas. Algumas dessas responsabilidades são estipuladas pelo GDPR e outras podem ser dispostas no contrato.

De acordo com o GDPR, quando o processador sempre precisa de uma autorização por escrito do controlador?

A) Quando o processador contrata uma empresa para proteger os dados durante transferências
B) Quando o processador contrata um terceiro para processar dados pessoais
C) Quando o processador implementa um novo método para coleta de dados pessoais
D) Quando o processador implementa um novo método para exclusão de dados pessoais

A) Incorreto. Este elemento é ou pode ser determinado pelo processador de acordo com o contrato, uma vez que não é definido com clareza no GDPR.
B) Correto. Este envolvimento de outro processador não pode ser realizado sem a autorização prévia por escrito, geral ou específica, do controlador. (Literatura A, Capítulo 12; Artigo 28(2) do GDPR)
C) Incorreto. Este elemento é ou pode ser determinado pelo processador de acordo com o contrato, uma vez que não é definido com clareza no GDPR.
D) Incorreto. Este elemento é ou pode ser determinado pelo processador de acordo com o contrato, uma vez que não é definido com clareza no GDPR.

21 / 40
Quem tem a obrigação legal de manter os registros das atividades de processamento?

A) O Diretor de Informações (CIO)
B) O Chief Privacy Officer
C) O controlador e o processador
D) O Data Protection Officer (DPO)

A) Incorreto. O CIO tem a responsabilidade geral pela tecnologia de informação e o gerenciamento de informações.
B) Incorreto. O Chief Privacy Officer deve criar o engajamento para conformidade com o GDPR na organização.
C) Correto. Tanto o controlador quanto o processador devem manter um registro de todas as atividades de processamento. (Literatura A, Capítulo 12; Artigo 30 do GDPR)
D) Incorreto. Embora, na prática, o DPO seja o profissional que cria inventários, mantém um registro das atividades de processamento e tem a responsabilidade de manter esses registros, isso está subordinado à obrigação legal do controlador ou do processador.

22 / 40
Uma organização norte-americana situada na Área Econômica Europeia (AEE) processa dados pessoais de pessoas físicas. Ela processa dados étnicos em larga escala.

De acordo com o GDPR, uma organização deve indicar um Data Protection Officer (DPO) em três casos específicos.

Neste caso, por qual motivo é obrigatório que a organização indique um DPO?

A) Os dados pessoais de estrangeiros são processados.
B) Os dados pessoais são processados por um país terceiro.
C) Os dados pessoais de minorias são processados.
D) As categorias especiais de dados pessoais são processadas.

A) Incorreto. Esta não é uma das três condições básicas especificadas no GDPR.
B) Incorreto. Esta não é uma das três condições básicas especificadas no GDPR.
C) Incorreto. Esta não é uma das três condições básicas especificadas no GDPR.
D) Correto. Este é um dos casos especificados no GDPR, quando as principais atividades do controlador ou do processador consistirem no processamento em larga escala de categorias especiais de dados, conforme o Artigo 9. Dados étnicos ou raciais são mencionados especificamente no Artigo 9 do GDPR. As outras duas condições são: (1) processamento realizado por uma autoridade ou agência pública, com exceção de tribunais atuando em sua capacidade jurídica, (2) processamento que exija o monitoramento regular e sistemático de titulares dos dados em larga escala. Estas três condições básicas são aplicáveis tanto a controladores quanto a processadores. (Literatura A, Capítulo 2; Artigos 9 e 37 do GDPR)

23 / 40
Um Data Protection Officer (DPO) trabalha para o Ministério dos Transportes, que é um departamento nacional.

Um novo projeto é anunciado para monitorar o comportamento das pessoas ao dirigir nas rodovias nacionais. O Ministério deseja usar um sistema inteligente de análise de vídeo para discriminar os carros e automaticamente reconhecer os números das placas.

O secretário de Estado tem pressa para iniciar o projeto e expressa a preocupação de que as questões de privacidade possam provocar atrasos indesejáveis.

O que o DPO deve fazer?

A) Pedir que o secretário de Estado entre em contato com a autoridade supervisora porque claramente isso está fora do escopo do DPO
B) Garantir ao secretário de Estado que uma DPIA é desnecessária se os titulares dos dados forem informados sobre o processamento dos dados
C) Informar o secretário de Estado que uma DPIA é obrigatória para o monitoramento em larga escala de um espaço público
D) Solicitar que o secretário de Estado reconsidere o projeto porque o processamento de dados de vigilância em massa é proibido

A) Incorreto. Um DPO deve ser suficientemente qualificado para discutir esse assunto.
B) Incorreto. Informar os titulares dos dados não isenta uma organização da responsabilidade de realizar uma DPIA.
C) Correto. O projeto requer o monitoramento sistemático em grande escala de uma área de acesso público, e este é um dos três cenários obrigatórios para a realização de uma DPIA. (Literatura: A, Capítulo 5; Artigo 35(3)(c) do GDPR)
D) Incorreto. Monitoramento, vigilância e definição de perfis não são proibidos, desde que os direitos e as liberdades das pessoas sejam suficientemente protegidos.

24 / 40
Os Data Protection Officers (DPOs) são limitados por sigilo ou confidencialidade em relação ao desempenho de suas tarefas.

Em relação a qual parte o DPO está **isento** desse sigilo ou confidencialidade para buscar orientação?

A) A diretoria da empresa
B) Os membros de uma rede de proteção de dados e privacidade
C) O Diretor de Segurança de Informações (ISO)
D) A autoridade supervisora

A) Incorreto. Estar facilmente acessível não significa que o DPO deva pedir a orientação de membros da diretoria. O DPO deve desempenhar um papel independente.
B) Incorreto. Estar facilmente acessível não significa que o DPO deva pedir a orientação a membros de uma rede de proteção de dados e privacidade.
C) Incorreto. Estar facilmente acessível não significa que o DPO deva pedir a orientação do ISO.
D) Correto. A obrigação de sigilo e/ou confidencialidade não proíbe o DPO de entrar em contato e buscar o aconselhamento da autoridade supervisora. (Literatura A, Capítulo 2; Artigos 36 e 39(1)(e) do GDPR)

25 / 40
Uma Avaliação de Impacto sobre a Proteção de Dados (DPIA) é uma ferramenta para identificar riscos à proteção de dados, em especial aqueles que provavelmente terão um grande efeito sobre os direitos e as liberdades de pessoas físicas.

Por que a DPIA pode ser vista como parte do gerenciamento de riscos mais amplo de uma organização?

A) Porque a DPIA avalia todos os riscos de segurança da organização examinada e substitui outras avaliações de risco ou gerenciamento de riscos
B) Porque a DPIA avalia os riscos pela probabilidade e gravidade do risco, de um modo semelhante a outros componentes bem definidos do gerenciamento de riscos
C) Porque a DPIA é obrigatória para cada projeto, de acordo com o GDPR, o que reduz todos os outros requisitos legais para gerenciamento de riscos

A) Incorreto. Uma DPIA enfoca apenas os riscos à proteção de dados pessoais e privacidade.
B) Correto. Esta é a relação entre a DPIA e o gerenciamento de riscos. (Literatura: A, Capítulo 2; Item 90 do Preâmbulo do GDPR)
C) Incorreto. Nem sempre uma DPIA é necessária e ela não diminui a necessidade de outro gerenciamento de riscos.

26 / 40
De acordo com o GDPR, o que deve sempre fazer parte de uma DPIA?

A) Desenvolver um procedimento de solicitação de acesso pelos indivíduos para garantir a conformidade com os direitos dos titulares dos dados
B) Identificar os dados pessoais que são processados e os objetivos buscados com o processamento
C) Notificar os titulares dos dados sobre a ocorrência de uma avaliação e solicitar seu consentimento explícito
D) Estabelecer um plano de resposta a incidentes e definir salvaguardas apropriadas para evitar violações de dados

A) Incorreto. Esta é uma medida possível, conforme o resultado de uma DPIA.
B) Correto. Toda DPIA deve começar com uma descrição do processamento pretendido e os objetivos do processamento. (Literatura: A, Capítulo 8; Artigo 35(7)(a) do GDPR)
C) Incorreto. Não é necessário o consentimento para a realização de uma DPIA.
D) Incorreto. Esta é uma medida possível, conforme o resultado de uma DPIA.

27 / 40
Uma organização desenvolve um novo produto para detectar funcionários com desempenho inferior. Ela pesquisa seu histórico na internet e analisa seu comportamento no trabalho usando inteligência artificial (IA).

Embora os engenheiros de software não compreendam totalmente o algoritmo, a gerência decide demitir os funcionários incluídos na faixa de 10% mais inferior.

O Data Protection Officer (DPO) está preocupado com o impacto desse produto e informa a diretoria que é necessária uma Avaliação de Impacto sobre a Proteção de Dados (DPIA).

Qual opção **não** faz parte do motivo pelo qual uma DPIA é obrigatória?

A) A automatização do processamento de dados pessoais
B) A avaliação que pode afetar os titulares dos dados de modo considerável
C) O processamento de categorias especiais de dados pessoais
D) A avaliação sistemática de aspectos pessoais de pessoas físicas

A) Incorreto. Esse é um motivo para a obrigatoriedade da DPIA.
B) Incorreto. Esse é um motivo para a obrigatoriedade da DPIA.
C) Correto. Embora o sistema esteja coletando dados pessoais, esses dados não são considerados como categorias especiais de dados. (Literatura: A, Capítulo 8; Artigo 35 do GDPR)
D) Incorreto. Esse é um motivo para a obrigatoriedade da DPIA.

28 / 40
O que **não** é considerado um resultado de uma Avaliação de Impacto sobre a Proteção de Dados (DPIA)?

A) Um registro de acesso a dados confidenciais, com uma verificação de autorização automatizada
B) Um registro das opiniões dos titulares dos dados sobre as operações de processamento pretendidas
C) Uma descrição sistemática das operações de processamento pretendidas
D) Uma avaliação dos riscos aos direitos e liberdades dos titulares dos dados

A) Correto. Este não é o resultado de uma DPIA, e sim uma atividade contínua realizada pela segurança de informação. (Literatura: A, Capítulo 8 e Capítulo 3; Artigo 35 do GDPR)
B) Incorreto. Este é um resultado possível de uma DPIA.
C) Incorreto. Este é um resultado possível de uma DPIA.
D) Incorreto. Este é um resultado possível de uma DPIA.

29 / 40
O GDPR detalha o que deve estar contido no resultado de uma Avaliação de Impacto sobre a Proteção de Dados (DPIA), no mínimo.

O que **não** é obrigatório em uma DPIA?

A) Uma descrição do processamento e seus objetivos
B) Uma avaliação da necessidade e da proporcionalidade das operações de processamento em relação às finalidades
C) Uma avaliação dos riscos aos direitos e liberdades dos titulares dos dados
D) A orientação da autoridade supervisora

A) Incorreto. Esta é uma parte obrigatória da DPIA.
B) Incorreto. Esta é uma parte obrigatória da DPIA.
C) Incorreto. Esta é uma parte obrigatória da DPIA.
D) Correto. Nem sempre é obrigatório consultar a autoridade supervisora e não é obrigatório incluir um registro da orientação na DPIA. (Literatura: A, Capítulo 5; Artigos 35(7) e 36(1) do GDPR)

30 / 40
Uma Avaliação de Impacto sobre a Proteção de Dados (DPIA) mostra que o processamento pretendido envolve a coleta de mais dados sobre clientes individuais que o necessário para obter o objetivo desejado.

De acordo com o GDPR, qual é a resposta **mais** apropriada?

A) Anonimizar os dados o mais rápido possível
B) Introduzir um programa de treinamento e conscientização
C) Limitar o período de tempo no qual os dados serão armazenados
D) Reduzir a quantidade de dados coletados

A) Incorreto. Esta é uma medida de mitigação de risco, mas, em primeiro lugar, os dados desnecessários não poderão ser processados.
B) Incorreto. Esta é uma medida de mitigação de risco, mas, em primeiro lugar, os dados desnecessários não poderão ser processados.
C) Incorreto. Esta é uma medida de mitigação de risco, mas, em primeiro lugar, os dados desnecessários não poderão ser processados.
D) Correto. Isto implementa o princípio de tratamento mínimo dos dados e reduz os riscos para os titulares dos dados. (Literatura: A, Capítulo 8; Artigo 5(1) do GDPR)

31 / 40
O que é melhor fazer **primeiro**, antes de iniciar uma Avaliação de Impacto sobre a Proteção de Dados (DPIA)?

A) Determinar medidas para abordar os riscos identificados
B) Determinar se há necessidade de uma DPIA
C) Identificar os riscos aos direitos e liberdades dos titulares dos dados

A) Incorreto. Isso faz parte de uma DPIA e é realizado após ser determinado que ela é necessária.
B) Correto. A organização precisa determinar se a lei requer uma DPIA ou se ela é exigida pelas necessidades da organização. (Literatura: A, Capítulo 5; Artigo 35(7) do GDPR)
C) Incorreto. Isso faz parte de uma DPIA e é realizado após ser determinado que ela é necessária.

32 / 40
Uma empresa realiza uma Avaliação de Impacto sobre a Proteção de Dados (DPIA).

Por que o mapeamento dos dados é útil em uma DPIA?

A) Ele avalia todos os riscos organizacionais à privacidade.
B) Ele ajuda a ter uma visão geral dos dados pessoais em uso.
C) Ele ajuda a informar todas as partes relevantes.

A) Incorreto. O mapeamento de dados não avalia riscos.
B) Correto. O mapeamento de dados identifica os dados em uso. Os fluxos de dados mapeados ajudam a identificar possíveis riscos que devam ser avaliados. (Literatura: A, Capítulo 7)
C) Incorreto. O mapeamento de dados não é usado para informar as partes.

33 / 40
Um especialista em privacidade é contratado por uma organização. Ela deseja terceirizar parte de suas atividades de processamento dos dados. O especialista realiza uma Avaliação de Impacto sobre a Proteção de Dados (DPIA) do processamento que envolve um processador de dados.

Uma das principais etapas de uma DPIA requer que o controlador forneça todas as informações e não requer o envolvimento do processador.

Que etapa é essa?

A) Avaliação da necessidade e da proporcionalidade do processamento
B) Avaliação dos riscos aos direitos e liberdades dos titulares dos dados
C) Medidas de mitigação para abordar os riscos, incluindo salvaguardas
D) Descrições sistemáticas das operações de processamento pretendidas

A) Correto. Isso é responsabilidade do controlador e não envolve o processador. (Literatura A, Capítulo 12)
B) Incorreto. São necessárias informações do processador sobre os possíveis riscos.
C) Incorreto. São necessárias informações sobre as medidas de mitigação adotadas pelo processador.
D) Incorreto. Para fazer uma descrição completa, são necessárias informações do processador.

34 / 40
Uma grande empresa está tendo dificuldades financeiras. A diretoria quer que os funcionários trabalhem com mais eficiência.

A diretoria inicia uma experiência, na qual as atividades dos funcionários na internet são monitoradas. Os dados são analisados para verificar onde é possível obter maior eficiência. As pessoas classificadas como *ineficientes* poderão ser demitidas.

Por que uma Avaliação de Impacto sobre a Proteção de Dados (DPIA) deve ser realizada antes de utilizar o novo procedimento?

A) Porque uma grande empresa tem muitos funcionários. Portanto, o processamento será realizado em larga escala.
B) Porque isso constitui um experimento. Uma DPIA é exigida para atividades de processamento novas e experimentais.
C) Porque isso constitui um processamento sistemático. As decisões podem afetar os funcionários de modo considerável.

A) Incorreto. A larga escala pode influenciar, mas não constitui um critério por si só. O monitoramento em larga escala em um espaço público seria um critério. Contudo, a empresa não é um espaço público.
B) Incorreto. É irrelevante se isso envolve um experimento ou uma atividade de processamento comum.
C) Correto. Isso é definido como um dos três casos em que uma DPIA é obrigatória. (Literatura: A, Capítulo 5; Artigo 35(3)(b) do GDPR)

35 / 40
Uma organização pretende tomar decisões automatizadas sobre seus clientes, com base na definição de perfis.

Que parte da Avaliação de Impacto sobre a Proteção de Dados (DPIA) requer uma atenção extra?

A) A avaliação da necessidade de realizar uma DPIA em relação a essa atividade de processamento
B) As medidas que serão implementadas para proteger os direitos do titular dos dados
C) As medidas para proteger os dados pessoais, evitando que sejam solicitados pelos titulares dos dados
D) Os procedimentos para apagamento dos dados após um titular dos dados solicitar que seus dados sejam removidos

A) Incorreto. Para atividades de processamento que envolvam a tomada de decisão automatizada, incluindo a definição de perfis, uma DPIA é sempre necessária.
B) Correto. Os riscos trazidos pela tomada de decisão automatizada exigem atenção especial. O modo para mitigar o risco deve ser descrito com atenção. Uma possível mitigação consistiria em permitir a intervenção humana. (Literatura: A, Capítulo 5; Artigo 35 do GDPR)
C) Incorreto. Os dados devem ser protegidos de um modo geral, mas os titulares dos dados têm direito ao acesso.
D) Incorreto. Isto faz parte de uma DPIA, mas não é o mais apropriado para atenção específica quando são efetuadas decisões automatizadas.

36 / 40
O GDPR declara que as organizações devem buscar modos de prevenir violações de dados pessoais. Portanto, é importante reconhecer rapidamente incidentes que possam ser classificados como violações de dados pessoais.

De acordo com o GDPR, que incidente **não** constitui uma violação de dados pessoais?

A) Um paciente está esperando um pacote contendo equipamento médico, mas ele é entregue no endereço errado.
B) Um funcionário de uma clínica de saúde mental não lembra onde colocou algumas pastas de pacientes que não podem ser rastreadas.
C) A destruição acidental de dados pessoais por um incêndio ou terremoto em um depósito de dados.
D) A divulgação não autorizada de dados financeiros confidenciais de uma empresa relativos a uma aquisição planejada.

A) Incorreto. Isso é uma violação de dados pessoais que envolve dados pessoais de categoria especial.
B) Incorreto. A perda acidental de qualquer dado pessoal, em particular dados pessoais de categoria especial, também é considerada como violação de dados pessoais.
C) Incorreto. Mesmo que o incidente seja causado por um desastre natural ou força maior, isso deve ser considerado como violação de dados pessoais.
D) Correto. Isso é um incidente, mas nenhum dado pessoal é comprometido. Não constitui uma violação de dados pessoais. (Literatura: A, Capítulo 3; Artigo 4(12) do GDPR)

37 / 40
Em que situação o relato de uma violação de dados pessoais à autoridade supervisora é necessário?

A) Se a organização não conseguir resolver o incidente dentro de um prazo de 72 horas após sua ocorrência
B) Em qualquer situação na qual exista uma ameaça de segurança aos direitos e liberdades de pessoas físicas
C) Apenas se o incidente for reconhecido como uma violação de dados pessoais dentro de um prazo de 72 horas
D) Quando uma violação de dados pessoais acarretar um risco aos direitos e liberdades de pessoas físicas

A) Incorreto. O prazo para resolução do incidente não é importante.
B) Incorreto. Uma ameaça não é suficiente. A notificação é obrigatória apenas quando ocorrer uma violação de dados pessoais que tenha a probabilidade de acarretar um risco aos direitos e liberdades de pessoas físicas.
C) Incorreto. O processo de gerenciamento de incidentes pode não ser capaz de identificar o incidente dentro de 72 horas. O GDPR declara que violações de dados pessoais devem ser relatadas “sem demora injustificada e, quando viável, no máximo 72 horas após tomar ciência do fato”.
D) Correto. A notificação à autoridade supervisora é obrigatória para incidentes que envolvam dados pessoais e possam acarretar um risco aos direitos e liberdades de pessoas físicas. (Literatura A, Capítulo 14; Artigo 33(1) do GDPR)

38 / 40
O chefe do departamento de Recursos Humanos (RH) perdeu um pendrive contendo as informações pessoais de 35 funcionários. O pendrive é protegido por criptografia robusta. O departamento de RH também tem essas informações pessoais armazenadas em um dispositivo de cópia de segurança.

De acordo com o GDPR, é obrigatório relatar essa violação de dados pessoais à autoridade supervisora?

A) Sim, porque todos os incidentes de segurança devem ser relatados à autoridade supervisora.
B) Sim, porque o relato permite que a autoridade supervisora informe os funcionários.
C) Não, porque o relato de violações de dados não constitui um interesse legítimo da empresa.
D) Não, porque esta violação de dados pessoais não produz riscos aos direitos dos titulares dos dados.

A) Incorreto. Apenas violações de dados pessoais que resultem em alto risco aos direitos dos titulares dos dados devem ser relatadas. Embora o relato de todas as violações de dados pessoais constitua uma boa prática para evitar o descumprimento da lei, isso não é obrigatório.
B) Incorreto. Os direitos dos titulares dos dados não correm riscos, portanto eles não precisam ser informados. A autoridade supervisora não tem a tarefa de informar os titulares dos dados.
C) Incorreto. O interesse legítimo da empresa é uma base legal para o processamento. Não está relacionado a violações de dados pessoais e o modo como elas devem ser relatadas.
D) Correto. A criptografia robusta e cópias de segurança são suficientes para garantir a confidencialidade e a disponibilidade dos dados pessoais. Portanto, é improvável que essa violação de dados produza um risco para os direitos e liberdades de pessoas físicas. Não é obrigatório relatar essa violação de dados pessoais à autoridade supervisora. (Literatura A, Capítulo 14; Artigo 33(1) do GDPR)

39 / 40
De acordo com o GDPR, em que situação uma violação de dados pessoais deve ser relatada aos titulares dos dados afetados?

A) Quando for provável que a violação de dados pessoais provoque um alto risco aos direitos e liberdades do titular dos dados
B) Quando a autoridade supervisora determinar que o consentimento constituiu a única base legal para o processamento
C) Quando houver um incidente de segurança rotulado como violação de dados pessoais dentro de 72 horas
D) Quando os dados pessoais forem comprometidos por fatores externos, como hackers ou outros cibercriminosos

A) Correto. Os titulares dos dados devem ser informados se a violação de dados pessoais representar um “alto risco” para seus direitos e liberdades. (Literatura A, Capítulo 14; Artigo 34(1) do GDPR)
B) Incorreto. Apenas violações de dados pessoais que representem um alto risco também devem ser relatadas aos titulares dos dados.
C) Incorreto. O período de 72 horas representa o prazo para relato da violação de dados pessoais à autoridade supervisora. Nem todas as violações de dados pessoais devem ser relatadas aos titulares dos dados.
D) Incorreto. A notificação não depende da causa subjacente da violação de dados pessoais.

40 / 40
No processo de resposta a incidentes para melhor prática, são definidas as fases de Preparação, Resposta e Acompanhamento. Em cada fase, a documentação é essencial.

Na fase de Resposta, é importante reunir e preservar as evidências para mostrar por que um incidente ocorreu e por que a organização não foi capaz de prevenir o incidente.

O que deve ser reunido e preservado?

A) Planos de controle de auditoria
B) Avaliações de Impacto sobre a Proteção de Dados (DPIAs)
C) Evidências para proporcionar um quadro claro
D) Planos de recuperação do sistema

A) Incorreto. Um plano de controle de auditoria não é documentado no processo de resposta a incidentes.
B) Incorreto. Uma DPIA não é documentada no processo de resposta a incidentes.
C) Correto. Ao longo de todo o processo de resposta a incidentes, deve-se reunir e preservar evidências para proporcionar um quadro claro do que aconteceu e por que a organização não conseguiu prevenir o incidente. (Literatura A, Capítulo 14)
D) Incorreto. Um plano de recuperação do sistema não é documentado no processo de resposta a incidentes.

Avaliação

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

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

Contato EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER