EXIN Privacy & Data Protection

PROFESSIONAL

Exame simulado

Edição 202302

Conteúdo

Introdução

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

Esse 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 esse exame é de 120 minutos.

Você é autorizado a utilizar o GDPR durante todo esse 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
Uma organização implementa o Sistema de Gestão de Informações de Privacidade (PIMS) usando a norma ISO/IEC 27701.

Durante a implementação, alguns prestadores de serviços da organização percebem que eles devem estar em conformidade com vários requisitos legais de diferentes países. Os prestadores de serviços decidem pedir orientação ao Data Protection Officer (DPO).

Segundo a ISO/IEC 27701, como o DPO deveria classificar os requisitos legais?

A) Questão interna, pois os requisitos legais impactam diretamente o PIMS, que é um assunto interno.
B) Questão interna, pois os elementos relevantes são os prestadores de serviços, que devem ser vistos como colegas de trabalho.
C) Questão externa, pois os prestadores de serviços atuam externamente em relação aos colegas de trabalho da organização.
D) Questão externa, pois os requisitos legais, apesar de relevantes, são independentes da organização.

6 / 40
Uma organização do tipo empresa para consumidor (B2C, "business to consumer") implementa um Sistema de Gestão de Informações de Privacidade (PIMS).

O Data Protection Officer (DPO) encontra os seguintes suportes contendo informações:

- Um **HD externo** com informações sobre os competidores e uma descrição de suas forças e fraquezas.
- Alguns **arquivos em papel** do time de recursos humanos (RH), com informações de saúde e informações de contato em caso de emergência.
- Um **servidor** de computador contendo um backup de todos os dados dos clientes, incluindo os dos consumidores diretos.
- **Pen drives** antigos com informações pessoais de ex-funcionários e seus últimos salários na organização.

Qual suporte **não** deve fazer parte do PIMS?

A) HD externo
B) Arquivos em papel
C) Servidor
D) Pen drives

7 / 40
Quando se define um Sistema de Gestão de Informações de Privacidade (PIMS), diferentes documentos são criados, como a Declaração de Aplicabilidade (SoA).

O que é uma SoA?

A) A SoA calcula a probabilidade de o processamento de dados resultar em alto risco para as pessoas.
B) A SoA registra onde e como os dados pessoais dos funcionários e clientes são processados.
C) A SoA especifica que controles devem ser aplicados para gerenciar ou minimizar os riscos no PIMS.

8 / 40
É fundamental para um Sistema de Gestão de Informações de Privacidade (PIMS), tanto a curto quanto a longo prazo, poder demonstrar como as políticas corporativas, os procedimentos operacionais e as instruções de trabalho são formulados. Isso garante a rastreabilidade das ações para decisões e políticas de gestão e a reprodutibilidade dos resultados.

Essa afirmação faz referência a que requisito do PIMS?

A) Auditoria
B) Documentação
C) Avaliação do sistema de gestão
D) Declaração de Aplicabilidade (SoA)

9 / 40
Por que a alta gestão deve avaliar o progresso do Sistema de Gestão de Informações de Privacidade (PIMS)?

A) Para assegurar que o PIMS esteja em conformidade com todos os requisitos legais relevantes
B) Para assegurar que o PIMS tenha controles de privacidade suficientes para mitigar riscos
C) Para assegurar que o PIMS seja auditado regularmente e esteja produzindo documentos
D) Para assegurar que o PIMS seja eficaz e cumpra os requisitos corporativos

10 / 40
O Sistema de Gestão de Informações de Privacidade (PIMS) pode ser auditado por diversas razões.

Segundo a ISO/IEC 27701, qual é o **principal** objetivo das auditorias do PIMS?

A) Confirmar que os requisitos das normas nacionais e internacionais relevantes sejam mantidos
B) Identificar áreas específicas de preocupação e abordar a seleção dos processos individuais de trabalho
C) Incluir atualizações das mudanças relevantes na legislação e na regulamentação e sua interpretação
D) Monitorar a conformidade entre os requisitos do sistema de gestão e as práticas de trabalho

11 / 40
Uma organização implementa um Sistema de Gestão de Informações de Privacidade (PIMS). Os requisitos específicos devem ser baseados em regras locais e requisitos contratuais.

Qual deve ser o próximo passo para a equipe jurídica da organização?

A) Contratar assessoria e orientação jurídicas locais e aplicar a ISO/IEC 27701 como norma contratual para clientes e fornecedores
B) Pesquisar as melhores práticas internacionais aplicáveis e revisar todos os contratos que envolvam processamento de dados pessoais
C) Mapear a legislação aplicável e as sanções legais correspondentes e revisar todos os contratos que envolvam processamento de dados pessoais
D) Solicitar orientação da autoridade de fiscalização local e aplicar a ISO/IEC 27701 como norma contratual para clientes e fornecedores

12 / 40
Uma organização está efetuando uma fusão com outra empresa. A organização já tem um Sistema de Gestão de Informações de Privacidade (PIMS).

A conclusão do processo depende da demonstração de que todas as operações de processamento de dados pessoais seguem a ISO/IEC 27701 e a legislação aplicável.

Qual é o meio **mais** adequado para demonstrar isso?

A) Um relatório de Avaliação de Impacto sobre a Proteção de Dados (DPIA)
B) Um relatório de Avaliação de Impacto à Privacidade (PIA)
C) Um relatório recente de auditoria do PIMS
D) Um relatório sobre Declaração de Aplicabilidade (SoA)

13 / 40
Uma pequena organização desenvolveu um serviço de software bem-sucedido. Como seu serviço é um enorme sucesso, a organização precisa de uma solução de nuvem (cloud) mais robusta e, assim, deve selecionar um fornecedor externo de nuvem.

A organização possui certificação ISO/IEC 27701. Durante a busca por um fornecedor, a organização encontra vários fornecedores de nuvem, alguns deles com certificação ISO/IEC 27701, mas outros sem.

Como a certificação ISO/IEC 27701 ajuda na seleção do fornecedor?

A) A certificação ISO/IEC 27701 de um fornecedor inclui uma análise de custo-benefício, o que garante menores custos para os serviços.
B) A certificação ISO/IEC 27701 de um fornecedor reduz a necessidade de auditar os fornecedores, o que é mais fácil para a organização.
C) A certificação ISO/IEC 27701 da organização tem procedimentos para o processamento de dados, os quais se extendem a qualquer fornecedor.
D) A certificação ISO/IEC 27701 da organização exige um fornecedor com certificação ISO/IEC 27701, o que limita as escolhas.

14 / 40
Quando se trabalha em função da certificação ISO/IEC 27701, há diversos sistemas de gestão envolvidos. Dois desses sistemas são:

- Sistema de Gestão de Informações de Privacidade (PIMS)
- Sistema de Gestão de Segurança da Informação (ISMS)

O que é verdadeiro sobre esses sistemas?

A) As auditorias do ISMS e do PIMS podem ser combinadas ou realizadas separadamente, embora os requisitos do PIMS dependam da manutenção do ISMS.
B) As auditorias do ISMS e do PIMS nunca devem ser realizadas em conjunto, pois os requisitos de sistema do PIMS e do ISMS não dependem uns dos outros.
C) O ISMS faz parte do PIMS e trata da proteção da informação, uma vez que o ISMS considera uma abordagem de risco de negócios para os dados pessoais.

15 / 40
Uma organização implementa um Sistema de Gestão de Informações de Privacidade (PIMS). O GDPR exige que "dados pessoais sejam processados de forma a garantir a segurança e a confidencialidade adequadas dos dados pessoais [...]".

Qual é a relação entre essa exigência e a norma ISO/IEC 27701?

A) Os princípios GDPR de integridade e confidencialidade formam a base do PIMS, que é exigido pela norma ISO/IEC 27701.
B) Os princípios GDPR de licitude, lealdade e transparência contribuem para o PIMS e para o Sistema de Gestão de Segurança da Informação (ISMS).
C) O princípio GDPR da limitação de finalidade estabelece com exatidão como os dados que fazem parte do PIMS devem ou não ser utilizados.
D) O princípio GDPR da limitação de armazenamento especifica o tempo que os dados pessoais ficam no PIMS antes do processamento.

16 / 40
A norma ISO/IEC 27701 contém um capítulo dedicado a diretrizes adicionais, que se alinha com a norma ISO/IEC 27002.

Que tipo de recomendação **não** está incluído nesse capítulo?

A) Desenvolver políticas de privacidade separadas das políticas de segurança da informação ou combinadas com elas
B) Assegurar pelo menos treinamento de conscientização para todos os funcionários que manejem ou processem dados pessoais
C) Rotular todos os dados de modo claro para identificar onde os dados pessoais são armazenados ou, de outra forma, processados
D) Planejar auditorias internas e externas em um intervalo específico, dependendo do âmbito da auditoria

17 / 40
Aplicar controles do Sistema de Gestão de Informações de Privacidade (PIMS) para gerenciar riscos não é tarefa fácil, e é recomendado passar por todas as etapas.

A primeira etapa é criar um conjunto de controles para gerenciar riscos. As outras etapas estão listadas abaixo (em ordem aleatória):

1. Comparar os controles ao Anexo A ou B da ISO/IEC 27701
2. Elaborar a Declaração de Aplicabilidade (SoA)
3. Implementar os controles de forma eficaz

Qual é a ordem **correta** das outras etapas?

A) 1, 2, 3
B) 1, 3, 2
C) 2, 1, 3
D) 2, 3, 1

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
Uma organização implementa o Sistema de Gestão de Informações de Privacidade (PIMS) usando a norma ISO/IEC 27701.

Durante a implementação, alguns prestadores de serviços da organização percebem que eles devem estar em conformidade com vários requisitos legais de diferentes países. Os prestadores de serviços decidem pedir orientação ao Data Protection Officer (DPO).

Segundo a ISO/IEC 27701, como o DPO deveria classificar os requisitos legais?

A) Questão interna, pois os requisitos legais impactam diretamente o PIMS, que é um assunto interno.
B) Questão interna, pois os elementos relevantes são os prestadores de serviços, que devem ser vistos como colegas de trabalho.
C) Questão externa, pois os prestadores de serviços atuam externamente em relação aos colegas de trabalho da organização.
D) Questão externa, pois os requisitos legais, apesar de relevantes, são independentes da organização.

A) Incorreto. Mesmo que os requisitos legais provavelmente impactem diretamente o PIMS, os requisitos legais em si são sempre questões externas.
B) Incorreto. Embora os prestadores de serviços devam, de fato, ser vistos como colegas de trabalho, e a gestão do pessoal e os relatórios sejam questões internas, os elementos a serem classificados são os requisitos legais.
C) Incorreto. Todos os colegas de trabalho, incluindo os prestadores de serviços externos, sua gestão e os relatórios devem ser considerados questões internas. Além disso, os elementos a serem classificados são os requisitos legais, que são questões externas.
D) Correto. Segundo o termo introduzido pela ISO/IEC 27701, requisitos legais são considerados questões externas. (Literatura: B, Capítulo 2)

6 / 40
Uma organização do tipo empresa para consumidor (B2C, "business to consumer") implementa um Sistema de Gestão de Informações de Privacidade (PIMS).

O Data Protection Officer (DPO) encontra os seguintes suportes contendo informações:

- Um **HD externo** com informações sobre os competidores e uma descrição de suas forças e fraquezas.
- Alguns **arquivos em papel** do time de recursos humanos (RH), com informações de saúde e informações de contato em caso de emergência.
- Um **servidor** de computador contendo um backup de todos os dados dos clientes, incluindo os dos consumidores diretos.
- **Pen drives** antigos com informações pessoais de ex-funcionários e seus últimos salários na organização.

Qual suporte **não** deve fazer parte do PIMS?

A) HD externo
B) Arquivos em papel
C) Servidor
D) Pen drives

A) Correto. O PIMS deve estar relacionado a informações pessoais e, nesse caso, o HD externo não contém nenhuma informação pessoal. (Literatura: B, Capítulo 1)
B) Incorreto. Todos os suportes, mesmo os não digitais, que contêm informações pessoais devem fazer parte do PIMS. Os arquivos do time de RH contêm informações pessoais e, portanto, devem estar no PIMS.
C) Incorreto. Todos os suportes contendo informações pessoais, mesmo que apenas backup, devem fazer parte do PIMS. O servidor contém dados dos consumidores, que são dados de pessoas físicas e, portanto, informações pessoais.
D) Incorreto. Todos os suportes que contêm informações pessoais devem fazer parte do PIMS, mesmo que as informações sejam de ex-funcionários.

7 / 40
Quando se define um Sistema de Gestão de Informações de Privacidade (PIMS), diferentes documentos são criados, como a Declaração de Aplicabilidade (SoA).

O que é uma SoA?

A) A SoA calcula a probabilidade de o processamento de dados resultar em alto risco para as pessoas.
B) A SoA registra onde e como os dados pessoais dos funcionários e clientes são processados.
C) A SoA especifica que controles devem ser aplicados para gerenciar ou minimizar os riscos no PIMS.

A) Incorreto. Isso é o que a Avaliação de Impacto sobre a Proteção de Dados (DPIA) faz.
B) Incorreto. Isso é registrado nos Registros das Atividades de Tratamento (ROPA).
C) Correto. Segundo a ISO/IEC 27701, essa é a definição de uma SoA. (Literatura: B, Capítulo 4)

8 / 40
É fundamental para um Sistema de Gestão de Informações de Privacidade (PIMS), tanto a curto quanto a longo prazo, poder demonstrar como as políticas corporativas, os procedimentos operacionais e as instruções de trabalho são formulados. Isso garante a rastreabilidade das ações para decisões e políticas de gestão e a reprodutibilidade dos resultados.

Essa afirmação faz referência a que requisito do PIMS?

A) Auditoria
B) Documentação
C) Avaliação do sistema de gestão
D) Declaração de Aplicabilidade (SoA)

A) Incorreto. Um programa de auditoria do sistema de gestão tem como principal objetivo monitorar a conformidade entre os requisitos do sistema de gestão e as práticas de trabalho.
B) Correto. É provável que a organização ache útil manter registros dos desenvolvimentos e das atividades, aos quais poderá recorrer, se necessário, no futuro. Muitos desses itens são registrados e a organização mantém os dados pelo tempo que for preciso. Criar registros das atividades operacionais para fins de avaliação e tomada de decisão também é importante. (Literatura: B, Capítulo 3)
C) Incorreto. A avaliação do sistema de gestão é um procedimento em que a alta gestão avalia o progresso do PIMS, do seu lançamento até a operação. Esse procedimento assegura que o progresso do PIMS seja eficaz e cumpra os requisitos corporativos ao longo do tempo.
D) Incorreto. A SoA é um documento que detalha quais controles são aplicados ou não no PIMS.

9 / 40
Por que a alta gestão deve avaliar o progresso do Sistema de Gestão de Informações de Privacidade (PIMS)?

A) Para assegurar que o PIMS esteja em conformidade com todos os requisitos legais relevantes
B) Para assegurar que o PIMS tenha controles de privacidade suficientes para mitigar riscos
C) Para assegurar que o PIMS seja auditado regularmente e esteja produzindo documentos
D) Para assegurar que o PIMS seja eficaz e cumpra os requisitos corporativos

A) Incorreto. Essa é uma responsabilidade que faz parte do PIMS, não o objetivo da avaliação do sistema de gestão.
B) Incorreto. Essa é uma responsabilidade que faz parte do PIMS, não o objetivo da avaliação do sistema de gestão.
C) Incorreto. Essa é uma responsabilidade que faz parte do PIMS, não o objetivo da avaliação do sistema de gestão.
D) Correto. Convém que a alta gestão avalie o progresso do PIMS, do seu lançamento até a operação, assegurando que seja eficaz e cumpra os requisitos corporativos ao longo do tempo. (Literatura: B, Capítulo 3)

10 / 40
O Sistema de Gestão de Informações de Privacidade (PIMS) pode ser auditado por diversas razões.

Segundo a ISO/IEC 27701, qual é o **principal** objetivo das auditorias do PIMS?

A) Confirmar que os requisitos das normas nacionais e internacionais relevantes sejam mantidos
B) Identificar áreas específicas de preocupação e abordar a seleção dos processos individuais de trabalho
C) Incluir atualizações das mudanças relevantes na legislação e na regulamentação e sua interpretação
D) Monitorar a conformidade entre os requisitos do sistema de gestão e as práticas de trabalho

A) Incorreto. Confirmar os requisitos das normas internacionais aplicáveis faz parte dos objetivos. Entretanto, o principal objetivo é monitorar a conformidade entre os requisitos do sistema de gestão e as práticas de trabalho.
B) Incorreto. Isso faz parte das melhorias que a auditoria pode proporcionar, mas não é um objetivo principal.
C) Incorreto. Isso faz parte das oportunidades de melhoria que a auditoria pode proporcionar, mas não é um objetivo principal.
D) Correto. O principal objetivo de um programa de auditoria do sistema de gestão é monitorar a conformidade entre os requisitos do sistema de gestão e as práticas de trabalho. (Literatura: B, Capítulo 3)

11 / 40
Uma organização implementa um Sistema de Gestão de Informações de Privacidade (PIMS). Os requisitos específicos devem ser baseados em regras locais e requisitos contratuais.

Qual deve ser o próximo passo para a equipe jurídica da organização?

A) Contratar assessoria e orientação jurídicas locais e aplicar a ISO/IEC 27701 como norma contratual para clientes e fornecedores
B) Pesquisar as melhores práticas internacionais aplicáveis e revisar todos os contratos que envolvam processamento de dados pessoais
C) Mapear a legislação aplicável e as sanções legais correspondentes e revisar todos os contratos que envolvam processamento de dados pessoais
D) Solicitar orientação da autoridade de fiscalização local e aplicar a ISO/IEC 27701 como norma contratual para clientes e fornecedores

A) Incorreto. Os requisitos específicos de um PIMS precisam ser determinados considerando as regras locais apropriadas e os requisitos contratuais. Pode ser que não haja necessidade de solicitar assessoria jurídica local, caso a equipe jurídica já esteja familiarizada com a legislação local, e nem todos os contratos terão necessariamente a ISO/IEC 27701 como requisito contratual.
B) Incorreto. Os requisitos específicos de um PIMS devem ser determinados considerando os requisitos contratuais e a legislação local aplicável, não as melhores práticas internacionais.
C) Correto. Os requisitos específicos de um PIMS precisam ser determinados considerando as regras locais apropriadas e os requisitos contratuais. (Literatura: B, Capítulo 4)
D) Incorreto. Os requisitos específicos de um PIMS precisam ser determinados considerando as regras locais apropriadas e os requisitos contratuais. Não há necessidade de solicitar orientação da autoridade de fiscalização local, e nem todos os contratos terão necessariamente a ISO/IEC 27701 como requisito contratual.

12 / 40
Uma organização está efetuando uma fusão com outra empresa. A organização já tem um Sistema de Gestão de Informações de Privacidade (PIMS).

A conclusão do processo depende da demonstração de que todas as operações de processamento de dados pessoais seguem a ISO/IEC 27701 e a legislação aplicável.

Qual é o meio **mais** adequado para demonstrar isso?

A) Um relatório de Avaliação de Impacto sobre a Proteção de Dados (DPIA)
B) Um relatório de Avaliação de Impacto à Privacidade (PIA)
C) Um relatório recente de auditoria do PIMS
D) Um relatório sobre Declaração de Aplicabilidade (SoA)

A) Incorreto. Um relatório DPIA registra uma avaliação de riscos, normalmente realizada antes da implementação de um projeto. Um DPIA é exigido para processamentos que provavelmente resultarão em alto risco para os indivíduos.
B) Incorreto. Um relatório PIA registra uma avaliação de riscos, normalmente realizada antes da implementação de um projeto. Um DPIA é exigido para processamentos que provavelmente resultarão em alto risco para os indivíduos.
C) Correto. Relatórios de auditoria identificam conformidade e não conformidade entre a prática real e os requisitos. (Literatura: B, Capítulo 3)
D) Incorreto. A SoA (que é uma declaração, não um relatório) é um documento que detalha quais controles são aplicados no PIMS e quais não são, porém não há garantia de que isso reflita a prática real. A SoA também não garante conformidade legal.

13 / 40

Uma pequena organização desenvolveu um serviço de software bem-sucedido. Como seu serviço é um enorme sucesso, a organização precisa de uma solução de nuvem (cloud) mais robusta e, assim, deve selecionar um fornecedor externo de nuvem.

A organização possui certificação ISO/IEC 27701. Durante a busca por um fornecedor, a organização encontra vários fornecedores de nuvem, alguns deles com certificação ISO/IEC 27701, mas outros sem.

Como a certificação ISO/IEC 27701 ajuda na seleção do fornecedor?

A) A certificação ISO/IEC 27701 de um fornecedor inclui uma análise de custo-benefício, o que garante menores custos para os serviços.
B) A certificação ISO/IEC 27701 de um fornecedor reduz a necessidade de auditar os fornecedores, o que é mais fácil para a organização.
C) A certificação ISO/IEC 27701 da organização tem procedimentos para o processamento de dados, os quais se extendem a qualquer fornecedor.
D) A certificação ISO/IEC 27701 da organização exige um fornecedor com certificação ISO/IEC 27701, o que limita as escolhas.

A) Incorreto. Uma certificação ISO/IEC 27701 não contém uma lista de fornecedores. Como o controlador é sempre responsável por garantir a proteção de dados, ele deve auditar os fornecedores. Fornecedores com certificação ISO/IEC 27701 já foram auditados.
B) Correto. É mais provável que um fornecedor com certificação ISO/IEC 27701 processe dados pessoais de forma responsável e possa cooperar com mais eficácia após uma violação de dados pessoais. (Literatura: B, Capítulo 5)
C) Incorreto. Como o controlador será sempre responsável por garantir a proteção de dados, ele deve auditar os fornecedores. Fornecedores com certificação ISO/IEC 27701 já foram auditados.
D) Incorreto. Uma certificação ISO/IEC 27701 não exige que todos os fornecedores tenham a mesma certificação. Como o controlador será sempre responsável por garantir a proteção de dados, ele deve auditar os fornecedores. Fornecedores com certificação ISO/IEC 27701 já foram auditados.

14 / 40
Quando se trabalha em função da certificação ISO/IEC 27701, há diversos sistemas de gestão envolvidos. Dois desses sistemas são:

- Sistema de Gestão de Informações de Privacidade (PIMS)
- Sistema de Gestão de Segurança da Informação (ISMS)

O que é verdadeiro sobre esses sistemas?

A) As auditorias do ISMS e do PIMS podem ser combinadas ou realizadas separadamente, embora os requisitos do PIMS dependam da manutenção do ISMS.
B) As auditorias do ISMS e do PIMS nunca devem ser realizadas em conjunto, pois os requisitos de sistema do PIMS e do ISMS não dependem uns dos outros.
C) O ISMS faz parte do PIMS e trata da proteção da informação, uma vez que o ISMS considera uma abordagem de risco de negócios para os dados pessoais.

A) Correto. As duas auditorias podem ser combinadas. A certificação ISO/IEC 27701 depende, em parte, das certificações e auditorias ISO/IEC 27001. (Literatura B, Capítulo 6)
B) Incorreto. As duas auditorias podem ser combinadas ou realizadas separadamente. A certificação ISO/IEC 27701 depende, em parte, das certificações e auditorias ISO/IEC 27001.
C) Incorreto. O ISMS serve para dar uma ideia dos riscos para todos os dados em geral na organização, além de mitigar esses riscos por meio de controles no ISMS. O ISMS não foca especificamente os dados pessoais.

15 / 40
Uma organização implementa um Sistema de Gestão de Informações de Privacidade (PIMS). O GDPR exige que "dados pessoais sejam processados de forma a garantir a segurança e a confidencialidade adequadas dos dados pessoais [...]".

Qual é a relação entre essa exigência e a norma ISO/IEC 27701?

A) Os princípios GDPR de integridade e confidencialidade formam a base do PIMS, que é exigido pela norma ISO/IEC 27701.
B) Os princípios GDPR de licitude, lealdade e transparência contribuem para o PIMS e para o Sistema de Gestão de Segurança da Informação (ISMS).
C) O princípio GDPR da limitação de finalidade estabelece com exatidão como os dados que fazem parte do PIMS devem ou não ser utilizados.
D) O princípio GDPR da limitação de armazenamento especifica o tempo que os dados pessoais ficam no PIMS antes do processamento.

A) Correto. O princípio da segurança de dados pessoais é condição essencial para um PIMS. Os princípios GDPR que determinam qual é a segurança apropriada dos dados pessoais são chamados "integridade e confidencialidade" e são, portanto, a base do PIMS. (Literatura: B, Capítulo 3 e GDPR, Art. 5.1.f)
B) Incorreto. O PIMS pode até contribuir para "licitude, lealdade e transparência", mas o princípio da "integridade e confidencialidade" é a base do PIMS e, portanto, é o que mais se relaciona com o PIMS.
C) Incorreto. O PIMS pode até contribuir para "limitação da finalidade", mas o princípio da "integridade e confidencialidade" é a base do PIMS e, portanto, é o que mais se relaciona com o PIMS.
D) Incorreto. O PIMS pode até contribuir para "limitação de armazenamento", mas o princípio da "integridade e confidencialidade" é a base do PIMS e, portanto, é o que melhor se relaciona com o PIMS.

16 / 40
A norma ISO/IEC 27701 contém um capítulo dedicado a diretrizes adicionais, que se alinha com a norma ISO/IEC 27002.

Que tipo de recomendação **não** está incluído nesse capítulo?

A) Desenvolver políticas de privacidade separadas das políticas de segurança da informação ou combinadas com elas
B) Assegurar pelo menos treinamento de conscientização para todos os funcionários que manejem ou processem dados pessoais
C) Rotular todos os dados de modo claro para identificar onde os dados pessoais são armazenados ou, de outra forma, processados
D) Planejar auditorias internas e externas em um intervalo específico, dependendo do âmbito da auditoria

A) Incorreto. A recomendação de desenvolver políticas de privacidade faz parte desse capítulo.
B) Incorreto. A recomendação de assegurar pelo menos algum treinamento está nesse capítulo.
C) Incorreto. A recomendação de rotular todos os dados de modo claro faz parte desse capítulo.
D) Correto. Apesar de a norma ISO/IEC 27701 não lidar especificamente com conformidade e auditorias, essa norma foi desenvolvida para se alinhar com as normas ISO/IEC 27001 e ISO/IEC 27002, que contêm essas categorias. (Literatura: B, Capítulo 5)

17 / 40
Aplicar controles do Sistema de Gestão de Informações de Privacidade (PIMS) para gerenciar riscos não é tarefa fácil, e é recomendado passar por todas as etapas.

A primeira etapa é criar um conjunto de controles para gerenciar riscos. As outras etapas estão listadas abaixo (em ordem aleatória):

1. Comparar os controles ao Anexo A ou B da ISO/IEC 27701
2. Elaborar a Declaração de Aplicabilidade (SoA)
3. Implementar os controles de forma eficaz

Qual é a ordem **correta** das outras etapas?

A) 1, 2, 3
B) 1, 3, 2
C) 2, 1, 3
D) 2, 3, 1

A) Incorreto. A ordem correta é 1, 3, 2.
B) Correto. Após a criação de um conjunto de controles, os controles devem ser comparados aos Anexos da ISO/IEC 27701 para assegurar o nível de segurança exigido contra riscos de privacidade. Em seguida, os controles devem ser implementados, e a SoA segue por último. (Literatura: B, Capítulo 4)
C) Incorreto. A ordem correta é 1, 3, 2.
D) Incorreto. A ordem correta é 1, 3, 2.

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	D	25	B
6	A	26	B
7	C	27	C
8	B	28	A
9	D	29	D
10	D	30	D
11	C	31	B
12	C	32	B
13	B	33	A
14	A	34	C
15	A	35	B
16	D	36	D
17	B	37	D
18	A	38	D
19	B	39	A
20	B	40	C

Contato EXIN

www.exin.com