examundo

Simulado CISSP em português

50 questões com respostas. Os guias e as traduções foram feitos e revisados por software. Ainda não foram revisados por nenhuma pessoa.

Atualizado em 25 de novembro de 2026 · examundo.tech/pt/cissp/

Domínio 3: Arquitetura e engenharia de segurança

1. Qual conceito criptográfico garante que o remetente não possa negar que enviou uma mensagem?

Which cryptographic concept ensures that a sender cannot deny having sent a message?

A. Confidencialidade
B. Integridade
C. Não repúdio
D. Autenticação

---

2. Um arquiteto de segurança está projetando um sistema para proteger dados governamentais classificados. Qual modelo de segurança deve ser implementado para impedir o fluxo de informações de níveis de classificação mais altos para níveis mais baixos?

A security architect is designing a system to protect classified government data. Which security model should be implemented to prevent information from flowing from higher classification levels to lower classification levels?

A. Modelo Bell-LaPadula
B. Modelo Clark-Wilson
C. Modelo Brewer-Nash
D. Modelo de integridade Biba

---

3. Uma aplicação de e-commerce precisa trocar com segurança chaves de criptografia simétrica com os navegadores dos clientes. Qual protocolo deve ser usado?

An e-commerce application needs to securely exchange symmetric encryption keys with customers' browsers. Which protocol should be used?

A. TLS com troca de chaves Diffie-Hellman
B. IPsec em modo de transporte com chaves pré-compartilhadas
C. Kerberos com tickets de concessão de tickets (TGT)
D. S/MIME com criptografia baseada em certificados

---

4. Uma instalação de alta segurança exige integridade de duas pessoas (two-person integrity) para acessar a sala de servidores. Que tipo de controle de acesso físico implementa esse requisito?

A secure facility requires two-person integrity for access to the server room. What type of physical access control implements this requirement?

A. Fechadura com senha numérica (cipher lock) e troca trimestral do código
B. Leitor de cartão com gravação em vídeo de todas as entradas
C. Leitor biométrico com teclado de PIN para autenticação multifator
D. Eclusa (mantrap) de dupla autenticação que exige duas pessoas autorizadas

---

5. Qual dos princípios de segurança a seguir MELHOR descreve a defesa em profundidade (defense in depth)?

Defense in depth is BEST described as which of the following security principles?

A. Implementar várias camadas de controles de segurança para proteger os ativos

B. Projetar sistemas para falhar em um estado seguro quando ocorrem erros

C. Conceder aos usuários o mínimo de acesso necessário para fazer seu trabalho

D. Reforçar a segurança dos sistemas (hardening), removendo serviços e recursos desnecessários

---

6. Uma eclusa de segurança (mantrap) é classificada como que tipo de controle de segurança física?

A mantrap is classified as which type of physical security control?

A. Controle preventivo

B. Controle compensatório

C. Controle detectivo

D. Controle corretivo

---

7. Um sistema financeiro deve impedir que usuários não autorizados modifiquem registros de transações, mas permitir leitura para auditoria. Qual modelo de segurança atende MELHOR a esse requisito?

A financial system must prevent unauthorized users from modifying transaction records while allowing read access for auditing. Which security model BEST supports this requirement?

A. Modelo de confidencialidade Bell-LaPadula

B. Modelo Brewer-Nash (Chinese Wall)

C. Modelo de integridade Biba

D. Modelo de controle de acesso Graham-Denning

---

8. Uma organização está implementando um novo sistema criptográfico para proteger dados em repouso em um ambiente de nuvem. O sistema deve atender a exigências regulatórias de custódia de chaves (key escrow) e manter independência operacional em relação ao provedor de nuvem. Qual abordagem atende MELHOR aos dois requisitos?

An organization is implementing a new cryptographic system to protect data at rest in a cloud environment. The system must support regulatory compliance requirements for key escrow while maintaining operational independence from the cloud provider. Which approach BEST satisfies both requirements?

A. Implementar criptografia no lado do cliente, com chaves gerenciadas em um HSM local, e entregar cópias custodiadas a um serviço terceirizado de custódia de chaves

B. Implantar criptografia em envelope com chaves gerenciadas pelo cliente, armazenadas no serviço de gerenciamento de chaves do provedor de nuvem

C. Implementar Transparent Data Encryption na camada do banco de dados, com chaves guardadas na configuração da aplicação

D. Usar o serviço nativo de criptografia do provedor de nuvem, com rotação automática de chaves e backup em outra região da nuvem

---

9. Um arquiteto de segurança deve escolher um modelo formal de segurança para um sistema de inteligência militar que trata documentos de vários níveis de classificação. O requisito PRINCIPAL é impedir que a informação flua para níveis de classificação mais baixos. Qual modelo é o MAIS adequado?

A security architect must select a formal security model for a military intelligence system handling documents at multiple classification levels. The PRIMARY requirement is preventing information from flowing to lower classification levels. Which model is MOST appropriate?

A. Modelo de integridade Biba

B. Modelo de integridade Clark-Wilson

C. Modelo Bell-LaPadula

D. Modelo Brewer-Nash (Chinese Wall)

---

10. Um cano de água estoura acima da sala de servidores de um data center. Qual controle ambiental teria sido o MELHOR para evitar danos causados pela água nos equipamentos críticos?

A data center experiences a water pipe burst above the server room. Which environmental control would have BEST prevented water damage to critical equipment?

A. Sistemas de pressão de ar positiva para impedir a entrada de umidade

B. Sensores de detecção de água com válvulas de corte automático

C. Piso elevado para colocar os equipamentos acima do nível do chão

D. Sistemas de climatização (HVAC) com monitoramento de umidade e alertas

---

Domínio 7: Operações de segurança

11. Qual prática de gerenciamento de configuração detecta MELHOR alterações não autorizadas nas configurações de servidores de produção?

Which configuration management practice BEST detects unauthorized changes to production server configurations?

A. Comparar regularmente as configurações reais com as linhas de base aprovadas

B. Aprovar automaticamente as alterações feitas por administradores privilegiados

C. Revisar registros de compra de hardware sem examinar as configurações dos servidores

D. Substituir as linhas de base aprovadas pelas configurações atuais após cada varredura

12. Em uma equipe de resposta a incidentes, qual função é responsável por identificar e conter o incidente inicialmente?

Which role in an incident response team is responsible for initially identifying and containing the incident?

A. Coordenador do incidente (incident coordinator)

B. Analista forense (forensic analyst)

C. Primeiro respondente (first responder)

D. Responsável pela comunicação (communications lead)

13. Um incidente que causa pequena interrupção em sistemas não críticos, sem perda de dados, normalmente seria classificado em qual nível de severidade?

An incident that causes minor disruption to non-critical systems with no data loss would typically be classified as what severity level?

A. Crítico

B. Alto

C. Baixo

D. Emergência

14. Em uma revisão pós-incidente, a equipe constata que o atacante manteve persistência por 87 dias antes de ser detectado. Qual melhoria de operações de segurança reduziria com MAIS eficácia o tempo de permanência (dwell time) em casos futuros?

During a post-incident review, the team identifies that the attacker maintained persistence for 87 days before detection. Which security operations improvement would MOST effectively reduce future dwell time?

A. Exigir treinamento obrigatório de conscientização em segurança para todos os funcionários a cada trimestre

B. Implantar firewalls adicionais nos limites de segmentação da rede

C. Aumentar a frequência das varreduras de vulnerabilidades de mensal para semanal

D. Implementar monitoramento contínuo de segurança com análise comportamental e caça a ameaças

15. A defesa em profundidade na segurança física costuma incluir várias camadas. Qual das opções a seguir apresenta a ordem CORRETA, da camada mais externa para a mais interna?

Defense in depth for physical security typically includes multiple layers. Which of the following represents the CORRECT order from outermost to innermost layer?

A. Cerca do perímetro, controle de acesso ao prédio, controle de acesso à sala, travas nos equipamentos

B. Travas nos equipamentos, controle de acesso à sala, controle de acesso ao prédio, cerca do perímetro

C. Controle de acesso à sala, travas nos equipamentos, cerca do perímetro, controle de acesso ao prédio

D. Controle de acesso ao prédio, cerca do perímetro, travas nos equipamentos, controle de acesso à sala

---

16. Qual tipo de evidência consiste em cópias ou reproduções da evidência original?

Which type of evidence consists of copies or reproductions of original evidence?

A. Evidência secundária

B. Melhor evidência (best evidence)

C. Evidência por ouvir dizer (hearsay)

D. Evidência corroborativa

---

17. Uma organização está definindo seus objetivos de recuperação de desastres. O negócio exige que os sistemas críticos sejam restaurados em até 4 horas após um desastre. Qual métrica de recuperação esse requisito define?

An organization is defining its disaster recovery objectives. The business requires that critical systems must be restored within 4 hours of a disaster. This requirement defines which recovery metric?

A. Tempo médio de reparo (MTTR)

B. Tempo máximo tolerável de inatividade (MTD)

C. Objetivo de tempo de recuperação (RTO)

D. Objetivo de ponto de recuperação (RPO)

---

18. O plano de recuperação de desastres de uma organização exige um objetivo de tempo de recuperação (RTO) de 4 horas e um objetivo de ponto de recuperação (RPO) de 1 hora para o banco de dados de clientes. Qual estratégia de backup atende MELHOR a esses requisitos?

An organization's disaster recovery plan requires a recovery time objective (RTO) of 4 hours and a recovery point objective (RPO) of 1 hour for its customer database. Which backup strategy BEST meets these requirements?

A. Backups diferenciais a cada 4 horas armazenados no local

B. Backups incrementais a cada 6 horas com fitas armazenadas fora do local

C. Backups completos semanais com backups incrementais diários

D. Backups completos noturnos com replicação contínua do banco de dados para um site morno

---

19. Um primeiro respondente chega a um servidor de produção comprometido que ainda está ligado e processando transações. Segundo as diretrizes da RFC 3227, qual fonte de dados deve ser coletada PRIMEIRO durante a aquisição de evidências em sistema ativo?

A first responder arrives at a compromised production server that is still powered on and actively processing transactions. Per RFC 3227 guidelines, which data source should be collected FIRST during live evidence acquisition?

A. Registradores da CPU e memória cache

B. Conteúdo da RAM do sistema (memória principal)

C. Cache ARP e entradas da tabela de roteamento

D. Sistema de arquivos temporário e dados da área de troca (swap)

---

20. Um departamento de TI segue um processo formal de gerenciamento de mudanças. Qual etapa de autorização deve ocorrer ANTES de implementar uma mudança nos sistemas de produção?

An IT department follows a formal change management process. Which authorization step should occur BEFORE implementing a change to production systems?

A. Testar a mudança em um ambiente fora da produção
B. Aprovação do Comitê Consultivo de Mudanças (CAB, Change Advisory Board)
C. Documentar a mudança no banco de dados de gerenciamento de configuração (CMDB)
D. Comunicar todas as partes interessadas afetadas

Domínio 4: Comunicação e segurança de redes

21. Uma organização implementa 802.1X para controle de acesso à rede. Qual componente atua como intermediário entre o suplicante (supplicant) e o servidor de autenticação?

An organization implements 802.1X for network access control. Which component acts as the intermediary between the supplicant and the authentication server?

A. Autoridade certificadora (certificate authority)
B. Controlador de rede (network controller)
C. Autenticador (authenticator)
D. Proxy RADIUS (RADIUS proxy)

22. Uma organização implementa WPA3-Enterprise para a segurança sem fio. Qual framework de autenticação o WPA3-Enterprise usa?

An organization implements WPA3-Enterprise for wireless security. What authentication framework does WPA3-Enterprise use?

A. 802.1X com EAP
B. Filtragem de endereços MAC
C. Chave pré-compartilhada (PSK)
D. LEAP

23. Uma organização precisa oferecer acesso remoto seguro a funcionários em campo, que se conectam de vários países com internet instável. A solução deve suportar tráfego TCP e UDP e funcionar na maioria dos firewalls. Qual protocolo de VPN é o MAIS adequado?

An organization needs to provide secure remote access for field personnel who connect from various international locations with unreliable internet connectivity. The solution must support both TCP and UDP traffic and work through most firewalls. Which VPN protocol is MOST appropriate?

A. PPTP
B. VPN SSL/TLS
C. L2TP/IPSec
D. IPSec em modo túnel

24. A aplicação web de uma empresa sofre um pico de tráfego vindo de várias origens, o que sobrecarrega a capacidade de resposta do servidor. Qual é o ataque MAIS provável?

A company's web application experiences a surge in traffic from multiple sources, overwhelming the server's ability to respond. Which attack is MOST likely occurring?

A. Homem no meio (Man-in-the-Middle, MitM)
B. Falsificação de solicitação entre sites (CSRF)
C. Sequestro de sessão (session hijacking)
D. Negação de serviço distribuída (DDoS)

25. Qual camada do modelo OSI é responsável pela entrega confiável de dados de ponta a ponta, pelo controle de fluxo e pela recuperação de erros entre os hosts que se comunicam?

Which OSI model layer is responsible for end-to-end reliable data delivery, flow control, and error recovery between communicating hosts?

A. Camada 2: Enlace de dados
B. Camada 4: Transporte
C. Camada 3: Rede
D. Camada 5: Sessão

---

26. Uma organização sofre ataques de SYN flood contra seu servidor web. Qual técnica de defesa seria a MAIS eficaz?

An organization is experiencing SYN flood attacks against its web server. Which defensive technique would be MOST effective?

A. Desativar os timestamps do TCP
B. Implementar filtragem de endereços MAC
C. Limitar a taxa de pacotes ICMP
D. SYN cookies

---

27. Ao implementar TLS em uma aplicação web, qual versão deve ser considerada o padrão MÍNIMO aceitável para novas implantações?

When implementing TLS for a web application, which version should be considered the MINIMUM acceptable standard for new deployments?

A. TLS 1.0
B. SSL 3.0
C. TLS 1.2
D. TLS 1.1

---

28. Uma instituição financeira exige autenticação mútua entre clientes e servidores. Qual recurso do TLS oferece essa capacidade?

A financial institution requires mutual authentication between clients and servers. Which TLS feature provides this capability?

A. Retomada de sessão
B. Autenticação por certificado de cliente
C. Sigilo futuro perfeito (Perfect Forward Secrecy, PFS)
D. Indicação de nome do servidor (SNI)

---

29. Um sistema de detecção de intrusão (IDS) está gerando muitos alertas para padrões normais de tráfego. Que tipo de erro está ocorrendo?

An intrusion detection system (IDS) is generating numerous alerts for normal traffic patterns. What type of error is occurring?

A. Falso positivo
B. Falso negativo
C. Verdadeiro negativo
D. Verdadeiro positivo

---

30. Uma multinacional sofre interrupções de roteamento na internet. A investigação mostra que um provedor (ISP) estrangeiro está anunciando via BGP o espaço de endereços IP da empresa. Qual é o ataque MAIS provável e qual é a diferença PRINCIPAL em relação ao envenenamento de rotas (route poisoning)?

A multinational corporation experiences Internet routing disruptions. Investigation reveals that a foreign ISP is advertising the company's IP address space via BGP. Which attack is MOST likely occurring, and what is the PRIMARY difference from route poisoning?

A. Sequestro de BGP (BGP hijacking); ele ataca a propriedade do prefixo, e não as métricas de rota

B. Envenenamento de rotas; ele afeta o roteamento externo, e não os protocolos internos de vetor de distância

C. Oscilação de rotas (route flapping); ela causa interrupção intermitente, e não redirecionamento persistente do tráfego

D. Prepend de AS path; ele manipula números de sistemas autônomos para influenciar decisões de roteamento

---

Domínio 2: Segurança de ativos

31. O padrão de segurança de base (baseline) de uma empresa de serviços financeiros exige criptografia AES-256 para todos os dados de clientes. Uma avaliação de risco revela que alguns sistemas legados não suportam AES-256. Qual processo o arquiteto de segurança deve aplicar para tratar essa limitação?

A financial services firm's baseline security standard requires AES-256 encryption for all customer data. A risk assessment reveals that certain legacy systems cannot support AES-256. What process should the security architect apply to address this constraint?

A. Adaptação (tailoring)

B. Controles compensatórios

C. Delimitação de escopo (scoping)

D. Aceitação do risco

32. Segundo a política de classificação do governo dos EUA, qual rótulo se aplica à informação cuja divulgação não autorizada poderia razoavelmente causar “dano grave” à segurança nacional?

Under U.S. government classification policy, which label applies to information whose unauthorized disclosure could reasonably be expected to cause 'serious damage' to national security?

A. Secreto (Secret)

B. Informação Não Classificada Controlada (CUI)

C. Confidencial (Confidential)

D. Ultrassecreto (Top Secret)

33. Quem é o responsável final por determinar o nível de classificação dos dados em uma organização?

Who is ultimately responsible for determining the classification level of data within an organization?

A. Custodiante dos dados (data custodian)

B. Proprietário dos dados (data owner)

C. Administrador de segurança

D. Diretor de segurança da informação (CISO)

34. Uma organização deve manter certa documentação de conformidade com a HIPAA por no mínimo 6 anos segundo a HIPAA e por no mínimo 10 anos segundo uma lei estadual aplicável. Qual prazo de retenção o gerente de segurança deve recomendar para essa documentação?

An organization must retain certain HIPAA compliance documentation for a minimum of 6 years under HIPAA and a minimum of 10 years under an applicable state law. What retention period should the security manager recommend for that documentation?

A. 8 anos, como meio-termo entre os requisitos
B. 10 anos, para atender ao requisito mais rigoroso
C. Retenção por prazo indefinido, para evitar riscos de conformidade
D. 6 anos, para cumprir os requisitos federais da HIPAA

---

35. Uma multinacional armazena dados de clientes da UE em data centers de nuvem. Clientes franceses temem que esses dados possam ser exigidos legalmente por entidades de fora da UE. Qual princípio atende MELHOR a essa preocupação?

A multinational corporation stores EU customer data in cloud data centers. French customers are concerned about their data being legally compelled from non-EU entities. Which principle BEST addresses this concern?

A. Soberania de dados (data sovereignty)
B. Localização de dados (data localization)
C. Redundância geográfica
D. Residência de dados (data residency)

---

36. A política de retenção de dados de uma organização exige manter os registros de transações de clientes por sete anos. Ao fim desse período, qual é a PRIMEIRA etapa do processo de descarte?

An organization's data retention policy requires keeping customer transaction records for seven years. At the end of this period, what is the FIRST step in the disposal process?

A. Verificar se não há ordem de preservação legal em vigor
B. Sobrescrever os dados com uma ferramenta compatível com DoD 5220.22-M
C. Destruir fisicamente todas as mídias de armazenamento que contêm os dados
D. Remover todas as cópias de backup do armazenamento externo

---

37. Qual função tem a responsabilidade PRINCIPAL de determinar o nível de classificação atribuído a um ativo de dados da organização?

Which role is PRIMARILY responsible for determining the classification level assigned to an organizational data asset?

A. Curador de dados (data steward)
B. Proprietário dos dados (data owner)
C. Custodiante dos dados (data custodian)
D. Operador de dados (data processor)

---

38. Uma organização de saúde está desativando notebooks que armazenavam prontuários de pacientes sem criptografia. Qual método de sanitização oferece o MAIOR grau de garantia de irrecuperabilidade dos dados?

A healthcare organization is decommissioning laptops that stored unencrypted patient health records. Which sanitization method provides the HIGHEST assurance of data irrecoverability?

A. Destruição física por trituração ou incineração
B. Apagamento criptográfico das chaves de criptografia
C. Sobrescrita em sete passagens com dados aleatórios
D. Desmagnetização (degaussing) com um desmagnetizador Tipo I ou Tipo II

---

39. Uma organização está classificando um novo banco de dados com avaliações de desempenho de funcionários, informações salariais e informações de identificação pessoal (PII). A divulgação não autorizada poderia causar desvantagem competitiva e possível responsabilidade legal. Qual nível de classificação é o MAIS adequado?

An organization is classifying a new database containing employee performance reviews, salary information, and personally identifiable information (PII). The unauthorized disclosure could result in competitive disadvantage and potential legal liability. What classification level is MOST appropriate?

A. Secreto
B. Confidencial
C. Uso interno
D. Público

---

40. Uma organização de saúde precisa definir quem responde por garantir que os prontuários dos pacientes sejam classificados corretamente, retidos conforme as exigências regulatórias e acessíveis somente a pessoas autorizadas. Quem tem a responsabilidade PRINCIPAL por essas decisões?

A healthcare organization must determine accountability for ensuring patient health records are properly classified, retained according to regulatory requirements, and accessible only to authorized personnel. Who has PRIMARY responsibility for these decisions?

A. Operador de dados (Data Processor)
B. Diretor de segurança da informação (CISO)
C. Proprietário dos dados (Data Owner)
D. Custodiante dos dados (Data Custodian)

Domínio 1: Segurança e gestão de riscos

41. Um analista de segurança descobre que um funcionário vem acessando arquivos confidenciais de RH sem justificativa de negócio. A função do funcionário não exige acesso a dados de RH. Qual é o princípio de segurança que MAIS provavelmente foi violado?

A security analyst discovers an employee has been accessing confidential HR files without business justification. The employee's role does not require access to HR data. Which security principle was MOST likely violated?

A. Necessidade de conhecer (need-to-know)
B. Defesa em profundidade (defense in depth)
C. Separação de funções (separation of duties)
D. Privilégio mínimo (least privilege)

---

42. O CISO de uma organização quer alinhar o programa de segurança aos objetivos de negócio. Qual framework é o MAIS adequado para essa finalidade?

An organization's CISO wants to align the security program with business objectives. Which framework is BEST suited for this purpose?

A. ISO 27002
B. COBIT
C. CIS Controls
D. NIST SP 800-53

---

43. Uma organização de saúde sofre um ataque de ransomware que criptografa prontuários de pacientes. O CISO relata o incidente ao conselho de administração. Qual conceito o CISO está demonstrando?

A healthcare organization suffers a ransomware attack that encrypts patient records. The CISO reports the incident to the board. Which concept is the CISO demonstrating?

A. Devida diligência (due diligence)
B. Separação de funções
C. Regra do homem prudente (prudent man rule)
D. Devido cuidado (due care)

---

44. Um CISO está explicando à diretoria executiva a relação entre o Planejamento de Continuidade de Negócios (BCP) e o Planejamento de Recuperação de Desastres (DRP). Qual afirmação é a MAIS precisa?

A CISO is explaining the relationship between Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) to the executive board. Which statement is MOST accurate?

A. O BCP trata apenas de sistemas e dados de TI, enquanto o DRP cobre todas as operações do negócio
B. BCP e DRP são termos intercambiáveis que descrevem o mesmo processo de planejamento
C. O DRP é o plano estratégico mais amplo, que contém o BCP como componente
D. O BCP é o plano estratégico mais amplo, e o DRP é um subconjunto tático voltado à recuperação de TI

---

45. Durante um exercício de recuperação de desastres, descobre-se que as fitas de backup estão ilegíveis. Qual é a fase do ciclo de vida do BCP/DRP que MAIS provavelmente foi negligenciada?

During a disaster recovery exercise, the backup tapes are found to be unreadable. Which phase of the BCP/DRP lifecycle was MOST likely neglected?

A. Avaliação de riscos
B. Análise de impacto nos negócios (BIA)
C. Desenvolvimento do plano
D. Testes e exercícios

---

46. Um analista de riscos determina que um servidor de arquivos tem 20% de probabilidade anual de ser comprometido por ransomware, com perda estimada de US$ 50.000 por incidente. Qual é a Expectativa de Perda Anualizada (ALE)?

A risk analyst determines that a file server has a 20% annual probability of being compromised by ransomware, with an estimated loss of $50,000 per incident. What is the Annualized Loss Expectancy (ALE)?

A. US$ 10.000
B. US$ 50.000
C. US$ 40.000
D. US$ 250.000

---

47. A equipe de segurança de uma organização está desenvolvendo uma nova política de controle de acesso. Qual tipo de documento deve ser o MAIS restritivo e trazer ações obrigatórias específicas?

An organization's security team is developing a new access control policy. Which document type should be MOST restrictive and provide specific mandatory actions?

A. Procedimento (procedure)
B. Padrão (standard)
C. Diretriz (guideline)
D. Política (policy)

---

48. Uma empresa está implementando os princípios de Privacidade desde a Concepção (Privacy by Design) em uma nova plataforma de dados de clientes. Qual abordagem demonstra MELHOR esse princípio?

A company is implementing Privacy by Design principles for a new customer data platform. Which approach BEST demonstrates this principle?

A. Adicionar criptografia e controles de acesso para proteger os dados dos clientes antes da implantação em produção

B. Incorporar controles de privacidade na arquitetura do sistema desde o projeto inicial, incluindo minimização de dados e configurações de privacidade padrão

C. Treinar os desenvolvedores em requisitos de privacidade e fazer revisões de código para conformidade de privacidade

D. Realizar uma avaliação de impacto à privacidade depois do desenvolvimento do sistema para identificar e corrigir riscos de privacidade

---

49. Uma empresa quer transferir o risco financeiro associado a uma violação de dados. Qual estratégia está sendo empregada?

A company wants to transfer financial risk associated with a data breach. Which strategy is being employed?

A. Mitigação do risco

B. Transferência do risco

C. Aceitação do risco

D. Evitação do risco

---

50. Durante um incidente de segurança com acesso não autorizado a sistemas financeiros, qual função tem a responsabilidade PRINCIPAL de decidir se a polícia deve ser notificada?

During a security incident involving unauthorized access to financial systems, which role is PRIMARILY responsible for determining whether law enforcement should be notified?

A. O líder da equipe de resposta a incidentes, pois tem as informações mais atuais sobre o incidente

B. O Diretor de Segurança da Informação (CISO), pois responde por todos os assuntos de segurança

C. A alta administração ou o departamento jurídico, pois é uma decisão de negócio e legal com implicações regulatórias

D. O responsável pela ligação com a polícia, pois mantém o relacionamento com órgãos externos

---

Resposta correta

1. C O não repúdio (non-repudiation) impede que alguém negue uma ação que realizou, em geral com assinaturas digitais. A chave privada do remetente cria a assinatura e a chave pública a verifica, o que prova a origem. A autenticação confirma a identidade, mas nem sempre gera prova indiscutível. Confidencialidade protege contra divulgação, e integridade garante que os dados não foram alterados, mas não prova quem os enviou.

2. A O Bell-LaPadula protege a confidencialidade com a propriedade * (sem escrita para baixo, no write down) e a propriedade de segurança simples (sem leitura para cima, no read up). Assim, a informação não vaza de níveis altos para baixos. Biba e Clark-Wilson tratam de integridade. O Brewer-Nash (Chinese Wall) evita conflito de interesses em ambientes comerciais, não controla acesso por classificação.

3. A O TLS com Diffie-Hellman permite que duas partes criem um segredo compartilhado em um canal inseguro, como no HTTPS. As variantes efêmeras (DHE/ECDHE) dão sigilo futuro perfeito (perfect forward secrecy). O IPsec serve para VPNs e exige configuração prévia. O S/MIME é para e-mail. O Kerberos exige confiança prévia e um KDC, o que não cabe em um e-commerce público.

4. D A integridade de duas pessoas exige que dois indivíduos autorizados estejam presentes, para impedir ação unilateral. A eclusa de dupla autenticação obriga os dois a se autenticarem antes da entrada. Biometria com PIN é multifator para uma só pessoa. O vídeo é controle detectivo e não impede acesso individual. Na fechadura com senha numérica, quem tem o código entra sozinho, e o código pode ser compartilhado.

5. A Defesa em profundidade, ou segurança em camadas, usa várias camadas independentes de controles. Se uma falha, as outras continuam protegendo. Exemplos: firewalls, IDS/IPS, controle de acesso, criptografia e barreiras físicas. O hardening reduz a superfície de ataque. Dar o acesso mínimo é o privilégio mínimo (least privilege). Falhar de forma segura é o princípio fail-safe/fail-secure.

6. A A eclusa (também chamada de vestíbulo de controle de acesso) é um controle preventivo. Ela exige autenticação em duas portas seguidas, com só uma aberta por vez, e assim impede o tailgating e o piggybacking antes que aconteçam. Controles detectivos identificam incidentes depois (CFTV, sensores, logs). Corretivos reparam danos. Compensatórios substituem um controle principal indisponível.

7. C O Biba protege a integridade com “sem escrita para cima” (no write up), que impede sujeitos de baixa integridade de corromper objetos de alta integridade, e “sem leitura para baixo” (no read down). Isso evita a modificação não autorizada dos registros. O Bell-LaPadula trata de confidencialidade. O Chinese Wall evita conflito de interesses. O Graham-Denning define operações entre sujeitos e objetos, sem foco em integridade. O requisito é de integridade, então Biba.

8. A A criptografia no cliente com chaves em HSM local dá independência do provedor e permite a custódia por terceiros exigida pela regulação. Isso separa a operação de criptografia do controle do provedor. O serviço nativo do provedor cria dependência. A criptografia em envelope com chaves na nuvem ainda amarra o acesso às chaves ao provedor. TDE com chaves na configuração não protege bem as chaves e não resolve a custódia.

9. C O Bell-LaPadula aplica controle de acesso obrigatório (mandatory access control) para confidencialidade, com duas regras: propriedade de segurança simples (sem leitura para cima) e propriedade * (sem escrita para baixo). Isso impede o fluxo de níveis altos para baixos, que é o requisito. Biba trata de integridade. Clark-Wilson usa transações bem formadas e separação de funções. Brewer-Nash evita conflito de interesses.

10. B Sensores de água com válvulas de corte automático detectam o vazamento, disparam alarmes e fecham o fornecimento de água, o que limita o dano. O sensor é controle detectivo e o corte automático é corretivo. O piso elevado ajuda em inundações vindas de baixo, não de um cano acima. A pressão positiva barra contaminantes externos. O monitoramento de umidade do HVAC não interrompe a água de um cano rompido.

11. A Comparar regularmente as configurações reais com as linhas de base aprovadas (baselines) detecta o desvio de configuração (configuration drift) e ajuda a investigar mudanças sem autorização. Aprovar automaticamente as mudanças de administradores ignora a autorização. Substituir a linha de base após cada varredura pode normalizar mudanças não autorizadas. Revisar compras de hardware não mostra mudanças nos servidores.

12. C O primeiro respondente é o ponto de contato inicial: identifica o incidente e toma as ações imediatas de contenção para evitar mais danos. O coordenador gerencia o processo de resposta e as atividades da equipe. O analista forense coleta e analisa evidências, inclusive as voláteis. O responsável pela comunicação cuida das comunicações internas e externas sobre o incidente.

13. C Incidentes de severidade baixa envolvem pequenas interrupções em sistemas não críticos, sem perda de dados nem impacto relevante no negócio. Os críticos envolvem falhas graves ou vazamentos que afetam as operações centrais. Os de severidade alta afetam sistemas importantes, mas não de missão crítica, ou expõem poucos dados. Emergência é ameaça imediata à vida, à segurança ou à infraestrutura crítica.

14. D O tempo de permanência (dwell time) cai com detecção ativa, não só com controles preventivos. Análise comportamental e caça a ameaças (threat hunting) identificam atividade anômala que indica comprometimento. Varreduras acham falhas, mas não ameaças ativas. O treinamento reduz o comprometimento inicial. Mais firewalls são preventivos. O MTTD (Mean Time to Detect) cai com monitoramento contínuo, UEBA e caça a ameaças.

15. A A defesa em profundidade física vai de fora para dentro: perímetro (cercas, portões, vigilantes), entrada do prédio (leitores de crachá, recepção), salas internas (sala de servidores) e, por fim, os próprios ativos (armários trancados, travas de cabo). Isso cria várias barreiras para o atacante. As outras opções trazem as camadas em ordem errada.

16. A A evidência secundária inclui cópias, fotografias ou reproduções do original. Em juízo, ela costuma ser menos preferida que a melhor evidência (best evidence), que é o original. A evidência corroborativa apoia ou confirma outra evidência, mas não é necessariamente uma cópia. Hearsay é o relato do que outra pessoa disse e em geral é inadmissível.

17. C O RTO (Recovery Time Objective) define o tempo-alvo para restaurar um sistema ou processo após uma interrupção. Restaurar em 4 horas é um RTO típico. O RPO define a perda aceitável de dados, medida em tempo. O MTD é a interrupção máxima que o negócio tolera, e o RTO deve caber dentro dele. O MTTR é uma métrica operacional do tempo médio de reparo, não um requisito do negócio.

18. D O RTO (4 horas) é o tempo de inatividade aceitável e o RPO (1 hora) é a perda de dados aceitável. Backup completo noturno com replicação contínua para um warm site é a melhor opção: a replicação contínua sustenta o RPO de 1 hora, e um warm site bem preparado e testado pode cumprir as 4 horas. Incrementais a cada 6 horas e diferenciais a cada 4 horas violam o RPO. Semanal ou diário perde até 24 horas de dados. É preciso testar a recuperação.

19. A A RFC 3227 dá uma ordem de volatilidade de exemplo que começa por registradores e cache. Depois vem um grupo com tabelas de roteamento, cache ARP, tabela de processos, estatísticas do kernel e memória. Em seguida vêm sistemas de arquivos temporários, disco, logs remotos, configuração física e topologia, e mídias de arquivamento. Por isso registradores e cache são os primeiros entre as opções. RAM e ARP estão no mesmo grupo, e a RFC não manda coletar a RAM antes das tabelas de rede.

20. B A aprovação do CAB é a etapa de autorização que deve vir antes da implementação no processo formal descrito. Ela garante que a mudança foi avaliada quanto ao risco e alinhada às necessidades do negócio. Testar e comunicar também costumam ocorrer antes, mas não autorizam nada. A documentação no CMDB é atualizada para refletir o estado já implementado. A prova CISSP valoriza governança junto com a preparação técnica.

21. C Na arquitetura 802.1X, o autenticador (em geral um switch ou ponto de acesso sem fio) é o intermediário: encaminha as solicitações do suplicante (o dispositivo cliente) ao servidor de autenticação, normalmente via RADIUS. Ele aplica o controle de acesso conforme a decisão do servidor. Um proxy RADIUS pode estar no caminho, mas não é o intermediário definido no 802.1X. A autoridade certificadora emite certificados. Controlador de rede não é componente padrão do 802.1X.

22. A O WPA3-Enterprise usa 802.1X com o Extensible Authentication Protocol (EAP) para autenticar cada usuário em um servidor RADIUS, com credenciais individuais. O WPA3-Personal usa SAE (Simultaneous Authentication of Equals) e chaves pré-compartilhadas. A filtragem de MAC é fraca, pois os endereços são fáceis de falsificar. O LEAP é um protocolo proprietário da Cisco, obsoleto e vulnerável, que não faz parte do WPA3.

23. B A VPN SSL/TLS é a melhor escolha, pois pode operar pela porta TCP 443, que costuma passar por firewalls e NAT. As implementações em túnel carregam tráfego TCP e UDP, e muitas têm canal de dados UDP com alternativa em TCP. O IPSec em modo túnel suporta NAT traversal, mas firewalls restritivos podem bloqueá-lo. O L2TP/IPSec depende do tráfego IPsec permitido (UDP 500 e 4500). O PPTP tem vulnerabilidades conhecidas e usa GRE, que firewalls e NAT costumam barrar.

24. D Ataques DDoS usam várias origens distribuídas para inundar o alvo com tráfego, esgotar os recursos do servidor e negar o serviço a usuários legítimos. Os indícios são o pico de tráfego de várias origens e o esgotamento de recursos. O MitM intercepta comunicações sem inundar. O sequestro de sessão toma sessões autenticadas sem gerar picos. O CSRF explora sessões autenticadas sem sobrecarregar com volume.

25. B A camada de Transporte (camada 4) fornece comunicação de ponta a ponta entre processos de origem e destino. O TCP garante confiabilidade com sequenciamento, confirmações, retransmissão de segmentos perdidos e controle de fluxo por janela deslizante. O UDP, na mesma camada, é sem conexão e de melhor esforço. O Enlace (camada 2) entrega entre nós de um mesmo segmento usando MAC. A Rede (camada 3) roteia com IP. A Sessão (camada 5) controla o diálogo, não a recuperação de erros.

26. D Os SYN cookies permitem que o servidor não aloque recursos durante o handshake TCP até a conexão ser verificada, o que elimina a vulnerabilidade de esgotamento de estado. O servidor codifica os dados da conexão no número de sequência, sem manter o estado de conexões semiabertas. Limitar o ICMP trata de outro vetor. A filtragem de MAC é controle de camada 2 e não ajuda contra ataques de camada 4 vindos da internet. Desativar timestamps não impede o esgotamento de recursos.

27. C O TLS 1.2 é a versão mínima aceitável para novas implantações segundo padrões do NIST e do PCI DSS. Ele oferece suítes de cifras fortes, suporte obrigatório a SHA-256 e proteção contra ataques conhecidos. O TLS 1.0 e o 1.1 são obsoletos por vulnerabilidades e cifras fracas. O SSL 3.0 tem falhas críticas (ataque POODLE) e nunca deve ser usado. O TLS 1.3 traz melhorias, mas o 1.2 é o mínimo para conformidade.

28. B A autenticação por certificado de cliente exige que o cliente apresente um certificado X.509 durante o handshake do TLS. Assim os dois lados verificam a identidade um do outro (autenticação mútua). O TLS padrão autentica só o servidor. O SNI permite vários sites TLS em um IP e não muda o sentido da autenticação. A retomada de sessão só acelera reconexões. O PFS protege chaves de sessão se a chave de longo prazo vazar, mas não dá autenticação mútua.

29. A Um falso positivo ocorre quando o IDS identifica por engano tráfego legítimo como malicioso e alerta sobre atividade normal. Isso causa fadiga de alertas e desperdiça tempo dos analistas. O falso negativo é o contrário: tráfego malicioso passa sem detecção. O verdadeiro positivo identifica corretamente um ataque, e o verdadeiro negativo identifica tráfego legítimo sem alertar. Falsos positivos pedem ajuste de assinaturas, limiares ou listas de permissão.

30. A No sequestro de BGP, um sistema autônomo não autorizado anuncia prefixos que não são dele, e outros ASes passam a rotear o tráfego para o atacante. O route poisoning é uma técnica legítima de convergência em protocolos de vetor de distância, como o RIP: anuncia-se métrica infinita para remover uma rota que falhou. O prepend de AS path é engenharia de tráfego legítima. A oscilação é instabilidade nos anúncios. O sequestro se define pela origem fraudulenta do prefixo.

31. A A adaptação (tailoring) ajusta os controles da linha de base às restrições da organização, às características do sistema e ao ambiente, que é o que se precisa quando um controle não pode ser implementado como especificado. O escopo define a quais sistemas a linha de base se aplica, não como adaptar controles que se aplicam, mas são tecnicamente inviáveis. Controles compensatórios podem ser escolhidos durante a adaptação. A aceitação do risco exige autorização do risco residual e não substitui o cumprimento dos requisitos.

32. A A Ordem Executiva 13526 define três níveis de informação classificada de segurança nacional. Secret se aplica quando a divulgação poderia causar “dano grave”. Top Secret é para “dano excepcionalmente grave”. Confidential cobre o que poderia causar “dano”, sem o qualificador “grave”. CUI não é nível classificado: é uma categoria separada, da NARA, para informação sensível não classificada. A ordem crescente é Confidential, Secret, Top Secret.

33. B O proprietário dos dados, em geral um gerente ou executivo da área de negócio, é o responsável final por definir o nível de classificação. Ele conhece o valor e a sensibilidade dos dados para o negócio e aceita o risco associado. O custodiante implementa controles técnicos, mas não define a classificação. O administrador de segurança aplica políticas definidas por outros. O CISO define a estrutura e a política geral, mas não classifica cada ativo de dados.

34. B Dez anos, para atender ao requisito mais rigoroso, cumpre os dois prazos mínimos aplicáveis. A exigência estadual de 10 anos não substitui a federal, e manter por 10 anos satisfaz as duas. Seis anos violaria a lei estadual. Oito anos não cumpriria a lei estadual. A retenção indefinida é desnecessária, cara e cria risco de privacidade ao manter dados além do exigido.

35. A Soberania de dados significa que os dados ficam sujeitos às leis e à jurisdição do país onde estão, inclusive quanto a quais governos podem exigir acesso. Isso responde ao receio de pedidos legais de governos de fora da UE (por exemplo, o CLOUD Act dos EUA). Residência é o local físico de armazenamento e não trata da autoridade jurisdicional: os dados podem estar na França e pertencer a uma matriz americana. Localização obriga os dados a ficar no país, mas é um meio de obter soberania, não o princípio. Redundância geográfica é questão de disponibilidade.

36. A Antes de descartar qualquer dado, é preciso confirmar que não há ordem de preservação legal (legal hold), litígio em andamento, auditoria regulatória ou outra obrigação que exija manter os dados. Destruir dados sob legal hold pode gerar penalidades graves, como sanções por destruição de provas (spoliation) e acusação de obstrução. Só depois dessa confirmação a destruição técnica pode seguir. Pense como gestor: risco legal e de conformidade vêm antes da execução técnica.

37. B O proprietário dos dados, em geral um gerente sênior ou executivo da área de negócio, atribui o nível de classificação e revisa essa definição periodicamente. O custodiante (em geral TI ou administrador de sistemas) implementa os controles que o proprietário define, como backups, listas de controle de acesso e criptografia, mas não decide a classificação. O curador cuida de qualidade, linhagem e fluxos de governança. O operador trata dados em nome de um controlador. Na prova CISSP: o proprietário decide, o custodiante implementa.

38. A A destruição física dá a maior garantia, pois deixa a mídia inutilizável e irrecuperável por qualquer meio. O apagamento criptográfico só funciona se os dados foram criptografados, e aqui eles estavam sem criptografia. A sobrescrita em sete passagens é eficaz, mas pode deixar áreas de firmware, setores defeituosos e espaço de provisionamento excedente, e é menos confiável em SSDs. A desmagnetização funciona em mídia magnética, não em SSDs (memória flash NAND).

39. B Confidencial é a classificação comercial adequada para dados cuja divulgação não autorizada causaria dano grave à organização, como prejuízo competitivo e responsabilidade legal. A combinação de PII, salários e avaliações de desempenho atinge esse nível. “Uso interno” é fraco demais para dados com implicação legal. “Secreto” é classificação governamental, pouco usada em empresas. “Público” é claramente inadequado para dados sensíveis de funcionários.

40. C O proprietário dos dados, em geral um gerente ou executivo de negócio, tem a responsabilidade principal por definir a classificação, os requisitos de retenção e as autorizações de acesso. Ele responde pelo valor de negócio e pela proteção dos dados. O custodiante implementa os controles técnicos definidos pelo proprietário. O operador trata dados em nome de um controlador. O CISO orienta e governa, mas não é dono de ativos de dados específicos, o que é função do negócio.

41. A Need-to-know significa que o acesso só deve ser concedido se for necessário para uma função específica, mesmo que o usuário tenha o nível de autorização. O funcionário pode ter tido a permissão técnica, mas não tinha necessidade de negócio. O privilégio mínimo é parecido, mas trata do nível mínimo de permissão. A separação de funções divide tarefas para evitar fraude. A defesa em profundidade é estratégia em camadas. A pista é “sem justificativa de negócio”.

42. B O COBIT (Control Objectives for Information and Related Technologies) foi feito para alinhar a governança de TI às metas de negócio e oferece uma estrutura de gestão. A ISO 27002 é um código de práticas de controles de segurança, técnico e operacional, sem foco em governança. A NIST SP 800-53 traz controles de segurança e privacidade para sistemas federais, muito detalhados. Os CIS Controls são ações táticas priorizadas. Se o enunciado fala em alinhar com o negócio, pense em COBIT.

43. D Devido cuidado (due care) é fazer a coisa certa na hora certa, agindo como uma pessoa razoável agiria. Relatar a violação ao conselho e, se exigido, aos reguladores é um exemplo. Devida diligência (due diligence) é investigar riscos e verificar continuamente se as salvaguardas continuam eficazes, e não só pesquisar e planejar antes da implantação. A regra do homem prudente fala do dever fiduciário dos executivos. A pergunta é sobre o ato de relatar, que é due care. Separação de funções não tem relação.

44. D O BCP é uma estrutura estratégica abrangente que trata da continuidade de todas as funções críticas do negócio durante e após uma interrupção: pessoas, processos, instalações, cadeia de suprimentos, comunicações e tecnologia. O DRP é mais estreito e tático e define os procedimentos para restaurar sistemas, dados e infraestrutura de TI. O DRP é um componente do BCP, e não o contrário. Os planos se complementam, mas não são intercambiáveis.

45. D Testes e exercícios regulares validam se os procedimentos de recuperação funcionam, inclusive a integridade dos backups. Se as fitas estão ilegíveis no exercício, os testes foram insuficientes ou inexistentes. A BIA identifica sistemas críticos e RTOs, mas não valida mídias de backup. A avaliação de riscos identifica ameaças e vulnerabilidades. O desenvolvimento do plano cria os procedimentos, mas sem testes não se sabe se funcionam.

46. A ALE = SLE × ARO. O SLE (Single Loss Expectancy) é a perda esperada em uma ocorrência: US$ 50.000. O ARO (Annualized Rate of Occurrence) é a frequência anual esperada: 0,20 (20%). ALE = 50.000 × 0,20 = US$ 10.000. US$ 50.000 é só o SLE, sem a frequência anual. US$ 250.000 vem de multiplicar por 5 (inverter a probabilidade). US$ 40.000 não tem base nos valores dados.

47. B Um padrão (standard) determina configurações, ajustes ou requisitos específicos, por exemplo “todas as senhas devem ter 12 ou mais caracteres”. Padrões são táticos e de cumprimento exigível. Políticas são declarações de alto nível da intenção da gestão, menos específicas. Procedimentos descrevem passos para implementar políticas e padrões e também podem ser obrigatórios. Diretrizes são recomendações, não obrigações. O padrão é a melhor resposta porque especifica requisitos exigíveis.

48. B Privacy by Design exige incorporar a privacidade à arquitetura desde o início, com princípios como minimização de dados (coletar só o necessário) e privacidade por padrão (as configurações mais protetoras como padrão). Uma avaliação de impacto depois do desenvolvimento é reativa. Criptografia e controles de acesso antes da implantação tratam de segurança, mas não mostram a abordagem completa. O treinamento ajuda, mas não garante que a privacidade esteja embutida no projeto.

49. B A transferência do risco desloca o impacto financeiro para outra parte, em geral por seguro (apólice de responsabilidade cibernética) ou contratos (SLA do provedor de nuvem com penalidades). A empresa não evita o risco (eliminar a atividade que o causa), não o mitiga (implementar controles para reduzir probabilidade ou impacto) e não o aceita (reconhecer e documentar sem agir). Transferir não elimina o risco: só desloca o ônus financeiro.

50. C Acionar a polícia é uma decisão de negócio e jurídica, que exige a aprovação da alta administração ou do departamento jurídico, por causa de obrigações regulatórias, riscos de litígio, divulgação pública e impacto no negócio. A equipe de resposta dá os detalhes técnicos, mas não toma essa decisão estratégica. O CISO orienta em segurança, mas a decisão envolve exposição legal e leis de notificação de violação. O responsável pela ligação facilita o contato, mas não decide. Equipes técnicas escalam, executivos decidem.

Palavras-chave em inglês

due care	devido cuidado	Agir como uma pessoa razoável, com controles adequados.
due diligence	devida diligência	Investigar riscos e verificar sempre se os controles funcionam.
risk acceptance	aceitação do risco	Manter o risco de forma consciente e com autorização.
risk transference	transferência do risco	Passar o impacto financeiro a outro, por seguro ou contrato.
risk avoidance	evitação do risco	Parar a atividade que cria o risco.
risk mitigation	mitigação do risco	Reduzir a chance ou o impacto com controles.
residual risk	risco residual	Risco que sobra depois dos controles.
single loss expectancy (SLE)	expectativa de perda única	Perda em dinheiro esperada em um único incidente.
annualized rate of occurrence (ARO)	taxa anualizada de ocorrência	Quantas vezes o incidente deve ocorrer por ano.
annualized loss expectancy (ALE)	expectativa de perda anualizada	Perda esperada por ano: SLE vezes ARO.
need-to-know	necessidade de conhecer	Acesso só quando o trabalho exige aquela informação.
least privilege	privilégio mínimo	Dar só as permissões necessárias para a função.
separation of duties	separação de funções	Dividir uma tarefa entre pessoas para evitar fraude.
business continuity plan (BCP)	plano de continuidade de negócios	Plano amplo para manter as funções críticas do negócio.
disaster recovery plan (DRP)	plano de recuperação de desastres	Plano para restaurar sistemas, dados e infraestrutura de TI.
business impact analysis (BIA)	análise de impacto nos negócios	Identifica sistemas críticos e prazos de recuperação.
recovery time objective (RTO)	objetivo de tempo de recuperação	Prazo definido para restaurar um sistema após a parada.

recovery point objective (RPO)	objetivo de ponto de recuperação	Perda de dados aceitável, medida em tempo.
maximum tolerable downtime (MTD)	tempo máximo tolerável de inatividade	Maior interrupção que o negócio suporta.
data owner	proprietário dos dados	Gestor que decide a classificação e o acesso.
data custodian	custodiante dos dados	Quem aplica os controles definidos pelo proprietário.
data classification	classificação de dados	Dar ao dado um nível conforme sua sensibilidade.
baseline	linha de base	Conjunto mínimo de controles ou configuração aprovada de referência.
scoping	delimitação de escopo	Decidir a quais sistemas os controles da linha de base se aplicam.
tailoring	adaptação dos controles	Ajustar os controles da linha de base à realidade da organização.
legal hold	preservação legal	Ordem de não destruir dados ligados a um processo.
degaussing	desmagnetização	Apagar mídia magnética com campo forte; não serve para SSD.
data sovereignty	soberania de dados	Dado sujeito às leis do país onde está.
non-repudiation	não repúdio	O autor não consegue negar que fez a ação.
key escrow	custódia de chaves	Cópia das chaves guardada por um terceiro de confiança.
defense in depth	defesa em profundidade	Várias camadas de controle; se uma falha, outras protegem.
preventive control	controle preventivo	Impede o incidente antes que aconteça.
detective control	controle detectivo	Identifica o incidente durante ou depois.
compensating control	controle compensatório	Proteção alternativa quando o controle principal não é possível.
mantrap	eclusa de acesso	Duas portas; só uma abre por vez.
supplicant	suplicante	Dispositivo cliente que pede acesso no 802.1X.
false positive	falso positivo	Alerta para atividade normal.
dwell time	tempo de permanência	Tempo que o invasor fica sem ser detectado.
order of volatility	ordem de volatilidade	Coletar primeiro a evidência que some mais rápido.
change advisory board (CAB)	comitê consultivo de mudanças	Grupo que autoriza mudanças antes que cheguem à produção.

O Examundo é independente. Não é afiliado às entidades que fazem essas provas nem tem a aprovação delas. As questões são originais, não são da prova real. examundo.tech/pt/cissp/