examundo

Simulado CompTIA Security+ 701 em português

70 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/comptia-security-plus/

Operações de segurança

1. Um administrador de rede quer identificar picos incomuns de tráfego de saída para uma faixa de IPs no exterior, sem capturar e armazenar o conteúdo completo dos pacotes em toda a empresa. Qual fonte de dados de log é a MAIS adequada para esse objetivo?

A network administrator wants to identify unusual spikes in outbound bandwidth to a foreign IP range without capturing and storing full packet payloads across the enterprise. Which log data source is MOST appropriate for this goal?

A. Captura completa de pacotes (PCAP)
B. Logs de eventos de segurança do Windows
C. Logs de consultas DNS
D. Dados de NetFlow

---

2. Um administrador analisa um servidor de banco de dados recém-provisionado e vê que Telnet e FTP estão ativados por padrão, além de várias contas locais sem uso. Qual princípio de hardening está sendo violado?

An administrator is reviewing a newly provisioned database server and finds Telnet and FTP services enabled by default, along with several unused local user accounts. Which hardening principle is being violated?

A. Funcionalidade mínima (least functionality)
B. Separação de funções (separation of duties)
C. Defesa em profundidade (defense in depth)
D. Privilégio mínimo (least privilege)

---

3. Uma varredura de vulnerabilidades indica que um servidor Linux usa uma versão desatualizada do OpenSSL, vulnerável a um CVE conhecido. Na verificação manual, o administrador confirma que a versão corrigida está instalada e que o scanner leu errado as informações do banner. Esse cenário descreve um:

A vulnerability scan flags a Linux server as running an outdated OpenSSL version vulnerable to a known CVE. Upon manual verification, the administrator confirms the patched version is actually installed and the scanner misread the banner information. This scenario describes a:

A. Verdadeiro negativo (true negative)
B. Verdadeiro positivo (true positive)
C. Falso negativo (false negative)
D. Falso positivo (false positive)

---

4. Um perito forense apreende um notebook suspeito de conter provas de roubo de dados por um funcionário interno e preenche um formulário de cadeia de custódia com todas as pessoas que manuseiam o aparelho. Qual é a finalidade PRINCIPAL desse registro?

A forensic investigator seizes a laptop suspected of containing evidence of insider data theft and completes a chain-of-custody form documenting every individual who handles the device. What is the PRIMARY purpose of this documentation?

A. Definir qual departamento é o responsável financeiro pela substituição do aparelho

B. Calcular o valor monetário do bem apreendido para fins de seguro

C. Manter um registro contínuo que comprove a integridade e a admissibilidade da prova em processos legais

D. Agendar a manutenção de rotina do aparelho quando a investigação terminar

---

5. Um disco rígido apreendido passa de um analista forense para outro. Cada transferência é registrada com data, hora, nome da pessoa e motivo do acesso. O que essa documentação mantém?

A seized hard drive is transferred between two forensic analysts. Each transfer is logged with the date, time, individual's name, and purpose of access. What is being maintained by this documentation?

A. Cadeia de custódia (chain of custody)

B. Ordem de volatilidade (order of volatility)

C. Retenção legal (legal hold)

D. Política de retenção de dados (data retention policy)

---

6. Um administrador de rede retira os direitos de administrador local das contas de usuários comuns e concede acesso elevado só quando é necessário para uma tarefa específica. Essa prática exemplifica qual princípio de segurança?

A network administrator removes local administrator rights from standard user accounts, granting elevated access only when required for a specific task. This practice exemplifies which security principle?

A. Defesa em profundidade (defense in depth)

B. Confiança zero (zero trust)

C. Privilégio mínimo (least privilege)

D. Separação de funções (separation of duties)

---

7. Um analista de segurança procura de forma proativa, na telemetria da empresa, sinais de uma técnica de ataque nova que ainda não gerou nenhum alerta no SIEM, com base em uma hipótese tirada de inteligência de ameaças recente. Qual prática descreve MELHOR essa atividade?

A security analyst proactively searches enterprise telemetry for evidence of a novel attack technique that has not yet triggered any SIEM alert, based on a hypothesis derived from recent threat intelligence. This activity is BEST described as which practice?

A. Caça a ameaças (threat hunting)

B. Varredura de vulnerabilidades (vulnerability scanning)

C. Correlação automática de logs

D. Triagem de incidentes (incident triage)

---

8. Uma equipe de segurança quer detectar um ataque de malware sem arquivo (fileless) que usa o PowerShell para injetar código malicioso direto na memória, sem gravar um executável no disco. Qual ferramenta de segurança é a MAIS indicada para detectar esse comportamento?

A security team wants to detect a fileless malware attack that uses PowerShell to inject malicious code directly into memory without writing an executable to disk. Which security tool is BEST suited to detect this behavior?

A. Agente de prevenção contra perda de dados (DLP)

B. Antivírus baseado em assinaturas

C. Detecção e resposta em endpoints (EDR)

D. Firewall de rede

---

9. Qual controle protege MELHOR a confidencialidade dos dados sensíveis gravados no disco de um notebook roubado?

Which control BEST protects the confidentiality of sensitive data stored on a stolen laptop's hard drive?

A. Sistema de detecção de intrusão (IDS)
B. Autenticação multifator
C. Criptografia de disco completo
D. Segmentação de rede

---

10. Durante o hardening de um servidor, um técnico desativa o Telnet, remove a conta de convidado padrão e fecha todas as portas de rede sem uso. Qual conceito de segurança essa atividade representa MELHOR?

During server hardening, a technician disables Telnet, removes the default guest account, and closes all unused network ports. Which security concept does this activity BEST represent?

A. Estabelecer uma linha de base de segurança (security baseline)
B. Aplicar o privilégio mínimo
C. Reduzir a superfície de ataque
D. Implementar a segmentação de rede

---

11. Durante a resposta a um incidente, um analista forense precisa coletar evidências de um servidor comprometido que ainda está ligado. Segundo a ordem de volatilidade, que tipo de dado deve ser coletado PRIMEIRO?

During incident response, a forensic analyst must collect evidence from a compromised server that is still powered on. According to the order of volatility, which type of data should be collected FIRST?

A. Conteúdo da RAM e processos em execução
B. Arquivos de log guardados em um servidor de backup remoto
C. Dados de configuração impressos na documentação do sistema
D. Arquivos gravados no disco rígido local

---

12. Qual técnica de hardening reduz a superfície de ataque de um servidor ao desativar portas e serviços sem uso?

Which hardening technique reduces a server's attack surface by disabling unused ports and services?

A. Ativar o registro detalhado (verbose logging)
B. Desativar serviços desnecessários
C. Instalar um antivírus
D. Configurar um honeypot

---

13. Em uma investigação forense, um analista leva um disco rígido apreendido a um laboratório de forense digital para criar a imagem. Qual documento deve acompanhar o disco para manter a integridade da prova?

During a forensic investigation, an analyst transfers a seized hard drive to a digital forensics lab for imaging. Which document must accompany the drive to maintain evidentiary integrity?

A. Playbook de resposta a incidentes
B. Formulário de cadeia de custódia
C. Plano de continuidade de negócios
D. Política de retenção de dados

---

14. Um analista de segurança faz a resposta a incidentes ao vivo em uma estação de trabalho que continua ligada e conectada à rede. Seguindo a ordem de volatilidade, qual artefato o analista deve coletar PRIMEIRO, antes de qualquer outra evidência?

A security analyst is performing live incident response on a workstation that is still powered on and connected to the network. Following the order of volatility, which artifact should the analyst collect FIRST, before any other evidence?

A. Tabelas de roteamento e cache ARP
B. Conteúdo da RAM e processos em execução
C. Arquivos temporários gravados no disco local
D. Registradores da CPU e cache do processador

Ameaças, vulnerabilidades e mitigações

15. Um administrador de rede suspeita que um atacante está interceptando e alterando o tráfego entre os clientes internos e o gateway padrão, respondendo a requisições ARP com um endereço MAC falsificado. Qual mitigação trataria MELHOR esse ataque específico?

A network administrator suspects an attacker is intercepting and altering traffic between internal clients and the default gateway by responding to ARP requests with a spoofed MAC address. Which mitigation would BEST address this specific attack?

A. Segmentação de rede com VLANs
B. Implementar a criptografia WPA3
C. Desativar portas de switch sem uso
D. Inspeção dinâmica de ARP (DAI)

16. Um funcionário abre o anexo de um e-mail e pouco depois todos os arquivos da unidade compartilhada aparecem criptografados, com uma mensagem exigindo pagamento em criptomoeda para devolver o acesso. Que tipo de malware causou o incidente?

An employee opens an email attachment and shortly afterward finds that all files on the shared drive have been encrypted, with a note demanding payment in cryptocurrency to restore access. Which type of malware caused this incident?

A. Rootkit
B. Bomba lógica (logic bomb)
C. Ransomware
D. Spyware

17. Um atacante liga para o help desk de TI fingindo ser um executivo da empresa que está 'bloqueado' durante uma ligação urgente com um cliente e pressiona o técnico a redefinir a senha na hora, sem verificar a identidade. Qual técnica de engenharia social está sendo usada?

An attacker calls the IT help desk posing as a company executive who is 'locked out' during an urgent client call, pressuring the technician to reset a password immediately without verifying identity. Which social engineering technique is being used?

A. Vasculhar o lixo (dumpster diving)
B. Pretexto (pretexting)
C. Carona (tailgating)
D. Espiar por cima do ombro (shoulder surfing)

18. Um atacante obtém uma grande lista de usuários e senhas vazada em uma invasão anterior a uma empresa sem relação e tenta, de forma sistemática, entrar com esses mesmos pares de credenciais em várias plataformas de banco on-line. Qual técnica de ataque está sendo usada?

An attacker obtains a large list of usernames and passwords leaked from a previous breach at an unrelated company and systematically attempts to log in with those exact credential pairs across several different online banking platforms. Which attack technique is being used?

A. Ataque de dicionário (dictionary attack)
B. Força bruta (brute-force attack)
C. Credential stuffing (preenchimento de credenciais)
D. Password spraying (pulverização de senhas)

19. Um usuário relata que os arquivos de uma unidade de rede compartilhada passaram de repente a ter uma extensão desconhecida e não abrem. Um arquivo de texto exigindo pagamento em criptomoeda por uma chave de descriptografia apareceu em cada pasta afetada. Qual ameaça é a MAIS provável?

A user reports that files on a shared network drive suddenly have a new, unfamiliar file extension and cannot be opened. A text file demanding cryptocurrency payment for a decryption key has appeared in each affected folder. Which threat is MOST likely responsible?

A. Rootkit
B. Bomba lógica (logic bomb)
C. Worm (verme)
D. Ransomware

---

20. Um atacante liga para um funcionário, diz ser do help desk da empresa e pede que ele leia o código de uso único que acabou de chegar ao seu celular. Qual vetor de engenharia social está sendo usado?

An attacker calls an employee, claiming to be from the corporate help desk, and asks the employee to read back a one-time passcode that was just sent to their phone. Which social engineering vector is being used?

A. Vishing
B. Smishing
C. Shoulder surfing
D. Tailgating

---

21. Um agente de ameaça invade um site muito visitado por funcionários de uma empresa contratada da área de defesa e insere JavaScript malicioso que só é executado quando o IP do visitante está na faixa conhecida dessa empresa. Qual técnica de ataque é descrita?

A threat actor compromises a website frequently visited by employees of a defense contractor and embeds malicious JavaScript that only executes when the visitor's IP address matches the contractor's known range. Which attack technique is being described?

A. Typosquatting
B. Envenenamento de DNS (DNS poisoning)
C. Ataque watering hole
D. Cross-site scripting (XSS)

---

22. Várias estações de trabalho de um escritório começam a esquentar demais, com os ventiladores sempre no máximo, e as ferramentas de monitoramento mostram uso de CPU perto de 100% mesmo quando ninguém está trabalhando. Qual indicador de comprometimento é o MAIS coerente com esse comportamento?

Several workstations in an office begin running unusually hot with fans at full speed continuously, and monitoring tools show sustained CPU usage near 100% even when employees are not actively working. Which indicator of compromise is MOST consistent with this behavior?

A. Conteúdo bloqueado por uma mudança em uma regra do firewall
B. Registros fora de ciclo gerados por uma tarefa agendada
C. Consumo de recursos causado por malware de mineração de criptomoedas
D. Logs ausentes por um SIEM comprometido

---

23. Um atacante registra um domínio quase idêntico ao do site legítimo de um banco e compromete um resolvedor DNS público, de modo que os usuários que digitam o endereço correto do banco são redirecionados em silêncio ao servidor do atacante. Qual ataque isso descreve?

An attacker registers a domain nearly identical to a bank's legitimate site and compromises a public DNS resolver so that users who type the correct bank URL are silently redirected to the attacker's server. Which attack does this describe?

A. Pharming
B. Pretexting (pretexto)
C. Vishing
D. Typosquatting

---

24. Um analista de segurança investiga uma invasão em que o atacante usou exploits de dia zero personalizados, manteve acesso persistente sem ser detectado por oito meses e exfiltrou dados ligados à proposta de um concorrente em um contrato de defesa. Que tipo de agente de ameaça MAIS provavelmente realizou o ataque?

A security analyst investigates a breach in which the attacker used custom zero-day exploits, maintained undetected persistent access for eight months, and exfiltrated data tied to a competitor's defense contract bid. Which threat actor type MOST likely conducted this attack?

A. Script kiddie
B. Ameaça interna não intencional
C. Hacktivista
D. APT de um Estado-nação

---

25. O departamento de contas a pagar recebe um e-mail que parece vir da conta do CEO, mandando transferir com urgência um valor para a conta de um novo fornecedor. Não há malware nem link malicioso. Que tipo de ataque isso representa?

The accounts payable department receives an email that appears to come from the CEO's account instructing them to urgently wire funds to a new vendor account. No malware or malicious link is involved. Which type of attack does this represent?

A. Credential stuffing
B. Ataque watering hole
C. Typosquatting
D. Comprometimento de e-mail corporativo (BEC)

---

26. Um administrador de sistemas demitido há pouco tempo usa credenciais que ainda não tinham sido desativadas para entrar remotamente e apagar arquivos de backup críticos. Qual categoria de agente de ameaça descreve MELHOR essa pessoa?

A systems administrator who was recently terminated uses credentials that had not yet been deactivated to log in remotely and delete critical backup archives. Which threat actor category BEST describes this individual?

A. Hacktivista
B. Agente de um Estado-nação
C. Script kiddie
D. Ameaça interna

---

27. Uma equipe de segurança nota milhares de tentativas de login bem-sucedidas no portal de clientes da empresa, usando combinações válidas de e-mail e senha que vazaram antes na invasão de um site de varejo sem relação. Qual ataque está ocorrendo?

A security team notices thousands of successful login attempts against the company's customer portal using valid email and password combinations that were previously leaked in a breach of an unrelated retail website. Which attack is occurring?

A. Credential stuffing
B. Ataque com rainbow table
C. Password spraying
D. Ataque de força bruta (brute-force)

---

28. Um atacante liga para o departamento de contas a pagar, diz ser um auditor externo e pede registros de faturas recentes para 'verificar a conformidade', antes de apresentar qualquer prova de identidade. Qual técnica de engenharia social está sendo usada?

An attacker calls the accounts payable department, claiming to be an external auditor, and requests recent invoice records to 'verify compliance' before offering any proof of identity. Which social engineering technique is being used?

A. Tailgating (carona)
B. Baiting (isca)
C. Pretexting (pretexto)
D. Quid pro quo

Gestão e supervisão do programa de segurança

29. A liderança de uma organização afirma que aceita até 5% de chance de uma interrupção crítica de sistema por ano antes de exigir mais investimento em segurança. Qual conceito essa afirmação descreve MELHOR?

An organization's leadership states that the company is willing to accept up to a 5% chance of a critical system outage annually before additional security investment is required. This statement BEST describes the organization's:

A. Registro de riscos (risk register)
B. Tolerância a risco (risk tolerance)
C. Apetite a risco (risk appetite)
D. Exceção de risco (risk exception)

---

30. Uma empresa de SaaS dos Estados Unidos hospeda dados de gestão de relacionamento com clientes (CRM) em nome de uma varejista europeia e os processa estritamente conforme as instruções por escrito da varejista sobre finalidade e retenção. Pelo GDPR, qual é o papel da empresa de SaaS?

A US-based SaaS company hosts customer relationship management data on behalf of a European retailer, processing that data strictly according to the retailer's written instructions on purpose and retention. Under GDPR, which role does the SaaS company hold?

A. Titular dos dados (data subject)
B. Encarregado de proteção de dados (data protection officer)
C. Controlador de dados (data controller)
D. Operador de dados (data processor)

---

31. Um cliente alemão envia um e-mail a uma loja on-line pedindo que todos os seus dados pessoais sejam excluídos em definitivo dos sistemas da empresa. Qual regulamentação dá a esse cliente o direito legal de fazer esse pedido?

A German customer emails an online retailer requesting that all of their personal data be permanently deleted from the company's systems. Which regulation grants this customer the legal right to make this request?

A. HIPAA
B. GDPR
C. PCI DSS
D. SOX

---

32. Uma empresa de serviços financeiros identifica um risco residual em um sistema legado de processamento de pagamentos que não pode ser totalmente corrigido dentro do orçamento. O CISO contrata uma apólice de seguro cibernético para cobrir possíveis perdas em uma invasão. Qual estratégia de gestão de riscos isso representa MELHOR?

A financial services firm identifies a residual risk from a legacy payment processing system that cannot be fully remediated within budget. The CISO purchases a cyber insurance policy to cover potential losses from a breach. Which risk management strategy does this BEST represent?

A. Transferência de risco (risk transference)
B. Aceitação de risco (risk acceptance)
C. Evitação de risco (risk avoidance)
D. Mitigação de risco (risk mitigation)

---

33. Um possível cliente pede evidências de que os controles de segurança de um provedor de nuvem funcionaram de forma eficaz ao longo de 12 meses antes de assinar o contrato. Qual tipo de relatório de auditoria o provedor deve apresentar?

A prospective client requests evidence that a cloud service provider's security controls have operated effectively over a 12-month period before signing a contract. Which type of audit report should the provider supply?

A. Relatório SOC 2 Tipo I
B. Relatório SOC 2 Tipo II
C. Relatório SOC 1 Tipo I
D. Attestation of Compliance (AOC) da PCI DSS

---

34. Uma organização pede evidências da eficácia dos controles de segurança de um fornecedor de nuvem durante um período operacional de 12 meses, e não em um único momento. Qual tipo de relatório atende MELHOR a esse requisito?

An organization requests evidence of a cloud vendor's security control effectiveness over a 12-month operating period rather than at a single point in time. Which type of report BEST satisfies this requirement?

A. SOC 1: focado em controles relevantes para relatórios financeiros, não para segurança
B. Certificação ISO 27001: confirma que um SGSI atende aos requisitos da norma na data da auditoria
C. SOC 2 Tipo I: atesta a adequação do desenho dos controles em um único momento
D. SOC 2 Tipo II: atesta a eficácia operacional dos controles em um período prolongado de revisão

---

35. Na negociação do contrato com um provedor de nuvem, um responsável por conformidade quer garantir que a organização possa verificar os controles de segurança do fornecedor a qualquer momento, sem precisar do consentimento prévio dele para agendar a revisão. Qual cláusula contratual deve ser negociada no SLA?

During contract negotiations with a cloud service provider, a compliance officer wants to ensure the organization can verify the vendor's security controls at any time without needing the vendor's advance consent to schedule the review. Which contractual clause should be negotiated into the SLA?

A. Cláusula de indenização (indemnification)
B. Cláusula de direito de auditoria (right-to-audit)
C. Acordo de confidencialidade (NDA)
D. Cláusula de força maior (force majeure)

---

36. Um administrador de sistemas quer aplicar uma mudança de emergência em uma regra do firewall para bloquear a exploração ativa de uma vulnerabilidade crítica, fora da janela semanal de manutenção. Segundo as práticas padrão de gestão de mudanças, o que deve acontecer PRIMEIRO?

A systems administrator wants to deploy an emergency firewall rule change to block active exploitation of a critical vulnerability outside the normal weekly maintenance window. According to standard change management practices, what should occur FIRST?

A. Enviar a mudança pelo processo de mudança de emergência para aprovação acelerada
B. Esperar a próxima reunião programada do Change Advisory Board (CAB)
C. Implementar a mudança imediatamente e documentá-la depois
D. Avisar os usuários finais sobre a previsão de indisponibilidade antes de qualquer alteração

---

37. Uma empresa de capital aberto contrata uma firma externa de contabilidade para verificar de forma independente se seus controles de relatórios financeiros cumprem as exigências regulatórias. Que tipo de auditoria está sendo feita?

A publicly traded company hires an outside accounting firm to independently verify that its financial reporting controls comply with regulatory requirements. Which type of audit is being performed?

A. Avaliação de vulnerabilidades
B. Auditoria interna
C. Autoavaliação de conformidade
D. Auditoria externa

---

38. Uma equipe de compras precisa de garantia independente de que os controles de um fornecedor de SaaS sobre segurança, disponibilidade e confidencialidade funcionaram de forma eficaz nos últimos 12 meses antes de assinar o contrato. Que documento a equipe deve pedir ao fornecedor?

A procurement team needs independent assurance that a SaaS vendor's controls over security, availability, and confidentiality operated effectively over the past 12 months before signing a contract. Which document should the team request from the vendor?

A. Relatório SOC 2 Tipo II
B. Questionário de autoatestação
C. Resumo de teste de intrusão (penetration test)
D. Análise de impacto nos negócios (BIA)

---

39. Uma avaliação de riscos em um banco regional identifica uma vulnerabilidade com baixa probabilidade de exploração e impacto financeiro mínimo se ocorrer. O custo de implementar um controle é maior que a perda potencial. Qual resposta ao risco a equipe de segurança deve recomendar à gestão?

A risk assessment at a regional bank identifies a vulnerability that has a low likelihood of exploitation and would cause minimal financial impact if realized. The cost of implementing a control exceeds the potential loss. Which risk response should the security team recommend to management?

A. Evitação de risco (risk avoidance)
B. Mitigação de risco (risk mitigation)
C. Aceitação de risco (risk acceptance)
D. Transferência de risco (risk transference)

---

40. Uma empresa recebe a notificação de um processo judicial iminente sobre suposta negligência em uma violação de dados, e a equipe jurídica emite uma retenção legal (legal hold). Que ação é exigida em relação à política padrão de retenção de dados da empresa?

A company receives notice of pending litigation involving alleged data breach negligence, and the legal team issues a legal hold. Which action is required regarding the company's standard data retention policy?

A. Transferir a custódia dos registros ao advogado da parte contrária para guarda
B. Suspender a destruição de rotina dos registros potencialmente relevantes até o fim da retenção legal
C. Apagar imediatamente todos os dados do caso para reduzir o escopo da produção de provas
D. Criptografar todos os registros sob retenção legal e manter o cronograma normal de retenção

---

41. Depois de implementar a autenticação multifator e a segmentação de rede para tratar um risco de phishing, ainda resta algum risco de comprometimento de contas, pela possibilidade de roubo de tokens de sessão por um adversário no meio (adversary-in-the-middle). Qual termo descreve esse risco restante?

After implementing multifactor authentication and network segmentation to address a phishing-related risk, some risk of account compromise still remains due to the possibility of adversary-in-the-middle session token theft. What term describes this remaining risk?

A. Risco residual (residual risk): o risco que permanece depois de aplicados os controles
B. Risco de controle (control risk): o risco de um controle não funcionar como projetado
C. Risco inerente (inherent risk): o nível de risco que existe antes de qualquer controle
D. Risco secundário (secondary risk): um novo risco criado como resultado direto da implementação de um controle

---

42. Um possível cliente pede evidências de que os controles de segurança de um fornecedor funcionaram de forma eficaz nos últimos seis meses, e não apenas de que foram bem projetados em um único momento. Qual relatório o fornecedor deve apresentar?

A prospective client requests evidence that a vendor's security controls have operated effectively over the preceding six months, not merely that they were properly designed at a single point in time. Which report should the vendor provide?

A. SOC 1 Tipo I
B. SOC 2 Tipo II
C. SOC 2 Tipo I
D. Certificado ISO 27001

Arquitetura de segurança

43. Uma empresa quer usar uma infraestrutura de nuvem provisionada exclusivamente para a sua organização e não compartilhada com nenhum outro cliente (tenant). Qual modelo de implantação de nuvem isso descreve?

A company wants to use cloud infrastructure that is provisioned exclusively for its own organization and is not shared with any other tenant. Which cloud deployment model does this describe?

A. Nuvem privada (private cloud)
B. Nuvem comunitária (community cloud)
C. Nuvem híbrida (hybrid cloud)
D. Nuvem pública (public cloud)

---

44. Um administrador de rede segmenta a rede corporativa para que as estações do financeiro não consigam se comunicar diretamente com os dispositivos do departamento de marketing. Qual tecnologia está sendo implementada?

A network administrator segments a corporate network so that finance workstations cannot directly communicate with marketing department devices. Which technology is being implemented?

A. Balanceador de carga (load balancer)
B. VLAN
C. NAT
D. VPN

---

45. O navegador de um usuário exibe um erro de certificado informando que ele não é confiável ao acessar um aplicativo web interno da empresa. Qual componente da hierarquia PKI MAIS provavelmente está faltando no repositório de confiança (trust store) do cliente?

A user's browser displays a certificate error stating the certificate is not trusted when visiting an internal company web application. Which component of the PKI hierarchy is MOST likely missing from the client's trust store?

A. A chave privada do servidor web
B. O ticket de sessão do cliente
C. O certificado da CA raiz
D. A chave de sessão simétrica

---

46. Um administrador de sistemas baixa um arquivo ISO e quer verificar se ele não foi corrompido nem alterado durante a transferência. Qual é o MELHOR método para isso?

A systems administrator downloads an ISO file and wants to verify that it was not corrupted or altered during transfer. Which method BEST achieves this?

A. Comparar o hash SHA-256 do arquivo baixado com o hash publicado pelo fornecedor
B. Comparar o tamanho do arquivo em bytes com o informado no site do fornecedor
C. Criptografar o arquivo com AES-256 e confirmar que ele descriptografa com sucesso
D. Abrir o ISO e inspecionar visualmente o conteúdo

---

47. Um engenheiro de rede precisa escolher um mecanismo de troca de chaves TLS que mantenha confidencial o tráfego de sessões passadas, mesmo que a chave privada de longo prazo do servidor seja comprometida mais tarde. Qual troca de chaves oferece essa propriedade?

A network engineer must select a TLS key exchange mechanism that ensures past session traffic remains confidential even if the server's long-term private key is later compromised. Which key exchange provides this property?

A. Troca de chaves RSA estática
B. Troca de chave pré-compartilhada (PSK) sem parâmetros efêmeros
C. Diffie-Hellman efêmero (DHE)
D. Troca de tickets Kerberos

---

48. Um fabricante de sensores IoT alimentados por bateria precisa implementar criptografia para dados em trânsito, mas os dispositivos têm capacidade de processamento e memória extremamente limitadas. Qual fator deve influenciar MAIS a escolha do algoritmo criptográfico?

A manufacturer of battery-powered IoT sensors must implement encryption for data in transit but has extremely limited processing power and memory. Which factor should MOST influence the choice of cryptographic algorithm?

A. Criptografia leve, otimizada para dispositivos com recursos limitados
B. Algoritmos resistentes a computação quântica com chaves grandes
C. O algoritmo mais forte disponível, sem considerar o consumo de recursos
D. DES legado, por compatibilidade com sistemas antigos

---

49. Uma instituição financeira isola fisicamente a rede principal de processamento de transações, que não tem conexão com a internet nem com nenhuma outra rede. Qual conceito de segurança está sendo aplicado?

A financial institution physically isolates its core transaction-processing network so it has no network connection to the internet or any other network. Which security concept is being applied?

A. Microssegmentação (micro-segmentation)
B. Air gap (isolamento físico)
C. Sub-rede protegida (screened subnet)
D. Confiança zero (zero trust)

---

50. Um administrador de data center precisa impedir o movimento lateral entre duas máquinas virtuais que compartilham a mesma VLAN e sub-rede, embora o tráfego leste-oeste entre elas seja necessário para o funcionamento do aplicativo. Qual controle atinge MELHOR esse objetivo?

A data center administrator must prevent lateral movement between two virtual machines that share the same VLAN and subnet, even though east-west traffic between them is required for the application to function. Which control BEST achieves this goal?

A. Implantar um IDS de rede em modo promíscuo
B. Criar uma VLAN nova para cada máquina virtual
C. Ativar o port security no switch físico
D. Microssegmentação com políticas de firewall no host

---

51. Uma empresa de comércio eletrônico exige que seus servidores web continuem disponíveis mesmo se um servidor falhar, sem que os usuários percebam indisponibilidade. Qual arquitetura atende MELHOR a esse requisito?

An e-commerce company requires its web servers to remain available even if one server fails, without users experiencing downtime. Which architecture BEST supports this requirement?

A. Criptografia de disco completo em cada servidor
B. Servidor de backup em air gap, desligado
C. Balanceamento de carga ativo-passivo com failover automático
D. Um único ponto de presença com procedimentos manuais de reinicialização

---

52. Uma empresa quer garantir que uma atualização de software assinada não possa ser contestada depois pelo fornecedor que a publicou. Qual conceito criptográfico dá MELHOR essa garantia?

A company wants to ensure that a signed software update cannot later be disputed by the vendor who published it. Which cryptographic concept BEST provides this assurance?

A. Ofuscação apenas por hash
B. Não repúdio por assinatura digital
C. Disponibilidade por balanceamento de carga
D. Confidencialidade por criptografia simétrica

---

53. Uma concessionária de energia mantém uma rede totalmente isolada, sem conexões físicas ou sem fio com a rede de TI corporativa, para seus sistemas de controle SCADA. Qual controle de segurança isso representa?

A power utility maintains a completely isolated network with no physical or wireless connections to the corporate IT network for its SCADA control systems. Which security control does this represent?

A. Sub-rede protegida (screened subnet)
B. Air gap (isolamento físico)
C. Servidor de salto (jump server)
D. Rede privada virtual (VPN)

---

54. Uma avaliação de segurança de um prédio inteligente descobre que vários termostatos IoT ainda usam as credenciais de administrador de fábrica e estão no mesmo segmento de rede das estações do financeiro. Qual ação trata o MAIOR risco imediato?

A security assessment of a smart building finds several IoT thermostats still using factory-default administrator credentials and connected to the same network segment as finance workstations. Which action addresses the GREATEST immediate risk?

A. Ativar a geocerca (geofencing) no aplicativo móvel
B. Desativar o SNMP nas estações do financeiro
C. Trocar as credenciais padrão e colocar os dispositivos IoT em uma VLAN isolada
D. Aumentar a frequência de atualização do firmware dos termostatos

---

55. Um administrador web quer verificar o status de revogação de certificados para clientes TLS sem expor à autoridade certificadora (CA) os padrões de navegação de cada cliente e sem adicionar uma ida e volta extra ao handshake TLS. Qual abordagem atende MELHOR a esses requisitos?

A web administrator wants to verify certificate revocation status for TLS clients without exposing individual client browsing patterns to the certificate authority and without adding an extra round trip to the TLS handshake. Which approach BEST meets these requirements?

A. OCSP stapling
B. Consulta OCSP padrão enviada direto à CA
C. Verificação por lista de certificados revogados (CRL)
D. Fixação de certificado (certificate pinning)

---

56. No Purdue Enterprise Reference Architecture, usado para segmentar redes de controle industrial, em qual nível ficam normalmente os controladores lógicos programáveis (CLPs/PLCs) e as unidades terminais remotas (RTUs), que se conectam diretamente a sensores e atuadores de campo?

In the Purdue Enterprise Reference Architecture used to segment industrial control networks, at which level do programmable logic controllers (PLCs) and remote terminal units (RTUs) that directly interface with field sensors and actuators typically reside?

A. Nível 3: operações do local
B. Nível 1: controle básico
C. Nível 2: controle supervisório da área
D. Nível 0: processo físico

Conceitos gerais de segurança

57. Um comitê consultivo de mudanças (change advisory board) analisa um pedido para implantar uma mudança crítica em uma regra do firewall durante uma janela de manutenção programada. Qual elemento do pedido de mudança é o MAIS importante para minimizar a indisponibilidade se a mudança causar uma interrupção inesperada do serviço?

A change advisory board is reviewing a request to deploy a critical firewall rule change during a scheduled maintenance window. Which element of the change request is MOST important for minimizing downtime if the change causes an unexpected service disruption?

A. Assinatura de aprovação da mudança
B. Análise de impacto nas partes interessadas
C. Plano de reversão
D. Resultados de testes em sandbox

---

58. Um data center instala alarmes com sensor de movimento que avisam a equipe de segurança sempre que movimento não autorizado é detectado em uma sala de servidores restrita fora do expediente. Que tipo de controle esse sistema de alarme representa?

A data center installs motion-activated alarms that alert security personnel whenever unauthorized movement is detected within a restricted server room after hours. Which type of control does this alarm system represent?

A. Controle preventivo
B. Controle corretivo
C. Controle dissuasivo
D. Controle detectivo

---

59. Um administrador de data center implanta fontes de alimentação redundantes, matrizes RAID 10 e um cluster de failover para um servidor de banco de dados crítico. Qual princípio da tríade CIA o administrador está tratando PRINCIPALMENTE?

A data center administrator deploys redundant power supplies, RAID 10 arrays, and a failover cluster for a critical database server. Which principle of the CIA triad is the administrator PRIMARILY addressing?

A. Não repúdio (non-repudiation)
B. Disponibilidade (availability)
C. Integridade (integrity)
D. Confidencialidade (confidentiality)

---

60. Uma empresa exige que o funcionário que inicia uma ordem de compra não possa ser o mesmo que aprova o pagamento dessa ordem. Qual princípio de segurança está sendo aplicado?

A company requires that the employee who initiates a purchase order cannot be the same employee who approves payment for that order. Which security principle is being enforced?

A. Separação de funções (separation of duties)
B. Privilégio mínimo (least privilege)
C. Férias obrigatórias (mandatory vacation)
D. Rodízio de funções (job rotation)

---

61. No modelo de segurança AAA, qual processo determina quais ações um usuário já verificado tem permissão para realizar em um sistema?

In the AAA security model, which process determines what actions an already-verified user is permitted to perform on a system?

A. Identificação (identification)
B. Contabilização (accounting)
C. Autenticação (authentication)
D. Autorização (authorization)

---

62. Uma organização migra para um modelo de segurança em que toda requisição de acesso, seja de um funcionário interno ou de um parceiro externo, precisa ser autenticada e autorizada, independentemente da localização de rede de quem pede. Qual modelo de segurança a organização adotou?

An organization migrates to a security model in which every access request, whether from an internal employee or an external partner, must be authenticated and authorized regardless of the requester's network location. Which security model has the organization adopted?

A. Confiança zero (zero trust)
B. Controle de acesso baseado em função (RBAC)
C. Defesa em profundidade (defense in depth)
D. Defesa baseada em perímetro

---

63. Um atacante intercepta uma solicitação de transferência bancária entre o servidor de aplicação de um banco e o seu banco de dados e altera o número da conta de destino antes de a transação ser concluída. Qual princípio da tríade CIA foi violado PRINCIPALMENTE?

An attacker intercepts a wire transfer request between a bank's application server and its database, altering the destination account number before the transaction completes. Which tenet of the CIA triad has been PRIMARILY violated?

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

---

64. Antes de implantar um patch crítico em servidores de produção, uma organização exige a revisão e a aprovação de um grupo designado. Qual é a finalidade PRINCIPAL desse grupo no processo de gestão de mudanças?

Before deploying a critical patch to production servers, an organization requires review and sign-off by a designated group. What is the PRIMARY purpose of this group in the change management process?

A. Escrever o plano de resposta a incidentes
B. Fazer a instalação técnica do patch
C. Avaliar o risco e aprovar ou negar as mudanças propostas
D. Conduzir o treinamento anual de conscientização em segurança

---

65. Durante uma mudança programada em uma regra de firewall, a mudança aprovada pela equipe de rede causa uma interrupção crítica nos serviços voltados aos clientes. Segundo a prática padrão de gestão de mudanças, o que deveria ter sido preparado ANTES da implementação para minimizar o impacto no negócio dessa falha?

During a scheduled firewall rule change, the network team's approved change causes a critical outage affecting customer-facing services. According to standard change management practice, what should have been prepared BEFORE implementation to minimize the business impact of this failure?

A. Um modelo de relatório pós-incidente para a equipe de segurança
B. Um inventário de ativos atualizado com todos os firewalls afetados
C. Um plano de continuidade de negócios revisado para todo o data center
D. Um plano de reversão documentado e testado para a janela de mudança

---

66. Pesquisadores demonstram que dois arquivos executáveis diferentes podem ser criados para produzir o mesmo hash SHA-1. Quando o SHA-1 é usado para verificar a autenticidade de um pacote de software baixado, essa vulnerabilidade de colisão compromete PRINCIPALMENTE qual propriedade de segurança?

Researchers demonstrate that two different executable files can be crafted to produce an identical SHA-1 digest. When SHA-1 is used to verify the authenticity of a downloaded software package, this collision vulnerability PRIMARILY undermines which security property?

A. Integridade
B. Autorização
C. Confidencialidade
D. Disponibilidade

---

67. Em uma arquitetura de confiança zero baseada no modelo NIST SP 800-207, qual componente avalia o algoritmo de confiança usando várias fontes de dados, como identidade, postura do dispositivo e inteligência de ameaças, para tomar a decisão final de conceder ou negar acesso a um recurso?

In a zero trust architecture based on the NIST SP 800-207 model, which component evaluates the trust algorithm using multiple data sources such as identity, device posture, and threat intelligence to render the final decision to grant or deny access to a resource?

A. Mecanismo de políticas (policy engine)
B. Sistema de diagnóstico e mitigação contínuos (CDM)
C. Ponto de aplicação de políticas (policy enforcement point)
D. Administrador de políticas (policy administrator)

---

68. Uma empresa de serviços financeiros quer que as decisões de acesso considerem o departamento do usuário, a classificação de sensibilidade do arquivo solicitado, o horário e a conformidade do dispositivo antes de conceder o acesso. Qual modelo de autorização atende MELHOR a esse requisito?

A financial services company wants access decisions to consider the user's department, the sensitivity classification of the requested file, the time of day, and the device's compliance status before granting access. Which authorization model BEST satisfies this requirement?

A. Controle de acesso baseado em atributos (ABAC)
B. Controle de acesso obrigatório (MAC)
C. Controle de acesso baseado em função (RBAC)
D. Controle de acesso discricionário (DAC)

---

69. Um novo técnico de help desk recebe direitos de administrador local apenas nas estações de trabalho do departamento de suporte, e não acesso de administrador em todo o domínio. Qual princípio de segurança essa configuração reflete?

A new help desk technician is granted local administrator rights to only the workstations in the support department rather than domain-wide administrator access. Which security principle does this configuration reflect?

A. Confiança zero (zero trust)
B. Separação de funções (separation of duties)
C. Privilégio mínimo (least privilege)
D. Defesa em profundidade (defense in depth)

---

70. Uma gerente financeira assina digitalmente a aprovação de uma transferência bancária com sua chave privada, para que não possa negar depois que autorizou a transação. Qual conceito de segurança esse cenário ilustra MELHOR?

A finance manager digitally signs a wire transfer approval using her private key so that she cannot later deny having authorized the transaction. Which security concept does this scenario BEST illustrate?

A. Autenticação (authentication)
B. Não repúdio (non-repudiation)
C. Confidencialidade (confidentiality)
D. Integridade (integrity)

Resposta correta

1. D O NetFlow registra metadados de cada conversa: IPs de origem e destino, porta, protocolo, bytes e duração. Por isso mostra tendências de volume sem o custo de armazenar o conteúdo. A captura completa de pacotes é inviável como monitoramento contínuo na empresa toda. Os logs DNS mostram resolução de nomes, não o volume transferido, e os eventos do Windows registram autenticação no host, não fluxos de rede.

2. A A funcionalidade mínima exige que o sistema rode só os serviços, protocolos e contas necessários. Telnet, FTP e contas antigas ampliam a superfície de ataque sem necessidade. O privilégio mínimo trata das permissões de uma conta, não de quais serviços estão ativos. A separação de funções divide tarefas críticas entre pessoas para evitar fraude, e a defesa em profundidade é a combinação de várias camadas de controle.

3. D Um falso positivo acontece quando o scanner aponta uma vulnerabilidade que não existe, como aqui, em que a versão corrigida já estava instalada. O falso negativo é o oposto: uma vulnerabilidade real passa sem ser detectada. Verdadeiro positivo seria o scanner acertar uma falha real, e verdadeiro negativo, acertar que não há falha. Nenhum dos dois descreve a leitura errada do banner.

4. C A cadeia de custódia cria um registro contínuo e verificável de quem teve acesso à prova e quando. Isso mostra que ela não foi adulterada e preserva sua admissibilidade em processos legais ou disciplinares. Valor de seguro e responsabilidade financeira são questões administrativas sem relação com a integridade da prova. A prova é mantida como foi apreendida, sem manutenção, pois qualquer alteração a comprometeria.

5. A A cadeia de custódia é o registro contínuo de quem manuseou a prova, quando e por quê. Ela serve para provar que a prova não foi alterada e continua admissível. A retenção legal é um aviso para preservar dados ligados a um litígio, não um registro de manuseio. A política de retenção define por quanto tempo os dados são guardados. A ordem de volatilidade define a sequência de coleta em um sistema ativo.

6. C O privilégio mínimo limita cada conta aos direitos necessários para o trabalho e concede acesso elevado só de forma temporária e justificada. A separação de funções divide tarefas críticas entre pessoas para evitar fraude, que é outro controle. A defesa em profundidade combina camadas de controles. A confiança zero é um modelo mais amplo, de verificação contínua de cada requisição, e o privilégio mínimo é só um dos seus princípios de apoio.

7. A A caça a ameaças é uma busca proativa, guiada por hipóteses, de ameaças não detectadas, usando inteligência e a experiência do analista. A varredura de vulnerabilidades procura fraquezas conhecidas, não sinais de invasão. A correlação automática é uma função passiva do SIEM, baseada em regras, sem teste de hipótese feito por pessoas. A triagem só ocorre depois que já existe um alerta, e a caça começa sem alerta algum.

8. C O EDR monitora de forma contínua o comportamento dos processos, a linha de comando e as operações em memória do endpoint. Assim consegue sinalizar um PowerShell anormal e a injeção de código na memória mesmo sem arquivo malicioso no disco. O antivírus por assinaturas compara padrões conhecidos; ele até pode detectar ameaças em memória, mas a telemetria comportamental do EDR é mais adequada aqui. O firewall de rede não enxerga processos locais, e o DLP evita vazamento de dados.

9. C A criptografia de disco completo (full disk encryption) deixa todos os dados ilegíveis sem a chave correta. Assim, mesmo que o disco seja retirado e lido offline, os dados do notebook roubado continuam confidenciais. A segmentação limita o movimento lateral na rede, mas não protege um disco removido. A autenticação multifator protege o login, mas é contornada se o disco for montado em outra máquina. O IDS detecta atividade suspeita na rede e não protege dados em repouso.

10. C Desativar serviços desnecessários, remover contas padrão e fechar portas sem uso elimina possíveis pontos de entrada para um atacante. Isso é, por definição, reduzir a superfície de ataque. A segmentação divide a rede em zonas isoladas. O privilégio mínimo restringe as permissões dos usuários, não os serviços. A linha de base é o padrão de configuração documentado, e o hardening é o ato de chegar a ela.

11. A A ordem de volatilidade prioriza a evidência pela rapidez com que ela se perde. O conteúdo da RAM, as conexões de rede ativas e os processos em execução somem assim que a máquina é desligada, por isso são coletados primeiro. Os arquivos do disco continuam depois do desligamento e podem esperar. Os logs do backup remoto já estão fora do host e são pouco voláteis. A documentação impressa é estática e a de menor prioridade.

12. B Desativar serviços desnecessários e fechar portas sem uso reduz diretamente os pontos de entrada que podem ser explorados, e é um passo básico do hardening. O registro detalhado melhora a visibilidade para detecção, mas não reduz a superfície de ataque. O antivírus pode prevenir, detectar e remover malware, mas não elimina serviços expostos. O honeypot é um sistema isca para estudar atacantes, não uma medida de hardening para servidores de produção.

13. B O formulário de cadeia de custódia registra todas as pessoas que manusearam a prova, com data, hora e motivo de cada transferência. Isso apoia a integridade e a admissibilidade da prova, mas por si só não garante que ela não foi alterada. O playbook orienta as ações de resposta, mas não rastreia o manuseio. O plano de continuidade trata da resiliência operacional, e a política de retenção define por quanto tempo os dados são guardados.

14. D A RFC 3227 coloca os registradores da CPU e o cache do processador no topo da ordem de volatilidade, pois o estado do processador muda muito rápido e se perde sem energia. A RAM com os processos e as tabelas de roteamento e ARP ficam no nível seguinte, junto das estatísticas do kernel; a RFC não define ranking separado entre eles. Os arquivos temporários do disco ficam abaixo, embora também possam mudar durante a coleta.

15. D A DAI valida os pacotes ARP com a tabela de bindings do DHCP snooping e descarta as respostas ARP falsificadas, combatendo diretamente o ataque on-path de ARP spoofing. As VLANs limitam o domínio de broadcast, mas não validam o ARP dentro da mesma VLAN. Desativar portas sem uso reduz a superfície física, mas não valida o ARP nas portas ativas. O WPA3 protege tráfego sem fio e não tem relação com ARP spoofing em rede cabeada.

16. C O ransomware criptografa os arquivos da vítima e exige pagamento, em geral em criptomoeda, pela chave de descriptografia, exatamente como no cenário. O spyware coleta dados em segredo, sem criptografar arquivos. O rootkit esconde processos maliciosos das ferramentas de detecção, mas não extorque por criptografia. A bomba lógica dispara um código destrutivo por uma condição ou data, sem exigir resgate. Backups e recuperação offline são a principal defesa contra o impacto do ransomware.

17. B No pretexto, o atacante inventa um cenário ou uma identidade crível, aqui o bloqueio urgente de um executivo, para levar a vítima a ignorar a verificação normal. A carona exige seguir fisicamente uma pessoa autorizada por uma porta protegida. O shoulder surfing é observar alguém digitando credenciais. Vasculhar o lixo é recuperar materiais descartados. Nenhum dos três ocorre numa ligação como essa.

18. C No credential stuffing, pares de usuário e senha já vazados são reaproveitados em vários serviços sem relação, explorando a reutilização de senhas. O password spraying testa uma ou poucas senhas comuns em muitos usuários para evitar bloqueios, sem usar pares válidos conhecidos. A força bruta testa combinações de senhas, e o ataque de dicionário usa uma lista de senhas prováveis. Nenhum deles reaproveita pares de credenciais já vazados.

19. D O ransomware criptografa os arquivos da vítima, muda as extensões e mostra uma nota de resgate exigindo pagamento, em geral em criptomoeda, pela chave. Isso corresponde exatamente ao cenário. O worm se espalha sozinho pela rede, mas não criptografa arquivos nem cobra resgate. O rootkit busca persistência discreta e elevação de privilégio. A bomba lógica dispara uma carga destrutiva por condição ou data, sem extorsão.

20. A Vishing é phishing por voz, feito em uma ligação. Aqui o atacante usa uma chamada ao vivo para convencer o funcionário a revelar o código de uso único, uma técnica clássica de burlar o MFA em tempo real. Smishing é phishing por SMS, não por ligação. Shoulder surfing é observar a informação por cima do ombro, sem pedi-la em voz alta. Tailgating é seguir alguém fisicamente para dentro de uma área protegida.

21. C Em um ataque watering hole, o atacante compromete um site legítimo que o grupo-alvo costuma visitar e entrega o conteúdo malicioso só às vítimas pretendidas, como no cenário. O typosquatting depende de registrar domínios com erros de digitação. O XSS pode até ser o mecanismo usado, mas descreve a técnica de injeção, não a estratégia do ataque direcionado. O envenenamento de DNS altera registros de resolução, não insere cargas condicionais em um site legítimo.

22. C Uso alto e constante da CPU e calor excessivo em períodos ociosos são o sinal clássico de malware de mineração de criptomoedas, que consome em silêncio o poder de processamento para minerar para o atacante. Uma mudança no firewall bloqueia ou altera tráfego, não eleva a CPU. Logs ausentes no SIEM indicam adulteração ou falha de registro. Registros fora de ciclo são entradas com horário inesperado, sem relação com desempenho do hardware.

23. A O pharming redireciona a vítima a um site malicioso por manipulação no nível do DNS, mesmo que ela digite o endereço correto. É isso que o distingue do typosquatting, em que o redirecionamento depende de o usuário errar o domínio. O pretexting é uma técnica de engenharia social baseada em um cenário ou identidade falsos. O vishing é phishing por ligação. Como o cenário envolve comprometer um resolvedor DNS, e não erro do usuário ou contato por voz, pharming é o termo exato.

24. D Grupos APT (ameaça persistente avançada) de Estados-nação têm muito financiamento, ferramentas de dia zero próprias e paciência para operações discretas e longas, com objetivo econômico ou político estratégico. Isso combina com os oito meses sem detecção e com a exfiltração direcionada. O script kiddie não tem habilidade para criar dias zero. O hacktivista busca divulgação ou perturbação por uma causa, não roubo silencioso. A ameaça interna não intencional é um vazamento acidental.

25. D O BEC (business email compromise) é um ataque direcionado em que uma conta de e-mail de executivo, falsificada ou comprometida, serve para enganar funcionários e levá-los a transferir dinheiro ou dados, sem precisar de malware. O typosquatting registra domínios com erros de digitação para levar usuários a sites falsos. O watering hole compromete um site visitado pelo alvo. O credential stuffing usa pares de usuário e senha roubados, não um pedido de transferência por engenharia social.

26. D A ameaça interna (insider threat) é um funcionário atual ou antigo que abusa do acesso legítimo ou do conhecimento dos sistemas internos para causar dano, como o administrador demitido com credenciais ainda ativas. O hacktivista age por causas políticas ou sociais. O agente de Estado-nação faz operações patrocinadas por governos, com recursos e objetivos estratégicos muito maiores. O script kiddie tem pouca habilidade e usa ferramentas prontas, não acesso interno legítimo.

27. A O credential stuffing usa pares de usuário e senha já roubados em outra invasão e os testa em outros sites, contando com a reutilização de senhas. A força bruta testa combinações desconhecidas, em vez de repetir credenciais válidas. O password spraying testa poucas senhas comuns em muitas contas. A rainbow table é uma técnica offline para reverter hashes de senha, não uma tentativa de login on-line com credenciais vazadas.

28. C No pretexting, o atacante inventa um cenário ou uma identidade falsa, como a de auditor, para criar confiança e levar a vítima a revelar informações sensíveis. O baiting atrai a vítima com um objeto físico ou digital tentador, como um pen drive etiquetado. O tailgating é seguir fisicamente uma pessoa autorizada até uma área protegida. O quid pro quo oferece um serviço ou benefício em troca de informação, o que não ocorre aqui.

29. B A tolerância a risco define o nível aceitável de variação para uma métrica de risco específica e mensurável, aqui o limite de 5% de probabilidade anual de interrupção. O apetite a risco é a declaração estratégica e mais ampla sobre quanto risco a organização aceita para atingir seus objetivos, sem um limite numérico específico. O registro de riscos é um documento que lista riscos. A exceção de risco é um desvio aprovado da política em um caso específico.

30. D O operador (processor) trata dados pessoais só em nome e conforme as instruções do controlador, que define as finalidades e os meios do tratamento. Aqui o controlador é a varejista, não a empresa de SaaS. O titular dos dados é a pessoa a quem os dados se referem. O encarregado de proteção de dados é uma função de supervisão exigida de certas organizações pelo artigo 37 do GDPR.

31. B O Regulamento Geral de Proteção de Dados da UE dá aos titulares o direito ao apagamento (direito de ser esquecido), no artigo 17, que permite pedir a exclusão dos dados pessoais em certas condições. A HIPAA trata de informações de saúde protegidas nos EUA e não dá um direito geral de apagamento. A PCI DSS é um padrão do setor de cartões de pagamento, não de direitos dos titulares. A SOX trata da precisão de relatórios financeiros de empresas abertas.

32. A Contratar um seguro cibernético para compensar a perda financeira de um risco que não pode ser totalmente corrigido é a definição de transferência de risco: o impacto financeiro passa a um terceiro, a seguradora. A mitigação adicionaria controles técnicos ou de processo para reduzir a probabilidade ou o impacto. A evitação eliminaria a atividade de risco, como desativar o sistema legado. A aceitação toleraria o risco sem ação, enquanto aqui há transferência ativa da exposição.

33. B O SOC 2 Tipo II avalia a eficácia operacional dos controles em um período longo, em geral de 6 a 12 meses, e atende à necessidade do cliente de garantia histórica, e não de um retrato do momento. O SOC 2 Tipo I só avalia o desenho dos controles em um único momento. O SOC 1 trata de controles ligados a relatórios financeiros, não de segurança, disponibilidade ou confidencialidade. O AOC da PCI DSS atesta apenas a conformidade com cartões de pagamento.

34. D O relatório SOC 2 Tipo II avalia se os controles funcionaram de forma eficaz durante uma janela de observação definida, em geral de seis a doze meses, o que atende ao requisito. O SOC 2 Tipo I só avalia se os controles estão bem desenhados em um único momento, sem testar a eficácia ao longo do tempo. Os relatórios SOC 1 tratam de controles que afetam as demonstrações financeiras dos clientes. A ISO 27001 confirma a conformidade na data da auditoria e é uma certificação, não uma atestação sobre um período.

35. B A cláusula de direito de auditoria dá à organização o poder contratual de inspecionar os controles e as evidências de conformidade do fornecedor por iniciativa própria, sem exigir o consentimento prévio dele para agendar. Isso é essencial para a supervisão contínua do risco de terceiros. O NDA só restringe a divulgação de informações. A força maior trata da responsabilidade em eventos fora do controle das partes, como desastres naturais. A indenização define quem arca com as perdas, mas não dá acesso para auditar.

36. A Os modelos maduros de gestão de mudanças têm um procedimento de emergência que permite revisão e aprovação aceleradas fora do ciclo normal, equilibrando urgência e responsabilização. Pular a aprovação enfraquece o controle de mudanças e a trilha de auditoria, mesmo sob pressão. Esperar o CAB regular deixa o sistema exposto e ignora a previsão feita justamente para esse caso. Avisar os usuários vem depois da autorização, não antes.

37. D A auditoria externa é feita por um terceiro independente, de fora da organização, para dar garantia objetiva a reguladores, acionistas e outras partes interessadas, como na contratação de uma firma externa de contabilidade. A auditoria interna é feita pela própria área de auditoria e serve principalmente à gestão interna. A autoavaliação de conformidade é uma revisão interna informal, sem verificação independente. A avaliação de vulnerabilidades procura falhas técnicas, não a conformidade de controles financeiros.

38. A O relatório SOC 2 Tipo II é preparado por um auditor independente e avalia a eficácia operacional dos controles do fornecedor em um período longo, em geral de seis a doze meses, o que atende à necessidade de garantia contínua. O questionário de autoatestação se baseia em declarações do próprio fornecedor, sem validação independente. O teste de intrusão avalia a explorabilidade técnica em um momento, não o ambiente de controles. A BIA é um documento interno de planejamento.

39. C A aceitação de risco é adequada quando a probabilidade e o impacto são baixos e o custo do controle supera a perda potencial: a gestão reconhece formalmente o risco e não toma mais nenhuma ação. A evitação eliminaria a atividade por completo, o que é desnecessário com uma exposição tão baixa. A transferência passa o impacto financeiro a um terceiro, como um seguro. A mitigação adicionaria controles, que o cenário diz não serem custo-efetivos.

40. B A retenção legal obriga a organização a suspender os cronogramas normais de retenção e destruição para preservar os registros que podem ser relevantes ao processo, evitando a destruição de provas (spoliation). Apagar dados sob retenção é ilegal e pode gerar sanções. Criptografar os registros e manter a destruição normal não atende ao requisito central, que é preservar os dados. A custódia permanece com a organização, não com a parte contrária, para manter uma cadeia de custódia defensável.

41. A O risco residual é justamente o que sobra depois dos controles de mitigação, aqui o MFA e a segmentação, no caso a possibilidade que resta de roubo de token de sessão. O risco inerente é a exposição antes de qualquer controle. O risco secundário surgiria se os próprios controles criassem um problema novo, como ataques de fadiga de MFA, e não um resto do risco original. O risco de controle é a falha de um controle em funcionar como previsto, não uma lacuna que ele nunca foi feito para cobrir.

42. B O relatório SOC 2 Tipo II atesta a eficácia operacional dos controles em um período prolongado de revisão, em geral de seis a doze meses, enquanto o SOC 2 Tipo I só confirma que os controles estavam bem projetados em um momento específico. Os relatórios SOC 1 tratam de controles ligados a relatórios financeiros, não de segurança da informação. O certificado ISO 27001 confirma que existe um sistema de gestão de segurança certificado, mas não audita a eficácia operacional ao longo de um período, como faz o SOC 2 Tipo II.

43. A A nuvem privada oferece infraestrutura dedicada a uma única organização, hospedada no local ou por um terceiro, com controle exclusivo e isolamento dos outros clientes. A nuvem pública compartilha a infraestrutura entre muitos clientes pela internet. A nuvem comunitária é compartilhada por várias organizações com interesses comuns, como requisitos de conformidade. A nuvem híbrida combina dois ou mais modelos, o que contradiz a descrição de uso exclusivo.

44. B Uma VLAN (LAN virtual) separa logicamente os domínios de broadcast na camada 2 e permite isolar departamentos no mesmo switch, de modo que o tráfego entre eles precisa passar por roteamento e pode ser controlado ou bloqueado. A VPN protege o tráfego em redes não confiáveis, como a internet, e não faz segmentação interna. O NAT traduz endereços IP, não controla acesso. O balanceador de carga distribui o tráfego entre servidores e não cria segmentos isolados.

45. C O erro indica que o cliente não consegue montar uma cadeia de confiança até uma raiz confiável, ou seja, falta o certificado da CA raiz no repositório de confiança. Sem ele, o navegador não valida a cadeia emissora, mesmo que o certificado do servidor esteja correto. A chave privada nunca sai do servidor e não faz parte do repositório do cliente. O ticket de sessão é um recurso de retomada do TLS, sem relação com a confiança PKI. A chave simétrica é negociada depois que a confiança já foi estabelecida.

46. A O hash criptográfico gera um valor único de tamanho fixo a partir do conteúdo do arquivo. Qualquer alteração, mesmo de um único bit, muda o hash por completo, então a correspondência com o valor publicado pelo fornecedor confirma a integridade. O tamanho do arquivo pode coincidir mesmo com conteúdo corrompido. A inspeção visual é inviável em um ISO binário e não revela corrupção sutil. Criptografar e descriptografar testa a cifra, não se os bytes originais foram alterados antes.

47. C O DHE (e sua variante de curva elíptica, ECDHE) gera um par de chaves novo e exclusivo da sessão a cada handshake e descarta a chave privada efêmera depois. Assim, comprometer mais tarde a chave estática do certificado do servidor não permite descriptografar sessões já capturadas: é o sigilo de encaminhamento perfeito (perfect forward secrecy). Na RSA estática, quem obtém a chave privada de longo prazo abre as sessões passadas. O PSK sem DH efêmero reutiliza o mesmo segredo e não dá esse sigilo. O Kerberos é autenticação, não troca de chaves TLS.

48. A A criptografia leve (lightweight cryptography) foi projetada para dar segurança adequada com mínimo de processamento, consumo de bateria e memória, o que é essencial em dispositivos embarcados e IoT com recursos limitados. Escolher o algoritmo mais forte sem olhar os recursos pode esgotar a bateria e causar falhas de desempenho. Os algoritmos resistentes à computação quântica costumam exigir chaves maiores e mais processamento do que esses dispositivos suportam hoje. O DES é obsoleto e quebrado, e não dá segurança adequada.

49. B O air gap isola fisicamente um sistema ou rede, sem conexão com ou sem fio com qualquer outra rede, o que impossibilita ataques remotos pela rede contra esse segmento. A sub-rede protegida ainda mantém conectividade controlada por firewalls. A confiança zero é uma filosofia de acesso que exige verificação contínua de cada conexão, não isolamento físico. A microssegmentação cria zonas lógicas granulares dentro de uma rede conectada, o oposto de não ter conexão alguma.

50. D A microssegmentação aplica políticas de firewall granulares por carga de trabalho, que podem permitir só o tráfego leste-oeste necessário entre as duas VMs e ainda bloquear o movimento lateral não autorizado, mesmo na mesma VLAN e sub-rede. Criar uma VLAN por VM quebraria o requisito de mesma sub-rede e não escala. O IDS em modo promíscuo só detecta, não bloqueia. O port security controla endereços MAC na porta física e não restringe a comunicação na camada de aplicação entre VMs.

51. C O balanceamento ativo-passivo com failover automático mantém um servidor em espera pronto para assumir quando o ativo falha, o que garante alta disponibilidade com interrupção mínima. As configurações ativo-ativo distribuem o tráfego entre vários servidores ativos. A criptografia de disco protege a confidencialidade, não a disponibilidade. Um único ponto de presença com reinício manual gera indisponibilidade e é um ponto único de falha. Um backup desligado e em air gap não faz failover automático e causa queda durante a falha.

52. B A assinatura digital usa a chave privada do signatário, então só aquele fornecedor poderia tê-la criado. Verificá-la com a chave pública prova a origem e impede que ele negue a autoria, que é o não repúdio (non-repudiation). A criptografia simétrica protege a confidencialidade, não prova a origem, e depende de uma chave compartilhada que as duas partes poderiam usar. O balanceamento de carga trata de disponibilidade. O hash isolado verifica a integridade, mas não a identidade, pois qualquer pessoa pode calculá-lo.

53. B O air gap isola a rede física e logicamente de todas as outras, inclusive a internet e a TI corporativa, eliminando os caminhos de ataque remoto. É um controle comum em ambientes críticos de SCADA e ICS, em que disponibilidade e segurança física (safety) pesam mais que conectividade. A sub-rede protegida ainda permite conectividade externa controlada por firewalls. O servidor de salto é um ponto de acesso controlado, o que pressupõe conectividade. A VPN cria um túnel criptografado, o oposto de isolamento.

54. C Credenciais padrão combinadas com uma rede plana, ao lado de sistemas financeiros sensíveis, são o maior risco imediato de comprometimento e movimento lateral. Trocar as credenciais e isolar os dispositivos IoT em uma VLAN própria fecha tanto a falha de autenticação quanto a exposição de rede. Atualizar o firmware com mais frequência é boa prática, mas não trata o risco imediato de credenciais e segmentação. Desativar o SNMP nas estações do financeiro não corrige a vulnerabilidade do IoT, e a geocerca não tem relação com esse risco de rede.

55. A No OCSP stapling, o servidor web consulta a CA de tempos em tempos e anexa ao handshake TLS a resposta OCSP assinada e com data e hora. O cliente nunca contata a CA, o que evita o vazamento de privacidade sobre os sites visitados e a latência de uma ida e volta extra. O OCSP padrão exige que o cliente consulte a CA em tempo real, expondo a navegação e atrasando. As CRLs são grandes, atualizadas raramente e ainda precisam ser baixadas pelo cliente. O pinning define em qual certificado confiar, não como o status de revogação é entregue.

56. B O Nível 1 (controle básico) é onde ficam os PLCs, RTUs e outros controladores que executam a lógica de controle em tempo real e se comunicam diretamente com os dispositivos do Nível 0. O Nível 0 é o próprio processo físico, com sensores, válvulas e motores, e não os controladores que os comandam. O Nível 2 reúne funções supervisórias, como IHMs e o software supervisório SCADA, que agregam vários controladores do Nível 1. O Nível 3 trata das operações do local, como o planejamento da produção, mais afastado do controle em tempo real.

57. C O plano de reversão (rollback/backout) define os passos exatos para devolver o sistema ao último estado em que funcionava, o que determina a rapidez com que o serviço volta quando há uma interrupção. A análise de impacto mostra quem é afetado, mas não traz um procedimento de recuperação. A assinatura de aprovação é uma formalidade de governança, não um mecanismo técnico de recuperação. Os testes em sandbox reduzem a chance de falha antes, mas não ajudam quando a mudança já causou uma queda em produção.

58. D Os controles detectivos identificam e alertam sobre um evento de segurança enquanto ocorre ou depois, e é isso que o alarme de movimento faz ao avisar a segurança quando há movimento não autorizado. Um controle preventivo impediria a entrada, como uma porta trancada ou um leitor de crachá. Um controle corretivo agiria depois do incidente para restaurar ou consertar sistemas, e não apenas alertar. Um controle dissuasivo desencoraja o atacante de tentar, como uma placa de aviso visível, sem detectar uma ação em andamento.

59. B Energia redundante, RAID 10 e cluster de failover eliminam pontos únicos de falha e mantêm o sistema acessível diante de uma falha de hardware, que é a definição de disponibilidade. Não é confidencialidade, pois nenhum desses controles restringe quem pode ver os dados. Não é integridade, pois essas medidas não verificam se os dados foram alterados. O não repúdio não faz parte da tríade CIA e trata da prova de uma ação, em geral por assinaturas digitais e logs, não de tempo de atividade.

60. A A separação de funções divide tarefas críticas entre várias pessoas, de modo que ninguém consiga completar sozinho um processo de alto risco, o que reduz as chances de fraude e erro. O privilégio mínimo limita o acesso do usuário ao necessário para o cargo, mas não divide um processo entre duas pessoas. O rodízio de funções troca os funcionários de cargo para expor fraudes ao longo do tempo, não para dividir uma transação. As férias obrigatórias permitem que outros revisem o trabalho, uma medida detectiva, não uma divisão estrutural de funções.

61. D A autorização ocorre depois que a identidade foi verificada e define as permissões ou os direitos de acesso concedidos ao usuário, muitas vezes aplicados por controle de acesso baseado em função (RBAC). A autenticação apenas confirma a identidade declarada por meio de credenciais. A contabilização registra e acompanha a atividade para auditoria, não decide permissões. A identificação é só a declaração inicial de identidade, como digitar um nome de usuário, antes de qualquer verificação.

62. A A confiança zero segue o princípio 'nunca confie, sempre verifique' e exige autenticação e autorização contínuas em cada requisição, venha de dentro ou de fora do limite tradicional da rede. A defesa por perímetro confia implicitamente em quem está dentro da borda da rede, o oposto. A defesa em profundidade descreve camadas de controles, não um modelo de confiança específico. O RBAC é um método de autorização usado dentro da confiança zero, não o modelo geral.

63. D Alterar dados em trânsito é uma modificação não autorizada da informação, que é a definição de violação de integridade. Haveria violação de confidencialidade se o atacante apenas visse ou extraísse os dados sem alterá-los. A disponibilidade trata da negação de acesso ou serviço; a transação foi processada, só que com dados corrompidos. O não repúdio não é um dos três princípios da CIA: é um conceito de responsabilização, útil na perícia desse ataque, mas o princípio comprometido aqui é a integridade.

64. C Isso descreve o Change Advisory Board (CAB), cujo papel principal é avaliar o risco, o impacto e o plano de reversão das mudanças propostas antes de aprová-las ou rejeitá-las, reduzindo paradas não planejadas. A instalação técnica cabe aos administradores de sistemas, não ao comitê. O plano de resposta a incidentes é uma função separada de planejamento. O treinamento de conscientização é um controle operacional sem relação com o controle de mudanças.

65. D O plano de reversão documentado e testado é avaliado antes da implementação e serve justamente para restaurar rápido o último estado que funcionava se a mudança falhar, minimizando a indisponibilidade. O plano de continuidade revisado ajuda durante interrupções, mas é menos adequado para desfazer essa mudança específica. O inventário de ativos ajuda a identificar sistemas afetados, mas não reduz o impacto de uma mudança que falhou. O modelo de relatório é reativo, usado depois da queda.

66. A Uma colisão de hash permite que o atacante troque o arquivo legítimo por um malicioso com o mesmo hash, anulando a função do hash de provar que o arquivo não foi alterado, que é a definição de integridade. A confidencialidade trata da divulgação não autorizada de dados, que a colisão não afeta. A disponibilidade trata do tempo de atividade dos sistemas, não da confiabilidade de um arquivo. A autorização define o que um sujeito autenticado pode fazer e não tem relação com verificar se o conteúdo do arquivo é o original.

67. A O policy engine é o componente de decisão do ponto de decisão de políticas: executa o algoritmo de confiança com entradas como identidade, conformidade do dispositivo e inteligência de ameaças e gera a decisão de permitir ou negar. O policy enforcement point é o porteiro que abre ou encerra a conexão conforme essa decisão, sem decidir. O policy administrator gera as credenciais de sessão que levam a decisão ao ponto de aplicação. O sistema CDM só fornece dados de postura do dispositivo como uma das entradas.

68. A O ABAC avalia vários atributos dinâmicos do sujeito, do recurso e do ambiente (departamento, classificação do arquivo, horário, conformidade do dispositivo) e gera uma decisão em tempo real, sendo base das arquiteturas de confiança zero. O RBAC considera só a função atribuída ao usuário e não tem essa granularidade contextual. No DAC, o dono do recurso define as permissões, sem mecanismo nativo para avaliar atributos do ambiente. O MAC usa rótulos e autorizações fixos, definidos pelos administradores, sem considerar o dispositivo ou o horário.

69. C O privilégio mínimo restringe os direitos de acesso ao mínimo necessário para a função, o que corresponde a limitar o técnico às estações do departamento e não dar acesso total ao domínio. A separação de funções divide uma tarefa entre várias pessoas, não limita o nível de acesso de uma. A defesa em profundidade é a combinação de camadas independentes de controles, não a delimitação do acesso de uma conta. A confiança zero é um modelo mais amplo, de verificação contínua de cada requisição.

70. B O não repúdio usa mecanismos criptográficos, como assinaturas digitais ligadas a uma chave privada, para provar a origem de uma ação e impedir que o signatário negue sua participação. Não é confidencialidade, pois o cenário não trata de manter a transferência em segredo. Não é só integridade, que garante apenas que a mensagem não foi alterada, sem tornar o remetente responsável. A autenticação verifica a identidade ou a origem da mensagem, mas o não repúdio é o que impede de negar uma ação assinada.

Palavras-chave em inglês

confidentiality	confidencialidade	Só pessoas autorizadas conseguem ler a informação.
integrity	integridade	A informação não foi alterada sem autorização.
availability	disponibilidade	O sistema e os dados estão acessíveis quando são necessários.
non-repudiation	não repúdio	Quem fez uma ação não consegue negar depois que a fez.
authentication	autenticação	Processo que prova a identidade de um usuário ou dispositivo.
authorization	autorização	Define o que um usuário autenticado pode fazer.
accounting	contabilização (registro de atividades)	Registro do que cada usuário fez e quando; o terceiro A de AAA.
multifactor authentication (MFA)	autenticação multifator	Login com dois ou mais fatores de tipos diferentes.
zero trust	confiança zero	Modelo que verifica cada acesso e não confia em ninguém por padrão.
least privilege	privilégio mínimo	Dar a cada usuário só o acesso necessário ao seu trabalho.
compensating control	controle compensatório	Controle alternativo usado quando o controle principal não é viável.
deterrent control	controle dissuasivo	Controle que desencoraja o atacante, como uma placa de aviso.
change management	gestão de mudanças	Processo para pedir, avaliar, aprovar e registrar mudanças em sistemas.
threat actor	agente de ameaça	Pessoa ou grupo que pode realizar um ataque ou causar dano.
vulnerability	vulnerabilidade	Fraqueza que um atacante pode explorar.
zero-day	vulnerabilidade de dia zero	Falha explorada antes de existir uma correção do fabricante.

social engineering	engenharia social	Manipular pessoas para obter acesso, dinheiro ou informação.
phishing	phishing	Mensagem falsa que tenta roubar dados ou instalar malware.
business email compromise (BEC)	comprometimento de e-mail corporativo	Fraude com uma conta de e-mail corporativa controlada pelo atacante.
typosquatting	typosquatting (domínio com erro de digitação)	Registrar um domínio quase igual ao verdadeiro para enganar o usuário.
ransomware	ransomware	Malware que bloqueia ou criptografa dados e exige pagamento.
indicator of compromise (IoC)	indicador de comprometimento	Sinal de que um sistema pode ter sido invadido.
patch	patch (correção)	Atualização que corrige uma falha no software.
hardening	hardening (reforço de segurança)	Reduzir a superfície de ataque, removendo serviços e ajustando configurações.
segmentation	segmentação	Dividir a rede em partes para limitar o movimento do atacante.
encryption	criptografia	Transformar dados para que só quem tem a chave possa ler.
hashing	cálculo de hash	Gera um valor de tamanho fixo para verificar a integridade dos dados.
public key infrastructure (PKI)	infraestrutura de chaves públicas	Sistema que emite, gerencia e revoga certificados digitais.
certificate revocation list (CRL)	lista de certificados revogados	Lista de certificados cancelados antes do vencimento.
Online Certificate Status Protocol (OCSP)	protocolo de status de certificado online	Consulta se um certificado específico está válido ou revogado.
operational technology (OT)	tecnologia operacional	Sistemas que controlam equipamentos físicos, como máquinas de uma fábrica.
security information and event management (SIEM)	gerenciamento de informações e eventos de segurança	Reúne e correlaciona logs de muitas fontes.
endpoint detection and response (EDR)	detecção e resposta em endpoints	Monitora os endpoints e pode isolar um deles.
security orchestration, automation and response (SOAR)	orquestração, automação e resposta de segurança	Automatiza os passos da resposta a incidentes.
data loss prevention (DLP)	prevenção contra perda de dados	Detecta e impede a saída não autorizada de dados.

incident response	resposta a incidentes	Processo para detectar, conter e erradicar um incidente e recuperar os sistemas.
chain of custody	cadeia de custódia	Registro de quem guardou e manuseou uma evidência, e quando.
recovery point objective (RPO)	objetivo de ponto de recuperação	Quantidade máxima de dados que você aceita perder, medida em tempo.
recovery time objective (RTO)	objetivo de tempo de recuperação	Prazo para colocar o sistema de volta no ar.
risk register	registro de riscos	Documento que lista riscos, responsáveis e o tratamento de cada um.
order of volatility	ordem de volatilidade	Sequência de coleta de evidências, da que se perde mais rápido à mais estável.
least functionality	funcionalidade mínima	Manter apenas serviços, protocolos e contas necessários ao propósito do sistema.
air gap	air gap (isolamento físico)	Rede sem nenhuma conexão com outras redes, com ou sem fio.
microsegmentation	microssegmentação	Políticas de firewall por carga de trabalho que bloqueiam o movimento lateral.
perfect forward secrecy	sigilo de encaminhamento perfeito	Sessões passadas continuam seguras mesmo se a chave do servidor vazar.
residual risk	risco residual	Risco que permanece depois de aplicar os controles.
risk tolerance	tolerância a risco	Limite específico e mensurável de risco que a organização aceita.
legal hold	retenção legal	Ordem de preservar registros relevantes a um litígio, suspendendo a destruição.
right to audit	direito de auditoria	Cláusula que permite ao cliente auditar os controles do fornecedor.
pretexting	pretexto	Inventar uma identidade ou um cenário para enganar a vítima.

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/comptia-security-plus/