Strecht Simulados · Guia de preparação



Guia de preparação CompTIA Security+ SY0-801

Tudo o que a prova cobra, organizado por domínio: conceitos-chave, comparações que confundem, pegadinhas reais, gatilhos do enunciado, questões comentadas e um plano para chegar pronto ao exame.

5 capítulos por domínio	**32** questões comentadas	**83%** nota de corte
6 provas completas no curso		

ANTES DE COMEÇAR

Como usar este guia

Este guia foi feito para ser estudado junto com as 6 provas completas do curso CompTIA Security+ SY0-801: o guia explica o que cai e onde estão as armadilhas; as provas treinam o ritmo e mostram o que você ainda não domina.

Quando	O que fazer
Semana 1	Faça o teste diagnóstico (página seguinte) e leia os capítulos 1 e 2. No fim da semana, faça a Prova 1 do curso no tempo do exame.
Semana 2	Leia os demais capítulos, começando pelos domínios em que você errou mais no diagnóstico. Faça as provas 2 e 3.
Semana 3	Releia os alertas de pegadinha e as tabelas de comparação. Faça as provas 4 e 5 e revise cada erro pela explicação.
Semana 4	Estude a folha de cola, faça a Prova 6 e refaça as provas abaixo de 80%. Agende o exame quando estiver acima de 80% em todas (a nota de corte é 83%).

Mapa do exame

Cada prova do curso tem 90 questões e 90 minutos, no formato do exame. Referência de aprovação: 83%.

Domínio (capítulo)	Peso	Neste guia
1. Ameaças, Vulnerabilidades e Ataques	24%	18 conceitos · 14 pegadinhas
2. Arquitetura de Segurança	19%	18 conceitos · 14 pegadinhas
3. Conceitos Gerais de Segurança	16%	19 conceitos · 14 pegadinhas
4. Gestão e Supervisão do Programa de Segurança	14%	17 conceitos · 14 pegadinhas
5. Operações de Segurança	27%	19 conceitos · 14 pegadinhas

Como ler os capítulos: os **tópicos-chave** são o que mais cai; a **tabela de memorização** separa o que a prova costuma confundir; os **alertas de prova** mostram as armadilhas das alternativas erradas; os **gatilhos** ligam palavras do enunciado à resposta; e o **checklist** diz se você está pronto para o domínio.

Estude um pouco todo dia, de graça

Instagram @strecht.simulados

Um post de prova por dia: questão comentada, pegadinhas e o “não confunda” de cada certificação.

Seguir no Instagram →

YouTube Strecht Simulados

Shorts diários com pegadinhas de prova e, aos sábados, um simulado comentado.

Inscrever-se no canal →

DIAGNÓSTICO

Você já sabe isso?

Responda às 12 questões sem consultar nada. As respostas, com a explicação e o capítulo para revisar, estão no fim do guia. Comece o estudo pelos capítulos em que errou.

D1 · Ameaças, Vulnerabilidades e Ataques

Um assistente de IA da Rede de Clínicas Saúde Total, com acesso à base de prontuários para ajudar os médicos, respondeu a um usuário comum, que pediu um exemplo de laudo, com o laudo real de outro paciente, incluindo nome e diagnóstico. Que risco associado à IA ocorreu?

A. Alucinação de um laudo fictício
B. Viés no treinamento do modelo
C. Perda de dados pela saída do modelo
D. Envenenamento da base de prontuários

D2 · Ameaças, Vulnerabilidades e Ataques

Minutos depois que um servidor sem patch da Rede Hospitalar Cuidar foi infectado, o mesmo malware apareceu em dezenas de outros servidores, explorando sozinho uma vulnerabilidade do protocolo SMB, sem nenhuma ação dos usuários. Que tipo de malware tem esse comportamento?

A. Worm autopropagável
B. Adware de navegador
C. Trojan de acesso remoto
D. Spyware de monitoramento

D3 · Ameaças, Vulnerabilidades e Ataques

Semanas antes de uma eleição nacional, perfis falsos coordenados e sites recém-criados passaram a divulgar documentos vazados e adulterados de candidatos, buscando mudar a opinião do eleitorado. As investigações apontaram ligação com o governo de outro país. Qual ator e qual motivação são mais prováveis?

A. Crime organizado, com motivação financeira
B. Atacante sem habilidade, por curiosidade
C. Concorrente comercial, por propriedade intelectual
D. Patrocinado por Estado, com motivação de influência

D4 · Arquitetura de Segurança

A Startup Nuvem Verde hospeda sua aplicação em um provedor que atende milhares de clientes na mesma infraestrutura, com isolamento lógico entre eles, cobrança por uso e contratação pela internet. Que modelo de implantação é esse?

A. Nuvem pública multilocatária
B. Datacenter próprio da startup
C. Nuvem comunitária setorial
D. Nuvem privada dedicada

D5 · Arquitetura de Segurança

Sem comprar switches novos, a Escola Técnica Futuro quer separar em redes distintas os computadores dos alunos, os da administração e as câmeras de segurança, aplicando regras entre elas no firewall. Que técnica atende?

A. Isolamento air gap das redes
B. Rede plana com IPs fixos
C. Segmentação física com cabos novos
D. Segmentação lógica por VLANs

D6 · Arquitetura de Segurança

Uma analista da Seguradora Ômega passou por três áreas em cinco anos e, a cada mudança, manteve os acessos antigos, acumulando permissões em sistemas de sinistros, financeiro e RH que não usa mais. Que problema de gestão de identidades isso caracteriza?

A. Credencial codificada no código
B. Federação entre domínios
C. Escalonamento de privilégio por exploit no kernel
D. Acúmulo de privilégios (privilege creep)

D7 · Conceitos Gerais de Segurança

Na Cooperativa Café do Vale, a analista de folha de pagamento recebeu permissão de leitura e escrita em todas as pastas do servidor de arquivos, para não precisar pedir acesso quando surgisse uma demanda. Qual princípio de segurança essa concessão viola?

A. Defesa em profundidade
B. Separação de funções
C. Não repúdio das ações
D. Menor privilégio

D8 · Conceitos Gerais de Segurança

Um analista da Rede Hoteleira Mar Azul quer alterar regras do firewall principal em produção. A política de gestão de mudanças exige que a solicitação, com análise de impacto e plano de reversão, seja avaliada antes por um grupo com representantes de TI, segurança e áreas de negócio. Que grupo é esse?

A. Comitê consultivo de mudanças (CAB)
B. Centro de operações de segurança (SOC)
C. Comitê de auditoria do conselho
D. Equipe de resposta a incidentes (CSIRT)

D9 · Conceitos Gerais de Segurança

O administrador da Editora Pinheiral vai obter de uma autoridade certificadora pública um certificado TLS para o portal do cliente. Ele gera o par de chaves no próprio servidor e cria a solicitação de assinatura (CSR). O que deve ir na CSR enviada à AC?

A. O certificado raiz da AC e a chave privada do servidor
B. A chave pública e os dados que identificam o servidor
C. A chave privada cifrada com a senha do administrador
D. A chave privada e os dados de identificação do servidor

D10 · Gestão e Supervisão do Programa de Segurança

A Fintech Andes quer contratar um provedor de SOC sediado em outro país, mas descobre que a legislação local permite que autoridades estrangeiras exijam acesso aos dados tratados pelo provedor e que transferências internacionais exigem salvaguardas específicas. Que limitação na gestão de terceiros está sendo considerada?

A. Geografia e jurisdição do fornecedor
B. Disponibilidade de pessoal interno
C. Aprisionamento tecnológico
D. Retorno sobre o investimento

D11 · Gestão e Supervisão do Programa de Segurança

Antes de iniciar um teste de intrusão na Prefeitura de Lago Azul, a contratada e a prefeitura documentam escopo, IPs permitidos e proibidos, horários, técnicas autorizadas e contatos de emergência. Como se chama esse documento?

A. Política de uso aceitável
B. Plano de continuidade de negócios
C. Acordo de nível de serviço
D. Regras de engajamento (RoE)

D12 · Gestão e Supervisão do Programa de Segurança

Antes de iniciar o programa de auditoria interna de segurança, o conselho da Cooperativa Central aprovou um documento que define o propósito, a autoridade, a independência, o escopo e a quem a auditoria se reporta. Como esse documento é chamado?

A. Declaração de trabalho (SOW)
B. Política de uso aceitável
C. Carta de auditoria
D. Plano de resposta a incidentes

01

CAPÍTULO 1 · 24% DA PROVA

Ameaças, Vulnerabilidades e Ataques

Este domínio vale 24% e no V8 passou a se chamar 'Threats, Vulnerabilities, and Attacks', com as mitigações levadas para Operações e um objetivo novo só de ameaças ligadas a IA. O que eu preciso dominar: atores e motivações, vetores (inclusive quishing, deepfake, RCS, ferramentas de colaboração e cadeia de suprimentos), tipos de malware, vulnerabilidades e superfícies de ataque (LLMs, IdP, repositórios públicos, armazenamento de objetos público), indicadores de atividade maliciosa e fontes de inteligência. As questões trazem trechos de log ou um cenário curto e pedem o nome exato do ataque, então cada detalhe conta: uma senha em muitas contas é spraying, a mesma falha com patch disponível não é dia zero. Onde mais erro: misturar os ataques de IA (injeção, jailbreak, evasão, envenenamento) e os pares de engenharia social (spear phishing x whaling, vishing x smishing).

Neste capítulo

18 tópicos-chave · 14 pegadinhas · 6 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Atores de ameaça

Patrocinado por Estado (recursos altos, espionagem ou influência, permanência longa), crime organizado (lucro e extorsão, estrutura de empresa com negociadores e afiliados), hacktivista (causa ideológica ou política, protesto público), ameaça interna (maliciosa por vingança ou dinheiro, ou acidental), concorrente (busca vantagem comercial, como propriedade intelectual), terrorista (medo e caos) e atacante sem habilidade (ferramentas prontas e tutoriais). APT é a ameaça persistente avançada: alta sofisticação e recursos, ferramentas próprias, troca constante de infraestrutura e permanência prolongada nas redes.

Motivações

Financeira e extorsão (crime organizado com resgate), espionagem, influência (Estado estrangeiro tentando mudar a opinião do eleitorado com vazamentos e perfis falsos), propriedade intelectual (fórmula sigilosa parando no concorrente), vingança, ideológica ou política (pressionar uma votação), notoriedade (ataque assinado e exibido nas redes), medo e caos (terrorista), curiosidade geral e ética (pentest autorizado com escopo).

Atributos de atores

Interno ou externo (já está dentro com acesso legítimo ou precisa obter acesso inicial), recursos e financiamento, e nível de sofisticação (capacidade de explorar falhas desconhecidas). Probabilidade e impacto são da análise de risco; vetor e superfície descrevem o caminho, não o ator.

Engenharia social por canal

Phishing em massa (genérico), spear phishing (sob medida para um funcionário), whaling (sob medida para executivo), vishing (voz), smishing (SMS ou RCS, inclusive com logotipo e botões), quishing (QR code forjado), pharming (DNS ou hosts alterados) e deepfake de voz ou vídeo gerado por IA. BEC é o e-mail de conta real de fornecedor comprometida pedindo troca de conta bancária.

Vetores baseados em mensagem e arquivo

Mensageria instantânea com personificação (foto do diretor pedindo cartões-presente), ferramenta de colaboração (falso 'Suporte de TI' no chat corporativo pedindo para instalar acesso remoto), e-mail que é só uma imagem com link para escapar do antispam, anexo com macro ('Habilitar Conteúdo'), PDF que explora o leitor desatualizado e CAPTCHA falso que manda pressionar Windows+R e colar um comando (ClickFix).

Cadeia de suprimentos

Provedor de serviços gerenciados (RMM do MSP comprometido atinge todos os clientes), provedor SaaS invadido expondo dados de centenas de clientes, provedor de logística (firmware trocado no transporte) e atualização maliciosa (backdoor inserido no pacote oficial, assinado e distribuído normalmente).

Vetores de endpoint, rede e sinal

Living off the land (certutil, PowerShell, WMI, sem executável próprio), dispositivo confiável comprometido (dispensado de MFA), USB que emula teclado, dispositivo rogue e ponto de acesso rogue, IoT com senha padrão, appliance virtual esquecido sem patch, roteador de borda com firmware explorado, Bluetooth detectável, clonagem de crachá RFID/NFC e acesso remoto exposto (RDP, VNC sem senha, appliance de VPN sem patch).

Tipos de malware

Worm se propaga sozinho (ex.: falha SMB, sem clique); vírus se anexa a programas e depende de execução; trojan parece útil e instala acesso remoto; rootkit esconde processos e conexões no kernel (ps e netstat mentem); keylogger grava teclas; spyware coleta dados às escondidas; adware injeta propaganda; bomba lógica dispara por condição ou data; ransomware cifra, apaga cópias de sombra e deixa nota; fileless executa em memória via PowerShell -EncodedCommand.

Vulnerabilidades de software e configuração

Dia zero (explorada antes de existir correção), sistema sem patch (correção disponível e não aplicada), produto sem suporte (fabricante não corrige mais), sistema obsoleto (sem peças nem especialistas), sistema não gerenciado (fora do CMDB, sem dono, sem EDR), má configuração (permissão para Todos, painel sem senha), portas e serviços desnecessários, credenciais obsoletas, segredo codificado no código, tratamento inseguro de exceções (stack trace e SQL na tela) e shadow IT (área contrata serviço sem conhecimento ou aprovação da TI, descoberto com CASB).

Falhas de código e memória

Estouro de buffer (entrada enorme sobrescreve o endereço de retorno na pilha), condição de corrida TOCTOU (verifica saldo e debita depois; pedidos simultâneos sacam além do saldo), injeção de SQL (aspas e UNION SELECT), travessia de diretório (../../etc/passwd), XSS (script roda no navegador da vítima) e CSRF (página maliciosa faz o navegador enviar requisição autenticada com o cookie).

Superfícies de ataque novas do V8

Armazenamento de objetos com leitura pública (bucket de testes aberto), repositório público com segredo (arquivo .env no GitHub), provedor de identidade comprometido (raiz de confiança de todos os acessos federados: o atacante emite tokens aceitos por tudo) e LLMs integrados a dados e ferramentas.

Ataques de rede e de credencial

Spoofing de ARP (MAC do atacante como gateway), envenenamento de cache DNS (nome correto, IP errado no resolvedor), DDoS por reflexão e amplificação (IP de origem falsificado, respostas grandes de resolvedores abertos), on-path, downgrade de protocolo, replay (token fixo reenviado), sequestro de sessão com cookie roubado (sem senha nem MFA), password spraying, credential stuffing, força bruta, fadiga de MFA e enumeração de usuários por mensagens de erro diferentes.

Indicadores de atividade maliciosa

Viagem impossível (mesmo usuário em continentes diferentes em minutos), sessões concorrentes, bloqueio de conta, manipulação de logs (evento 1102 de log de auditoria limpo logo após login administrativo fora do horário) e IoCs compartilháveis como hash do executável, IP de comando e controle e domínio de entrega.

Identificação e pontuação de vulnerabilidades

CVE é o identificador único; CVSS pontua a severidade; CWE classifica o tipo de fraqueza; NVD enriquece o CVE com CVSS, CPE e CWE; o catálogo KEV da CISA lista o que está sendo explorado ativamente e ajuda a priorizar. No CVSS v4.0 os grupos são Base, Threat, Environmental e Supplemental; o Threat substituiu o Temporal do v3.x.

Fontes de inteligência

Proprietária (paga, restrita a assinantes), OSINT (blogs, redes sociais, repositórios públicos), governamental (alertas do CERT e da agência nacional) e ISAC (compartilhamento setorial sob confidencialidade). Para feed automatizado: STIX é o formato dos dados e TAXII é o transporte.

Ameaças a modelos de IA

Injeção de prompt direta ou indireta (instrução escondida em e-mail ou documento lido pela IA), jailbreak (fazer o modelo ignorar suas regras, como 'interpretar um personagem sem regras'), evasão (entrada ajustada para o classificador errar na inferência, sem mudar o modelo), envenenamento de dados de treino, extração do modelo por consultas e inversão (reconstruir dados de treino).

Riscos do uso de IA

Alucinação (cita cláusula inexistente), falta de explicabilidade, viés herdado do histórico, perda de dados pela saída (devolve laudo real de outro paciente), tratamento inadequado da saída (HTML do LLM vira XSS), agente induzido a executar código e a usar a sessão do usuário, manipulação dos pesos por API de ajuste fino mal protegida, questões éticas de transparência e dados pessoais colados em chatbot público sem contrato (podem ser usados para treino).

Ataques físicos

Tailgating (entrar colado em quem passou o crachá), barrado por vestíbulo de controle de acesso com duas portas que nunca abrem juntas; skimming (leitor clandestino sobre o original); shoulder surfing (espiar tela ou digitação); falsificação de biometria (molde de digital); personificação de prestador com uniforme e ordem de serviço falsa.

Macetes para memorizar

💡 Identificadores de vulnerabilidade

CVE é o nome, CVSS é a nota, CWE é o tipo, NVD é a ficha completa, KEV é a lista do que já está sendo explorado.

💡 Spraying x força bruta

Uma senha, muitas contas: spraying. Muitas senhas, uma conta: força bruta.

💡 Canais de phishing

V de voz (vishing), S de SMS/RCS (smishing), Q de QR code (quishing), W de whale, o peixe grande (whaling).

💡 IA: quando acontece o ataque

Treino envenenado = poisoning; entrada disfarçada na hora = evasão; instrução escondida = injeção; 'esqueça as regras' = jailbreak.

Sem patch x dia zero x sem suporte

Tem patch e não aplicou: sem patch. Não tem patch ainda: dia zero. Nunca mais terá: sem suporte.

Motivação pelo comportamento

Pediu dinheiro: financeira. Protestou: ideologia. Exibiu: notoriedade. Ficou quieto meses roubando: espionagem. Quis mudar a opinião pública: influência.

Tabela de memorização: não confunda

Quando é...	...e quando é
Password spraying Uma senha comum (ex.: Verao2026!) testada em muitas contas, uma tentativa por conta.	**Credential stuffing / força bruta** Stuffing usa pares usuário e senha vazados, diferentes por conta; força bruta testa muitas senhas contra a mesma conta.
Dia zero Explorada antes de existir qualquer correção; recomendação provisória é mitigar e monitorar indicadores.	**Sistema sem patch / produto sem suporte** Sem patch: correção disponível e não aplicada. Sem suporte: fabricante encerrou o suporte e não corrigirá novas falhas.
Injeção de prompt Instruções maliciosas (diretas ou escondidas em conteúdo lido) desviam o que o modelo faz, como encaminhar a caixa de entrada.	**Jailbreak** O usuário convence o modelo a ignorar as próprias políticas de segurança e gerar conteúdo proibido.
Ataque de evasão Altera a entrada no momento da inferência; o modelo não muda.	**Envenenamento de dados** Altera os dados de treino (parceiro envia fraudes marcadas como legítimas) e o modelo passa a decidir errado.
Spear phishing Mensagem personalizada para um funcionário comum, como um analista de compras.	**Whaling** Mensagem personalizada para executivo do alto escalão.
Worm Propaga-se sozinho pela rede explorando falha, sem ação do usuário.	**Vírus / trojan** Vírus se anexa a programas e depende de execução; trojan é programa útil por fora que instala acesso remoto por dentro.
Envenenamento de cache DNS O usuário digita o nome correto e o resolvedor devolve o IP do atacante.	**Typosquatting** O atacante registra domínio parecido e conta com o erro de digitação da vítima.

Números que caem

Item	Valor

Peso do domínio na prova	**24%**
Porta do RDP	**TCP 3389**
Porta do VNC	**5900**
Porta do SSH	**22**
Portas de FTP, Telnet e MySQL	**21, 23 e 3306**
Evento do Windows de log de auditoria limpo	**1102**
Grupos de métricas do CVSS v4.0	**Base, Threat, Environmental e Supplemental**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Chamar de credential stuffing o log com cerca de 400 contas diferentes e a mesma senha.
Como não cair: Mesma senha em muitas contas é password spraying; stuffing usa pares vazados distintos por conta.

⚠ **Alerta de prova:** Classificar como dia zero a falha divulgada oito meses antes com correção disponível.
Como não cair: Se havia patch e ele não foi aplicado, é sistema sem patch; dia zero é explorado antes de existir correção.

⚠ **Alerta de prova:** Chamar de produto sem suporte um appliance cuja correção só ainda não existe.
Como não cair: Sem suporte significa que o fabricante não corrige mais; se ele ainda dá suporte, a falha explorada antes do patch é dia zero.

⚠ **Alerta de prova:** Tratar como alucinação o chatbot que devolveu o laudo real de outro paciente.
Como não cair: Alucinação inventa; devolver dado real indevido é perda de dados pela saída do modelo.

⚠ **Alerta de prova:** Chamar de envenenamento o arquivo malicioso com pequenas alterações que engana o classificador sem mudar o modelo.
Como não cair: Se o modelo não mudou e a entrada foi ajustada na inferência, é evasão.

⚠ **Alerta de prova:** Marcar whaling para e-mail personalizado enviado só a um analista.
Como não cair: Whaling exige alvo executivo; para funcionário comum é spear phishing.

⚠ **Alerta de prova:** Achar que o ataque RCS com logotipo e botões não é smishing porque não é SMS.
Como não cair: Isca por mensagem de texto, seja SMS ou RCS, é smishing.

⚠ **Alerta de prova:** Chamar de typosquatting o BEC em que a mensagem veio da conta real do fornecedor.
Como não cair: Conta real comprometida pedindo troca de dados bancários é BEC; typosquatting usa domínio parecido.

⚠ **Alerta de prova:** Escolher grupo Temporal ou 'Exploitability' para incluir maturidade de exploração no CVSS v4.
Como não cair: No v4.0 o Temporal virou Threat, e Exploitability é conjunto de métricas dentro do Base; contexto da empresa é Environmental.

⚠ **Alerta de prova:** Dizer que o CVE mede a severidade ou classifica o tipo de falha.
Como não cair: CVE é o nome (identificador); CVSS é a nota; CWE é o tipo de fraqueza.

⚠ **Alerta de prova:** Atribuir a crime organizado a invasão de 14 meses, silenciosa, com ferramentas próprias e roubo de projetos.
Como não cair: Sem resgate, longa permanência e espionagem apontam para ator patrocinado por Estado.

⚠ **Alerta de prova:** Chamar de vírus o malware que se espalhou por SMB para dezenas de servidores sem ação dos usuários.
Como não cair: Propagação automática sem clique é worm; vírus depende de execução pelo usuário.

⚠ **Alerta de prova:** Classificar como ameaça interna maliciosa o envio acidental da planilha com CPFs.
Como não cair: Sem intenção maliciosa é ameaça interna acidental (não intencional).

⚠ **Alerta de prova:** Confundir XSS armazenado com CSRF quando outra aba envia uma transferência com o cookie da vítima.
Como não cair: Nenhum script foi armazenado no portal; o navegador anexou o cookie a uma requisição forjada: CSRF.

Como cai na prova

📝 **Como cai:** Trecho de log ou saída de ferramenta pedindo o nome do ataque.
Como resolver: Procure o detalhe técnico decisivo (../, UNION SELECT, mesma senha em várias contas, evento 1102, -EncodedCommand) e só depois leia as alternativas.

📝 **Como cai:** 'Qual ator e qual motivação são mais prováveis?'
Como resolver: Use as pistas: pedido de resgate e estrutura de empresa = crime organizado; silêncio e longa permanência = Estado; protesto = hacktivista; funcionário demitido = interno por vingança. As duas metades da alternativa precisam bater.

📝 **Como cai:** Cenário de IA com resultado errado ou ação indevida.
Como resolver: Pergunte: os dados de treino mudaram? a entrada foi disfarçada? havia instrução escondida? o modelo inventou? devolveu dado real? A resposta aponta envenenamento, evasão, injeção, alucinação ou perda de dados pela saída.

📝 **Como cai:** Escolha DUAS ou TRÊS com IoCs, riscos de IA ou mitigação de injeção de prompt.
Como resolver: Elimine o que não ajuda a detectar ou não aparece no cenário (versão do antivírus, nome do analista, energia do datacenter) e marque apenas o que o cenário evidencia.

📝 **Como cai:** Vulnerabilidade descrita por suas consequências (sem patch, sem dono, sem peças).
Como resolver: Diferencie pelo estado da correção e da gestão: correção disponível, inexistente, encerrada; fora do inventário = não gerenciado; tecnologia ultrapassada sem especialistas = obsoleto.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
GET com ../../etc/passwd e resposta 200	**Travessia de diretório (path traversal)**
Aspas e UNION SELECT no parâmetro	**Injeção de SQL**
Mesmo usuário em São Paulo e Frankfurt em minutos	**Viagem impossível**
Evento 1102 logo após login administrativo fora do horário	**Manipulação de logs para ocultar rastros**
Dezenas de notificações push até a vítima aprovar	**Fadiga de MFA**
Mensagem de erro diferente para conta existente e inexistente	**Enumeração de usuários**
Respostas DNS grandes de milhares de resolvedores abertos com IP falsificado	**DDoS por reflexão e amplificação**
ps e netstat não mostram nada, mas a análise de memória acha módulo de kernel	**Rootkit**
powershell.exe -EncodedCommand e nada gravado no disco	**Malware sem arquivo (fileless)**
Renomeação em massa, vssadmin apagando cópias de sombra, LEIA-ME.txt	**Ransomware**
Texto oculto em fonte branca instruindo o assistente de IA	**Injeção de prompt indireta**

Site do setor que as vítimas já visitam é comprometido	**Watering hole**
Pendrive que se apresenta como teclado e digita comandos	**USB malicioso emulando teclado**
Formato padronizado de indicadores e transporte automático	**STIX (dados) + TAXII (transporte)**

🎯 Se você lembrar de só uma coisa deste capítulo...

- Correção disponível e não aplicada nunca é dia zero.
- CVE identifica, CVSS pontua, CWE classifica o tipo; KEV prioriza o que já é explorado.
- IdP comprometido é crítico porque é a raiz de confiança de todos os acessos federados.
- Evasão não muda o modelo; envenenamento muda o treino.
- Leia a ordem das duas metades (ator e motivação) antes de marcar.

Essenciais para a prova (checklist)

- ☐ Sei associar cada ator de ameaça às suas motivações típicas.
- ☐ Sei diferenciar spear phishing, whaling, vishing, smishing, quishing, BEC e deepfake.
- ☐ Sei reconhecer worm, vírus, trojan, rootkit, keylogger, spyware, adware, bomba lógica, ransomware e fileless pelo comportamento.
- ☐ Sei separar dia zero, sem patch, sem suporte, obsoleto e não gerenciado.
- ☐ Sei identificar SQLi, traversal, XSS, CSRF, TOCTOU e estouro de buffer em um log ou cenário.
- ☐ Sei diferenciar spraying, stuffing, força bruta, fadiga de MFA, replay e sequestro de sessão.
- ☐ Sei os papéis de CVE, CVSS (grupos do v4.0), CWE, NVD e KEV.
- ☐ Sei distinguir injeção de prompt, jailbreak, evasão, envenenamento, extração, alucinação e perda de dados pela saída.
- ☐ Sei citar os vetores de cadeia de suprimentos: MSP, SaaS, logística e atualização maliciosa.

Questões de revisão do capítulo

R1.1 · Ameaças, Vulnerabilidades e Ataques

Testes no portal da Clínica Vida Plena mostraram que a mensagem de erro no login muda conforme a conta existe ou não: senha incorreta para contas válidas e usuário não encontrado para as inexistentes. Um atacante usou essa diferença para descobrir milhares de contas válidas. Que ataque de credencial foi possível?

A. Injeção de SQL no login
B. Bomba lógica no portal
C. Ataque de replay de sessão
D. Enumeração de usuários

R1.2 · Ameaças, Vulnerabilidades e Ataques

Um pesquisador avisa a EdTech Saber Mais que encontrou, sem autenticação, milhares de contratos de alunos em um endereço do serviço de armazenamento de objetos da empresa na nuvem. O bucket foi criado por um desenvolvedor para testes e ficou com leitura pública. Qual vulnerabilidade foi explorada?

A. Credencial codificada no aplicativo
B. Ataque de dia zero no hipervisor
C. Armazenamento de objetos com acesso público
D. Injeção de SQL no portal de matrículas online

R1.3 · Ameaças, Vulnerabilidades e Ataques

Um provedor de CRM em nuvem usado pela Imobiliária Casa Forte sofreu uma invasão em sua própria infraestrutura, e os dados de clientes de centenas de empresas, inclusive os da imobiliária, foram expostos. Que vetor de ameaça da cadeia de suprimentos isso representa?

A. Ataque físico ao escritório local
B. Provedor de software como serviço (SaaS)
C. Mídia removível com malware
D. Fornecedor de hardware adulterado

R1.4 · Ameaças, Vulnerabilidades e Ataques

A Prefeitura de Lagoa Seca ainda mantém um servidor de arquivos com um sistema operacional cujo fabricante encerrou o suporte há dois anos; novas vulnerabilidades descobertas nele não receberão correção. Que tipo de vulnerabilidade isso representa?

A. Má configuração de permissões
B. Condição de corrida no kernel do sistema
C. Produto sem suporte do fabricante
D. Credencial padrão não alterada

Respostas comentadas

R1.1. D) Enumeração de usuários

Por quê: A enumeração de usuários explora diferenças em mensagens, tempos de resposta ou fluxos de recuperação para descobrir contas válidas; mensagens genéricas e respostas uniformes mitigam o problema.

✗ A) Incorreta. Não houve entrada maliciosa interpretada pelo banco.
✗ B) Incorreta. Bomba lógica é código malicioso com gatilho, não uma técnica de descoberta de contas.
✗ C) Incorreta. Não houve reutilização de sessões capturadas.

> **Dica de prova:** Mensagem de erro diferente para conta existente: enumeração de usuários.

R1.2. C) Armazenamento de objetos com acesso público

Por quê: Armazenamento de objetos público é uma superfície de ataque comum: buckets criados com permissões abertas expõem dados. Bloqueios de acesso público no nível da conta e revisão contínua de configuração evitam o problema.

✗ A) Incorreta. Não foi preciso nenhuma credencial; o acesso era público.
✗ B) Incorreta. Não houve falha desconhecida explorada; a causa foi configuração.
✗ D) Incorreta. Os arquivos foram lidos diretamente do armazenamento, sem explorar o portal.

> **Dica de prova:** Bucket aberto para leitura sem autenticação: armazenamento de objetos público.

R1.3. B) Provedor de software como serviço (SaaS)

Por quê: Provedores de SaaS fazem parte da cadeia de suprimentos: uma falha neles expõe os dados de muitos clientes ao mesmo tempo. Due diligence, cláusulas contratuais e monitoramento do fornecedor reduzem esse risco.

✗ A) Incorreta. O ataque não ocorreu nas instalações da imobiliária.
✗ C) Incorreta. Nenhuma mídia removível foi usada.
✗ D) Incorreta. Não houve equipamento adulterado.

> **Dica de prova:** Provedor de nuvem invadido expõe os dados de vários clientes: vetor SaaS.

R1.4. C) Produto sem suporte do fabricante

Por quê: Produtos sem suporte (fim de vida) deixam de receber correções de segurança; devem ser substituídos ou, enquanto isso, isolados com controles compensatórios.

✗ A) Incorreta. O problema não é a configuração, e sim a falta de atualizações.
✗ B) Incorreta. Nada no cenário descreve operações concorrentes.
✗ D) Incorreta. Não há menção a senhas padrão.

> **Dica de prova:** Fabricante não corrige mais: produto sem suporte.

02

CAPÍTULO 2 · 19% DA PROVA

Arquitetura de Segurança

Este domínio vale 19% e cobra como desenhar a arquitetura: modelos de nuvem e responsabilidade compartilhada, considerações de negócio e técnicas, infraestrutura de rede segura, proteção de dados e resiliência. As questões são cenários que pedem o 'conceito que orienta a decisão' ou a solução que atende requisitos, e muitas misturam dois requisitos para cobrar pares (RTO e RPO, UPS e gerador, disponibilidade e resiliência). Preciso ter na ponta da língua os métodos de proteção de dados (mascaramento, tokenização, hash, criptografia, filtragem, desidentificação) e os papéis de dados (proprietário, custodiante, steward, operador, suboperador). Onde mais erro: confundir RTO com RPO, fail-open com fail-closed, nuvem comunitária com híbrida e SSE com SASE.

Neste capítulo

18 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Modelos de implantação de nuvem

Pública é multilocatária, aberta ao público, com isolamento lógico e cobrança por uso; privada tem autosserviço e elasticidade, mas é exclusiva de uma organização (pode estar no próprio datacenter); comunitária é compartilhada só por um grupo de organizações com requisitos comuns; híbrida integra dois ou mais modelos, como datacenter próprio com nuvem pública. Multicloud usa vários provedores e aumenta a dificuldade de manter políticas consistentes.

Responsabilidade compartilhada

No IaaS o cliente aplica patches no sistema operacional convidado das VMs; no SaaS o provedor opera toda a pilha; em serverless o provedor cuida do hipervisor e do sistema operacional, e o cliente protege o código da função, os dados e as permissões que ela usa. Segurança física do datacenter é sempre do provedor; em datacenter próprio, todas as camadas são da empresa.

Infraestrutura como código (IaC)

Templates versionados permitem varredura estática antes do deploy (bloquear bucket público, grupo de segurança aberto para 0.0.0.0/0, banco sem criptografia) e detecção de desvios (drift) quando alguém muda algo pelo console. Também favorece a facilidade de recuperação: recriar a infraestrutura em minutos.

Microsserviços

Dividir o monólito em serviços que conversam por APIs exige autenticar e autorizar cada chamada entre serviços; abandonar TLS interno ou liberar portas entre contêineres amplia a movimentação lateral.

Considerações de negócio e técnicas

Disponibilidade (percentual no ar) x resiliência (aguentar falhas e voltar rápido), escalabilidade (crescer nos picos e encolher), usabilidade (controle incômodo vira contorno, como tokens presos ao monitor), custo x risco aceitável, facilidade de recuperação, requisitos de energia e computação, requisitos ambientais (poeira, calor, vibração), soberania (onde o dado mora define a lei), propriedade dos dados e classificação dos dados.

Segmentação e zonas

VLAN é segmentação lógica no mesmo switch; segmentação física usa switches, cabos e firewalls dedicados; air gap é nenhuma conexão física ou sem fio com outras redes; DMZ entre dois níveis de firewall publica serviços sem dar acesso direto à rede interna; zona de gerenciamento dedicada concentra interfaces administrativas, acessível só por estações dedicadas. Gerenciamento fora de banda (out-of-band) dá acesso aos consoles por caminho separado, como conexão celular.

Modos de falha

Fail-open libera quando falha (fechadura de saída de emergência destrava pela segurança das pessoas); fail-closed bloqueia tudo quando falha (nenhum tráfego passa sem inspeção, mesmo parando vendas). Failover é redundância entre equipamentos, não o comportamento de um dispositivo que falhou.

Posicionamento de sensores

IPS fica inline e bloqueia em tempo real (borda da DMZ); IDS fica passivo recebendo cópia por SPAN ou TAP e só monitora, adequado a rede industrial em que um falso positivo não pode parar a produção.

Acesso remoto seguro

VPN site a site com IPsec liga redes inteiras com cifra na camada 3; full tunnel faz todo o tráfego do usuário remoto passar pelos controles da empresa (split tunnel deixa a internet sem inspeção); VPN exige MFA contra credential stuffing; bastion host reforçado com MFA e gravação de sessão evita expor RDP e SSH; SSH com chave pública substitui Telnet; SFTP ou FTPS substituem FTP sem cifra.

ZTNA, SSE e SASE

ZTNA concede acesso por aplicação após verificar identidade e dispositivo, sem expor a rede. SSE é SWG + CASB + ZTNA entregues pela nuvem, sem SD-WAN; com SD-WAN é SASE. SWG na nuvem filtra sites, inspeciona TLS e bloqueia downloads de quem navega direto de casa.

Identidades na arquitetura

Conta de serviço gerenciada de grupo (gMSA) dá a mesma identidade a vários servidores sem senha gerida por pessoas; administradores usam conta comum no dia a dia e conta administrativa separada; a aplicação acessa o banco com conta de permissões mínimas, nunca como administrador do SGBD; privilege creep é acumular acessos ao mudar de área.

Tipos e classificação de dados

Estruturados (tabela com colunas) x não estruturados (PDF, áudio, e-mail). Na LGPD: dado pessoal identifica a pessoa; dado pessoal sensível inclui saúde e genética, com regras mais restritas; dados de crianças seguem o melhor interesse da criança. Também cobrados: dados financeiros, propriedade intelectual, dados jurídicos e PCI DSS para cartões. Hierarquia: confidencial (dano), secreto (dano grave), ultrassecreto (dano excepcionalmente grave).

Estados e ciclo de vida dos dados

Em trânsito (TLS ou VPN), em repouso (criptografia de disco) e em uso (memória, computação confidencial com enclaves de hardware). No ciclo de vida, rótulo aplicado quando o arquivo nasce é a etapa de criação; guardar por cinco anos e eliminar depois é retenção e descarte.

Métodos de proteção de dados

Mascaramento mostra só parte (XXX.XXX.X89-01) mantendo o valor completo; tokenização troca por substituto sem relação matemática, com cofre separado; hash detecta alteração sem comparar o arquivo inteiro; criptografia garante que só quem tem a chave lê; filtragem envia só registros e campos necessários; desidentificação remove identificadores e generaliza datas e CEPs; marcação e rotulagem; geofencing pelo MDM; controle de localização (regiões permitidas); posicionamento por sensibilidade (zona restrita x DMZ).

Papéis de dados

Proprietário (owner) classifica e aprova acesso; custodiante aplica backups, criptografia e permissões conforme as decisões; steward cuida de qualidade, metadados e dicionário; controlador e operador são papéis jurídicos de privacidade; o provedor contratado pelo operador é suboperador.

Alta disponibilidade e redundância

Instâncias redundantes atrás de balanceador e distribuídas entre zonas; autoscaling para picos; balanceador com health checks tira da rotação o servidor que não responde; cluster ativo-passivo tem nó em espera que assume com o mesmo nome e endereço; RAID 5 aguenta a falha de um disco (RAID 0 perde tudo); diversidade de plataforma e de fornecedores evita que uma falha comum derrube várias camadas.

Energia

UPS (nobreak) cobre a transição; gerador sustenta por horas e precisa de abastecimento de combustível planejado; protetor contra surtos absorve picos; fonte redundante (RPS) mantém o servidor ligado se uma fonte interna falhar.

Recuperação: sites, métricas, backups e testes

Site quente retoma em minutos; morno tem equipamentos mas não dados, cerca de dias; frio só tem espaço e energia. RTO é o prazo para voltar; RPO é quanto dado se aceita perder; MTBF é tempo médio entre falhas; MTTR é tempo médio de reparo. Backup precisa de cópia offline ou isolada em outro local, imutabilidade, escopo, retenção e testes periódicos de restauração. Testes: failover (transfere de verdade), processamento paralelo (processa junto sem assumir) e exercício de mesa (só discussão).

Macetes para memorizar

💡 RTO x RPO

RPO = Ponto (quanto dado perco). RTO = Tempo (quando volto).

💡 MTBF x MTTR

MTBF: Between = entre falhas, quanto dura.
MTTR: Repair = quanto demora para consertar.

💡 Temperatura dos sites

Quente liga em minutos, morno em dias, frio é só o prédio vazio.

💡 Owner x custodian x steward

Dono decide, custodiante guarda, steward arruma (qualidade e metadados).

💡 SSE x SASE

SASE = SSE + SD-WAN (o A de 'Access' traz a rede junto).

💡 Energia

Nobreak segura o susto, gerador segura as horas, diesel segura o gerador.

💡 Fail-open x fail-closed

Porta de pessoas abre; porta de pacotes fecha.

Tabela de memorização: não confunda

Quando é...	...e quando é
RTO Prazo máximo para o sistema voltar a funcionar; define a velocidade do ambiente de recuperação.	**RPO** Quantidade máxima de dados que se aceita perder; define a frequência de backup ou replicação (backup diário às 22h não atende RPO de 1 hora).
Fail-open Falhou e libera: fechaduras de saída de emergência, pela segurança das pessoas.	**Fail-closed** Falhou e bloqueia: nenhum tráfego passa sem inspeção, mesmo que isso pare as vendas.

Site quente Hardware, dados replicados e conectividade ativos; retomada em minutos.	**Site morno / site frio** Morno: equipamentos prontos, restaura backups e volta em cerca de dois dias. Frio: só espaço e energia, mais barato e mais lento.
Tokenização Substituir o número do cartão por valor sem relação matemática, mantido em cofre separado, para análises funcionarem sem o dado real.	**Mascaramento** Mostrar só parte do dado na tela (atendente vê parte do CPF) enquanto o sistema guarda o valor completo.
Proprietário dos dados Classifica, aprova quem acessa e responde pelas decisões.	**Custodiante dos dados** Aplica backups, criptografia e permissões conforme as decisões do proprietário.
IPS inline Precisa bloquear ataques em tempo real, como na borda da DMZ.	**IDS passivo via SPAN/TAP** Só monitorar sem risco de falso positivo derrubar o processo, como na rede industrial.
SSE SWG, CASB e ZTNA entregues pela nuvem, sem a parte de rede.	**SASE** Os mesmos serviços de segurança somados ao SD-WAN.

Números que caem

Item	Valor
Peso do domínio na prova	**19%**
Fórmula do MTTR	**Horas totais de reparo ÷ número de falhas (6 falhas e 18 horas = 3 horas)**
Tolerância do RAID 5	**Falha de um disco sem perda de dados nem parada**
Níveis de classificação governamental	**Confidencial (dano), secreto (dano grave), ultrassecreto (dano excepcionalmente grave)**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Dizer que o backup completo diário atende ao RPO de 1 hora 'porque existe backup'.
Como não cair: Com backup às 22h e sem replicação, a perda pode chegar a quase 24 horas; limite de perda é RPO, não RTO.

⚠ **Alerta de prova:** Marcar 18 horas como MTTR de 6 falhas que somaram 18 horas de reparo.
Como não cair: MTTR é a média: horas de reparo divididas pelo número de falhas, ou seja, 3 horas.

⚠ **Alerta de prova:** Achar que multicloud aumenta o aprisionamento ou elimina backups.
Como não cair: Multicloud reduz a dependência de um fornecedor; o desafio que cresce é manter políticas e controles consistentes.

⚠ **Alerta de prova:** Chamar de nuvem híbrida a infraestrutura compartilhada só por organizações do mesmo setor.
Como não cair: Grupo restrito com requisitos comuns é nuvem comunitária; híbrida combina modelos diferentes.

⚠ **Alerta de prova:** Achar que nuvem privada exige provedor externo, ou que nuvem com autosserviço é sempre pública.
Como não cair: Autosserviço e elasticidade dedicados a uma só organização, mesmo no datacenter próprio, é nuvem privada.

⚠ **Alerta de prova:** Colocar patch do sistema operacional como responsabilidade do cliente no SaaS ou no serverless.
Como não cair: Só no IaaS o sistema operacional convidado é do cliente; em serverless o cliente cuida do código e das permissões.

⚠ **Alerta de prova:** Escolher fail-closed para as fechaduras de saída de emergência 'priorizando o sigilo'.
Como não cair: Em fail-closed a porta ficaria trancada no incêndio; vida em primeiro lugar é fail-open.

⚠ **Alerta de prova:** Usar criptografia assimétrica ou hash para mostrar só parte do CPF.
Como não cair: Exibir dígitos parciais mantendo o valor completo armazenado é mascaramento.

⚠ **Alerta de prova:** Achar que criptografia simétrica serve para guardar cartões sem relação matemática com o original.
Como não cair: O texto cifrado tem relação matemática e é reversível com a chave; sem relação e com cofre é tokenização.

⚠ **Alerta de prova:** Achar que código aberto não tem vulnerabilidades porque pode ser revisado.
Como não cair: Código aberto é auditável e tem suporte da comunidade, mas também tem falhas; garantia contratual de correção é do modelo proprietário.

⚠ **Alerta de prova:** Chamar de failover completo o teste em que o site alternativo processa junto sem assumir a produção.
Como não cair: Processar em paralelo e comparar resultados é teste de processamento paralelo; failover transfere a produção.

⚠ **Alerta de prova:** Escolher outro nobreak para proteger contra picos de tensão e queima de fonte.
Como não cair: Pico de tensão pede protetor contra surtos; fonte interna queimada pede fonte redundante (RPS).

⚠ **Alerta de prova:** Confundir disponibilidade e resiliência na ordem 'ficar 99,9% no ar' e 'continuar degradado e voltar rápido'.
Como não cair: Percentual no ar é disponibilidade; aguentar falhas e se recuperar é resiliência; respeite a ordem pedida.

⚠ **Alerta de prova:** Colocar o servidor web público na mesma VLAN dos bancos ou na rede de gerenciamento.
Como não cair: Serviço exposto à internet vai para a DMZ entre dois níveis de firewall; a rede de gerenciamento nunca hospeda serviços públicos.

Como cai na prova

📝 **Como cai:** 'Que consideração de negócio ou técnica orienta essa decisão?'
Como resolver: Encontre a palavra-chave do cenário: picos = escalabilidade; lei do país = soberania; de quem são os dados = propriedade; incômodo que gera contorno = usabilidade; templates = facilidade de recuperação; poeira e calor = ambientais.

📝 **Como cai:** RTO, RPO, MTBF ou MTTR com números.
Como resolver: Calcule só o pedido: MTTR = horas de reparo / falhas; compare a frequência do backup com o RPO e a velocidade do site com o RTO.

📝 **Como cai:** Escolha DUAS para alta disponibilidade ou energia.
Como resolver: Descarte o que só recupera dados (backup) ou não mantém nada no ar (janela de manutenção, logs); marque redundância ativa (zonas, balanceador, autoscaling) ou UPS + gerador.

📝 **Como cai:** Método de proteção de dados descrito pelo efeito.
Como resolver: Parte visível = mascaramento; substituto em cofre = tokenização; detectar alteração = hash; só o destinatário lê = criptografia; enviar menos campos = filtragem; tirar identificadores = desidentificação.

📝 **Como cai:** Responsabilidade compartilhada por modelo de serviço.
Como resolver: Desenhe a pilha: no IaaS o cliente começa no sistema operacional; no serverless começa no código e nas permissões; no SaaS fica com dados e acessos; física é sempre do provedor.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Nem o provedor do serviço consegue ler as mensagens	**Criptografia de ponta a ponta**
Dados protegidos na memória durante o processamento, inclusive do administrador do provedor	**Dados em uso, computação confidencial**
Acesso aos consoles por rede separada com conexão celular quando a produção cai	**Gerenciamento fora de banda (out-of-band)**
Mesma falha derrubando firewalls de borda e internos do mesmo fabricante	**Diversidade de fornecedores e tecnologias**
Conta de serviço em vários servidores sem senha manual	**gMSA**
Mudou de área três vezes e manteve todos os acessos	**Privilege creep**
Ransomware apagou os backups com credencial de administrador	**Backup imutável com retenção que nem administradores alteram**
Backups com sucesso por anos, mas corrompidos no incidente real	**Testes periódicos de restauração**
Tablet só abre o aplicativo dentro das unidades	**Geofencing aplicado pelo MDM**
Template barrado por bucket público ou 0.0.0.0/0 antes do deploy	**Varredura estática de IaC**
Pipeline acusa diferença entre o ambiente e o código	**Detecção de drift da IaC**
Onde o dado fica define qual lei se aplica	**Soberania dos dados**
Remover nomes e CPF e generalizar datas e CEPs para pesquisadores	**Desidentificação**
Gerador parou por falta de diesel	**Planejamento do abastecimento de combustível**

🎯 Se você lembrar de só uma coisa deste capítulo...

- RPO é perda de dados e dita a frequência da cópia; RTO é tempo e dita a velocidade da recuperação.
- Backup só vale se restaurar: cópia isolada, imutável e testada.
- Em OT, disponibilidade e segurança física dos processos vêm antes da confidencialidade; patch só com teste e janela.
- No IaaS o patch do sistema operacional é do cliente; em serverless o cliente cuida do código e das permissões.
- Saúde e genética são dados pessoais sensíveis na LGPD.

Essenciais para a prova (checklist)

- ☐ Sei diferenciar nuvem pública, privada, comunitária, híbrida e multicloud.
- ☐ Sei dividir responsabilidades entre cliente e provedor em IaaS, SaaS, serverless e datacenter próprio.
- ☐ Sei escolher entre VLAN, segmentação física, air gap, DMZ e zona de gerenciamento.
- ☐ Sei quando usar fail-open e fail-closed, e IPS inline ou IDS passivo.
- ☐ Sei diferenciar ZTNA, SWG, SSE e SASE.
- ☐ Sei aplicar mascaramento, tokenização, hash, criptografia, filtragem e desidentificação.
- ☐ Sei os papéis de proprietário, custodiante, steward, controlador, operador e suboperador.
- ☐ Sei calcular MTTR e interpretar RTO, RPO e MTBF.
- ☐ Sei diferenciar site quente, morno e frio e os testes de failover, paralelo e de mesa.

Questões de revisão do capítulo

R2.1 · Arquitetura de Segurança

Ao decidir onde hospedar um novo sistema, a Autarquia Previdência Sul percebe que ele vai armazenar dados classificados como restritos, que por norma interna não podem sair de ambientes com criptografia gerida pela própria autarquia. Qual consideração de negócio orienta essa decisão de arquitetura?

A. Classificação dos dados
B. Facilidade de uso
C. Custo de licenciamento
D. Escalabilidade elástica do provedor

R2.2 · Arquitetura de Segurança

A plataforma de ingressos da Arena Show precisa suportar picos de 50 vezes o tráfego normal quando abrem as vendas de grandes shows e voltar ao tamanho mínimo depois, sem pagar por capacidade ociosa o ano inteiro. Que consideração de negócio orienta a escolha por nuvem elástica?

A. Escalabilidade
B. Soberania dos dados
C. Usabilidade
D. Propriedade

R2.3 · Arquitetura de Segurança

Uma healthtech brasileira trata prontuários com diagnósticos, exames e dados genéticos de pacientes. Segundo a LGPD, como esses dados são classificados e qual é a consequência dessa classificação?

A. Dados financeiros, regulados só pelo Banco Central
B. Dados públicos, que dispensam base legal para tratamento
C. Dados anonimizados, fora do alcance da lei
D. Dados pessoais sensíveis, com regras mais restritas de tratamento

R2.4 · Arquitetura de Segurança

Em um órgão de defesa, um relatório cuja divulgação não autorizada poderia causar dano grave à segurança nacional recebe uma classificação abaixo da mais alta. Considerando a hierarquia confidencial, secreto e ultrassecreto, qual nível se aplica?

A. Confidencial
B. Público
C. Secreto
D. Ultrassecreto

Respostas comentadas

R2.1. A) Classificação dos dados

Por quê: A classificação dos dados é uma consideração de negócio da arquitetura: quanto mais sensível o dado, maiores os requisitos de proteção, de localização e de controle de chaves, o que influencia a escolha de modelo e de fornecedor.

✗ B) Incorreta. Usabilidade não define onde dados restritos podem ficar.
✗ C) Incorreta. O custo não é o critério descrito.
✗ D) Incorreta. Escalabilidade é relevante, mas não é o que restringe a escolha no cenário.

> **Dica de prova:** Dado restrito definindo onde o sistema pode morar: classificação dos dados.

R2.2. A) Escalabilidade

Por quê: Escalabilidade é a capacidade de aumentar ou reduzir recursos conforme a demanda; a elasticidade rápida é uma característica essencial da computação em nuvem segundo o NIST SP 800-145.

✗ B) Incorreta. Soberania trata da jurisdição sobre os dados.
✗ C) Incorreta. Usabilidade trata da experiência de uso.
✗ D) Incorreta. Propriedade trata de quem é dono dos ativos e dados.

> **Dica de prova:** Crescer nos picos e encolher depois: escalabilidade.

R2.3. D) Dados pessoais sensíveis, com regras mais restritas de tratamento

Por quê: Dados de saúde são uma categoria de conformidade específica; na LGPD, dados referentes à saúde, à vida sexual e dados genéticos ou biométricos são dados pessoais sensíveis, com regras mais rígidas de tratamento e proteção.

✗ A) Incorreta. São dados de saúde, não financeiros.
✗ B) Incorreta. Prontuários não são dados públicos e exigem base legal.
✗ C) Incorreta. Os dados identificam pacientes, então não são anonimizados.

> **Dica de prova:** Saúde e genética na LGPD: dado pessoal sensível.

R2.4. C) Secreto

Por quê: Classificações governamentais seguem o impacto da divulgação: confidencial (dano), secreto (dano grave) e ultrassecreto (dano excepcionalmente grave); empresas usam rótulos equivalentes, como público, interno, confidencial e restrito.

✗ A) Incorreta. Confidencial corresponde a dano, sem a gravidade descrita.
✗ B) Incorreta. Informação pública não exige proteção contra divulgação.
✗ D) Incorreta. Ultrassecreto é reservado a dano excepcionalmente grave.

> **Dica de prova:** Dano grave: secreto. Excepcionalmente grave: ultrassecreto.

03

CAPÍTULO 3 · 16% DA PROVA

Conceitos Gerais de Segurança

Este domínio vale 16% da prova e é a base de todo o resto: categorias e tipos de controle, tríade CIA, AAA, Zero Trust, gestão de mudanças, PKI e criptografia. Quase tudo cai como cenário curto pedindo para classificar uma medida, muitas vezes em pares ('como se classificam, respectivamente'), então eu preciso saber a definição exata de cada rótulo e respeitar a ordem pedida. Na gestão de mudanças, a prova quer o passo certo do processo (análise de impacto, backout, janela, CAB, registro de emergência). Na criptografia, o que derruba é confundir hash com HMAC e assinatura, CRL com OCSP, e qual chave (pública ou privada, de quem) usar em cada operação. Meus erros mais comuns: chamar placa de controle preventivo, achar que 'compensatório' é categoria e esquecer que Zero Trust nunca confia na rede interna.

Neste capítulo

19 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Categorias de controle (técnica, gerencial, operacional, física)

A categoria diz QUEM ou O QUE implementa o controle. Técnica (lógica) é executada por sistemas, como WAF, TLS e MFA; gerencial trata da gestão do risco e do programa, como avaliação anual de riscos e plano de ação aprovado pela diretoria; operacional é rotina executada por pessoas, como rotação de mídias de backup com livro assinado ou treinamento conduzido pela equipe; física protege instalações e ambiente, como cerca, sala-cofre, climatização redundante e supressão de incêndio por gás inerte.

Tipos de controle (preventivo, detectivo, corretivo, dissuasivo, compensatório, diretivo)

O tipo diz o OBJETIVO do controle. Preventivo impede antes (catraca, firewall bloqueando entrada não solicitada); detectivo identifica e alerta (SIEM revisando logs); corretivo restaura depois (restaurar do backup imutável e reinstalar de imagem limpa); dissuasivo desencoraja (placa de área monitorada, iluminação); compensatório substitui um controle ideal inviável (VLAN isolada para sistema que não pode receber patch); diretivo orienta conduta (norma que obriga bloquear a tela).

Tríade CIA

Confidencialidade impede acesso não autorizado (disco cifrado de notebook furtado); integridade garante que o dado não foi alterado (comparar o SHA-256 do arquivo baixado com o publicado); disponibilidade garante acesso quando necessário (DDoS derruba a disponibilidade sem ler nem alterar dados). Não repúdio, autenticação e rastreabilidade NÃO fazem parte da tríade.

Não repúdio

Impede que alguém negue ter feito uma ação; normalmente obtido com assinatura digital usando o certificado pessoal do signatário. Ter permissão para aprovar (autorização) não prova que a pessoa aprovou; a assinatura prova.

AAA (autenticação, autorização, contabilização)

Autenticação prova quem é (senha + autenticador); autorização define o que pode fazer (perfil que permite fechar chamados); contabilização (accounting) registra quem fez o quê, quando e de onde. Federação não faz parte do AAA. Para login centralizado em switches e roteadores com permissão por comando e registro de cada sessão, use servidor AAA como RADIUS ou TACACS+.

Zero Trust: PDP e PEP

O ponto de decisão de política (PDP) avalia identidade, dispositivo, contexto e risco para decidir; o ponto de aplicação de política (PEP) fica no caminho do tráfego e abre ou encerra a sessão. Cada acesso é avaliado de novo, por recurso e por sessão, com menor privilégio; uma autenticação anterior ou estar na rede interna não dá confiança implícita.

Assume breach

Princípio de Zero Trust de projetar controles como se o invasor já estivesse dentro: segmentar, minimizar o raio de impacto, cifrar de ponta a ponta e monitorar continuamente. O oposto é o foco exclusivo no perímetro.

Defesa em profundidade x menor privilégio

Defesa em profundidade são várias camadas diferentes (firewall, segmentação, MFA, EDR, backup offline) para que a falha de uma não exponha o ativo; um ransomware que se espalha porque só havia firewall de borda é falta de defesa em profundidade. Menor privilégio é conceder só o necessário à função; dar leitura e escrita em todas as pastas 'para não precisar pedir' viola o menor privilégio.

Gestão de mudanças: CAB, análise de impacto e ownership

O comitê consultivo de mudanças (CAB), com TI, segurança e negócio, avalia a solicitação antes da execução. A análise de impacto levanta quem e o que será afetado (ex.: parceiros que ainda dependem do TLS 1.0). A mudança precisa de um responsável (ownership) do início ao fim e do envolvimento das partes interessadas que serão afetadas.

Plano de backout x fail forward

Backout é o caminho documentado e testado para voltar à versão anterior; é a escolha quando a reversão é rápida e não houve mudança de dados. Fail forward é corrigir e seguir com a versão nova quando voltar atrás seria mais arriscado, por exemplo depois que a migração já alterou o esquema do banco.

Implicações técnicas da mudança

Inclui atualizar listas de permissões (software atualizado deixa de abrir em allow list por hash) e de bloqueio (extensão vulnerável), restringir as atividades ao escopo aprovado, planejar downtime, reinício de serviços e aplicações em janela com aviso, mapear dependências e tratar aplicações legadas testando antes em ambiente espelho com backout.

Documentação da mudança e mudança emergencial

Depois da mudança é preciso atualizar diagramas de rede, políticas e procedimentos afetados e manter controle de versão das configurações (saber o que mudou, quem mudou e voltar atrás). Tarefa repetitiva e de baixo risco pré-aprovada segue um SOP. Mudança emergencial pode ser aprovada rápido pelo procedimento emergencial, mas precisa ser registrada e revisada depois pelo CAB.

PKI: AC, CSR e cadeia de confiança

A autoridade certificadora (AC), diretamente ou por uma autoridade de registro, confirma a identidade, assina os certificados com sua chave privada e publica a revogação. A CSR leva a chave pública e os dados que identificam o servidor; a chave privada nunca sai do servidor. Boa prática: AC raiz offline, intermediárias emitindo e certificado raiz distribuído às máquinas como âncora de confiança.

Revogação: CRL, OCSP e OCSP stapling

A CRL é a lista completa publicada periodicamente pela AC; quem não consulta online só recusa o certificado ao baixar a próxima lista. O OCSP consulta o status de um certificado na hora. No OCSP stapling o próprio servidor obtém a resposta OCSP assinada e a anexa ao handshake TLS, reduzindo consultas à AC e não revelando a ela os sites que o cliente visita.

Simétrica, assimétrica e troca de chaves

AES (simétrica) cifra grandes volumes com bom desempenho; RSA (assimétrica) é lento para terabytes e serve para proteger a chave. Diffie-Hellman permite combinar uma chave secreta por canal público sem transmiti-la. Forward secrecy com chaves efêmeras (DHE/ECDHE) garante que roubar a chave privada do servidor depois não decifra sessões gravadas antes; RSA estático não tem isso, qualquer que seja o tamanho da chave.

Hash, sal, HMAC e assinatura digital

Hash verifica integridade; MD5 e SHA-1 têm colisões, use SHA-256 ou superior; CRC32 só detecta erro acidental. Sal aleatório e único por senha faz senhas iguais gerarem hashes diferentes e derruba tabelas pré-calculadas. HMAC dá integridade e origem com chave compartilhada, sem custo assimétrico e sem não repúdio. Assinatura digital dá integridade, autenticidade e não repúdio, mas não sigilo.

Níveis de criptografia em repouso

Disco inteiro protege notebook roubado, mas fica decifrado para quem usa o sistema em funcionamento; partição cifra só uma parte do disco; volume cifra um volume lógico inteiro; arquivo protege cada documento individualmente; TDE cifra arquivos e backups do banco sem mexer na aplicação; coluna ou registro protege só alguns campos, inclusive contra o DBA.

Ferramentas criptográficas: TPM, HSM, KMS e enclave seguro

TPM vincula a chave do disco à placa do notebook; HSM protege a chave da AC; KMS gerencia centralmente, com rotação e auditoria, chaves de serviços em nuvem; enclave seguro é área isolada do processador do celular de onde a chave não pode ser exportada. Raiz de confiança em hardware é o componente imutável que verifica a assinatura do firmware no boot.

Ofuscação: esteganografia, tokenização e mascaramento

Esteganografia esconde dados dentro de outro arquivo, como fórmulas dentro de fotos sem alteração visível; criptografia torna ilegível mas não esconde que há mensagem. Tokenização troca o dado por token guardado em cofre; mascaramento oculta parte do dado na exibição. Base64 é só codificação reversível, nunca proteção.

Macetes para memorizar

💡 Chaves assimétricas

Tranca com a PÚBLICA de quem recebe; assina com a PRIVADA de quem envia.

💡 AAA

Quem é você? (autenticação) O que pode? (autorização) O que fez? (contabilização).

💡 Revogação

CRL é a lista do jornal de ontem; OCSP é a ligação na hora; stapling é o servidor que já traz o atestado grampeado.

💡 Placa x trava

Placa avisa: dissuasivo. Trava impede: preventivo. Backup restaura: corretivo.

Simétrica x assimétrica

Volume grande vai de AES; entregar a chave vai de RSA.

Curinga

Um asterisco, um nível: *.empresa.com não pega a.b.empresa.com.

Categoria x tipo

Categoria = quem faz (sistema, gestão, pessoa, prédio). Tipo = para que serve (impede, detecta, corrige, desencoraja, substitui, orienta).

Tabela de memorização: não confunda

Quando é...	...e quando é
CRL Lista completa de revogados publicada periodicamente pela AC; o sistema só passa a recusar quando baixa a próxima lista.	**OCSP (e OCSP stapling)** Status de um certificado no momento da conexão sem baixar a lista; com stapling, o servidor entrega a resposta OCSP assinada no handshake.
Plano de backout Falhou, não houve mudança de dados e a versão anterior está empacotada e testada: reverter.	**Fail forward** A mudança já alterou o esquema ou voltar seria mais arriscado: corrigir rápido e seguir com a versão nova.
Controle compensatório Substitui um controle ideal que não pode ser aplicado, como VLAN restrita e monitoramento para equipamento que não pode ser atualizado.	**Controle corretivo** Atua depois do incidente para restaurar, como restaurar do backup e reinstalar a partir de imagem limpa.
Controle dissuasivo Só desencoraja, como placa de área monitorada 24 horas e iluminação forte.	**Controle preventivo** Impede de fato, como porta com trava eletrônica, catraca com crachá ou firewall bloqueando entrada não solicitada.
HMAC Partes que já compartilham uma chave secreta querem integridade e origem sem custo assimétrico e sem precisar de não repúdio.	**Assinatura digital** É preciso não repúdio e autenticidade verificável por terceiros, usando a chave privada do signatário.
Criptografia de disco inteiro Notebook perdido ou furtado: os dados ficam ilegíveis fora do sistema em funcionamento.	**Criptografia de coluna/registro ou de arquivo** Proteger campos ou documentos específicos inclusive de quem tem acesso ao sistema ligado, como o DBA ou colegas com acesso à pasta.
Autenticação Login com senha e código do autenticador: provar quem é.	**Autorização** Verificar se o perfil permite a ação, como fechar chamados de outros setores; o registro do que foi feito é contabilização.

Números que caem

Item	Valor
Peso do domínio na prova	**16%**
Tamanho mínimo de chave RSA para novas emissões	**2048 bits ou mais (ou curva elíptica equivalente); 1024 é fraco e 512 é inseguro**
Versão de TLS recomendada	**TLS 1.3, com TLS 1.2 só para compatibilidade; TLS 1.0 e 1.1 descontinuados**
Níveis cobertos por certificado curinga	**Um único nível de subdomínio**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Liberar o segundo acesso porque o médico já se autenticou na rede interna mais cedo.
Como não cair: Zero Trust avalia cada recurso e sessão de novo, com identidade, dispositivo e contexto; não existe confiança por localização nem por login anterior.

⚠ **Alerta de prova:** Colocar a chave privada (mesmo cifrada) na CSR.
Como não cair: A CSR leva só a chave pública e os dados de identificação; a chave privada nunca é enviada à AC nem a terceiros.

⚠ **Alerta de prova:** Manter o certificado autoassinado no site público porque 'a criptografia é a mesma'.
Como não cair: A cifra pode ser igual, mas o navegador não confia em quem assinou e mostra alerta; site público usa certificado de AC pública confiável.

⚠ **Alerta de prova:** Renovar o certificado com a mesma chave privada depois que ela vazou.
Como não cair: Chave privada comprometida: revogar o certificado e emitir outro com novo par de chaves.

⚠ **Alerta de prova:** Usar SHA-256 sem chave para provar que a mensagem da API veio da outra parte.
Como não cair: Hash sem chave pode ser recalculado por quem alterou a mensagem; com chave compartilhada e sem não repúdio, a resposta é HMAC.

⚠ **Alerta de prova:** Trocar MD5 por SHA-1 'porque é mais rápido e ainda seguro', ou por CRC32.
Como não cair: SHA-1 também tem colisões demonstradas; CRC32 só pega erro acidental. A troca adequada é SHA-256 ou superior.

⚠ **Alerta de prova:** Achar que o certificado *.empresa.com.br cobre pagamentos.sul.empresa.com.br, ou que validação estendida resolve.
Como não cair: Curinga vale para um único nível de subdomínio; o tipo de validação não muda a regra de correspondência.

⚠ **Alerta de prova:** Classificar a placa de 'área monitorada' como preventivo físico ou detectivo.
Como não cair: Placa não impede nem registra nada; ela só desencoraja: dissuasivo.

⚠ **Alerta de prova:** Marcar 'compensatória' como categoria do treinamento conduzido por pessoas.
Como não cair: Compensatório é TIPO de controle; a categoria de algo executado por pessoas é operacional.

⚠ **Alerta de prova:** Exigir RSA estático de 4096 bits para proteger sessões já gravadas.
Como não cair: Na troca RSA estática, quem obtiver a chave privada decifra sessões gravadas; só chaves efêmeras (ECDHE) dão forward secrecy.

⚠ **Alerta de prova:** Usar criptografia de disco inteiro para impedir que o DBA leia CPF e diagnóstico.
Como não cair: O disco fica decifrado para o sistema em funcionamento; para campos específicos use criptografia de coluna ou registro.

⚠ **Alerta de prova:** Cifrar o contrato com a própria chave pública (ou com a privada do destinatário) para enviá-lo em sigilo.
Como não cair: Sigilo: chave pública do destinatário. Assinatura: chave privada do remetente. Ninguém tem a chave privada de outra pessoa.

⚠ **Alerta de prova:** Dispensar o registro da mudança porque foi emergência.
Como não cair: A emergência só acelera a aprovação; a mudança deve ser registrada e submetida à revisão posterior do CAB.

⚠ **Alerta de prova:** Dizer que a criptografia do notebook furtado preservou a disponibilidade ou a integridade.
Como não cair: O que se preservou foi a confidencialidade; o equipamento perdido não está disponível, e o risco era leitura, não alteração.

Como cai na prova

📝 **Como cai:** 'Como se classificam, respectivamente, X e Y?' com uma alternativa idêntica em ordem invertida.
Como resolver: Classifique cada item separadamente, escreva a ordem do enunciado e só então compare; a alternativa invertida é a armadilha clássica.

📝 **Como cai:** Cenário descreve uma medida e pergunta a categoria OU o tipo de controle.
Como resolver: Veja se a pergunta é 'categoria' (técnica, gerencial, operacional, física) ou 'tipo' (preventivo, detectivo etc.) e elimine as alternativas do outro eixo.

📝 **Como cai:** Mudança planejada com algum complicador (legado sem suporte, dependências, reinício, falha após implantação).
Como resolver: Identifique a fase: antes (análise de impacto, testes, janela, aviso), durante (escopo restrito) ou depois (backout ou fail forward, atualizar documentação, registro de emergência).

📝 **Como cai:** Dois requisitos criptográficos no mesmo enunciado (Escolha DUAS ou TRÊS).
Como resolver: Associe cada requisito a uma ferramenta: sigilo com pública do destinatário, autoria com privada do remetente; chave da AC em HSM, disco em TPM, nuvem em KMS.

📝 **Como cai:** Pergunta qual algoritmo ou versão manter ou aposentar.
Como resolver: Mantenha AES (GCM), TLS 1.3 (1.2 só para compatibilidade), SHA-256 e RSA de 2048 bits ou mais; aposente DES, RC4, MD5, SHA-1, SSL 3.0 e TLS 1.0/1.1.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Revisão de logs, alertas no SIEM, sem impedir a ação	**Controle detectivo**
Não dá para aplicar o controle ideal e se usa outro no lugar	**Controle compensatório**
Norma ou política dizendo o que os funcionários devem fazer	**Controle diretivo**
Quem fez a alteração, quando e de qual estação	**Contabilização (accounting) do AAA**
Um componente decide e outro, no caminho do tráfego, aplica	**PDP e PEP, nessa ordem**
Projetar como se o invasor já estivesse dentro	**Assume breach (Zero Trust)**
Combinar chave secreta por rede pública sem transmiti-la	**Diffie-Hellman**
Chave roubada no futuro não pode decifrar sessões gravadas	**Forward secrecy com ECDHE**
Hashes idênticos para senhas iguais, tabelas pré-calculadas	**Faltou sal único por senha**

Servidor anexa a resposta OCSP ao handshake TLS	**OCSP stapling**
Cópia da chave privada com terceiro confiável para recuperar dados	**Custódia de chaves (key escrow)**
Componente imutável verifica a assinatura do firmware antes de executar código	**Raiz de confiança em hardware**
Caminho documentado para voltar à versão anterior com backup testado	**Plano de backout**
Dados escondidos dentro de foto sem alteração visível	**Esteganografia**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- Zero Trust nunca confia na rede interna nem em login anterior: cada acesso é avaliado de novo.
- Assinatura digital dá integridade, autenticidade e não repúdio, mas não confidencialidade.
- A chave privada nunca vai na CSR; se vazar, revogue e gere novo par.
- Compensatório é tipo, não categoria; operacional é o que pessoas executam.
- Base64 é codificação, nunca criptografia nem hash.

Essenciais para a prova (checklist)

- ☐ Sei classificar uma medida nas quatro categorias e nos seis tipos de controle.
- ☐ Sei separar autenticação, autorização e contabilização em um cenário.
- ☐ Sei explicar PDP, PEP, assume breach e acesso por sessão no Zero Trust.
- ☐ Sei quando usar backout e quando usar fail forward.
- ☐ Sei o que vai na CSR e por que a AC raiz fica offline.
- ☐ Sei diferenciar CRL, OCSP e OCSP stapling.
- ☐ Sei escolher entre hash, HMAC e assinatura digital conforme o requisito.
- ☐ Sei qual nível de criptografia (disco, partição, volume, arquivo, TDE, coluna) atende cada cenário.
- ☐ Sei onde guardar cada chave: HSM, TPM, KMS ou enclave seguro.

Questões de revisão do capítulo

R3.1 · Conceitos Gerais de Segurança

A equipe do ERP da Distribuidora Ventos do Sul vai atualizar o banco de dados em uma janela noturna. O CAB só aprova a mudança se houver um caminho documentado para restaurar a versão anterior, com backup testado, caso a atualização falhe. O que está sendo exigido?

A. Lista de bloqueio de aplicativos
B. Plano de reversão (backout)
C. Análise de causa raiz
D. Relatório pós-incidente

R3.2 · Conceitos Gerais de Segurança

Uma atualização de configuração do serviço DNS interno da Universidade Lago Sul exigirá reiniciar o serviço; por alguns segundos as consultas falharão, afetando autenticação, e-mail e acesso a sistemas. O que a gestão de mudanças deve prever?

A. Desligamento dos serviços que dependem do DNS
B. Reinício imediato em horário de pico, sem comunicação
C. Cancelamento da mudança até haver novo servidor
D. Reinício na janela, com redundância ou aviso aos afetados

R3.3 · Conceitos Gerais de Segurança

A Rede de Laboratórios Exame Certo instalou catracas com crachá na entrada da área técnica e configurou o firewall para bloquear conexões de entrada não solicitadas. O objetivo das duas medidas é impedir que um acesso indevido aconteça. Que tipo de controle elas representam?

A. Compensatório
B. Detectivo
C. Corretivo
D. Preventivo

R3.4 · Conceitos Gerais de Segurança

Após uma alteração indevida na tabela de preços do e-commerce da Loja Mundo Pet, a gerência quer saber qual administrador fez a mudança, em que horário e a partir de qual estação. Qual componente do AAA fornece essas informações?

A. Federação de identidades
B. Contabilização (accounting)
C. Autenticação (authentication)
D. Autorização (authorization)

Respostas comentadas

R3.1. B) Plano de reversão (backout)

Por quê: Um bom processo de gestão de mudanças exige análise de impacto, testes, janela de manutenção e plano de reversão (backout), que permite voltar à última configuração funcional se a mudança falhar.

✗ A) Incorreta. Listas de bloqueio controlam quais programas podem rodar, não como desfazer mudanças.
✗ C) Incorreta. Análise de causa raiz investiga por que um problema ocorreu, depois do fato.
✗ D) Incorreta. O relatório pós-incidente é produzido depois de um incidente, não antes da mudança.

> **Dica de prova:** Como desfazer se der errado: plano de backout.

R3.2. D) Reinício na janela, com redundância ou aviso aos afetados

Por quê: O reinício de serviços é uma implicação técnica da gestão de mudanças: serviços centrais, como DNS, afetam muitos dependentes, e a mudança deve considerar redundância, janela e comunicação.

✗ A) Incorreta. Desligar os serviços dependentes amplia a indisponibilidade.
✗ B) Incorreta. Reiniciar no pico e sem aviso maximiza o impacto.
✗ C) Incorreta. Cancelar a mudança deixa a configuração necessária sem aplicar.

> **Dica de prova:** Reiniciar serviço do qual muitos dependem: janela, redundância e aviso.

R3.3. D) Preventivo

Por quê: Controles preventivos buscam impedir que um evento indesejado ocorra, como fechaduras, catracas, regras de firewall e controle de acesso; um mesmo tipo pode existir em categorias diferentes, física e técnica.

✗ A) Incorreta. Compensatórios substituem um controle principal inviável, o que não é o caso.
✗ B) Incorreta. Controles detectivos registram e alertam, sem impedir.
✗ C) Incorreta. Controles corretivos atuam depois do incidente.

> **Dica de prova:** Impede o acesso antes que aconteça: preventivo, seja físico ou técnico.

R3.4. B) Contabilização (accounting)

Por quê: No modelo AAA, a autenticação verifica a identidade, a autorização concede permissões e a contabilização (accounting) registra as atividades, sustentando auditoria e responsabilização.

✗ A) Incorreta. Federação permite usar uma identidade entre domínios e não faz parte do AAA.
✗ C) Incorreta. A autenticação confirma a identidade no login, mas não registra as ações seguintes.
✗ D) Incorreta. A autorização define o que o usuário pode fazer, não o que ele fez.

> **Dica de prova:** Quem fez, o quê, quando e de onde: accounting.

04

CAPÍTULO 4 · 14% DA PROVA

Gestão e Supervisão do Programa de Segurança

Este domínio caiu para 14% no V8, mas é o que mais tem vocabulário de gestão: artefatos de governança, gestão de riscos com cálculos, terceiros, conformidade e privacidade, auditorias e conscientização. Entraram EOI, MOA, AML/CTF, antissuborno e pontuação de risco comportamental de pessoas. As questões dão um cenário e pedem o nome do documento, da etapa ou do tratamento, e as erradas são outros documentos reais (SLA, MOU, SOW, NDA, AUP). Preciso saber de cor SLE = valor x fator de exposição, ALE = SLE x ARO e ARO = 1/N. Onde mais erro: RFI x RFP x RFQ x EOI, padrão x diretriz x runbook, risco inerente x residual e os direitos do titular.

Neste capítulo

17 tópicos-chave · 14 pegadinhas · 6 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Políticas, padrões, diretrizes e procedimentos

Política declara intenção e regras de alto nível; padrão é obrigatório e mensurável (AES-256 em repouso, TLS 1.2 ou superior, RSA de no mínimo 3072 bits); diretriz é recomendação; procedimento ou runbook é o passo a passo com comandos exatos (isolar endpoint no EDR e coletar evidências). RFC da IETF é a especificação técnica de protocolos de internet, como SPF, DKIM e DMARC.

Políticas cobradas

AUP define o que o usuário pode fazer com a TI e é assinada antes do acesso; política de resposta a incidentes, aprovada pela diretoria, define compromisso, o que é incidente, autoridade, papéis, escalonamento e comunicação; classificação e retenção de dados; descarte de dados; mesa limpa; BYOD; política de privacidade para clientes. Arquitetura de referência é modelo publicado e testado com vários fornecedores.

Identificação e análise de riscos

Primeiro passo: identificar ativos e seus donos. Análise qualitativa usa baixo, médio e alto com opinião de especialistas; quantitativa usa valores como SLE, ARO e ALE. Pontuação (ex.: probabilidade x impacto de 1 a 25) e categorização (tecnológico, regulatório, operacional) facilitam priorizar.

SLE, ARO e ALE

SLE = valor do ativo x fator de exposição (R$ 300.000 x 60% = R$ 180.000 por evento). ARO = 1/N para um evento a cada N anos (a cada quatro anos = 0,25). ALE = SLE x ARO (R$ 200.000 x 40% = R$ 80.000; x 0,2 = R$ 16.000 por ano).

Risco inerente, residual e apetite

Inerente é o nível antes dos controles; mitigações atuais são os controles que já existem; residual é o que sobra depois dos controles; apetite é o limite que a diretoria aceita. Residual acima do apetite precisa de tratamento ou aprovação formal.

Tratamentos de risco

Mitigar reduz probabilidade ou impacto com controles (WAF e autenticação forte); aceitar assume o risco, de preferência com exceção formal assinada pelo dono, controles compensatórios e data de revisão; transferir repassa o impacto, como seguro cibernético (sem contrato não há transferência); evitar encerra a atividade que gera o risco.

Registro de riscos e governança

O proprietário do risco decide o tratamento, aprova orçamento e presta contas. O registro precisa de revisões periódicas com os donos e de comunicação às partes interessadas, com escalonamento imediato do que passa do apetite. Supervisão da gestão (management oversight) é a alta gestão acompanhando o painel, cobrando atrasos e aprovando riscos acima do apetite.

BIA, plano de continuidade e plano de recuperação de desastres

A BIA identifica processos críticos, impacto de cada hora de parada e tempos máximos toleráveis, antes do plano de continuidade. O plano de continuidade mantém o negócio funcionando (atendimento e entregas na crise); o plano de recuperação de desastres restaura servidores, rede e dados no site alternativo.

Seleção de fornecedores

RFI coleta informações de mercado antes do escopo; EOI pede que interessados se apresentem para montar lista curta; RFP pede propostas para escopo definido; RFQ pede só preços para escopo fechado. Due diligence investiga o candidato (saúde financeira, certificações, incidentes, localização dos datacenters, referências). Conflito de interesses é avaliador ligado a concorrente.

Acordos com terceiros

MSA é o contrato-mestre com termos gerais para vários projetos; SOW detalha escopo, entregas, prazos e valor de cada projeto; MOU registra só intenção de cooperar, sem obrigações; NDA obriga ao sigilo antes de compartilhar informação sensível; SLA é o compromisso contratual com multa e SLO é a meta interna mais rígida; cláusula de direito de auditoria permite verificar os controles do fornecedor.

Monitoramento de fornecedores

Registro de fornecedores é a base central com serviços, dados acessados, criticidade, contratos e data da última avaliação. Avaliação com atestação usa relatório SOC 2 Tipo II de auditor independente e questionário. Também: monitoramento do nível de serviço com multas e teste de intrusão no ambiente do fornecedor, conforme regras acordadas.

Limitações de terceiros

Aprisionamento ao fornecedor (lock-in) por formatos e APIs exclusivos; geografia e jurisdição (autoridades estrangeiras exigindo acesso, salvaguardas para transferência internacional); pessoal interno limitado e retorno do investimento a justificar.

Privacidade: papéis e direitos

Controlador decide o porquê do tratamento; operador executa em nome dele. Direitos do titular: correção (retificação), eliminação ou esquecimento (apagar), restrição do tratamento (guardar sem usar durante contestação), oposição (parar o marketing), portabilidade e acesso. Opt-in exige que o titular marque a caixa desmarcada; consentimento tácito ou caixa pré-marcada não vale no GDPR.

Conformidade e obrigações legais

Consequências da não conformidade: multas e sanções, perda de licença ou suspensão de atividades e danos à reputação. Retenção legal (legal hold) suspende qualquer exclusão, inclusive automática, até o fim do processo. Ordem judicial: validar com o jurídico e entregar só o pedido, no prazo. ISO/IEC 27001 é referencial internacional; GDPR é regional (UE). Reconhecimento é o colaborador confirmando leitura; atestação é o gestor declarando que o controle funciona.

Auditorias e avaliações

Carta de auditoria (audit charter), aprovada pelo conselho, define propósito, autoridade, independência, escopo e linhas de reporte da auditoria interna; o comitê de auditoria supervisiona controles e auditorias. Gap analysis lista o que falta para cumprir uma norma; auditoria externa independente gera certificação aceita por terceiros; avaliação regulatória é o regulador verificando o cumprimento; técnicas de coleta incluem amostragem e questionários.

Testes de intrusão

Regras de engajamento definem escopo, IPs permitidos e proibidos, horários, técnicas e contatos de emergência. Ambiente conhecido recebe documentação completa; parcialmente conhecido recebe parte (lista de IPs e conta comum); desconhecido não recebe nada. Reconhecimento passivo coleta sem tocar no alvo (DNS público, redes profissionais, logs de transparência); ativo interage. Red team ataca, blue team defende, purple team integra os dois.

Conscientização

Tipos: inicial (primeiro dia), contínuo (mensal), direcionado (grupo específico, como financeiro), corretivo (quem falhou na simulação). Entrega: um-para-muitos, um-para-um, LMS (escala com avaliação e relatório) e portal de autoatendimento. Eficácia se mede por taxa de cliques e de reporte em simulações ao longo do tempo e pela pontuação de risco comportamental. Temas gerais: BEC, mídias removíveis, trabalho remoto; treinamentos de conformidade: AML/CTF (operações suspeitas, KYC, comunicação às autoridades) e anticorrupção e antissuborno.

Macetes para memorizar

Fórmulas de risco

SLE = Valor x Exposição; ALE = SLE x ARO; ARO = 1 ÷ anos entre eventos.

Ordem da compra

RFI pergunta (informação), EOI chama (interessados), RFP pede proposta, RFQ pede o preço.

Contratos

MSA é a casa, SOW é cada cômodo; MOU é só o aperto de mão; NDA é o cadeado na boca.

Tratamento de risco

Seguro = transferir; desligar = evitar; controle = mitigar; conviver por escrito = aceitar.

Times de teste

Red ataca, blue defende, purple (vermelho + azul) trabalham juntos.

Treinamento

Primeiro dia = inicial; todo mês = contínuo; um grupo = direcionado; quem errou = corretivo.

Tabela de memorização: não confunda

Quando é...	...e quando é
RFI Ainda pesquisando o mercado e como as soluções são licenciadas, antes de definir o escopo.	**RFP / RFQ / EOI** RFP: propostas para escopo definido. RFQ: só preço para escopo fechado. EOI: interessados se apresentam para formar lista curta.
MSA Termos gerais (responsabilidades, pagamento) válidos para vários projetos.	**SOW** Escopo, entregas, prazos e valor de um projeto específico.

SLA Compromisso contratual com o cliente, com multa se não cumprido (99,9%).	**SLO** Meta interna mais rígida para ter margem (99,95%).
Risco inerente Estimado antes de considerar os controles.	**Risco residual** O que sobra depois dos controles; comparado com o apetite de risco.
Padrão Requisito obrigatório e mensurável, como algoritmos e tamanhos de chave.	**Diretriz / runbook** Diretriz é recomendação opcional; runbook é a sequência de passos com comandos para uma tarefa.
Plano de continuidade de negócios Manter atendimento e operação durante a crise, com processos prioritários e meios alternativos.	**Plano de recuperação de desastres** Restaurar servidores, rede e dados de TI no site alternativo.
Direito ao esquecimento (eliminação) Apagar todos os dados pessoais quando não há obrigação legal de mantê-los.	**Oposição / restrição do tratamento** Oposição: parar um tratamento específico, como marketing. Restrição: guardar sem usar enquanto a contestação é verificada.

Números que caem

Item	Valor
Peso do domínio na prova	**14% (caiu em relação ao SY0-701)**
SLE	**Valor do ativo x fator de exposição**
ALE	**SLE x ARO**
ARO de um evento a cada N anos	**1/N (a cada 4 anos = 0,25)**
Escala de pontuação de risco por probabilidade x impacto	**1 a 25**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Calcular a SLE com o valor total do ativo (R$ 300.000).
Como não cair: SLE aplica o fator de exposição: 60% de R$ 300.000 = R$ 180.000 por evento.

⚠ **Alerta de prova:** Dar como ALE a perda de um único evento (R$ 80.000) ou multiplicar a ARO duas vezes.
Como não cair: ALE = SLE x ARO uma vez só: R$ 80.000 x 0,2 = R$ 16.000 por ano.

⚠ **Alerta de prova:** Marcar ARO = 4 para um roubo a cada quatro anos.
Como não cair: ARO = 1/N: um evento a cada quatro anos é 0,25 por ano.

⚠ **Alerta de prova:** Chamar de mitigação a contratação de seguro cibernético.
Como não cair: Seguro repassa o impacto: transferência. Mitigar é reduzir com controles.

⚠ **Alerta de prova:** Considerar 'transferir ao fornecedor sem contrato' ou 'adiar a análise' como tratamento.
Como não cair: Sem contrato não há transferência, e adiar deixa o risco sem dono; aceitar formalmente é tratamento legítimo quando o controle custa mais que o dano.

⚠ **Alerta de prova:** Chamar de risco inerente o nível reavaliado depois dos controles.
Como não cair: Depois dos controles é residual; o limite da diretoria é o apetite.

⚠ **Alerta de prova:** Classificar como diretriz o documento obrigatório que fixa AES-256 e RSA de 3072 bits.
Como não cair: Obrigatório e mensurável é padrão; diretriz é recomendação.

⚠ **Alerta de prova:** Inverter SLA e SLO.
Como não cair: O contrato com multa é o SLA; a meta interna é o SLO.

⚠ **Alerta de prova:** Usar RFQ para pesquisar quais soluções existem no mercado.
Como não cair: Sem escopo definido é RFI; RFQ só pede preço para escopo pronto.

⚠ **Alerta de prova:** Achar que a agência de marketing que só executa campanhas é controladora conjunta.
Como não cair: Quem segue instruções sem definir finalidades é operadora; quem decide o porquê é controladora. Custodiante e proprietário são papéis internos, não de privacidade.

⚠ **Alerta de prova:** Pedir autorização do cliente antes de cumprir a ordem judicial, ou entregar a base inteira.
Como não cair: A ordem não depende do cliente; valide com o jurídico e entregue só o escopo pedido, no prazo.

⚠ **Alerta de prova:** Usar ambiente desconhecido (caixa preta) para o pentest que recebeu IPs e uma conta comum.
Como não cair: Algumas informações e credencial comum é ambiente parcialmente conhecido.

⚠ **Alerta de prova:** Medir a eficácia da conscientização por cartazes, horas de preparo ou slides.
Como não cair: Mede-se comportamento: taxa de cliques e de reporte em simulações ao longo do tempo.

⚠ **Alerta de prova:** Aplicar palestra geral ou advertência no RH a quem clicou na simulação.
Como não cair: Quem falhou recebe treinamento corretivo direcionado.

Como cai na prova

📝 **Como cai:** Cálculo de SLE, ARO ou ALE com valores em reais.
Como resolver: Escreva a fórmula antes: aplique o fator de exposição, converta 'a cada N anos' em 1/N e multiplique uma vez; as erradas usam o valor total, deslocam a vírgula ou aplicam a ARO duas vezes.

📝 **Como cai:** 'Que documento é esse?' entre SLA, MOU, SOW, MSA, NDA, AUP, RoE.
Como resolver: Pergunte o propósito: metas com multa (SLA), intenção (MOU), detalhe do projeto (SOW), termos gerais (MSA), sigilo (NDA), regras do usuário (AUP), limites do pentest (RoE).

📝 **Como cai:** Escolha DUAS com dois riscos diferentes para tratar.
Como resolver: Compare custo do controle com o dano: controle viável e eficaz = mitigar; controle mais caro que o dano = aceitar formalmente; desligar o negócio é desproporcional quando há mitigação.

📝 **Como cai:** 'Como se chamam, respectivamente?' em pares como inerente/residual, SLA/SLO, MSA/SOW, BCP/DRP.
Como resolver: Defina cada termo isolado e confira a ordem; a alternativa invertida está sempre presente.

📝 **Como cai:** Pedido do titular de dados.
Como resolver: Corrigir = retificação; apagar tudo = esquecimento; parar marketing = oposição; guardar sem usar = restrição; levar para outro = portabilidade; cópia = acesso.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Escopo, IPs permitidos e proibidos, horários e contatos de emergência do pentest	**Regras de engajamento (RoE)**
Documento que dá autoridade e independência à auditoria interna	**Carta de auditoria (audit charter)**
Comparar controles atuais com a norma antes do projeto	**Análise de lacunas (gap analysis)**
Processo judicial e nada pode ser apagado, nem pela retenção automática	**Retenção legal (legal hold)**
Relatório SOC 2 Tipo II e questionário do fornecedor	**Avaliação do fornecedor com atestação**

Formatos e APIs exclusivos tornam a migração cara	**Aprisionamento ao fornecedor (lock-in)**
Leis estrangeiras exigindo acesso aos dados do provedor	**Geografia e jurisdição do fornecedor**
Só intenção de cooperar, sem obrigações financeiras	**MOU**
Operações suspeitas, KYC e comunicação às autoridades	**Treinamento AML/CTF**
Vantagem oferecida a servidor público para ganhar contrato	**Anticorrupção e antissuborno**
Nota de risco por colaborador com cliques, reportes e violações	**Pontuação de risco comportamental**
DNS público, perfis profissionais e logs de transparência sem enviar pacotes	**Reconhecimento passivo**
Caixa de consentimento desmarcada que o cliente precisa marcar	**Opt-in**
Colaborador confirma leitura e gestor declara que o controle funciona	**Reconhecimentos e atestações**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- SLE usa o fator de exposição; ALE multiplica pela ARO uma única vez.
- Seguro é transferência; aceitar exige registro formal, dono e data de revisão.
- RFI antes do escopo, RFQ com escopo fechado só para preço.
- Padrão é obrigatório; diretriz é recomendação; runbook é passo a passo.
- Eficácia da conscientização se mede por comportamento, não por esforço.

Essenciais para a prova (checklist)

- ☐ Sei diferenciar política, padrão, diretriz, procedimento e runbook.
- ☐ Sei calcular SLE, ARO e ALE sem errar o fator de exposição.
- ☐ Sei diferenciar risco inerente, residual, apetite e os quatro tratamentos.
- ☐ Sei a ordem e o uso de RFI, EOI, RFP e RFQ.
- ☐ Sei para que servem MSA, SOW, MOU, NDA, SLA, SLO e direito de auditoria.
- ☐ Sei as limitações de terceiros: lock-in, jurisdição, pessoal e ROI.
- ☐ Sei os direitos do titular e os papéis de controlador e operador.
- ☐ Sei diferenciar gap analysis, auditoria externa, avaliação regulatória e audit charter.
- ☐ Sei os tipos de ambiente de pentest, reconhecimento passivo e ativo e red, blue e purple team.
- ☐ Sei os tipos, mecanismos de entrega e métricas de conscientização.

Questões de revisão do capítulo

R4.1 · Gestão e Supervisão do Programa de Segurança

A Construtora Base Forte quer um documento aprovado pela diretoria que estabeleça o compromisso com a resposta a incidentes, defina o que é um incidente, a autoridade e os papéis da equipe, os critérios de escalonamento e as obrigações de comunicação. Que artefato é esse?

A. Política de resposta a incidentes
B. Relatório pós-incidente
C. Plano de recuperação de desastres de TI
D. Playbook técnico de ransomware

R4.2 · Gestão e Supervisão do Programa de Segurança

No registro de riscos da Seguradora Atlas, o risco de indisponibilidade do portal de sinistros foi atribuído à diretora de operações, que decide sobre o tratamento, aprova o orçamento das mitigações e presta contas à diretoria. Qual papel ela exerce em relação a esse risco?

A. Proprietária do risco
B. Analista de risco independente
C. Auditora interna do processo
D. Custodiante dos dados do portal

R4.3 · Gestão e Supervisão do Programa de Segurança

Antes de elaborar o plano de continuidade, a Cooperativa Agrícola Terra Boa quer identificar os processos críticos, o impacto financeiro e operacional de cada hora de parada e os tempos máximos toleráveis de interrupção. Que atividade deve ser realizada?

A. Análise de impacto nos negócios (BIA)
B. Teste de intrusão externo
C. Auditoria de conformidade com a LGPD
D. Análise de vulnerabilidades técnicas

R4.4 · Gestão e Supervisão do Programa de Segurança

Durante uma ronda noturna na Corretora Valor Real, a segurança encontrou contratos de clientes sobre as mesas, um post-it com senha colado no monitor e um crachá esquecido em uma gaveta aberta. Que política está sendo descumprida?

A. Política de BYOD
B. Política de retenção de dados
C. Política de mesa limpa
D. Política de resposta a incidentes

Respostas comentadas

R4.1. A) Política de resposta a incidentes

Por quê: A política de resposta a incidentes é aprovada pela alta gestão e define escopo, conceitos, papéis, autoridade, prioridades e requisitos de comunicação; planos e playbooks detalham a execução.

✗ B) Incorreta. O relatório é produzido depois de um incidente.
✗ C) Incorreta. O plano de recuperação trata da restauração de TI após desastres.
✗ D) Incorreta. O playbook detalha passos para um tipo específico de incidente.

> **Dica de prova:** Compromisso, definições e papéis aprovados pela diretoria: política de resposta a incidentes.

R4.2. A) Proprietária do risco

Por quê: Cada risco do registro deve ter um proprietário com autoridade para decidir o tratamento, alocar recursos e responder pelo resultado; isso garante responsabilização e acompanhamento.

✗ B) Incorreta. Analistas avaliam riscos, mas não respondem pela decisão.
✗ C) Incorreta. A auditoria avalia de forma independente e não deve ser dona dos riscos.
✗ D) Incorreta. Custodiante aplica controles sobre dados, sem decidir o tratamento de riscos.

> **Dica de prova:** Quem decide e responde pelo tratamento do risco: risk owner.

R4.3. A) Análise de impacto nos negócios (BIA)

Por quê: A análise de impacto nos negócios estima as consequências da interrupção de funções e processos, definindo prioridades de recuperação e tempos máximos de parada que alimentam os planos de continuidade e de recuperação.

✗ B) Incorreta. O pentest avalia a segurança técnica, não o impacto de interrupções no negócio.
✗ C) Incorreta. Uma auditoria de LGPD verifica conformidade com a privacidade, não a criticidade dos processos.
✗ D) Incorreta. Varreduras encontram falhas técnicas, sem medir impacto operacional.

> **Dica de prova:** Processos críticos e impacto da parada antes do plano de continuidade: BIA.

R4.4. C) Política de mesa limpa

Por quê: A política de mesa limpa determina que documentos sensíveis, mídias, senhas e crachás não fiquem expostos quando o posto está vazio, reduzindo vazamentos e acesso indevido.

✗ A) Incorreta. BYOD trata de dispositivos pessoais.
✗ B) Incorreta. Retenção define prazos de guarda, não o cuidado com a mesa.
✗ D) Incorreta. Resposta a incidentes trata do tratamento de incidentes.

> **Dica de prova:** Documento, senha e crachá largados na mesa: política de mesa limpa.

05

CAPÍTULO 5 · 27% DA PROVA

Operações de Segurança

É o domínio mais pesado da prova (27%) e no V8 recebeu as técnicas de mitigação, IA nas operações (agentic, chatbot, análise preditiva, baselines aumentadas por IA) e novidades como CSPM, IPAM, varredura de segredos, BIMI, Group Policy, SELinux, passkeys, códigos de backup, contas de emergência, just-in-time e monitoramento de credenciais comprometidas. O formato típico é 'qual controle, ferramenta ou etapa atende ao cenário', e as alternativas erradas costumam ser ferramentas reais que resolvem outro problema. Preciso dominar IAM e modelos de acesso, autenticação de e-mail, gestão de vulnerabilidades, monitoramento, automação e o ciclo de resposta a incidentes com forense. Onde mais erro: NIDS x NIPS x HIDS x HIPS, DLP de rede x de endpoint, MDM x MAM e a ordem das fases de resposta.

Neste capítulo

19 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Modelos de controle de acesso

DAC: o dono do recurso decide quem acessa; MAC: rótulos de classificação e habilitação definidos centralmente, que os donos não alteram; RBAC: permissões por cargo ou função; baseado em regras: regra central que vale para todos por condição, independentemente do cargo; baseado em horário: só entra em certa faixa de horário. ACL é o mecanismo no próprio recurso (pasta com leitura para Auditoria e escrita para Compras).

Privilégios: JIT, segregação de funções e contas

Acesso just-in-time ativa o privilégio por solicitação aprovada, com prazo e remoção automática. Segregação de funções divide etapas críticas entre pessoas (quem cadastra não aprova, quem aprova não paga). Administrador local atua em uma máquina; global, no domínio inteiro. Herança de permissões: leitura para Todos na pasta mãe vaza para as subpastas.

Ciclo de vida de identidades

Verificação de identidade (proofing) comprova quem é antes de criar a conta (documento, selfie com vivacidade, bases oficiais). Provisionamento e desprovisionamento automáticos a partir de eventos do RH. Revisão periódica de acessos pelos gestores, removendo o que não for confirmado. Conta de terceiro: individual, com MFA, escopo mínimo e data de expiração. Auditoria de contas compara as contas com a política (sem MFA, inativas, senhas que nunca expiram).

Federação e SSO: SAML, OAuth e LDAP

SAML 2.0: o IdP envia ao SaaS uma asserção XML assinada com identidade e atributos. OAuth 2.0: autorização delegada, o app recebe token com escopo limitado sem conhecer a senha. LDAP consulta o diretório e deve usar TLS (LDAPS ou StartTLS). SSO concentra o risco, então o IdP precisa de MFA resistente a phishing.

Autenticação moderna

Passkey FIDO2/WebAuthn resiste a phishing porque a credencial é vinculada ao domínio legítimo. Passwordless usa biometria ou PIN local que desbloqueia credencial criptográfica do dispositivo. Token físico (hard) é aparelho dedicado; token de software (soft) é aplicativo no celular. Recuperação de MFA mantendo fator de posse: códigos de backup de uso único ou hard token.

Senhas segundo o NIST SP 800-63B-4

Senhas longas (no mínimo 15 caracteres quando são o único fator; 8 quando fazem parte de MFA), sem regras de composição, sem troca periódica sem indício de comprometimento, bloqueio de senhas em listas de vazadas e permissão para gerenciadores de senha e colar. Proibido: perguntas de segurança e dicas de senha visíveis. Gerenciador de senhas corporativo e monitoramento de credenciais comprometidas complementam.

Contas de emergência (break glass)

Contas de acesso de emergência, monitoradas e de uso restrito, evitam ficar sem acesso administrativo ao locatário se o MFA ou a federação falharem. Não é tirar o MFA de um administrador comum nem liberar logins pela rede interna.

Sensores de intrusão

NIDS só detecta e alerta; NIPS fica inline e descarta pacotes; HIDS com monitoramento de integridade de arquivos alerta quando binários ou páginas mudam; HIPS bloqueia no próprio servidor, inclusive o que chega cifrado; WIPS detecta e contém ponto de acesso falso e evil twin. SPAN (espelhamento de porta) entrega cópia do tráfego a sensor passivo.

EDR e XDR

EDR registra continuamente o comportamento do endpoint, permite investigar a linha do tempo e isolar a máquina remotamente; pega abuso de ferramentas legítimas que assinaturas não pegam. XDR correlaciona endpoint, e-mail, identidade e nuvem em incidentes únicos com resposta coordenada. Detecção heurística ou comportamental bloqueia executável sem assinatura que tenta desativar backup e alterar centenas de arquivos.

Controles de rede e web

Firewall baseado em regras: lista ordenada, primeira correspondência decide e negação implícita no final. Firewall de camada 7 filtra por URL (bloquear /admin); camadas 3 e 4 só veem IP e porta. WAF bloqueia padrões de injeção como patch virtual quando o código não pode mudar; rate limiting freia muitas requisições de poucos IPs. UTM reúne firewall, IPS, antimalware, filtro web e VPN em um appliance; proxy centralizado filtra a navegação sem agente.

DLP, CASB, CSPM, IPAM, MDM e MAM

DLP com agente no endpoint bloqueia cópia para pendrive mesmo fora do proxy; DLP de rede só vê o que passa pela matriz. CASB descobre SaaS não aprovados e aplica DLP na nuvem. CSPM avalia continuamente as configurações das contas de nuvem contra benchmarks. IPAM centraliza faixas de IP, escopos DHCP e zonas DNS. MDM gerencia o aparelho inteiro (PIN, criptografia, apagamento remoto); MAM protege só os dados corporativos dentro dos apps aprovados no aparelho pessoal.

NAC e 802.1X

802.1X só libera a porta do switch após autenticação no RADIUS; portal cativo exibe página de aceite ou login no navegador depois da conexão (hóspedes). Verificação de postura do NAC exige antivírus, disco cifrado e patches, mandando o não conforme para VLAN de correção; agente nos gerenciados, sem agente em visitantes e IoT. Filtro de MAC é facilmente falsificado.

Hardening e configuração

Hardening remove pacotes e serviços desnecessários, desativa contas padrão, aplica benchmark e restringe administração. CIS Benchmarks são a referência pública de configuração segura; SCAP (XCCDF e OVAL) verifica conformidade automaticamente; GPO aplica configuração em massa em Windows do domínio; SELinux em enforcing nega e registra AVC denied mesmo com permissão tradicional (em permissive só registra); SNMPv3 com autenticação e privacidade substitui SNMPv2c; syslog sobre TLS envia eventos ao SIEM.

Segurança de aplicações

Validação de entrada no servidor por lista de permissões (a do navegador é contornável); cookie de sessão com Secure e HttpOnly; SAST examina o código sem executar e DAST testa a aplicação rodando; varredura de segredos com proteção no push barra a chave antes do repositório remoto; segredo achado no histórico deve ser revogado e rotacionado; assinatura de código prova origem e integridade; controles integrados no pipeline de CI/CD.

Autenticação de e-mail

SPF (registro TXT) lista os servidores autorizados a enviar; DKIM assina a mensagem e publica a chave pública no DNS; DMARC define a política com base em SPF e DKIM: p=none só observa e coleta relatórios agregados (rua), p=quarantine ou p=reject barram falsificações; BIMI exibe o logotipo da marca e depende de DMARC em aplicação. MX indica quem recebe.

Gestão de vulnerabilidades

Varredura credenciada vê patches e bibliotecas internas; externa não credenciada mostra o que o atacante vê de fora; agentes para notebooks que saem da rede, sem agente para impressoras e câmeras. Priorize por exposição e criticidade (mesma nota base, contexto diferente) e pela cadeia de exploração demonstrada no pentest. Sem correção possível: exceção formal com prazo, dono e controles compensatórios. Depois do patch, confirme com nova varredura.

Monitoramento e automação

SIEM correlaciona eventos de ferramentas diferentes em um incidente; agregação centralizada de logs evita logs dispersos e apagáveis; arquivamento em armazenamento de baixo custo atende retenção longa; alertas ruidosos de padrão conhecido pedem ajuste da regra com exceções. Automação: tickets automáticos, estado desejado, provisionamento de recursos, detecção de anomalias; SOAR executa playbooks entre ferramentas; integrações via APIs. Riscos: complexidade e ponto único de falha.

Resposta a incidentes e forense

Preparação (papéis e simulação), detecção, contenção (isolar o dispositivo), erradicação (remover persistências e redefinir credenciais), recuperação, lições aprendidas, análise de causa raiz e relatório pós-incidente (PIR). Negociação com atacantes entrou no ciclo do V8. Forense: ordem de volatilidade (RAM antes do disco), bloqueador de escrita com hash do original e da cópia, cadeia de custódia, e-discovery para ordem judicial e metadados do arquivo.

Tecnologias de engano

Honeypot é servidor falso isolado para atrair e estudar atacantes; honeynet é uma rede inteira de iscas; honeyfile é arquivo isca auditado; honeytoken é dado ou credencial isca, como registros fictícios com e-mails monitorados ou conta canário no AD que ninguém usa.

Macetes para memorizar

💡 IDS x IPS

D de Detecta (só olha); P de Previne (está no caminho e bloqueia). N de rede, H de host, W de wireless.

💡 Modelos de acesso

DAC = Dono decide; MAC = Marca (rótulo) manda; RBAC = Role (cargo); regra = vale para todos; horário = relógio.

E-mail

SPF diz QUEM pode enviar, DKIM ASSINA, DMARC diz O QUE FAZER e manda relatório, BIMI mostra o LOGO.

Fases de resposta

Preparar, detectar, conter, erradicar, recuperar, aprender: primeiro isola, depois limpa, depois volta.

Ordem de volatilidade

Colete primeiro o que some primeiro: memória antes do disco, disco antes do backup.

Iscas

Pot = um servidor, net = uma rede, file = um arquivo, token = um dado ou conta.

NetFlow x pcap

NetFlow é a conta telefônica (quem ligou e quanto tempo); pcap é a gravação da conversa.

Tabela de memorização: não confunda

Quando é...	...e quando é
NIDS Sensor passivo que só detecta e alerta, geralmente recebendo cópia do tráfego por SPAN.	**NIPS** Sensor inline que descarta pacotes com assinaturas de exploração.
HIDS com integridade de arquivos Alertar quando binários ou páginas do servidor mudam fora de mudança aprovada.	**HIPS** Bloquear localmente alterações e processos não autorizados, inclusive quando o ataque chega cifrado.
MDM Aparelho corporativo: PIN, criptografia, apps aprovados e apagamento remoto do aparelho inteiro.	**MAM** Aparelho pessoal: proteger só os dados da empresa dentro dos apps, bloquear copiar e colar e apagar só esses dados.
802.1X Porta do switch só libera após autenticação com certificado ou credencial no RADIUS.	**Portal cativo** Hóspedes informam dados e aceitam termos no navegador antes de navegar.
SAML IdP envia ao SaaS asserção XML assinada com identidade e atributos para SSO.	**OAuth 2.0** App de terceiro recebe token com escopo limitado para acessar dados sem conhecer a senha.
NetFlow/IPFIX Quem conversou com quem, por quanto tempo e quantos bytes.	**Captura completa de pacotes (pcap)** O conteúdo exato das conexões suspeitas.
DLP de rede Inspecionar o tráfego que passa pelo proxy ou pela matriz.	**DLP com agente no endpoint** Bloquear cópia para pendrive e vazamentos mesmo quando o notebook não passa pela rede da empresa.

Números que caem

Item	Valor
Peso do domínio na prova	**27% (maior da prova)**
Comprimento mínimo de senha sem MFA no NIST SP 800-63B-4	**15 caracteres**
Porta do LDAP sem cifra	**389**
Porta do SNMP	**UDP 161**
Políticas DMARC	**p=none (observa), p=quarantine, p=reject**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Manter troca de senha a cada 30 dias e regras de composição para seguir o NIST.
Como não cair: O NIST atual quer senha longa, sem composição obrigatória, sem expiração periódica sem indício de comprometimento e com bloqueio de senhas vazadas.

⚠ **Alerta de prova:** Apagar o commit com a chave de nuvem e manter a mesma chave ativa.
Como não cair: Cópias podem já existir; segredo exposto é revogado, rotacionado e tem o uso verificado.

⚠ **Alerta de prova:** Usar degausser comum para sanitizar SSDs, ou formatação rápida.
Como não cair: Desmagnetização não funciona em memória flash e formatação não remove dados; exija purga ou destruição com certificado.

⚠ **Alerta de prova:** Tratar igualmente duas vulnerabilidades com a mesma nota CVSS base.
Como não cair: A nota base ignora o contexto; priorize o ativo exposto à internet e crítico.

⚠ **Alerta de prova:** Manter como médio o achado que, encadeado no pentest, deu administrador do domínio.
Como não cair: Priorize pelo impacto demonstrado na cadeia de exploração, não pela nota isolada.

⚠ **Alerta de prova:** Marcar como falso positivo a vulnerabilidade que não pode ser corrigida agora.
Como não cair: A vulnerabilidade é real; registre exceção com prazo, dono e controles compensatórios.

⚠ **Alerta de prova:** Excluir a regra que gera 2.000 alertas por dia de plantonistas conhecidos.
Como não cair: Ajuste a regra com exceções baseadas na escala; excluir elimina a detecção.

⚠ **Alerta de prova:** Coletar primeiro a imagem do disco do servidor com malware sem arquivo.
Como não cair: Ordem de volatilidade: o que some primeiro (RAM) antes do que persiste (disco).

⚠ **Alerta de prova:** Trocar a community 'public' por outra mais longa no SNMPv2c.
Como não cair: O SNMPv2c continua em texto claro; migre para SNMPv3 com autenticação e privacidade.

⚠ **Alerta de prova:** Achar que SELinux em permissive bloqueou o acesso registrado como AVC denied.
Como não cair: Permissive só registra e permite; quem nega é o enforcing.

⚠ **Alerta de prova:** Escolher reinstalar o notebook como primeira resposta ao ransomware.
Como não cair: Reinstalar é erradicação; cortar a rede do equipamento mantendo só o EDR é contenção, que vem antes.

⚠ **Alerta de prova:** Confundir conta de emergência com honeytoken ou conta de serviço gerenciada.
Como não cair: Conta de emergência é real, para crises; conta canário não é usada por nada e dispara alerta; gMSA executa serviços reais.

⚠ **Alerta de prova:** Achar que DMARC p=none já impede e-mails falsos com o domínio.
Como não cair: p=none só observa e gera relatórios; para barrar falsificações mude para quarantine ou reject.

⚠ **Alerta de prova:** Escolher JIT quando a regra vale para todos por condição (rede interna e status 'Em análise').
Como não cair: Regra central por condição, independentemente do cargo, é controle baseado em regras; JIT é privilégio temporário sob solicitação.

Como cai na prova

📝 **Como cai:** 'Qual controle ou ferramenta atende?' com quatro ferramentas reais de áreas diferentes.
Como resolver: Defina o objeto protegido (porta de rede, host, aparelho, app, nuvem, e-mail) e a ação pedida (detectar, bloquear, gerenciar, descobrir); a alternativa que casa os dois é a resposta.

📝 **Como cai:** Cenário de incidente perguntando a fase ou atividade.
Como resolver: Localize no tempo: antes (preparação, tabletop), durante (contenção, erradicação, negociação), depois (recuperação, lições aprendidas, causa raiz, PIR).

📝 **Como cai:** Política de senhas 'segundo o NIST' com Escolha TRÊS.
Como resolver: Marque comprimento maior, bloqueio de senhas vazadas e não reutilização; elimine troca periódica, composição obrigatória, perguntas e dicas de senha.

📝 **Como cai:** Priorização de vulnerabilidades com notas iguais ou achado encadeado.
Como resolver: Contexto vence a nota base: exposição, criticidade e impacto demonstrado; se não dá para corrigir, exceção com controles compensatórios; depois, nova varredura.

📝 **Como cai:** Combinação de abordagens com agente e sem agente (NAC ou varredura).
Como resolver: Gerenciado ou que sai da rede recebe agente; IoT, impressoras, câmeras e visitantes ficam sem agente; desconfie da alternativa que inverte.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Porta do switch só libera após o RADIUS	**802.1X**
Página falsa capturando senha e OTP em tempo real	**Passkey FIDO2/WebAuthn, vinculada ao domínio**
Medo de ficar trancado fora do locatário se o MFA falhar	**Contas de acesso de emergência (break glass) monitoradas**
Privilégio ativado por solicitação aprovada, com duração máxima (ex.: quatro horas) e remoção automática	**Just-in-time (JIT)**
Quem cadastra não aprova e quem aprova não paga	**Segregação de funções**
Logotipo da marca na caixa de entrada	**BIMI, com DMARC em aplicação**
Visibilidade de quem envia pelo domínio antes de endurecer o DMARC	**Relatórios agregados DMARC (rua)**
Código não pode mudar e chega ' OR 1=1 --	**Regras de WAF como patch virtual**
Banco exposto e contas sem MFA descobertos por acaso na nuvem	**CSPM**
Planilhas de IP, DHCP e DNS com conflitos	**IPAM**
Verificar baseline com XCCDF e OVAL	**SCAP**
Procurar invasores sem alerta, a partir de uma hipótese	**Threat hunting**
Ordem judicial pedindo e-mails e documentos de um período	**E-discovery**
Agente de IA que pode isolar máquinas	**Menor privilégio e aprovação humana em ações críticas**

🎯 Se você lembrar de só uma coisa deste capítulo...

- Contenção vem antes de erradicação; reinstalar é erradicação.
- Memória antes do disco na coleta forense; hash do original e da cópia prova que são idênticos.
- DMARC p=none não bloqueia nada; BIMI exige DMARC em aplicação.
- Segredo vazado se revoga e rotaciona, não basta apagar o commit.
- IA que age sozinha precisa de menor privilégio, guardrails e humano no circuito.

Essenciais para a prova (checklist)

- ☐ Sei diferenciar DAC, MAC, RBAC, baseado em regras e baseado em horário.
- ☐ Sei aplicar JIT, segregação de funções, contas de emergência e revisão de acessos.
- ☐ Sei as recomendações de senha do NIST SP 800-63B-4.
- ☐ Sei quando usar SAML, OAuth, LDAPS, passkey e passwordless.
- ☐ Sei escolher entre NIDS, NIPS, HIDS, HIPS, WIPS, EDR e XDR.
- ☐ Sei a função de SPF, DKIM, DMARC (políticas e rua) e BIMI.
- ☐ Sei diferenciar DLP de rede e de endpoint, CASB, CSPM, IPAM, MDM e MAM.
- ☐ Sei priorizar vulnerabilidades por contexto e tratar exceções.
- ☐ Sei a ordem das fases de resposta a incidentes e da coleta por volatilidade.
- ☐ Sei diferenciar honeypot, honeynet, honeyfile e honeytoken.

Questões de revisão do capítulo

R5.1 · Operações de Segurança

O EDR da Agência Criativa Pixel detectou ransomware começando a cifrar arquivos em um notebook. Antes de qualquer análise, o SOC usou o console para cortar todas as conexões de rede do equipamento, exceto a comunicação com o próprio EDR. Que ação de resposta a incidentes é essa?

A. Erradicação por reinstalação completa do sistema
B. Lições aprendidas com a diretoria
C. Recuperação a partir do backup
D. Contenção por isolamento do dispositivo

R5.2 · Operações de Segurança

No SOC da Rede de Varejo Estrela, cada alerta crítico do SIEM passou a abrir automaticamente um chamado na ferramenta de ITSM, já preenchido com host, usuário e IoCs, atribuído à fila certa e com prazo conforme a severidade. Que caso de uso de automação é esse?

A. Gerenciamento de estado desejado
B. Gerenciamento automatizado de tickets
C. Provisionamento automático de recursos de nuvem
D. Detecção de anomalias por IA

R5.3 · Operações de Segurança

Antes de comprar 300 switches, a Prefeitura de Campo Verde quer reduzir o risco de receber equipamentos falsificados ou adulterados. Qual prática do processo de aquisição é a mais adequada?

A. Comprar de canais autorizados e conferir a integridade
B. Escolher o menor preço em marketplaces abertos
C. Dispensar o inventário dos switches recebidos
D. Instalar os equipamentos antes de conferir a nota fiscal

R5.4 · Operações de Segurança

Uma varredura de segredos executada pela primeira vez nos repositórios da Software House Código Limpo encontrou uma chave de acesso de nuvem válida em um commit de dois anos atrás, já removida do código atual. Qual é a ação correta?

A. Revogar e rotacionar a chave e verificar seu uso
B. Tornar o repositório público para auditoria
C. Manter a chave, pois já saiu da versão atual do código
D. Apagar o commit e manter a mesma chave ativa

Respostas comentadas

R5.1. D) Contenção por isolamento do dispositivo

Por quê: A contenção limita o dano e a propagação; o isolamento ou quarentena de dispositivos pelo EDR corta a comunicação de rede, preservando o canal com o console para coleta e análise.

✗ A) Incorreta. Reinstalar é erradicação e vem depois da contenção.
✗ B) Incorreta. Lições aprendidas são a etapa final.
✗ C) Incorreta. A recuperação ocorre após conter e erradicar.

> **Dica de prova:** Cortar a rede do equipamento infectado: contenção por isolamento.

R5.2. B) Gerenciamento automatizado de tickets

Por quê: Casos de uso de automação em segurança incluem provisionamento de usuários e recursos, estado desejado, detecção de anomalias e gerenciamento de tickets; regras de automação e playbooks do SIEM ou SOAR criam e atualizam chamados com contexto.

✗ A) Incorreta. Estado desejado mantém configurações de servidores.
✗ C) Incorreta. Provisionamento cria infraestrutura, não chamados.
✗ D) Incorreta. Detecção de anomalias identifica desvios, sem abrir chamados.

> **Dica de prova:** Alerta virando chamado preenchido e encaminhado sozinho: gestão automatizada de tickets.

R5.3. A) Comprar de canais autorizados e conferir a integridade

Por quê: A gestão de riscos da cadeia de suprimentos começa na aquisição: fornecedores e revendas autorizados, verificação de integridade e autenticidade na entrega e registro no inventário reduzem riscos de falsificação e adulteração.

✗ B) Incorreta. Marketplaces abertos aumentam o risco de produtos falsificados.
✗ C) Incorreta. Sem inventário, não há rastreabilidade dos ativos recebidos.
✗ D) Incorreta. Instalar sem conferir pode introduzir equipamentos adulterados na rede.

> **Dica de prova:** Compra segura: canal autorizado e verificação na entrega.

R5.4. A) Revogar e rotacionar a chave e verificar seu uso

Por quê: A varredura de segredos inclui o histórico dos repositórios; segredo exposto deve ser considerado comprometido: revogar, rotacionar, investigar o uso e só então limpar o histórico, se necessário.

✗ B) Incorreta. Tornar público aumentaria a exposição.
✗ C) Incorreta. O histórico do repositório continua acessível a quem tem acesso a ele.
✗ D) Incorreta. Apagar o commit não invalida cópias que já possam existir.

> **Dica de prova:** Segredo encontrado no histórico: revogue e rotacione, não basta apagar.

DIA DA PROVA

Estratégia de prova

A SY0-801 tem até 90 questões em 90 minutos, mistura múltipla escolha com questões baseadas em desempenho (PBQ) e aprova com 750 numa escala de 100 a 900; é aplicada em inglês, com lançamento previsto para 17/11/2026. Quase tudo é cenário: o enunciado descreve uma empresa, um log ou uma saída de ferramenta e pede o controle, o ataque ou a etapa 'mais adequada', 'primeira providência' ou 'como se classificam, respectivamente'. As alternativas erradas costumam ser ferramentas e conceitos reais que resolvem outro problema, então vence quem identifica exatamente o objeto e a ação pedidos. Operações de Segurança (27%) e Ameaças, Vulnerabilidades e Ataques (24%) somam mais da metade da prova, e o V8 trouxe IA, identidade moderna e novas superfícies de ataque para o centro.

Como responder

✓ Leia a última frase do enunciado primeiro para saber se pedem tipo, categoria, fase, ferramenta ou cálculo, e só então leia o cenário procurando o detalhe decisivo.

✓ Em 'como se classificam, respectivamente', escreva as duas respostas na ordem do enunciado antes de olhar as alternativas: a versão invertida sempre aparece.

✓ Nas PBQs (logs, saídas de ferramentas, sequências de passos), procure a assinatura técnica (../, UNION SELECT, mesma senha em várias contas, evento 1102, AVC denied) e ignore o ruído do restante.

✓ Em 'Escolha DUAS/TRÊS', avalie cada alternativa como verdadeiro ou falso de forma independente e confira se cada uma atende a uma parte diferente do requisito.

✓ Quando duas alternativas parecerem certas, escolha a que resolve a causa com o menor impacto e dentro do escopo (ajustar a regra em vez de excluí-la; WAF como patch virtual quando o código não pode mudar).

✓ Em cálculos de risco e resiliência, escreva a fórmula (SLE, ARO, ALE, MTTR) antes de calcular; as erradas são construídas com os erros previsíveis.

✓ Administre o tempo: 90 minutos para até 90 itens dá cerca de um minuto por item; não deixe um item longo consumir o tempo dos demais.

✓ Pense nos termos em inglês da prova (fail-open, backout, tailgating, password spraying, legal hold) e associe cada um ao conceito em português que você estudou.

Erros que derrubam candidatos

✗ Escolher uma ferramenta real que resolve outro problema (SIEM para bloquear pacotes, MDM para detectar evil twin, IPAM para auditar nuvem).

✗ Confundir os pares mais cobrados: RTO e RPO, NIDS e NIPS, CRL e OCSP, SLA e SLO, risco inerente e residual, spear phishing e whaling.

✗ Chamar de dia zero uma falha com patch disponível e não aplicado.

✗ Seguir regras antigas de senha (troca periódica, composição obrigatória) em vez das recomendações atuais do NIST.

✗ Pular etapas da resposta a incidentes, como erradicar ou reinstalar antes de conter e preservar evidências.

✗ Errar o cálculo de SLE e ALE usando o valor total do ativo ou invertendo a ARO.

✗ Confiar na rede interna ou em um login anterior em cenários de Zero Trust.

Na semana da prova

- ☐ Refaça as provas simuladas cronometrando 90 minutos e revise cada erro anotando o par de conceitos que você confundiu.
- ☐ Revise os quadros de comparação e os macetes de cada capítulo, com atenção a Operações (27%) e Ameaças (24%).
- ☐ Treine as fórmulas de risco (SLE, ARO, ALE) e de resiliência (MTTR, RTO, RPO) até resolver sem hesitar.
- ☐ Revise os termos novos do V8: IA (injeção de prompt, jailbreak, evasão, envenenamento, agentic), passkeys, contas de emergência, JIT, SSE, gMSA, CSPM, IPAM, BIMI, quishing e deepfake.
- ☐ Revise o vocabulário em inglês dos objetivos oficiais, já que a prova é aplicada em inglês.
- ☐ Na véspera, só revisão leve do 'lembrar' de cada capítulo; durma bem e chegue com folga.

REVISÃO FINAL

Folha de cola

Leia na véspera e na manhã da prova: os gatilhos e as pegadinhas mais importantes de cada domínio.

1. Ameaças, Vulnerabilidades e Ataques

‣ GET com ../../etc/passwd e resposta 200 → **Travessia de diretório (path traversal)**

‣ Aspas e UNION SELECT no parâmetro → **Injeção de SQL**

‣ Mesmo usuário em São Paulo e Frankfurt em minutos → **Viagem impossível**

‣ Evento 1102 logo após login administrativo fora do horário → **Manipulação de logs para ocultar rastros**

‣ Dezenas de notificações push até a vítima aprovar → **Fadiga de MFA**

⚠ Mesma senha em muitas contas é password spraying; stuffing usa pares vazados distintos por conta.

⚠ Se havia patch e ele não foi aplicado, é sistema sem patch; dia zero é explorado antes de existir correção.

⚠ Sem suporte significa que o fabricante não corrige mais; se ele ainda dá suporte, a falha explorada antes do patch é dia zero.

2. Arquitetura de Segurança

‣ Nem o provedor do serviço consegue ler as mensagens → **Criptografia de ponta a ponta**

‣ Dados protegidos na memória durante o processamento, inclusive do administrador do provedor → **Dados em uso, computação confidencial**

‣ Acesso aos consoles por rede separada com conexão celular quando a produção cai → **Gerenciamento fora de banda (out-of-band)**

‣ Mesma falha derrubando firewalls de borda e internos do mesmo fabricante → **Diversidade de fornecedores e tecnologias**

‣ Conta de serviço em vários servidores sem senha manual → **gMSA**

⚠ Com backup às 22h e sem replicação, a perda pode chegar a quase 24 horas; limite de perda é RPO, não RTO.

⚠ MTTR é a média: horas de reparo divididas pelo número de falhas, ou seja, 3 horas.

⚠ Multicloud reduz a dependência de um fornecedor; o desafio que cresce é manter políticas e controles consistentes.

3. Conceitos Gerais de Segurança

‣ Revisão de logs, alertas no SIEM, sem impedir a ação → **Controle detectivo**

‣ Não dá para aplicar o controle ideal e se usa outro no lugar → **Controle compensatório**

‣ Norma ou política dizendo o que os funcionários devem fazer → **Controle diretivo**

‣ Quem fez a alteração, quando e de qual estação → **Contabilização (accounting) do AAA**

‣ Um componente decide e outro, no caminho do tráfego, aplica → **PDP e PEP, nessa ordem**

⚠ Zero Trust avalia cada recurso e sessão de novo, com identidade, dispositivo e contexto; não existe confiança por localização nem por login anterior.

⚠ A CSR leva só a chave pública e os dados de identificação; a chave privada nunca é enviada à AC nem a terceiros.

⚠ A cifra pode ser igual, mas o navegador não confia em quem assinou e mostra alerta; site público usa certificado de AC pública confiável.

4. Gestão e Supervisão do Programa de Segurança

‣ Escopo, IPs permitidos e proibidos, horários e contatos de emergência do pentest → **Regras de engajamento (RoE)**

‣ Documento que dá autoridade e independência à auditoria interna → **Carta de auditoria (audit charter)**

‣ Comparar controles atuais com a norma antes do projeto → **Análise de lacunas (gap analysis)**

‣ Processo judicial e nada pode ser apagado, nem pela retenção automática → **Retenção legal (legal hold)**

‣ Relatório SOC 2 Tipo II e questionário do fornecedor → **Avaliação do fornecedor com atestação**

⚠ SLE aplica o fator de exposição: 60% de R$ 300.000 = R$ 180.000 por evento.

⚠ ALE = SLE x ARO uma vez só: R$ 80.000 x 0,2 = R$ 16.000 por ano.

⚠ ARO = 1/N: um evento a cada quatro anos é 0,25 por ano.

5. Operações de Segurança

‣ Porta do switch só libera após o RADIUS → **802.1X**

‣ Página falsa capturando senha e OTP em tempo real → **Passkey FIDO2/WebAuthn, vinculada ao domínio**

‣ Medo de ficar trancado fora do locatário se o MFA falhar → **Contas de acesso de emergência (break glass) monitoradas**

▸ Privilégio ativado por solicitação aprovada, com duração máxima (ex.: quatro horas) e remoção automática → **Just-in-time (JIT)**

▸ Quem cadastra não aprova e quem aprova não paga → **Segregação de funções**

⚠ O NIST atual quer senha longa, sem composição obrigatória, sem expiração periódica sem indício de comprometimento e com bloqueio de senhas vazadas.

⚠ Cópias podem já existir; segredo exposto é revogado, rotacionado e tem o uso verificado.

⚠ Desmagnetização não funciona em memória flash e formatação não remove dados; exija purga ou destruição com certificado.

GABARITO

Respostas do diagnóstico

D1. C) Perda de dados pela saída do modelo → revise o capítulo 1

Por quê: Modelos com acesso a dados sensíveis podem expô-los nas respostas; controles de acesso aplicados também às fontes consultadas pela IA, filtragem de saída e menor privilégio evitam essa perda de dados.

✗ A) Incorreta. O laudo era real, não inventado.
✗ B) Incorreta. Não houve resultado discriminatório.
✗ D) Incorreta. A base não foi adulterada.

> **Dica de prova:** IA devolvendo dado real de outra pessoa: perda de dados pela saída.

D2. A) Worm autopropagável → revise o capítulo 1

Por quê: Worms são malwares autopropagáveis que exploram vulnerabilidades de rede para infectar outros sistemas sem ação do usuário; patches, segmentação e bloqueio de serviços expostos contêm a propagação.

✗ B) Incorreta. Adware exibe anúncios e não se espalha por SMB.
✗ C) Incorreta. Trojans dependem de o usuário executar o programa disfarçado.
✗ D) Incorreta. Spyware coleta dados discretamente, sem propagação automática.

> **Dica de prova:** Espalha sozinho pela rede, sem clique: worm.

D3. D) Patrocinado por Estado, com motivação de influência → revise o capítulo 1

Por quê: Atores estatais conduzem, além de espionagem, operações de influência, combinando vazamentos, desinformação e redes de contas falsas para afetar a opinião pública e processos democráticos.

✗ A) Incorreta. Não há ganho financeiro direto.
✗ B) Incorreta. A campanha é coordenada e com recursos, não curiosidade.
✗ C) Incorreta. Não há disputa comercial nem roubo de segredos de negócio.

> **Dica de prova:** Governo estrangeiro tentando mudar a opinião do eleitorado: Estado com motivação de influência.

D4. A) Nuvem pública multilocatária → revise o capítulo 2

Por quê: Na nuvem pública, a infraestrutura é provisionada para uso aberto pelo público em geral e pertence a um provedor; os clientes compartilham recursos com isolamento lógico, o que torna configurações e identidades pontos críticos.

✗ B) Incorreta. A startup não opera a própria infraestrutura.
✗ C) Incorreta. A nuvem comunitária atende um grupo restrito com requisitos comuns.
✗ D) Incorreta. A nuvem privada é exclusiva de uma organização.

> **Dica de prova:** Muitos clientes na mesma infraestrutura do provedor: nuvem pública.

D5. D) Segmentação lógica por VLANs → revise o capítulo 2

Por quê: A segmentação lógica usa VLANs, sub-redes e ACLs para separar redes sobre a mesma infraestrutura física; o tráfego entre segmentos passa por roteamento e regras de firewall.

✗ A) Incorreta. Air gap eliminaria a comunicação controlada pelo firewall que a escola quer manter.
✗ B) Incorreta. Rede plana não separa os grupos.
✗ C) Incorreta. A segmentação física exigiria equipamentos e cabeamento novos.

> **Dica de prova:** Separar redes no mesmo switch: VLAN (segmentação lógica).

D6. D) Acúmulo de privilégios (privilege creep) → revise o capítulo 2

Por quê: Privilege creep é o acúmulo gradual de permissões desnecessárias quando usuários mudam de função sem que os acessos antigos sejam removidos; revisões periódicas de acesso e o RBAC combatem o problema.

✗ A) Incorreta. Não há segredo embutido em código no cenário.
✗ B) Incorreta. Federação trata de confiança entre provedores de identidade.
✗ C) Incorreta. Escalonamento por exploit explora falhas técnicas, e aqui os acessos foram concedidos.

> **Dica de prova:** Mudou de área e levou os acessos antigos junto: privilege creep.

D7. D) Menor privilégio → revise o capítulo 3

Por quê: O princípio do menor privilégio determina que cada usuário ou processo tenha apenas as permissões necessárias para executar suas tarefas, reduzindo o impacto de erros e de contas comprometidas.

✗ A) Incorreta. Defesa em profundidade trata de camadas de controles, não da amplitude de uma permissão.
✗ B) Incorreta. Separação de funções divide etapas críticas entre pessoas diferentes, o que não está em questão.
✗ C) Incorreta. Não repúdio garante que ações não sejam negadas, sem relação com o excesso de acesso.

> **Dica de prova:** Acesso além do necessário para a função: viola o menor privilégio.

D8. A) Comitê consultivo de mudanças (CAB) → revise o capítulo 3

Por quê: Na gestão de mudanças, o comitê consultivo de mudanças (CAB), chamado pelo NIST de configuration control board, reúne as partes interessadas para avaliar e aprovar mudanças antes da implementação.

✗ B) Incorreta. O SOC monitora e responde a eventos de segurança, sem papel de aprovação de mudanças.
✗ C) Incorreta. O comitê de auditoria supervisiona controles e auditorias, não mudanças operacionais.
✗ D) Incorreta. O CSIRT responde a incidentes; não aprova mudanças planejadas.

> **Dica de prova:** Grupo que aprova mudanças antes da execução: CAB.

D9. B) A chave pública e os dados que identificam o servidor → revise o capítulo 3

Por quê: A CSR contém a chave pública e os dados de identificação do requerente, assinados com a chave privada correspondente para provar a posse; a AC valida o pedido e devolve o certificado assinado.

✗ A) Incorreta. O certificado raiz pertence à AC e a chave privada não sai do servidor.
✗ C) Incorreta. Mesmo cifrada, a chave privada não faz parte da CSR.
✗ D) Incorreta. A chave privada nunca deve ser enviada à AC nem a terceiros.

> **Dica de prova:** CSR = chave pública + identidade; chave privada fica em casa.

D10. A) Geografia e jurisdição do fornecedor → revise o capítulo 4

Por quê: Geografia e jurisdição limitam a escolha de terceiros: leis locais podem permitir acesso de autoridades aos dados, e normas como a LGPD exigem condições específicas para transferências internacionais.

✗ B) Incorreta. A limitação descrita não é de pessoal.
✗ C) Incorreta. Lock-in trata da dificuldade de trocar de fornecedor.
✗ D) Incorreta. O retorno financeiro não é o ponto do cenário.

> **Dica de prova:** Fornecedor em outro país e leis diferentes: limitação de jurisdição.

D11. D) Regras de engajamento (RoE) → revise o capítulo 4

Por quê: As regras de engajamento documentam o que pode e o que não pode ser feito em um teste: escopo, alvos, técnicas, janelas de horário, tratamento de dados e contatos para emergências, protegendo as duas partes.

✗ A) Incorreta. A AUP regula o uso de recursos pelos funcionários.
✗ B) Incorreta. O plano de continuidade trata da manutenção das operações em crises.
✗ C) Incorreta. O SLA trata de metas de serviço.

> **Dica de prova:** Escopo, limites e contatos do pentest: regras de engajamento.

D12. C) Carta de auditoria → revise o capítulo 4

Por quê: No escopo de auditorias, a carta de auditoria (audit charter), aprovada pelo conselho, estabelece propósito, autoridade, independência e linhas de reporte da função de auditoria interna, como preveem as normas globais do IIA.

✗ A) Incorreta. A SOW detalha um trabalho contratado.
✗ B) Incorreta. A AUP regula o uso de recursos de TI.
✗ D) Incorreta. O plano de resposta trata de incidentes.

> **Dica de prova:** Documento que dá autoridade e escopo à auditoria interna: audit charter.

Agora, treine no formato real

Faça as 6 provas completas do curso CompTIA Security+ SY0-801: 540 questões inéditas, tempo do exame, explicação de cada alternativa e link da documentação para revisar.

Ver as 6 provas completas e o cupom do mês →

Até o dia da prova, uma revisão por dia no seu feed

Instagram @strecht.simulados

Um post de prova por dia: questão comentada, pegadinhas e o "não confunda" de cada certificação.

Seguir no Instagram →

YouTube Strecht Simulados

Shorts diários com pegadinhas de prova e, aos sábados, um simulado comentado.

Inscrever-se no canal →

Material independente de preparação, sem afiliação ou endosso de CompTIA. As questões são inéditas e não reproduzem a prova real.