Strecht Simulados · Guia de preparação



Guia de preparação CompTIA Security+ SY0-701

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+ SY0-701: 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 Mitigações	22%	16 conceitos · 14 pegadinhas
2. Arquitetura de Segurança	18%	18 conceitos · 14 pegadinhas
3. Conceitos Gerais de Segurança	12%	17 conceitos · 13 pegadinhas
4. Gestão e Supervisão do Programa de Segurança	20%	18 conceitos · 14 pegadinhas
5. Operações de Segurança	28%	18 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 Mitigações

Um atacante explora uma falha no hipervisor para sair de uma máquina virtual e acessar outras VMs do mesmo host. Que vulnerabilidade é essa?

A. Escape de máquina virtual
B. Reutilização de recursos
C. Injeção de SQL em aplicação
D. Configuração de nuvem incorreta

D2 · Ameaças, Vulnerabilidades e Mitigações

Um roteador de filial ainda usa usuário e senha de fábrica e está acessível pela Internet. Qual vulnerabilidade existe?

A. Criptografia de disco desativada
B. Firmware com assinatura válida
C. Falta de backup de configuração
D. Credenciais padrão não alteradas

D3 · Ameaças, Vulnerabilidades e Mitigações

Um atacante altera a tabela ARP da rede local para receber o tráfego destinado ao gateway. Que ataque é esse?

A. Envenenamento de ARP
B. Bomba lógica agendada
C. Clonagem de crachá RFID
D. Colisão de hash MD5

D4 · Arquitetura de Segurança

A empresa testa o plano de continuidade reunindo os responsáveis numa sala para discutir, passo a passo, como reagiriam a um desastre, sem acionar sistemas. Que teste é esse?

A. Teste de penetração externo
B. Teste de failover completo
C. Simulação com troca de site
D. Exercício de mesa (tabletop)

D5 · Arquitetura de Segurança

A empresa publica um servidor web para a Internet, mas quer mantê-lo separado da rede interna. Onde o servidor deve ficar?

A. Na mesma rede dos computadores internos
B. Na rede de gerenciamento dos switches
C. Em uma zona desmilitarizada (DMZ)
D. Em uma estação de trabalho de usuário

D6 · Arquitetura de Segurança

Administradores acessam servidores de uma rede isolada apenas por meio de um servidor intermediário reforçado e monitorado. Qual é esse servidor?

A. Servidor de impressão
B. Servidor de e-mail
C. Jump server
D. Servidor DHCP

D7 · Conceitos Gerais de Segurança

Qual princípio da segurança diz que o sistema deve confirmar que a informação não foi alterada de forma não autorizada?

A. Integridade da informação
B. Disponibilidade do serviço
C. Confidencialidade dos dados
D. Autorização de usuários

D8 · Conceitos Gerais de Segurança

Uma aplicação de blockchain registra transações em um livro distribuído, e cada bloco contém o hash do anterior. Qual propriedade isso reforça?

A. Disponibilidade sem internet
B. Integridade do histórico
C. Confidencialidade total dos dados
D. Velocidade de processamento

D9 · Conceitos Gerais de Segurança

Uma equipe aplica uma mudança sem autorização para corrigir um problema urgente e só registra depois. Qual risco isso traz para a organização?

A. Aumento da segurança do ambiente
B. Melhoria automática da documentação
C. Redução do número de incidentes
D. Mudanças sem análise de impacto

D10 · Gestão e Supervisão do Programa de Segurança

Qual documento define, de forma obrigatória e de alto nível, as regras de uso aceitável dos recursos de TI pelos funcionários?

A. Guia de boas práticas opcional
B. Procedimento de backup
C. Acordo de nível de serviço
D. Política de uso aceitável (AUP)

D11 · Gestão e Supervisão do Programa de Segurança

Um funcionário nota que um colega fotografa telas com dados de clientes fora do horário. Segundo o treinamento, o que ele deve reconhecer?

A. Comportamento normal de trabalho
B. Problema de desempenho de rede
C. Falha de hardware da estação
D. Comportamento anômalo de risco

D12 · Gestão e Supervisão do Programa de Segurança

Novos funcionários recebem o manual de segurança e assinam um termo dizendo que leram e entenderam as políticas. Qual é o objetivo da assinatura?

A. Dispensar o monitoramento de acessos
B. Registrar o reconhecimento das políticas
C. Substituir o treinamento de segurança
D. Garantir que nunca haverá incidentes

01

CAPÍTULO 1 · 22% DA PROVA

Ameaças, Vulnerabilidades e Mitigações

Aqui o jogo é reconhecer o ataque pelo sintoma descrito: ator de ameaça e motivação, vetor (mensagem, imagem, arquivo, voz, mídia removível, cadeia de suprimentos), tipo de malware, ataque de senha, de aplicação, de rede, criptográfico, sem fio ou físico, e os indicadores de comprometimento. Depois vem a mitigação certa: segmentação, isolamento, allow list, patch, controle compensatório, hardening e menor privilégio. O enunciado quase sempre traz uma pista literal ('../', ' OR '1'='1', 'dois países em minutos'). Onde mais erro: XSS x CSRF, spraying x força bruta x credential stuffing, escalada de privilégios x movimentação lateral, e confundir hacktivista com estado-nação.

Neste capítulo

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

Tópicos-chave

Atores de ameaça

Estado-nação: muitos recursos, alta sofisticação, APT silenciosa e persistente por meses. Crime organizado: estrutura profissional e foco em lucro (ransomware, venda de dados de cartão). Hacktivista: motivação ideológica e busca de visibilidade. Ameaça interna: acesso legítimo e conhecimento dos processos, inclusive terceirizados com acesso às instalações. Atacante pouco sofisticado: usa ferramentas prontas. Shadow IT: serviço contratado sem aprovação da TI.

Motivações

Ganho financeiro, chantagem (pagar ou vazar), espionagem corporativa ou estatal, disrupção de serviços essenciais, crença ideológica ou filosófica, vingança (funcionário descontente), guerra e exfiltração. Erro acidental não tem intenção.

Vetores de ameaça

Mensagem (e-mail, SMS, mensageria instantânea), imagem (incluindo QR code falso), arquivo (PDF que explora o leitor), voz (vishing, deepfake de áudio), mídia removível (pendrive largado), software vulnerável, porta de serviço aberta, credencial padrão, redes sem fio e Bluetooth inseguros, e cadeia de suprimentos (fornecedores, MSP com acesso VPN, bibliotecas).

Engenharia social

Phishing (e-mail), spear phishing (pessoa específica), whaling (alto executivo), vishing (voz), smishing (SMS), pretexting (história falsa, como recrutador falso), personificação, tailgating, watering hole (contamina site frequentado pelo alvo) e typosquatting (domínio com erro de digitação). Defesas: treinamento, filtros, SPF, DKIM, DMARC, MFA e verificação de identidade por procedimento no suporte.

Malware

Ransomware cifra e pede resgate. Worm se espalha sozinho explorando serviço. Trojan se disfarça de programa legítimo; RAT dá controle remoto. Keylogger registra digitação. Bomba lógica dispara por condição ou data. Rootkit esconde o invasor. Spyware coleta dados ocultamente. Adware/PUP troca página inicial e mostra propaganda. Cryptojacking minera com CPU alta. Injeção de memória (fileless) roda no processo legítimo sem gravar em disco.

Ataques de senha

Password spraying: poucas senhas comuns em muitas contas, para fugir do bloqueio. Força bruta online: muitas senhas na mesma conta. Força bruta offline: milhões de tentativas contra o hash roubado, sem gerar bloqueio. Credential stuffing: senhas vazadas de outro site. Defesas: MFA, bloqueio após falhas, limitação de taxa, senhas fortes, proibição de reutilização e hash lento com salt.

Injeções e falhas de aplicação

SQLi: entrada concatenada vira parte da consulta (' OR '1'='1); consultas parametrizadas evitam. Injeção de comando: entrada executa comandos do SO. Travessia de diretório: '../' lê arquivos do servidor. Estouro de buffer: grava além da memória reservada; mitigam ASLR, DEP e linguagens seguras. Condição de corrida TOC/TOU: troca entre checar e usar.

XSS, CSRF, SSRF e IDOR

XSS executa script no navegador da vítima: armazenado (persiste no servidor, como comentário de fórum), refletido (volta na resposta do link) ou baseado em DOM; evita-se com validação de entrada e codificação de saída. CSRF faz o navegador do usuário logado executar ação sem ele perceber; mitigam tokens anti-CSRF e cookies SameSite. SSRF faz o servidor buscar endereços internos, como o serviço de metadados da nuvem. IDOR: trocar o ID na URL mostra dados de outro cliente (falha de autorização).

Ataques de rede

On-path (man-in-the-middle) lê e altera o tráfego; certificado falso com alerta ignorado é on-path com interceptação de TLS (HSTS ajuda). Envenenamento de ARP desvia o tráfego do gateway na rede local. Envenenamento ou sequestro de DNS aponta o domínio para servidor falso (DNSSEC ajuda). Túnel DNS usa consultas longas e frequentes para C2 e exfiltração. Replay reenvia token capturado (nonces, carimbos de tempo e tokens curtos mitigam). Pass-the-hash usa o hash como senha.

Negação de serviço

DDoS com botnet (milhares de IoT infectados) derruba o serviço; mitigam serviços anti-DDoS e CDN. Amplificação: consultas com origem falsificada da vítima geram respostas grandes contra ela. DoS de aplicação (Slowloris): requisições HTTP lentas e incompletas esgotam conexões; limites e proxies reversos ajudam.

Ataques criptográficos

Colisão: duas mensagens diferentes com o mesmo hash permitem falsificar assinatura (MD5 é fraco). Paradoxo do aniversário explica por que colisões em hashes curtos são mais fáceis do que parecem. Downgrade força versão antiga e fraca do protocolo; desativar versões antigas evita. Algoritmo quebrado, como DES, é vulnerabilidade criptográfica e se resolve trocando por AES.

Ataques sem fio e físicos

Evil twin: AP falso com o mesmo nome da rede corporativa. Rogue AP: roteador não autorizado ligado à rede (funcionário com roteador pessoal); NAC e varreduras sem fio detectam. Desautenticação derruba clientes para forçar reconexão; WPA3 e 802.11w mitigam. Físicos: clonagem de crachá RFID, força bruta física e ataque ambiental (climatização do datacenter).

Vulnerabilidades por categoria

SO desatualizado, web (drive-by por navegador desatualizado), hardware (firmware não atualizado, fim de vida, legado sem suporte), virtualização (VM escape; reutilização de recursos, como disco liberado a outro cliente sem limpeza), nuvem (configuração incorreta, como regra aberta ou listagem de diretórios), móvel (sideloading, jailbreak, permissões excessivas, token em texto puro), dia zero (sem correção), segredos no código e atualização aceita sem verificar assinatura.

Indicadores de comprometimento

Viagem impossível (logins em dois países em minutos), sessões simultâneas em locais diferentes, bloqueios de conta em massa (spraying ou força bruta), logs ausentes ou lacunas (apagamento), consumo anormal de recursos e conteúdo bloqueado de forma anormal (lista alterada por conta não autorizada). Conta de serviço acessando dezenas de máquinas de madrugada indica movimentação lateral.

Escalada de privilégios x movimentação lateral

Escalada é ganhar mais permissões: vertical (usuário comum vira administrador) ou horizontal (outras contas). Movimentação lateral é ir para outros sistemas da rede, por exemplo usando credenciais armazenadas na estação comprometida para entrar no servidor de arquivos.

Técnicas de mitigação

Segmentação com controle de acesso e isolamento limitam a movimentação lateral. Allow list de aplicativos bloqueia por padrão o que não foi aprovado. Patch do fabricante ou, até corrigir, controle compensatório (WAF para aplicação web, isolamento para legado). Hardening: patches, troca de senhas padrão, EDR, firewall de host e desativar o desnecessário. Menor privilégio dá só o acesso necessário. Descomissionamento seguro remove acessos e sanitiza discos.

Macetes para memorizar

💡 Canais de phishing

Phishing = e-mail; Smishing = SMS; Vishing = voz (Voice); Whaling = baleia, o executivo grande.

💡 XSS x CSRF x SSRF

XSS: script no navegador da vítima. CSRF: o navegador logado faz a ação. SSRF: o Servidor faz a requisição interna.

💡 Escalada x lateral

Escalada sobe de nível; lateral anda para o lado, para outro sistema.

💡 Atores

Estado: dinheiro e paciência. Crime: lucro. Hacktivista: causa e holofote. Insider: tem crachá.

💡 Worm x vírus

Worm anda sozinho; vírus precisa de hospedeiro e de ação do usuário.

💡 Ataques de senha

Spraying = uma senha, muitas contas. Força bruta = muitas senhas, uma conta. Stuffing = senha vazada reaproveitada. Offline = contra o hash, sem bloqueio.

Tabela de memorização: não confunda

Quando é...	...e quando é
XSS Script injetado roda no navegador de quem abre a página ou clica no link.	**CSRF** Link faz o navegador do usuário já logado enviar uma ação (como transferência) sem ele perceber.
Password spraying Mesma senha comum testada em muitas contas, poucas tentativas por conta.	**Força bruta em uma conta** Muitas senhas testadas na mesma conta.
Worm Se espalha sozinho pela rede explorando falha de serviço, sem o usuário abrir nada.	**Trojan** Se disfarça de programa legítimo e depende de o usuário instalar; o RAT dá controle remoto.
Spear phishing E-mail direcionado a uma pessoa específica.	**Whaling** E-mail direcionado a alto executivo, como o diretor financeiro.
Escalada de privilégios Usuário comum passa a executar comandos como administrador no mesmo sistema.	**Movimentação lateral** Atacante usa credenciais obtidas para acessar outros sistemas da rede.
Evil twin AP falso, do atacante, com o mesmo nome da rede corporativa para capturar conexões.	**Rogue AP** AP não autorizado conectado à rede interna, como o roteador pessoal de um funcionário.
Hacktivista Motivação ideológica, ação visível (protesto, interromper serviço por causa).	**Estado-nação** Financiado por governo, muitos recursos, acesso silencioso e persistente por meses.

Números que caem

Item	Valor
Peso do domínio no exame	**22%**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Chamar de 'ataque de dicionário offline' as milhares de tentativas de login com a mesma senha em contas diferentes.
Como não cair: Ataque offline não gera tentativas de login no sistema. Mesma senha em muitas contas é password spraying.

⚠ **Alerta de prova:** Marcar 'força bruta com todas as combinações' quando o atacante usa senhas vazadas de outro site.
Como não cair: Reaproveitar senhas vazadas é credential stuffing; MFA e proibição de reutilização mitigam.

⚠ **Alerta de prova:** Confundir typosquatting com envenenamento de DNS.
Como não cair: Typosquatting registra domínio parecido e espera o erro de digitação. Envenenamento altera as respostas de resolução de nomes.

⚠ **Alerta de prova:** Marcar pharming ou smishing quando há AP falso com o mesmo nome da rede.
Como não cair: Pharming redireciona pelo DNS. Wi-Fi falso com o mesmo SSID é evil twin.

⚠ **Alerta de prova:** Confundir reutilização de recursos com VM escape.
Como não cair: VM escape sai da VM pelo hipervisor e chega a outras VMs. Reutilização de recursos expõe dados deixados em disco ou memória realocados a outro cliente.

⚠ **Alerta de prova:** Chamar de 'criptografia fraca' a falha explorada que ainda não tem correção.
Como não cair: Sem correção disponível é dia zero. Criptografia fraca tem correção pela troca de algoritmo.

⚠ **Alerta de prova:** Classificar atualização maliciosa vinda do repositório ou servidor oficial como engenharia social ou configuração incorreta.
Como não cair: Componente confiável comprometido é ataque à cadeia de suprimentos.

⚠ **Alerta de prova:** Classificar o terceirizado de limpeza que fotografa senhas como ator externo.
Como não cair: Terceiros com acesso às instalações ou sistemas são ameaça interna.

⚠ **Alerta de prova:** Atribuir ao hacktivista a campanha silenciosa de meses financiada por governo.
Como não cair: Hacktivista costuma agir de forma visível por uma causa. Recursos de governo e persistência apontam estado-nação.

⚠ **Alerta de prova:** Marcar rootkit ou spyware quando os arquivos ganharam nova extensão e surgiu pedido de pagamento.
Como não cair: Arquivos inacessíveis com pedido de resgate é ransomware. Rootkit esconde; spyware coleta.

⚠ **Alerta de prova:** Achar que mensagens de erro diferentes ('usuário não existe' x 'senha incorreta') só deixam o login mais claro.
Como não cair: Elas permitem enumerar usuários. Use mensagens genéricas.

⚠ **Alerta de prova:** Confundir envenenamento de cache DNS com amplificação.
Como não cair: Amplificação usa origem falsificada para fazer respostas grandes inundarem a vítima. Envenenamento altera respostas armazenadas.

⚠ **Alerta de prova:** Para conter estação comprometida, desativar o EDR 'para investigar melhor' ou remover regras do firewall interno.
Como não cair: Isso reduz a proteção. Isole em quarentena e segmente a rede por função.

⚠ **Alerta de prova:** Tratar consultas DNS longas e frequentes para domínio estranho como tráfego normal ou NTP.
Como não cair: Esse padrão indica túnel DNS para exfiltração ou C2.

Como cai na prova

📝 **Como cai:** Sintoma técnico descrito em uma frase pede o nome do ataque.
Como resolver: Procure a pista literal (caminho com '../', aspas na consulta, ID trocado, consulta DNS longa, SSID igual) e associe ao ataque. Elimine alternativas de outra camada (física, sem fio, criptográfica).

📝 **Como cai:** Perfil e objetivo do atacante pedem ator ou motivação.
Como resolver: Veja recursos (governo = estado-nação), objetivo (lucro = crime; causa = hacktivista; prejudicar a empresa por ressentimento = vingança) e acesso (legítimo = ameaça interna).

📝 **Como cai:** Sistema que não pode ser corrigido agora pede mitigação.
Como resolver: Escolha isolar ou segmentar, controle compensatório (WAF, monitoramento) e menor privilégio. Descarte expor na Internet, dar admin a todos, desligar firewall ou logs.

📝 **Como cai:** Indicadores em logs pedem o que está ocorrendo.
Como resolver: Dois países em minutos = viagem impossível; dois logins ao mesmo tempo = sessões simultâneas; bloqueios em massa = ataque de senha; lacuna = logs apagados; conta de serviço em muitas máquinas = movimentação lateral.

📝 **Como cai:** 'Escolha DUAS' de mitigação.
Como resolver: As duas certas costumam ser uma técnica e uma humana ou duas técnicas complementares (MFA e bloqueio; isolar e segmentar; patch e compensatório). As erradas aumentam a exposição.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Login em outro país minutos depois de login no Brasil	**Viagem impossível**
'../../etc/passwd' na URL	**Travessia de diretório**
' OR '1'='1 no campo de login	**Injeção de SQL**
Servidor web busca o serviço de metadados da nuvem	**SSRF**
Trocar o número do ID na URL mostra outro cliente	**IDOR / falha de autorização**
Arquivo trocado entre a verificação de permissão e a abertura	**Condição de corrida TOC/TOU**
Mesma senha comum em muitas contas, poucas tentativas por conta	**Password spraying**
CPU em 100% e comunicação com servidores de criptomoeda	**Cryptojacking**
Ex-administrador deixou código que apaga o banco se ele sair da folha	**Bomba lógica**
Pendrives com logotipo da empresa no estacionamento	**Vetor de mídia removível (baiting)**
QR code colado sobre o original	**Vetor baseado em imagem (quishing)**
Intervalo de duas horas sem nenhum evento nos logs	**Logs apagados por invasor**
Requisições HTTP lentas e incompletas esgotando conexões	**DoS de aplicação (Slowloris)**
Site do setor muito visitado pelos funcionários do alvo é contaminado	**Watering hole**

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

- Spraying, força bruta, stuffing e offline se diferenciam por quantas senhas, quantas contas e onde o teste ocorre.
- XSS roda no navegador da vítima; CSRF abusa da sessão logada; SSRF usa o servidor.
- Terceirizado com acesso às instalações é ameaça interna.
- Sistema sem patch: isolar, segmentar e aplicar controle compensatório.
- Viagem impossível, sessões simultâneas, bloqueios em massa e logs ausentes são indicadores de comprometimento.

Essenciais para a prova (checklist)

- ☐ Sei diferenciar estado-nação, crime organizado, hacktivista, ameaça interna e atacante pouco sofisticado.
- ☐ Sei associar cada vetor (mensagem, imagem, arquivo, voz, mídia removível, cadeia de suprimentos) a um cenário.
- ☐ Sei diferenciar phishing, spear phishing, whaling, vishing, smishing, pretexting e watering hole.
- ☐ Sei identificar ransomware, worm, trojan/RAT, keylogger, bomba lógica, rootkit, adware e cryptojacking.
- ☐ Sei diferenciar spraying, força bruta online e offline e credential stuffing.
- ☐ Sei reconhecer SQLi, XSS, CSRF, SSRF, IDOR, travessia de diretório, buffer overflow e TOC/TOU.
- ☐ Sei reconhecer on-path, ARP poisoning, DNS poisoning, túnel DNS, replay, pass-the-hash e downgrade.
- ☐ Sei diferenciar evil twin, rogue AP e desautenticação.
- ☐ Sei listar os indicadores de comprometimento.
- ☐ Sei escolher a mitigação para sistema legado, aplicação web sem patch e estação comprometida.

Questões de revisão do capítulo

R1.1 · Ameaças, Vulnerabilidades e Mitigações

Um atacante compromete um site de notícias do setor financeiro, muito visitado pelos funcionários de um banco, para infectar quem o acessa. Que ataque é esse?

A. Ataque de força bruta
B. Ataque watering hole
C. Ataque de negação de serviço
D. Ataque de pass-the-hash

R1.2 · Ameaças, Vulnerabilidades e Mitigações

Um atacante envia muitas requisições de consulta DNS com o endereço de origem falsificado da vítima, para que as respostas grandes sobrecarreguem a vítima. Que ataque é esse?

A. Sequestro de domínio
B. Envenenamento de cache DNS
C. Tunelamento por DNS
D. DDoS por amplificação

R1.3 · Ameaças, Vulnerabilidades e Mitigações

Um atacante captura o token de autenticação de um usuário e o reenvia depois para acessar o sistema como se fosse ele. Que ataque é esse?

A. Ataque de DDoS
B. Ataque de dicionário
C. Ataque de aniversário
D. Ataque de replay

R1.4 · Ameaças, Vulnerabilidades e Mitigações

Um aplicativo web mostra a mensagem 'usuário não existe' ou 'senha incorreta' conforme o caso. Que problema isso causa?

A. Permite enumerar os usuários existentes
B. Bloqueia ataques de força bruta sozinho
C. Acelera o login de usuários legítimos
D. Criptografa as senhas durante o envio

Respostas comentadas

R1.1. B) Ataque watering hole

Por quê: No watering hole, o atacante contamina um recurso que o grupo-alvo costuma usar.

✗ A) Incorreta. Testa muitas senhas.
✗ C) Incorreta. Busca indisponibilizar um serviço.
✗ D) Incorreta. Reutiliza hashes de senha capturados.

> **Dica de prova:** Site frequentado pelo alvo: watering hole.

R1.2. D) DDoS por amplificação

Por quê: Ataques de amplificação refletem tráfego ampliado para a vítima a partir de serviços abertos.

✗ A) Incorreta. Toma o controle do registro do domínio.
✗ B) Incorreta. Altera respostas armazenadas.
✗ C) Incorreta. Esconde dados em consultas DNS.

> **Dica de prova:** Resposta maior que a consulta: amplificação.

R1.3. D) Ataque de replay

Por quê: Nonces, carimbos de tempo e tokens de curta duração mitigam ataques de replay.

✗ A) Incorreta. Busca derrubar o serviço.
✗ B) Incorreta. Testa senhas de uma lista.
✗ C) Incorreta. Busca colisões de hash.

> **Dica de prova:** Reenviar credencial capturada: replay.

R1.4. A) Permite enumerar os usuários existentes

Por quê: Mensagens de erro genéricas evitam a enumeração de contas.

✗ B) Incorreta. Não tem esse efeito.

✗ C) Incorreta. Não é um problema de segurança.

✗ D) Incorreta. Não tem relação com a mensagem.

Dica de prova: Erro diferente por caso: enumeração de usuários.

02

CAPÍTULO 2 · 18% DA PROVA

Arquitetura de Segurança

Neste domínio eu preciso escolher a peça certa da arquitetura para cada cenário: tipo de firewall (camada 4, NGFW, WAF, UTM), posicionamento (DMZ, jump server, IDS passivo ou IPS em linha), modos de falha, VPN, zero trust, SASE e CASB, e o modelo de responsabilidade compartilhada na nuvem. Também caem muito resiliência e recuperação (sites quente, morno e frio, tipos de backup, RAID, UPS e gerador, testes de continuidade) e proteção de dados (estados dos dados, hash, tokenização, mascaramento, soberania). O enunciado costuma trazer um requisito ('voltar em minutos', 'mostrar só os quatro últimos dígitos') e pede a solução que atende exatamente. Onde mais erro: incremental x diferencial, tokenização x hash e achar que o IDS não vê o mesmo tráfego que o IPS.

Neste capítulo

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

Tópicos-chave

Estados dos dados

Em repouso (armazenados em disco): criptografia de disco completo (FDE), como BitLocker, protege um notebook furtado. Em trânsito (circulando na rede): TLS. Em uso (na memória, sendo processados): enclaves seguros e computação confidencial.

Responsabilidade compartilhada na nuvem

Em IaaS, configurar as permissões de um bucket é do cliente. Em SaaS, o provedor cuida da aplicação e da infraestrutura física; o cliente define quem acessa, cria senhas e classifica seus dados. Em serverless, o provedor cuida da infraestrutura e do sistema operacional; o cliente responde pelo código, pelos dados e pelas permissões da função.

Firewall de camada 4 x NGFW

O firewall de camada 4 decide por IP, porta e protocolo. O NGFW atua na camada de aplicação: identifica aplicações (redes sociais, armazenamento em nuvem), inspeciona conteúdo e TLS e combina IPS e reputação. Firewalls seguem a ordem das regras e terminam com negação implícita (deny all).

WAF e UTM

O WAF atua na camada de aplicação, inspeciona requisições HTTP e bloqueia padrões como SQLi e XSS. O UTM junta firewall, VPN, antivírus de gateway, filtro web e IPS numa só caixa: simplifica a gestão em ambientes menores, mas concentra funções e vira ponto único de falha e possível gargalo.

IPS em linha x IDS passivo

O IPS fica no caminho do tráfego e pode bloquear o ataque, mas exige dimensionamento e definição de modo de falha para não virar gargalo ou ponto de falha. O IDS passivo recebe cópia do tráfego por TAP de rede ou porta de espelhamento (SPAN) e só alerta. Os dois veem tráfego e geram alertas; o diferencial do IPS é bloquear.

Fail-closed x fail-open

Fail-closed bloqueia todo o tráfego quando o dispositivo falha e favorece a confidencialidade (área crítica). Fail-open libera o tráfego e favorece a disponibilidade (serviço crítico de emergência). A escolha depende do que é mais crítico.

Zonas, DMZ e jump server

A DMZ (screened subnet) fica entre a Internet e a rede interna, com firewalls separando zonas de confiança diferentes; servidor web público fica nela. Banco de dados fica em zona interna, falando só com o servidor de aplicação, e regras entre zonas seguem o menor privilégio. Jump server é o servidor intermediário reforçado e monitorado por onde administradores acessam redes protegidas.

Proxies e balanceadores

Forward proxy fica entre usuários internos e a Internet, filtrando e registrando sites. Proxy reverso fica na frente dos servidores, esconde a origem e pode filtrar, balancear, cachear e encerrar TLS. Balanceador distribui requisições entre servidores (ativo/ativo ou ativo/passivo) e elimina ponto único de falha.

VPN, IPsec e TLS

IPsec cifra na camada de rede, usa AH e ESP, e o modo túnel é típico de VPN site a site (matriz e filial). VPN de acesso remoto conecta usuários e usa IPsec ou TLS. TLS cifra o tráfego entre navegador e servidor sobre TCP. HTTP (80), Telnet (23), FTP, SMTP sem criptografia e SNMPv1 não cifram.

802.1X, zero trust, ZTNA, SD-WAN, SASE e CASB

802.1X com EAP e RADIUS autentica o dispositivo antes de liberar a porta do switch. Zero trust verifica identidade, dispositivo e contexto a cada acesso, sem confiança implícita. ZTNA dá acesso só a aplicações específicas, não à rede inteira. SD-WAN escolhe o melhor link entre filiais; SASE junta SD-WAN e segurança entregue pela nuvem. CASB dá visibilidade e controle sobre SaaS e combate shadow IT, sem a parte de rede.

Sites de recuperação

Hot site: equipado e com dados sincronizados, volta em minutos, maior custo. Warm site: energia, rede e alguns servidores, mas exige restaurar dados e configurar sistemas. Cold site: só espaço e energia, sem equipamentos.

Backup, snapshot, replicação e journaling

Incremental copia o que mudou desde o último backup de qualquer tipo (rápido para gravar, lento para restaurar); diferencial copia tudo desde o último completo. Backup deve ser testado com restauração periódica, cifrado e guardado offsite; imutável ou offline resiste a ransomware. Snapshot captura o estado de uma VM antes de mudanças, mas não substitui backup. Replicação contínua para outro site reduz o RPO. Journaling grava cada transação num diário antes de aplicar.

Alta disponibilidade e resiliência

RAID 1 espelha dois discos; RAID 5 usa paridade; RAID 0 não tem redundância. Cluster faz outro servidor assumir com os mesmos dados. Várias regiões resistem à perda de uma região inteira; multinuvem reduz a dependência de um provedor. UPS (nobreak) cobre minutos até o gerador entrar; gerador cobre quedas longas.

Testes de continuidade e planejamento de capacidade

Tabletop: discussão em sala, sem acionar sistemas. Simulação e failover real (transferir de verdade as operações para o site secundário) têm custo e risco crescentes. Planejamento de capacidade considera pessoas, tecnologia e infraestrutura: só um funcionário saber operar a folha é problema de pessoas.

Métodos de proteção de dados

Hashing é unidirecional e permite comparar sem guardar o original. Tokenização troca o dado por token sem significado, com o mapeamento num cofre, e permite recuperar o número para cobrar. Mascaramento mostra só parte (quatro últimos dígitos). Anonimização permite estatística sem identificar. Também: restrição geográfica, segmentação e restrição de permissões por necessidade de saber. Base de teste usa dados mascarados, tokenizados ou sintéticos.

Classificação e tipos de dados

Classificações comuns: público, interno/privado, confidencial, restrito e crítico; a classificação determina rotulagem, acesso, armazenamento, transmissão e descarte. Tipos: regulamentados (prontuários médicos), segredos comerciais, propriedade intelectual (código-fonte que dá vantagem), jurídicos, financeiros, legíveis por humanos ou por máquinas. Soberania de dados obriga a manter dados no país exigido pela lei.

Armazenamento de senhas

Senhas são guardadas com hash, salt e algoritmo lento (key stretching), como bcrypt, scrypt ou Argon2. Base64 é reversível, cifra com chave no código permite extrair a chave e texto puro expõe tudo num vazamento.

Embarcados, ICS, IoT, contêineres e IaC

RTOS e embarcados têm pouco recurso e atualização difícil: segmentar e monitorar pela rede. ICS/SCADA priorizam disponibilidade: isolar e controlar acessos, sem aplicar todos os patches de uma vez. IoT frágil vai para rede segmentada. Contêineres rodam sem root, com imagens atualizadas. Microsserviços autenticam e autorizam cada chamada de API. IaC cria ambientes idênticos, versionados e auditáveis. Centralizar cria ponto único de falha; descentralizar gera configurações inconsistentes.

Macetes para memorizar

Sites de recuperação

Quente já está ligado; morno precisa esquentar (restaurar dados); frio é só a sala vazia com energia.

Incremental x diferencial

Incremental = desde o último qualquer. Diferencial = desde o completo (Diferencial, Do completo).

RAID

RAID 0 = zero proteção; RAID 1 = um espelho; RAID 5 = paridade.

Modos de falha

Closed fecha a porta (protege o sigilo); Open abre a porta (mantém o serviço).

Estados dos dados

Repouso = FDE; trânsito = TLS; uso = enclave.

Energia

UPS segura a queda curta (minutos, até o gerador entrar); gerador segura as quedas longas.

Proteção de dados

Preciso de volta? Tokenizo. Só comparar? Hash. Só esconder na tela? Mascaro. Estatística sem nome? Anonimizo.

Tabela de memorização: não confunda

Quando é...	...e quando é
Backup incremental Copia só o que mudou desde o último backup de qualquer tipo: grava rápido, restaura devagar.	**Backup diferencial** Copia tudo o que mudou desde o último completo: grava mais, restaura mais rápido.

Hot site Operações voltam em minutos, local equipado e dados sincronizados, maior custo.	**Warm site** Tem energia, rede e alguns servidores, mas precisa restaurar dados e configurar antes de operar; equilibra custo e tempo.
Fail-closed Firewall de área crítica que deve bloquear tudo ao falhar; prioriza a segurança.	**Fail-open** Serviço crítico de emergência que precisa continuar no ar; prioriza a disponibilidade.
Forward proxy Usuários internos saindo para a Internet, com filtragem e registro de sites.	**Proxy reverso** Clientes externos chegando aos servidores da empresa; esconde a origem.
Tokenização Precisa guardar o número do cartão para cobranças futuras, reduzindo o impacto de vazamento.	**Hashing** Precisa só comparar (cadastros, senhas) sem nunca recuperar o original.
UPS (nobreak) Manter o datacenter por alguns minutos até o gerador entrar.	**Gerador** Manter o datacenter durante longas quedas de energia.
ZTNA Terceiros ou usuários acessam só aplicações específicas, com verificação contínua.	**VPN com acesso total** Túnel cifrado para a rede interna inteira; dá acesso amplo demais quando o requisito é zero trust.

Números que caem

Item	Valor
Peso do domínio no exame	**18%**
Porta padrão do HTTP (sem cifra)	**80**
Porta padrão do Telnet (sem cifra)	**23**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Escolher RAID 0 ou JBOD para tolerar a falha de um disco.
Como não cair: RAID 0 e JBOD não têm redundância. Dois discos gravados ao mesmo tempo é RAID 1.

⚠ **Alerta de prova:** Achar que o IPS se destaca por ver tráfego espelhado ou gerar alertas por e-mail.
Como não cair: O IDS também faz isso. A capacidade exclusiva do IPS em linha é bloquear o ataque.

⚠ **Alerta de prova:** Usar hash com salt para guardar número de cartão que será cobrado depois.
Como não cair: Hash não permite recuperar o número. Para cobrar depois, use tokenização.

⚠ **Alerta de prova:** Tratar Base64 como proteção de senha ou de dado.
Como não cair: Base64 é codificação reversível. Senha exige hash com salt e algoritmo lento.

⚠ **Alerta de prova:** Proteger a tela do atendente com criptografia de disco completo.
Como não cair: FDE protege o armazenamento, não o que aparece na tela. Mostrar só parte do dado é mascaramento.

⚠ **Alerta de prova:** Escolher CASB quando o enunciado quer unir SD-WAN e segurança na nuvem.
Como não cair: CASB controla o uso de serviços de nuvem, sem a parte de rede. SD-WAN mais segurança entregue pela nuvem é SASE.

⚠ **Alerta de prova:** Achar que um firewall de pacotes sem estado ou um roteador básico identifica aplicações dentro do HTTPS.
Como não cair: Identificar aplicações e inspecionar TLS é função do NGFW.

⚠ **Alerta de prova:** Considerar que implantação em uma só zona resiste à perda de uma região inteira da nuvem.
Como não cair: Perda de região pede implantação em várias regiões (ou multinuvem).

⚠ **Alerta de prova:** Em serverless, atribuir ao cliente a atualização do sistema operacional; em IaaS, atribuir ao provedor a configuração do bucket.
Como não cair: Serverless: SO é do provedor, código e permissões são do cliente. IaaS: configuração, dados e acessos são do cliente.

⚠ **Alerta de prova:** Aplicar todos os patches no mesmo dia em um ICS/SCADA que não pode parar.
Como não cair: Isso pode interromper a operação. A abordagem é isolar a rede e controlar os acessos.

⚠ **Alerta de prova:** Apontar ponto único de falha como risco típico de arquitetura descentralizada.
Como não cair: Ponto único de falha é risco da centralização. Descentralização gera configurações inconsistentes.

⚠ **Alerta de prova:** Achar que snapshot ou journaling substituem o backup, ou guardar o backup na mesma sala ou pasta dos originais.
Como não cair: Snapshot não substitui backup completo. Backup deve ser offsite e, contra ransomware, imutável ou offline.

⚠ **Alerta de prova:** Achar que virtualização elimina vulnerabilidades, patches ou backups.
Como não cair: Ela isola serviços em VMs, mas traz riscos como VM escape; VMs continuam precisando de patches e backup.

⚠ **Alerta de prova:** Escolher teste de failover completo quando o cenário descreve discussão em sala sem acionar sistemas.
Como não cair: Discussão passo a passo sem sistemas é tabletop. Failover transfere as operações de verdade.

Como cai na prova

📝 **Como cai:** Requisito de tempo de recuperação ou de perda de dados e pergunta de site ou técnica.
Como resolver: Minutos com dados sincronizados = hot site; perda mínima de dados = replicação; parte pronta = warm; só espaço = cold. Backup em fita exige restauração demorada.

📝 **Como cai:** Cenário de nuvem pergunta de quem é a responsabilidade.
Como resolver: Identifique o modelo (IaaS, SaaS, serverless). Infraestrutura física é sempre do provedor; dados, acessos e configuração do cliente (bucket, permissões, código da função) são do cliente.

📝 **Como cai:** Requisito de inspeção ou bloqueio pede o dispositivo certo.
Como resolver: IP e porta = camada 4; aplicações e TLS = NGFW; HTTP com SQLi/XSS = WAF; várias funções numa caixa = UTM; bloquear ataque = IPS em linha; só alertar sem afetar tráfego = IDS passivo.

📝 **Como cai:** Proteger dado sensível em cenário de negócio.
Como resolver: Leia o verbo: guardar para usar depois (tokenização), comparar (hash), mostrar parte (mascaramento), pesquisa sem identificar (anonimização), base de teste (mascarar ou tokenizar), restringir por país (geográfica).

📝 **Como cai:** Sistema legado, embarcado ou industrial que não aceita agente ou patch.
Como resolver: A resposta quase sempre é segmentar/isolar a rede e controlar ou monitorar acessos. Descarte expor à Internet, instalar software extra ou reiniciar todo dia.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Operações voltam em minutos em outro local equipado e sincronizado	**Hot site**

Local com energia, rede e alguns servidores, mas precisa restaurar dados	**Warm site**
Copia apenas o que mudou desde o último backup de qualquer tipo	**Incremental**
Backup que ransomware não altera nem apaga, mesmo com admin comprometido	**Armazenamento imutável ou offline**
Inspecionar HTTPS e identificar aplicações	**NGFW**
Inspecionar requisições HTTP e bloquear injeção de SQL	**WAF**
Firewall, VPN, filtro web e IPS numa caixa só	**UTM (cuidado: ponto único de falha)**
Serviços de nuvem não aprovados e políticas para SaaS	**CASB**
Acesso só a aplicações específicas, sem VPN para a rede inteira	**ZTNA / zero trust**
IDS ligado a porta de espelhamento ou TAP	**Posicionamento passivo, fora do caminho do tráfego**
Autenticar o dispositivo antes de liberar a porta do switch	**802.1X com EAP e RADIUS**
Exibir só os últimos quatro dígitos do cartão	**Mascaramento**
Dados precisam ficar armazenados no Brasil por exigência legal	**Soberania e localização dos dados**
Notebook com dados de clientes furtado	**Criptografia completa do disco (FDE)**

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

- Incremental = desde o último backup de qualquer tipo; diferencial = desde o último completo.
- O que o IPS faz e o IDS não faz é bloquear; o IDS passivo usa TAP ou SPAN.
- Tokenização permite recuperar o dado; hash não.
- Fail-closed prioriza segurança; fail-open prioriza disponibilidade.
- Backup só vale se a restauração for testada; contra ransomware, imutável ou offline.

Essenciais para a prova (checklist)

- ☐ Sei proteger dados em repouso, em trânsito e em uso.
- ☐ Sei dividir responsabilidades entre cliente e provedor em IaaS, SaaS e serverless.
- ☐ Sei diferenciar firewall de camada 4, NGFW, WAF e UTM.
- ☐ Sei quando posicionar IPS em linha ou IDS passivo e qual modo de falha usar.
- ☐ Sei diferenciar forward proxy, proxy reverso, balanceador e jump server.
- ☐ Sei quando usar VPN site a site, VPN de acesso remoto, ZTNA, SASE e CASB.

- ☐ Sei comparar hot, warm e cold site e backups completo, incremental e diferencial.
- ☐ Sei a diferença entre RAID 0, 1 e 5, e entre UPS e gerador.
- ☐ Sei escolher entre hashing, tokenização, mascaramento e anonimização.
- ☐ Sei como proteger ICS, RTOS, IoT e contêineres.

Questões de revisão do capítulo

R2.1 · Arquitetura de Segurança

A empresa exige que, se o datacenter principal parar, as operações voltem em minutos em outro local já equipado e com dados sincronizados. Que tipo de site atende?

A. Cold site
B. Backup em fita externa
C. Warm site
D. Hot site (site quente)

R2.2 · Arquitetura de Segurança

Um IPS em linha precisa inspecionar o tráfego e bloquear ataques. Qual é o principal cuidado ao posicioná-lo?

A. Instalá-lo só na rede de visitantes
B. Evitar que vire gargalo ou ponto de falha
C. Desativar as assinaturas para ganhar tempo
D. Colocá-lo fora do caminho do tráfego

R2.3 · Arquitetura de Segurança

A empresa faz um backup completo no domingo e, nos outros dias, copia apenas o que mudou desde o último backup de qualquer tipo. Que estratégia é essa?

A. Completo com diferenciais
B. Completo com incrementais
C. Snapshot único mensal
D. Apenas backups completos

R2.4 · Arquitetura de Segurança

Um notebook com dados de clientes foi furtado. Qual controle, se estivesse ativo, protegeria os dados armazenados?

A. Firewall de host bem configurado
B. Criptografia completa do disco
C. Filtro de conteúdo web ativo
D. Antivírus com assinaturas novas

Respostas comentadas

R2.1. D) Hot site (site quente)

Por quê: Hot sites oferecem o menor tempo de recuperação, com o maior custo.

✗ A) Incorreta. Tem só espaço e energia, sem equipamentos.
✗ B) Incorreta. Exige restauração demorada.
✗ C) Incorreta. Tem parte dos recursos e exige preparo.

> **Dica de prova:** Voltar em minutos: hot site.

R2.2. B) Evitar que vire gargalo ou ponto de falha

Por quê: Dispositivos em linha exigem dimensionamento e definição de modo de falha.

✗ A) Incorreta. Não protege o essencial.
✗ C) Incorreta. Reduz a proteção.
✗ D) Incorreta. Assim não bloquearia nada.

> **Dica de prova:** IPS em linha: cuidado com gargalo e falha.

R2.3. B) Completo com incrementais

Por quê: Incrementais são rápidos para gravar e lentos para restaurar; diferenciais são o contrário.

✗ A) Incorreta. Copiaria tudo o que mudou desde o completo.
✗ C) Incorreta. Não é diário.
✗ D) Incorreta. Copiaria tudo todos os dias.

> **Dica de prova:** Desde o último backup de qualquer tipo: incremental.

R2.4. B) Criptografia completa do disco

Por quê: Dados em repouso são protegidos por criptografia de disco completo (FDE), como BitLocker.

✗ A) Incorreta. Não protege o disco furtado.
✗ C) Incorreta. Não protege os dados locais.
✗ D) Incorreta. Não impede ler o disco.

> **Dica de prova:** Dispositivo furtado: criptografia de disco.

03

CAPÍTULO 3 · 12% DA PROVA

Conceitos Gerais de Segurança

É o domínio de menor peso, mas é base para todos os outros: tríade CIA e não repúdio, AAA, categorias e tipos de controle, zero trust (policy engine, policy administrator e PEP), controles físicos, tecnologias de engano (honeypot, honeynet, honeyfile, honeytoken), gestão de mudanças e criptografia (simétrica, assimétrica, hash, salt, key stretching, assinatura digital, PKI, TPM e HSM). A prova costuma pedir para classificar um controle em duas dimensões ao mesmo tempo (ex.: técnico e preventivo) e para escolher a técnica criptográfica pela necessidade. Onde mais erro: dissuasivo x detectivo (câmera sem gravar), compensatório x preventivo, e achar que hash ou assinatura dão sigilo.

Neste capítulo

17 tópicos-chave · 13 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Tríade CIA e não repúdio

Confidencialidade é o sigilo; integridade garante que a informação não foi alterada sem autorização (hashes, assinaturas, controles de acesso); disponibilidade é o acesso quando necessário (DoS afeta disponibilidade). Não repúdio impede alguém de negar a autoria de uma ação; assinatura digital é o mecanismo típico.

AAA

Identificação declara quem é. Autenticação comprova a identidade (login). Autorização define o que o usuário pode fazer (só ler relatórios). Contabilização (accounting) registra as ações executadas depois de entrar.

Categorias de controle

Técnicos (implementados por tecnologia: firewall, bloqueio de tela), gerenciais (políticas, procedimentos escritos, avaliações de risco), operacionais (executados por pessoas: treinamentos, guardas) e físicos (cercas, iluminação, bollards, fechaduras).

Tipos de controle

Preventivo impede (firewall bloqueando, guarda barrando). Detectivo identifica e alerta (IDS, sensor de movimento com alarme). Corretivo restaura após o incidente (backup, restaurar imagem limpa e aplicar patch). Dissuasivo desencoraja (câmera visível, placa de aviso). Diretivo orienta (aviso na tela de login, política). Compensatório substitui o controle que não pode ser aplicado.

Classificação dupla de controles

Um mesmo controle é classificado por categoria e por tipo: regra de firewall e bloqueio automático de tela são técnicos e preventivos; guarda verificando crachás é físico e preventivo; sensor com alarme é físico e detectivo. Biometria com registro de cada acesso previne e também apoia o accounting.

Controle compensatório

Reduz o risco quando o controle principal não é viável: isolar sistema legado em VLAN porque não dá para cifrar; monitorar em tempo real porque não dá para aplicar MFA. Não é preventivo direto (seria o próprio MFA) nem corretivo.

Análise de lacunas (gap analysis)

Compara os controles atuais com um padrão de referência, como NIST Cybersecurity Framework ou ISO 27001, e prioriza o que falta implementar. Não é BIA, varredura de portas nem pentest.

Zero trust

Não existe zona implicitamente confiável. O plano de controle tem o policy engine (decide o acesso por identidade, dispositivo e contexto) e o policy administrator (configura o PEP e gera credenciais). O plano de dados tem o PEP, que fica no caminho do tráfego e aplica a decisão. Negar acesso porque o notebook está sem atualizações é autenticação adaptativa por contexto.

Controles físicos

Bollards (pilares de concreto) impedem a entrada de veículos. Vestíbulo de acesso (mantrap), com duas portas intertravadas, combate tailgating e piggybacking. Também cercas, iluminação, guardas, câmeras e sensores. Cruzar registro de entrada com login nos computadores ajuda a detectar uso indevido de credencial.

Tecnologias de engano

Honeypot é um sistema falso para atrair e estudar atacantes. Honeynet é uma rede de honeypots que simula um ambiente inteiro. Honeyfile é arquivo-isca (como 'senhas_admin.xlsx') que alerta ao ser acessado. Honeytoken é credencial ou token falso que alerta se for usado.

Gestão de mudanças

Solicitação, análise de impacto e de dependências, aprovação (comitê de mudanças, CAB), teste em homologação, implantação em janela de manutenção e documentação. Define dono e partes interessadas, prevê plano de reversão (backout) e atualiza diagramas e documentação depois. Implicações técnicas: allow list e block list, controle de versão, reinícios e tempo de parada. Mesmo mudança emergencial segue processo, ainda que acelerado.

Criptografia simétrica e assimétrica

Simétrica usa a mesma chave, é rápida e serve para dados em repouso e em trânsito (AES). Assimétrica usa par de chaves (RSA, ECC), costuma ser mais lenta e resolve a troca de chaves; TLS usa assimétrica ou Diffie-Hellman para estabelecer a chave simétrica de sessão. ECC dá segurança semelhante ao RSA com chaves menores e serve a dispositivos com poucos recursos.

Hash, salt e key stretching

Hash (SHA-256) verifica integridade sem decifrar nada; MD5 está quebrado. Salt é valor aleatório diferente por senha, adicionado antes do hash, que impede tabelas pré-calculadas (rainbow tables). Key stretching aplica o hash milhares de vezes para fortalecer senha fraca: PBKDF2, bcrypt e Argon2.

Assinatura digital e carimbo de tempo

Assina-se com a chave privada do remetente e verifica-se com a chave pública: prova quem enviou e que não houve alteração. Não garante sigilo (isso exige criptografia) nem ausência de vírus. Com carimbo de tempo, prova também o momento da assinatura. Code signing aplica o mesmo a software.

PKI e certificados

A PKI inclui CA (emite e assina certificados), RA (verifica a identidade de quem pede antes da emissão), certificados, CRL e OCSP (status de revogação) e políticas. A cadeia de confiança vai do certificado do servidor, por intermediárias, até a raiz confiável; se não valida, o navegador exibe alerta. CA pública já é confiável nos navegadores; CA interna e autoassinado exigem distribuir a raiz. Curinga (*.empresa.com) ou SAN protegem vários nomes.

Key escrow, TPM e HSM

Key escrow guarda cópia das chaves com terceiro confiável para recuperação. TPM é o chip do computador que guarda chaves e apoia inicialização medida e criptografia de disco (BitLocker). HSM é hardware dedicado e resistente a violação para chaves de servidores e grande volume de operações.

Ofuscação, esteganografia e blockchain

Ofuscação dificulta entender o código sem cifrá-lo e não substitui criptografia. Esteganografia esconde a existência da mensagem, por exemplo dentro de uma imagem. Blockchain encadeia blocos pelo hash do anterior, o que reforça a integridade do histórico, não a confidencialidade.

Macetes para memorizar

Tipos de controle no tempo

Antes: preventivo, dissuasivo, diretivo. Durante: detectivo. Depois: corretivo. No lugar de outro: compensatório.

AAA

Autenticação = quem é; Autorização = o que pode; Accounting = o que fez.

Assinatura digital

Assino com a minha privada, você confere com a minha pública.

Tecnologias de engano

Pot = um sistema; net = uma rede; file = um arquivo; token = uma credencial.

TPM x HSM

TPM mora no notebook; HSM mora no datacenter.

Zero trust

Policy engine é o juiz, policy administrator é o escrivão que repassa, PEP é o porteiro.

Simétrica x assimétrica

Simétrica = mesma chave nos dois lados; assimétrica = par (pública e privada).

Tabela de memorização: não confunda

Quando é...	...e quando é
Criptografia simétrica Cifrar volume de dados com rapidez usando uma chave só (AES).	**Criptografia assimétrica** Trocar a chave inicial sem segredo prévio, assinar e verificar (RSA, ECC), com par de chaves.
Policy engine Decide se o pedido de acesso é liberado com base em identidade, dispositivo e contexto.	**PEP (ponto de aplicação de política)** Fica no caminho do tráfego e aplica, na prática, a decisão de liberar ou bloquear.
TPM Chip no computador para chaves locais, inicialização medida e BitLocker.	**HSM** Hardware dedicado, resistente a violação, para chaves privadas de certificados e servidores.

CA Emite e assina os certificados como autoridade confiável.	**RA** Verifica a identidade do solicitante antes da emissão.
Autenticação Comprovar quem é o usuário (senha, biometria).	**Autorização** Definir o que o usuário autenticado pode fazer (ler, editar).
Controle dissuasivo Aviso de câmeras ou câmera visível para desencorajar, mesmo sem gravar.	**Controle detectivo** Sensor, alarme ou câmera gravando que identifica e alerta o evento.
Controle compensatório Substitui o controle principal inviável (isolar porque não dá para cifrar).	**Controle corretivo** Atua depois do incidente para restaurar o estado (backup, imagem limpa).

Números que caem

Item	Valor
Peso do domínio no exame	**12% (o menor)**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Marcar SHA-256 ou MD5 como algoritmo de criptografia simétrica.
Como não cair: SHA e MD5 são hashes, não cifram; MD5 está quebrado. Simétrico padrão é AES; RSA é assimétrico.

⚠ **Alerta de prova:** Cifrar o arquivo com AES para verificar se ele foi alterado.
Como não cair: Cifrar protege o sigilo, não a integridade. Para verificar alteração, compare o hash.

⚠ **Alerta de prova:** Achar que a assinatura digital garante que ninguém mais leu a mensagem ou que o anexo não tem vírus.
Como não cair: Assinatura prova autoria e integridade. Sigilo exige criptografia; malware exige outra verificação.

⚠ **Alerta de prova:** Classificar o aviso de 'área monitorada' sem câmeras instaladas como controle detectivo.
Como não cair: Não há nada gravando. O efeito é dissuasivo.

⚠ **Alerta de prova:** Classificar o monitoramento adotado porque o MFA não pôde ser aplicado como preventivo.
Como não cair: Preventivo seria o próprio MFA. O que substitui o controle inviável é compensatório.

⚠ **Alerta de prova:** Classificar o IDS que só alerta como preventivo.
Como não cair: IDS é detectivo; IPS, que bloqueia, é preventivo.

⚠ **Alerta de prova:** Achar que catraca com leitor ou câmera na porta impedem que alguém entre junto com o funcionário.
Como não cair: Catraca não impede totalmente a carona e câmera só registra. Duas portas intertravadas (vestíbulo de acesso) impedem.

⚠ **Alerta de prova:** Escolher o policy administrator ou o policy engine como componente que fica no caminho do tráfego.
Como não cair: O engine decide, o administrator configura o PEP; quem aplica no tráfego é o PEP.

⚠ **Alerta de prova:** Achar que certificado curinga emitido por CA interna dispensa instalar algo nos clientes.
Como não cair: Continua exigindo confiança na CA interna. Sem instalar nada, só CA pública.

⚠ **Alerta de prova:** Deixar o técnico aprovar a própria mudança, ou achar que testes em homologação dispensam o plano de reversão.
Como não cair: Mudanças significativas são aprovadas pelo comitê (CAB), e o plano de backout continua necessário.

⚠ **Alerta de prova:** Confundir salt com nonce de sessão TLS.
Como não cair: Nonce evita repetição em protocolos. Valor aleatório por senha antes do hash é salt.

⚠ **Alerta de prova:** Marcar jump server, bastion host ou proxy reverso como sistema-isca.
Como não cair: Esses servidores são reais. Sistema falso para atrair atacantes é honeypot.

⚠ **Alerta de prova:** Usar chave RSA enorme em dispositivo IoT com pouca capacidade.
Como não cair: Seria pesado demais. IoT limitado pede criptografia leve, como ECC.

Como cai na prova

📝 **Como cai:** Descreve um controle e pede categoria e tipo juntos (ex.: 'técnico e preventivo').
Como resolver: Primeiro decida quem executa (tecnologia = técnico; documento = gerencial; pessoas = operacional; barreira = físico). Depois o momento e o efeito (impede, detecta, corrige, desencoraja, orienta, substitui). A alternativa certa precisa acertar as duas partes.

📝 **Como cai:** Necessidade criptográfica pede a técnica.
Como resolver: Verificar alteração = hash; provar autor = assinatura; provar data = assinatura com carimbo de tempo; trocar chave sem segredo prévio = assimétrica ou DH; cifrar volume = AES; guardar senha = salt e key stretching.

📝 **Como cai:** Cenário de PKI ou certificado.
Como resolver: Quem valida identidade = RA; quem emite = CA; revogação = CRL ou OCSP; confiança sem instalar = CA pública; vários subdomínios = curinga ou SAN; cadeia inválida = alerta no navegador.

📝 **Como cai:** Etapa ou falha da gestão de mudanças.
Como resolver: Surpresa durante a mudança = faltou análise de impacto e dependências; precisa desfazer = backout; reinício de servidores = janela de manutenção; depois de aplicar = atualizar documentação; quem aprova = CAB.

📝 **Como cai:** Componente do zero trust.
Como resolver: Decide = policy engine; configura e gera credenciais = policy administrator; fica no tráfego e aplica = PEP. Qualquer 'zona implicitamente confiável' é o que o modelo evita.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Aprovador não consegue negar depois que aprovou	**Não repúdio (assinatura digital)**
Registrar quais ações o usuário executou depois de entrar	**Contabilização (accounting)**
Usuário autenticado pode apenas ler, sem editar	**Autorização**
Valor aleatório diferente por senha antes do hash	**Salt**
Hash aplicado milhares de vezes para fortalecer senha	**Key stretching (PBKDF2, bcrypt, Argon2)**
Cópia das chaves com terceiro confiável	**Key escrow**
Chip do computador que guarda chaves e verifica a inicialização (BitLocker)	**TPM**
Certificado comprometido antes de expirar	**CRL ou OCSP**
Um certificado para www, loja e api do mesmo domínio	**Certificado curinga (ou SAN)**
Duas portas em que a segunda só abre depois que a primeira fecha	**Vestíbulo de acesso (mantrap)**
Pilares de concreto na frente da entrada	**Bollards contra veículos**

Arquivo falso que gera alerta ao ser acessado / token falso plantado	**Honeyfile / honeytoken**
Comparar controles atuais com ISO 27001 ou NIST CSF	**Gap analysis**
Mensagem escondida dentro de uma imagem	**Esteganografia**

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

- Hash verifica integridade, não cifra; assinatura prova autoria e integridade, não sigilo.
- Câmera visível ou placa é dissuasiva; câmera gravando, sensor e alarme são detectivos.
- Compensatório é o substituto do controle que não pode ser aplicado.
- No zero trust, o policy engine decide e o PEP aplica.
- Toda mudança tem dono, aprovação do CAB, análise de impacto, teste, janela, plano de reversão e documentação atualizada.

Essenciais para a prova (checklist)

- ☐ Sei classificar um controle por categoria (técnico, gerencial, operacional, físico) e por tipo (preventivo, detectivo, corretivo, dissuasivo, diretivo, compensatório).
- ☐ Sei diferenciar identificação, autenticação, autorização e accounting.
- ☐ Sei os componentes do zero trust e o que cada um faz.
- ☐ Sei diferenciar honeypot, honeynet, honeyfile e honeytoken.
- ☐ Sei as etapas da gestão de mudanças e para que serve o plano de backout.
- ☐ Sei quando usar criptografia simétrica, assimétrica e hash.
- ☐ Sei para que servem salt e key stretching.
- ☐ Sei o papel de CA, RA, CRL e OCSP e quando usar certificado curinga.
- ☐ Sei diferenciar TPM, HSM e key escrow.

Questões de revisão do capítulo

R3.1 · Conceitos Gerais de Segurança

Para dificultar ataques de dicionário contra senhas armazenadas, o sistema adiciona um valor aleatório diferente a cada senha antes de calcular o hash. Como se chama esse valor?

A. Nonce de sessão TLS
B. Certificado curinga
C. Salt aleatório por senha
D. Chave pública do servidor

R3.2 · Conceitos Gerais de Segurança

Depois de aplicar uma mudança aprovada, a equipe atualiza os diagramas de rede e a documentação do sistema. Por que isso é importante?

A. Mantém a documentação fiel ao ambiente
B. Elimina a necessidade de testes
C. Dispensa o plano de reversão
D. Substitui a etapa de aprovação da mudança

R3.3 · Conceitos Gerais de Segurança

Uma empresa aplica a mesma regra de firewall para todos os escritórios a partir de um console central. A regra que nega tráfego não autorizado é um controle:

A. Operacional e corretivo de pessoas
B. Técnico e preventivo, por tecnologia
C. Físico e compensatório de perímetro
D. Gerencial e diretivo por política

R3.4 · Conceitos Gerais de Segurança

Uma empresa compara seus controles atuais com o NIST Cybersecurity Framework e prioriza o que falta implementar. Que atividade é essa?

A. Varredura de portas da rede interna
B. Análise de lacunas com o framework
C. Revisão do código da aplicação
D. Teste de penetração nos servidores web

Respostas comentadas

R3.1. C) Salt aleatório por senha

Por quê: Salt impede o uso de tabelas pré-calculadas (rainbow tables); key stretching, como bcrypt, torna o cálculo mais lento.

✗ A) Incorreta. Evita repetição em protocolos.
✗ B) Incorreta. Protege vários subdomínios.
✗ D) Incorreta. Serve para cifrar ou verificar assinaturas.

> **Dica de prova:** Valor aleatório antes do hash: salt.

R3.2. A) Mantém a documentação fiel ao ambiente

Por quê: A gestão de mudanças inclui atualizar diagramas, políticas e procedimentos.

✗ B) Incorreta. Os testes continuam necessários.

✗ C) Incorreta. O plano continua necessário.

✗ D) Incorreta. A aprovação ocorre antes.

> **Dica de prova:** Depois da mudança: atualizar documentação.

R3.3. B) Técnico e preventivo, por tecnologia

Por quê: Regras de firewall são controles técnicos preventivos.

✗ A) Incorreta. Seria ação humana após incidente.

✗ C) Incorreta. Seria barreira física alternativa.

✗ D) Incorreta. Seria orientação escrita.

> **Dica de prova:** Regra de firewall: técnico e preventivo.

R3.4. B) Análise de lacunas com o framework

Por quê: Gap analysis compara o estado atual com um padrão como NIST CSF ou ISO 27001.

✗ A) Incorreta. Descobre serviços expostos.

✗ C) Incorreta. Analisa software específico.

✗ D) Incorreta. Busca falhas técnicas exploráveis.

> **Dica de prova:** Atual x framework: gap analysis.

04

CAPÍTULO 4 · 20% DA PROVA

Gestão e Supervisão do Programa de Segurança

Aqui eu preciso dominar governança (política, norma, procedimento, diretriz e papéis sobre os dados), gestão de riscos (apetite, tolerância, registro de riscos, BIA e as contas de SLE e ALE), risco de terceiros (MSA, SOW, SLA, MOU, NDA, BPA e cláusulas como direito de auditoria), conformidade e privacidade, auditorias e pentests, e conscientização. A prova traz cenários curtos e pede que eu dê nome ao documento, ao papel, à estratégia ou ao tipo de avaliação. Onde mais erro: trocar aceitar, mitigar, transferir e evitar; confundir RTO, RPO e MTD; e errar a ALE quando o evento acontece 'uma vez a cada N anos'. Também caio em alternativas radicais (punir, bloquear tudo, suspender simulações) quando a resposta certa é treinar, medir e documentar.

Neste capítulo

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

Tópicos-chave

Política, norma, procedimento e diretriz

Política é obrigatória e de alto nível: define o quê (ex.: AUP, continuidade, resposta a incidentes, SDLC, gestão de mudanças). Norma (standard) traz requisitos obrigatórios e específicos, como tamanho mínimo de senha e algoritmos aprovados. Procedimento detalha o como (onboarding, offboarding, playbooks). Diretriz (guideline) é recomendação opcional.

Política de uso aceitável (AUP)

Documento obrigatório e de alto nível com as regras de uso dos recursos de TI pelos funcionários. Não é guia opcional, não é procedimento técnico e não é SLA. O termo assinado na admissão serve para registrar o reconhecimento das políticas.

Estruturas de governança

Incluem conselhos, comitês, órgãos governamentais e modelos centralizados ou descentralizados. O comitê de governança de segurança, com representantes de várias áreas, aprova políticas. O conselho de administração define a estratégia de risco e cobra resultados (supervisão). Na governança descentralizada, cada unidade define suas regras; na centralizada, uma área única define.

Papéis sobre os dados

Proprietário (data owner) decide a classificação e quem acessa. Custodiante (ou steward) guarda os dados e aplica os controles técnicos definidos pelo proprietário. Na privacidade (LGPD), controlador decide finalidades e meios; operador trata em nome do controlador; titular é a pessoa a quem os dados se referem; encarregado (DPO) faz a ponte com titulares e autoridade.

Apetite e tolerância a risco

Apetite é quanto risco a empresa está disposta a aceitar para atingir objetivos e pode ser expansionista (aceita mais risco para crescer), neutro ou conservador (prefere reduzir riscos mesmo com custo maior). Tolerância e limites (thresholds) definem quem pode aceitar cada nível, por exemplo exigir aprovação do conselho acima de certo impacto.

Risco inerente e residual

Inerente é o risco antes de qualquer controle. Residual é o que sobra depois dos controles. Risco aceito é o assumido pela organização; transferido é o passado a terceiros.

Estratégias de tratamento de risco

Mitigar: aplicar controles que reduzem probabilidade ou impacto (ex.: detecção de incêndio). Transferir: passar o impacto financeiro a terceiros (seguro é o exemplo clássico). Evitar: deixar de fazer a atividade arriscada. Aceitar: assumir formalmente, dentro da tolerância, por exemplo quando o custo de corrigir supera o prejuízo esperado.

Exceção e isenção

São formas controladas de aceitação de risco: o sistema fica fora do padrão por um período, com aprovação da diretoria, prazo, revisão agendada e, muitas vezes, controles compensatórios. O risco continua existindo; não houve correção nem transferência.

Análise quantitativa (SLE, ARO, ALE)

SLE = AV x EF (valor do ativo vezes fator de exposição). ALE = SLE x ARO (frequência anual). Se o evento ocorre uma vez a cada quatro anos, o ARO é 0,25. A análise de custo e benefício compara o custo do controle com a ALE evitada: controle mais caro que a perda pode não se justificar.

Análise qualitativa

Classifica riscos em escalas como alto, médio e baixo, com base na opinião de especialistas, sem valores em dinheiro. Se o enunciado fala em probabilidade anual e valor monetário de cada ocorrência, é quantitativa.

Registro de riscos e KRI

O registro de riscos reúne descrição, dono, indicadores e tratamento planejado. Indicadores-chave de risco (KRI), como número de tentativas de login falhas, sinalizam quando um risco está aumentando e trabalham com limites (thresholds).

Tipos de avaliação de risco

Ad hoc (quando surge uma necessidade), recorrente (periódica), única (uma vez, por exemplo antes de um projeto) e contínua (permanente, com ferramentas automáticas).

Análise de impacto no negócio (BIA)

Identifica processos críticos, dependências e impactos, e define MTD (quanto tempo pode ficar parado), RTO (em quanto tempo voltar) e RPO (quanto dado pode perder, em tempo), além de MTTR e MTBF. É a BIA que orienta a ordem de restauração.

Tipos de acordos

MSA: termos gerais para vários serviços futuros. SOW e ordem de serviço (WO): trabalho específico com entregas, prazos e preço dentro do MSA. SLA: metas de desempenho, como restabelecer o serviço em até X horas. MOU: registra intenções, sem obrigações. NDA: protege informações sigilosas. BPA: parceria comercial de longo prazo.

Gestão de risco de terceiros

Seleção com due diligence (histórico de incidentes, saúde financeira, referências) e verificação de conflito de interesses. Avaliação com questionários complementados por evidências e auditorias independentes (como SOC 2), pentests do fornecedor e análise da cadeia de suprimentos. Contrato com direito de auditoria, notificação de incidentes e aprovação prévia de subcontratados. Monitoramento contínuo e reavaliação após incidente no fornecedor. Due diligence é investigar; due care é manter os controles.

Conformidade

Monitoramento pode ser interno, externo e automatizado; inclui atestação e reconhecimento (confirmar formalmente, todo ano, que leu a política ou que os controles estão conformes). Relatórios podem ser internos (diretoria) ou externos (investidores e reguladores). Consequências da não conformidade: multas, sanções, danos à reputação, perda de licença e impactos contratuais. Considerações externas: regulatórias, legais, setoriais, locais, nacionais e globais. Quem processa cartão segue o PCI DSS.

Privacidade

Exige inventário de dados, finalidade, base legal, retenção definida e respeito aos direitos do titular: acesso (cópia dos dados), correção, portabilidade e eliminação. Guardar sem prazo viola a limitação da retenção; coletar sem finalidade viola a minimização. Em vazamento de dados pessoais, a LGPD exige comunicar a ANPD e os titulares afetados.

Pentest, auditorias e conscientização

Pentest em ambiente conhecido (recebe tudo), parcialmente conhecido (recebe parte, como a lista de IPs) ou desconhecido (nada); pode ser ofensivo, defensivo, integrado (purple team) ou físico, sempre com regras de engajamento. Auditoria externa traz imparcialidade; interna inclui autoavaliação e comitê de auditoria. O programa de conscientização começa por riscos e público, tem etapas de desenvolvimento, execução, relatório e monitoramento, e mede eficácia por taxa de cliques e relatos.

Macetes para memorizar

Contas de risco

AV x EF = SLE; SLE x ARO = ALE. Tudo multiplica. 'Uma vez a cada N anos' vira ARO = 1/N.

Estratégias de risco

Seguro transfere, controle mitiga, desistir evita, assinar embaixo aceita.

RPO x RTO

RPO = Ponto no passado (quanto dado perco). RTO = Tempo para voltar.

Hierarquia documental

Política diz o quê, norma diz quanto (requisito exato), procedimento diz como, diretriz só sugere.

Papéis de privacidade

Controlador Comanda (decide), Operador Obedece (executa), Titular é o Tal da informação.

Acordos

MOU = intenção; MSA = contrato-mãe; SOW = serviço específico; SLA = meta de desempenho; NDA = boca fechada; BPA = parceria longa.

Ambientes de pentest

Conhecido = antigo white box; parcialmente conhecido = gray box; desconhecido = black box.

Tabela de memorização: não confunda

Quando é...	...e quando é
RPO (objetivo de ponto de recuperação) Quanto dado a empresa aceita perder, em tempo; orienta a frequência dos backups.	**RTO (objetivo de tempo de recuperação)** Em quanto tempo o sistema precisa voltar; orienta a velocidade da recuperação.

MTD (tempo máximo tolerável de parada) Quanto tempo o negócio aguenta sem o sistema antes do impacto ficar inaceitável.	**MTTR / MTBF** MTTR mede o tempo típico de conserto; MTBF mede a confiabilidade (tempo médio entre falhas).
Controlador Decide as finalidades e os meios do tratamento de dados pessoais.	**Operador** Trata os dados em nome do controlador, seguindo as instruções dele.
Proprietário dos dados Decide a classificação e quem pode acessar.	**Custodiante dos dados** Guarda os dados e implementa os controles técnicos definidos pelo proprietário.
MOU Registra intenções de cooperar, sem valor jurídico nem obrigações, antes de um contrato formal.	**MSA** Contrato com termos gerais que valerão para vários serviços futuros, detalhados em SOW ou ordens de serviço.
Risco inerente Risco antes de aplicar qualquer controle.	**Risco residual** Risco que sobra depois dos controles.
Reconhecimento passivo Coleta OSINT em redes sociais e sites públicos, sem interagir com os sistemas do alvo.	**Reconhecimento ativo** Varreduras de portas e interação com serviços do alvo; gera tráfego e pode ser detectado.

Números que caem

Item	Valor
Peso do domínio no exame	**20%**
ARO de evento que ocorre uma vez a cada quatro anos	**0,25**
SLE de R$ 50 mil com ARO 2	**ALE de R$ 100 mil**
Ativo de R$ 200 mil com EF de 40%	**SLE de R$ 80 mil**
Ativo de R$ 400 mil, EF de 25%, uma vez a cada quatro anos	**SLE de R$ 100 mil e ALE de R$ 25 mil**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Somar SLE e ARO (R$ 50 mil e 2 vezes por ano viram R$ 52 mil) ou dividir em vez de multiplicar.
Como não cair: ALE = SLE x ARO, sempre multiplicação: R$ 50 mil x 2 = R$ 100 mil.

⚠ **Alerta de prova:** Responder a SLE quando o enunciado pede a ALE de um evento que ocorre uma vez a cada quatro anos.
Como não cair: Converta a frequência: ARO = 1/4 = 0,25. Com AV de R$ 400 mil e EF de 25%, a SLE é R$ 100 mil e a ALE é R$ 25 mil.

⚠ **Alerta de prova:** Achar que instalar detecção de incêndio é transferir ou aceitar o risco.
Como não cair: Controle técnico ou físico que reduz probabilidade ou impacto é mitigar. Transferir seria contratar seguro; evitar seria deixar de ter o datacenter.

⚠ **Alerta de prova:** Chamar de 'aceitar' a decisão de não lançar um serviço por causa dos riscos.
Como não cair: Desistir da atividade é evitar. Aceitar é assumir o risco e seguir com a atividade.

⚠ **Alerta de prova:** Marcar 'guia de boas práticas opcional' como o documento que define regras obrigatórias de uso.
Como não cair: Diretriz é opcional. Regras obrigatórias de uso dos recursos de TI estão na política (AUP).

⚠ **Alerta de prova:** Após muitos cliques numa simulação de phishing, punir quem clicou, divulgar nomes, bloquear o e-mail ou encerrar as simulações.
Como não cair: Punição desestimula relatos, bloqueio é desproporcional e suspender perde a medição. A resposta é reforçar o treinamento, de forma direcionada ao setor que mais clica.

⚠ **Alerta de prova:** Aceitar uma nova declaração verbal do fornecedor, ou exigir o código-fonte inteiro, para comprovar o que ele disse no questionário.
Como não cair: Comprovação vem de evidências ou de auditoria independente. Declaração não comprova e código-fonte é desproporcional.

⚠ **Alerta de prova:** Achar que o relatório de auditoria independente do fornecedor transfere toda a responsabilidade legal.
Como não cair: O objetivo é obter evidência dos controles do fornecedor; a responsabilidade não é toda transferida.

⚠ **Alerta de prova:** Confundir varredura de vulnerabilidades autenticada com teste de penetração.
Como não cair: A varredura não tenta explorar as falhas. Tentar invadir com conhecimento limitado do ambiente é pentest com conhecimento parcial.

⚠ **Alerta de prova:** Tratar a exceção formal ao padrão como eliminação do risco ou como transferência.
Como não cair: Na exceção o risco continua; é aceitação controlada, com aprovação, prazo e revisão.

⚠ **Alerta de prova:** Dizer que due care acontece só antes do contrato.
Como não cair: É o contrário: due diligence investiga e avalia; due care é agir de forma responsável e manter os controles.

⚠ **Alerta de prova:** Comprar o controle na hora mesmo quando ele custa mais que a perda anual que evitaria, ou ignorar a ALE.
Como não cair: A ALE é base da decisão. Controle mais caro que a perda esperada pode não se justificar.

⚠ **Alerta de prova:** Nas regras de engajamento do pentest, desligar o monitoramento, entregar senhas de todos os administradores ou definir o resultado esperado.
Como não cair: Regras de engajamento definem por escrito escopo, métodos permitidos, horários e contatos de emergência. Monitoramento não se desliga e resultado não se define antes.

⚠ **Alerta de prova:** Marcar 'ambiente de produção simulado' ou 'ambiente sem autorização' como tipo de pentest.
Como não cair: A classificação por conhecimento é conhecido, parcialmente conhecido e desconhecido. Teste sem autorização não é legítimo.

Como cai na prova

📝 **Como cai:** Enunciado dá valor do ativo, fator de exposição e frequência e pede a ALE.
Como resolver: 1) Calcule SLE = AV x EF. 2) Converta a frequência em ARO por ano (uma vez em quatro anos = 0,25). 3) Multiplique SLE x ARO. As alternativas erradas costumam ser a SLE pura, a soma ou a divisão.

📝 **Como cai:** Cenário descreve uma ação da empresa diante de um risco e pergunta a estratégia.
Como resolver: Pergunte: houve controle (mitigar), seguro ou terceiro assumindo o impacto (transferir), desistência da atividade (evitar) ou decisão formal de conviver com o risco (aceitar)?

📝 **Como cai:** Cenário de contrato pergunta qual documento ou cláusula atende.
Como resolver: Identifique o verbo: intenção (MOU), termos gerais (MSA), trabalho específico (SOW), meta de desempenho (SLA), sigilo (NDA), inspecionar (direito de auditoria), subcontratação (aprovação prévia).

📝 **Como cai:** Resultado ruim em simulação de phishing ou programa de conscientização pergunta a próxima ação.
Como resolver: Descarte punir, expor nomes, bloquear e-mail e suspender simulações. Escolha treinar (de forma direcionada) e medir com métricas de comportamento.

📝 **Como cai:** Cenário descreve quem avalia os controles e pede o tipo de avaliação.
Como resolver: Regulador inspecionando = exame regulatório externo; terceiro independente = auditoria externa; própria equipe com questionário = autoavaliação interna; amostra de mudanças do ano = auditoria interna de processo.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Perda por evento e quantas vezes por ano ocorre	**ALE = SLE x ARO**
Valor do ativo e percentual que seria destruído	**SLE = AV x EF**
Nível de risco que a empresa está disposta a aceitar para atingir objetivos	**Apetite a risco**
Risco acima de certo valor precisa de aprovação do conselho para ser aceito	**Tolerância a risco com limite de aprovação**
Contratar seguro contra ataques	**Transferir o risco**
Acordo geral para vários serviços futuros, detalhados depois	**MSA**
Documento sem valor jurídico registrando intenções	**MOU**
Fornecedor deve restabelecer o serviço em até X horas	**SLA**
Inspecionar os controles do fornecedor quando quiser	**Direito de auditoria (right-to-audit)**
Equipe de pentest recebe diagramas e credenciais / só a lista de IPs / nada	**Ambiente conhecido / parcialmente conhecido / desconhecido**
Diretor da empresa é sócio do fornecedor	**Conflito de interesses na seleção**
Quem decide finalidades e meios do tratamento	**Controlador**
Empresa processa pagamentos com cartão	**PCI DSS**
Titular pede cópia dos dados / pede que apaguem tudo	**Direito de acesso / direito à eliminação**

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

- ALE = SLE x ARO e SLE = AV x EF; frequência menor que anual vira fração.
- Seguro é transferir; controle é mitigar; desistir é evitar; exceção formal é aceitar com prazo.
- Proprietário decide classificação e acesso; custodiante aplica os controles; controlador decide finalidade; operador executa.
- Questionário de fornecedor precisa de evidência ou auditoria independente; obrigações do fornecedor vão no contrato.
- Conscientização se corrige com treino direcionado e métricas, nunca com punição ou fim das simulações.

Essenciais para a prova (checklist)

- ☐ Sei calcular SLE e ALE, inclusive com ARO fracionário.
- ☐ Sei distinguir política, norma (standard), procedimento e diretriz.
- ☐ Sei classificar uma ação como aceitar, mitigar, transferir ou evitar.
- ☐ Sei diferenciar MTD, RTO, RPO, MTTR e MTBF.
- ☐ Sei para que servem MSA, SOW, SLA, MOU, NDA e BPA.
- ☐ Sei os papéis proprietário, custodiante, controlador, operador, titular e encarregado.
- ☐ Sei classificar pentest por conhecimento (conhecido, parcial, desconhecido) e por tipo (ofensivo, defensivo, integrado, físico).
- ☐ Sei diferenciar reconhecimento passivo e ativo.
- ☐ Sei listar consequências da não conformidade e os direitos do titular.
- ☐ Sei as etapas de um programa de conscientização e como medir sua eficácia.

Questões de revisão do capítulo

R4.1 · Gestão e Supervisão do Programa de Segurança

Qual papel é responsável pela guarda e pelos controles técnicos dos dados, conforme definido pelo proprietário?

A. O controlador dos dados
B. O custodiante dos dados
C. O auditor externo
D. O titular dos dados

R4.2 · Gestão e Supervisão do Programa de Segurança

Um pentest é feito sem que a equipe de testes receba informações sobre o ambiente, como um atacante externo. Qual tipo de ambiente é esse?

A. Ambiente conhecido
B. Ambiente parcialmente conhecido
C. Ambiente desconhecido
D. Ambiente de produção simulado

R4.3 · Gestão e Supervisão do Programa de Segurança

Uma empresa deixa de cumprir uma obrigação contratual de segurança com um grande cliente, que decide rescindir o contrato. Que consequência é essa?

A. Redução do risco de terceiros envolvidos
B. Certificação automática de conformidade
C. Aumento de receita no trimestre seguinte
D. Impacto contratual com perda do cliente

R4.4 · Gestão e Supervisão do Programa de Segurança

Uma empresa mede se o número de incidentes causados por erro humano caiu após o programa de conscientização. O que essa medição mostra?

A. O número de servidores ativos
B. A eficácia do programa
C. O custo das licenças de software
D. A velocidade da rede interna

Respostas comentadas

R4.1. B) O custodiante dos dados

Por quê: O custodiante (ou steward) aplica os controles definidos pelo proprietário.

✗ A) Incorreta. Decide finalidades e meios.
✗ C) Incorreta. Avalia os controles.
✗ D) Incorreta. É a pessoa a quem os dados se referem.

> **Dica de prova:** Guarda e controles técnicos: custodiante.

R4.2. C) Ambiente desconhecido

Por quê: Conhecido, parcialmente conhecido e desconhecido substituem white, gray e black box.

✗ A) Incorreta. O testador recebe todas as informações.

✗ B) Incorreta. O testador recebe parte das informações.

✗ D) Incorreta. Não é classificação de conhecimento.

> **Dica de prova:** Sem informações: ambiente desconhecido.

R4.3. D) Impacto contratual com perda do cliente

Por quê: Consequências de não conformidade incluem multas, sanções, reputação, perda de licença e impactos contratuais.

✗ A) Incorreta. Não é consequência.

✗ B) Incorreta. Não é consequência.

✗ C) Incorreta. Não é consequência.

> **Dica de prova:** Cliente rescinde: impacto contratual.

R4.4. B) A eficácia do programa

Por quê: Métricas de resultado mostram se o programa reduz riscos humanos.

✗ A) Incorreta. Não tem relação.

✗ C) Incorreta. Não tem relação.

✗ D) Incorreta. Não tem relação.

> **Dica de prova:** Menos erro humano: programa eficaz.

05

CAPÍTULO 5 · 28% DA PROVA

Operações de Segurança

É o domínio de maior peso, então preciso dele afiado: hardening e linhas de base, gestão de ativos, ciclo de gestão de vulnerabilidades (CVE, CVSS, falso positivo e negativo), monitoramento (SIEM, SOAR, XDR, EDR, UEBA, NetFlow, PCAP), resposta a incidentes e forense, IAM e controle de acesso (RBAC, ABAC, MAC, DAC, MFA, SSO, federação, OAuth, PAM), segurança de e-mail (SPF, DKIM, DMARC), filtros web, MDM, Wi-Fi e protocolos seguros. A prova descreve uma necessidade operacional e pede a ferramenta ou a próxima fase. Onde mais erro: a ordem das fases de resposta a incidentes, SIEM x SOAR, NetFlow x PCAP e o que conta como MFA de verdade.

Neste capítulo
18 tópicos-chave · 14 pegadinhas · 8 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Hardening e linha de base segura

Hardening desativa serviços não usados, troca senhas padrão, fecha portas e aplica patches. Linhas de base seguras (baselines) garantem que todo servidor novo nasça com a mesma configuração aprovada, verificada com benchmarks do CIS e SCAP. Em equipamentos de rede: administração só por SSH, pela rede de gerência e com contas individuais. GPO aplica configurações centralizadas no domínio Windows.

Gestão de ativos

Ciclo: aquisição (fornecedores confiáveis, firmware verificado), atribuição (dono e classificação), inventário, monitoramento e rastreamento (descoberta contínua evita servidores esquecidos sem patch) e descarte. Descarte inclui retenção pelo prazo legal, sanitização ou destruição com método adequado à mídia e certificado. Apagar só a pasta de documentos não sanitiza: os dados podem ser recuperados.

Ciclo de gestão de vulnerabilidades

Identificar (varredura autenticada, bug bounty, divulgação responsável, monitoramento de pacotes e SBOM), analisar e priorizar (CVE identifica, CVSS mede a gravidade, contexto do ativo e fator de exposição ajustam), responder (patch, seguro, segmentação, controle compensatório, exceção documentada com prazo), validar (nova varredura, auditoria) e relatar (métricas de correção no prazo).

Falso positivo e falso negativo

Falso positivo aponta falha que não existe e consome tempo. Falso negativo deixa de apontar falha real e é o mais perigoso, pois dá falsa sensação de segurança. Varreduras autenticadas encontram mais vulnerabilidades e geram menos falsos positivos.

SIEM, SOAR e XDR

SIEM agrega e normaliza logs, correlaciona eventos e gera alertas. SOAR complementa o SIEM com automação e orquestração de resposta a partir de playbooks (isolar máquina, abrir chamado). XDR correlaciona endpoints, rede, nuvem e e-mail numa plataforma de detecção e resposta.

EDR, UEBA, FIM e sandbox

EDR vai além do antivírus por assinatura: detecção comportamental e isolamento remoto do endpoint. UBA/UEBA detecta desvio do padrão do usuário (baixar gigabytes à noite). FIM compara hashes de arquivos críticos e alerta sobre alterações. Sandbox executa anexos suspeitos isolados para observar o comportamento.

Atividades de monitoramento

Agregação, normalização, alertas, varredura, relatórios e arquivamento de logs. Tuning (ajuste fino) cria exceções para processos legítimos e reduz a fadiga de alertas. Quarentena isola a estação, por exemplo em VLAN isolada. Agentes que param de reportar ao console podem indicar desativação ou adulteração por atacante. Coleta pode ser com agente ou sem agente.

Fontes de dados

Logs do SO (no Windows, falha de login é o evento 4625), de aplicação, firewall, IPS/IDS, proxy (sites acessados) e DNS (comunicação com C2). NetFlow resume conexões por origem, destino, portas e volume, sem conteúdo. Captura de pacotes (PCAP) guarda o conteúdo exato. Dashboard dá visão resumida em tempo real.

Resposta a incidentes

Sequência: preparação, detecção, análise, contenção, erradicação, recuperação e lições aprendidas. Depois de identificar a máquina infectada, contenha. Erradicação remove malware e contas do invasor. Recuperação restaura e monitora. Testes: tabletop (discussão) e simulação (aciona equipes e ferramentas). Threat hunting busca invasores proativamente por hipóteses; MITRE ATT&CK classifica táticas e técnicas.

Forense digital

Legal hold preserva dados para processo e se sobrepõe à retenção. Aquisição faz cópia bit a bit sem mexer no original; o hash da imagem prova que a evidência não mudou. Preservação guarda com controle de acesso e hash, e a cadeia de custódia documentada garante a admissibilidade. Ordem de volatilidade: primeiro registradores, cache e memória RAM; mídias de arquivo e fitas por último. E-discovery localiza e entrega documentos eletrônicos pedidos pela justiça.

Ciclo de identidade (IAM)

Identity proofing (documento e selfie) vem antes do provisionamento. Provisionamento com aprovação do gestor e revisão periódica de acessos evita privilege creep. Offboarding revoga os acessos de imediato. Automação a partir do sistema de RH reduz erros. SSO usa SAML ou OpenID Connect; federação aceita a credencial da organização parceira; OAuth 2.0 autoriza acesso delegado à API sem entregar a senha.

Modelos de controle de acesso

RBAC: permissões por função ou grupo; ao mudar de cargo, troca-se o papel. ABAC: atributos de usuário, recurso e ambiente (departamento, local, horário), o mais granular. MAC: rótulos e habilitação definidos pela organização, comum em ambientes militares. DAC: o dono decide. Restrições por horário e localização complementam esses modelos.

MFA e passwordless

Fatores: algo que sabe (senha, PIN, pergunta secreta), algo que tem (token de hardware, app autenticador), algo que é (biometria) e onde está (localização). MFA exige tipos diferentes. FIDO2 e passkeys permitem autenticação sem senha e resistente a phishing. Gerenciador de senhas garante senhas longas e únicas, mas não dispensa MFA.

Gestão de acesso privilegiado (PAM)

Privilégio elevado só quando preciso, por tempo limitado e com registro (just-in-time), cofre de senhas com rotação automática após o uso, credenciais efêmeras criadas e descartadas no acesso e gravação de sessões. Contas compartilhadas, senhas sem expiração e chaves no código são o oposto.

Segurança de e-mail e web

SPF e DKIM verificam se o e-mail veio do domínio informado; DMARC define a política (none, quarantine, reject) e envia relatórios. Gateway de e-mail coloca anexos executáveis em quarentena e analisa URLs. Filtros web usam categorização, reputação e varredura de URL; podem ser por proxy central ou por agente (protege fora da rede). Filtragem de DNS bloqueia domínios maliciosos sem inspecionar conteúdo.

Dispositivos móveis e sem fio

MDM aplica PIN, criptografia, limpeza remota, lista de permissão de aplicativos e bloqueia aparelhos fora de conformidade. BYOD (aparelho do funcionário) usa contêiner corporativo; COPE é da empresa com uso pessoal. WPA3-Personal usa SAE e serve sem RADIUS; WPA3-Enterprise usa 802.1X para credencial individual. Site survey com mapa de calor e ajuste de posição e potência dos APs evitam vazamento de sinal.

Protocolos seguros e controle de rede

SSH no lugar de Telnet, SFTP (porta 22) no lugar de FTP (21), HTTPS (443), SNMPv3 com autenticação e cifra, LDAPS (636) no lugar de LDAP (389). Traps SNMP avisam proativamente. NAC verifica a postura (antivírus, patches) antes de liberar a rede, com agente permanente, dissolúvel ou sem agente. Port security por MAC restringe dispositivos por porta. Firewall stateful só deixa voltar resposta de conexão iniciada de dentro.

Desenvolvimento seguro e automação

SAST analisa o código sem executar; DAST testa a aplicação em execução; fuzzing envia entradas aleatórias e malformadas. Validação de entrada deve ser no servidor, com lista de permissão de formato. Cookies de sessão usam HttpOnly, Secure e SameSite. Code signing prova autenticidade e integridade. Automação acelera a resposta e aplica guardrails, mas traz complexidade, custo, ponto único de falha e dívida técnica.

Macetes para memorizar

💡 Fases de resposta a incidentes

P-D-A-C-E-R-L: Preparar, Detectar, Analisar, Conter, Erradicar, Recuperar, Lições.

💡 Ordem de volatilidade

Colete primeiro o que some primeiro: CPU e RAM, depois disco, por último fita.

💡 Fatores de autenticação

Sei, tenho, sou, estou. MFA = pelo menos dois verbos diferentes.

💡 Modelos de acesso

DAC = Dono; MAC = Mandatório por rótulo; RBAC = cargo (Role); ABAC = Atributos.

💡 SAST x DAST

Static = Sem rodar; Dynamic = rodando.

💡 E-mail

SPF e DKIM checam a origem; DMARC é o chefe: decide (none, quarantine, reject) e pede relatório.

💡 Portas

22 SSH/SFTP, 25 SMTP, 53 DNS, 443 HTTPS, 636 LDAPS, 3389 RDP.

💡 Dispositivos móveis

BYOD = Bring Your Own (é seu); COPE = Corporate Owned (é da empresa, com uso pessoal).

Tabela de memorização: não confunda

Quando é...	...e quando é
IDS Detectar e alertar sem interferir no tráfego.	**IPS** Detectar e bloquear o tráfego malicioso automaticamente, em linha.
SIEM Agregar logs e correlacionar alertas repetidos de várias ferramentas num só lugar.	**SOAR** Automatizar a resposta com playbooks, como isolar a máquina e abrir chamado.

NetFlow Ver volumes e padrões de tráfego entre hosts sem guardar o conteúdo.	**Captura de pacotes (PCAP)** Reconstruir exatamente o que foi transmitido, com conteúdo.
Falso positivo A ferramenta aponta uma falha que não existe.	**Falso negativo** A ferramenta não detecta uma falha real, que depois é explorada.
SAST Analisar o código-fonte antes de ser executado.	**DAST** Testar a aplicação em execução enviando requisições como um atacante.
DAC O próprio dono define com quem compartilha seus arquivos.	**MAC** A organização impõe o acesso por rótulos e níveis de habilitação, não o dono.
WPA3-Personal Pequena empresa sem servidor RADIUS; senha forte compartilhada com SAE.	**WPA3-Enterprise** Cada funcionário autentica com suas próprias credenciais via 802.1X e RADIUS.

Números que caem

Item	Valor
Peso do domínio no exame	**28% (o maior)**
Evento do Windows para falha de login	**4625**
SSH / SFTP	**Porta 22**
FTP	**Porta 21**
SMTP	**Portas 25 ou 587**
DNS	**Porta 53**
HTTPS	**Porta 443**
LDAP / LDAPS	**389 / 636**
RDP	**Porta 3389**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Depois de identificar a máquina infectada, partir para recuperação ou lições aprendidas.
Como não cair: A próxima fase é contenção. Recuperação só vem depois da erradicação; lições aprendidas fecham o ciclo.

⚠ **Alerta de prova:** Desligar da tomada, reiniciar ou formatar a estação comprometida para conter o malware.
Como não cair: Desligar perde dados voláteis e formatar destrói evidências. Isole a estação da rede mantendo-a ligada.

⚠ **Alerta de prova:** Validar a entrada só no navegador ou exibir mensagens de erro detalhadas.
Como não cair: Validação no cliente pode ser contornada; deve ser no servidor. Erros detalhados ajudam o atacante.

⚠ **Alerta de prova:** Com CVSS 9,8 em sistema isolado e sem dados sensíveis, tratar como falso positivo ou ignorar o CVSS.
Como não cair: A falha é real e a gravidade importa; ajuste a prioridade pelo ambiente.

⚠ **Alerta de prova:** Ignorar ou apagar o achado quando já existe controle que impede a exploração.
Como não cair: Registre o controle compensatório e reavalie o risco; apagar perde rastreabilidade.

⚠ **Alerta de prova:** Contar PIN mais senha, senha mais pergunta secreta ou dois códigos no mesmo e-mail como MFA.
Como não cair: São fatores do mesmo tipo ou dependem da mesma posse. MFA de verdade: senha mais código do app autenticador.

⚠ **Alerta de prova:** No RBAC, somar o papel de gerente ao de analista quando o usuário é promovido.
Como não cair: Somar gera acúmulo de privilégios (privilege creep). Troque o papel.

⚠ **Alerta de prova:** Escolher SAML 1.0, LDAP ou RADIUS para o app acessar outra API em nome do usuário.
Como não cair: Acesso delegado sem senha é OAuth 2.0; OpenID Connect acrescenta autenticação.

⚠ **Alerta de prova:** Com excesso de alertas, desligar o SIEM ou gerar ainda mais alertas.
Como não cair: Ajuste regras e limites (tuning) e crie exceções para processos legítimos.

⚠ **Alerta de prova:** Achar que criptografar as caixas de e-mail preserva mensagens pedidas pela justiça.
Como não cair: Criptografia não impede a exclusão. Use legal hold, que se sobrepõe à retenção.

⚠ **Alerta de prova:** Escolher NetFlow quando o analista precisa do conteúdo da conexão.
Como não cair: NetFlow não guarda conteúdo; use PCAP.

⚠ **Alerta de prova:** Trocar SNMPv2c por SNMPv1, ou usar Telnet ou TFTP para gerência.
Como não cair: SNMPv1 é ainda mais inseguro; Telnet e TFTP não cifram. Use SNMPv3 com autenticação e cifra.

⚠ **Alerta de prova:** Marcar NAC com agente permanente quando o visitante não pode instalar software.
Como não cair: Sem software permanente é NAC agentless.

⚠ **Alerta de prova:** Achar que automação elimina supervisão humana, documentação ou custo.
Como não cair: Automação acelera a resposta, mas mantém supervisão e traz dívida técnica e risco de ponto único de falha.

Como cai na prova

📝 **Como cai:** Cenário de incidente em andamento pergunta a próxima fase.
Como resolver: Localize onde o enunciado parou (identificou? removeu? restaurou?) e avance uma casa em preparação, detecção, análise, contenção, erradicação, recuperação, lições aprendidas.

📝 **Como cai:** Necessidade de monitoramento pede a ferramenta certa.
Como resolver: Correlacionar = SIEM; automatizar resposta = SOAR; várias fontes com resposta = XDR; endpoint com isolamento = EDR; desvio de comportamento = UEBA; arquivo crítico alterado = FIM; conteúdo do tráfego = PCAP; padrões sem conteúdo = NetFlow.

📝 **Como cai:** Descrição de acesso pede o modelo ou a solução de identidade.
Como resolver: Quem decide? Dono (DAC), organização por rótulo (MAC), função (RBAC), atributos e contexto (ABAC). Login único = SSO; credencial de outra empresa = federação; delegação de API = OAuth.

📝 **Como cai:** Resultado de varredura pede a ação certa.
Como resolver: Priorize por CVSS mais contexto do ativo; sem patch use compensatório, seguro ou exceção com prazo; depois do patch, nova varredura para validar.

📝 **Como cai:** Evidência para processo judicial.
Como resolver: Preservar com legal hold, adquirir por cópia bit a bit, calcular hash, manter cadeia de custódia documentada e seguir a ordem de volatilidade.

📝 **Como cai:** Questão de 'Escolha DUAS' sobre e-mail ou fontes de dados.
Como resolver: Descarte registros DNS que não autenticam (MX, PTR, CNAME, AAAA, NS) e fontes não técnicas (organograma, planilha de férias, contrato). Sobram SPF, DKIM, DMARC ou logs de firewall, proxy e DNS.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Evento 4625 em investigação de força bruta	**Log de segurança do sistema operacional**
Rejeitar e-mail que falha em SPF e DKIM e receber relatórios	**DMARC**
Documento e selfie antes de abrir a conta	**Identity proofing**
Usuário do parceiro entra com as credenciais da própria organização	**Federação de identidades**
App acessa API de terceiro em nome do usuário sem a senha	**OAuth 2.0**
Privilégio elevado só quando precisar, por tempo limitado e com registro	**PAM / just-in-time**
Acesso decidido por departamento, localização e horário	**ABAC**
Nível de habilitação definido pela organização, não pelo dono	**MAC**
Usuário que baixava pouco passa a baixar gigabytes à noite	**UBA/UEBA**
Busca proativa por invasores com base em hipóteses	**Threat hunting**
Cópia bit a bit do disco sem mexer no original	**Aquisição forense**
Processo judicial exige preservar e-mails	**Legal hold**
Notebook sem antivírus atualizado não pode entrar na rede	**NAC**
Bancos membros trocando indicadores de ataque	**ISAC**

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

- Identificou o incidente: conter. Removeu o invasor: erradicação. Restaurou e monitorou: recuperação.
- Máquina comprometida se isola da rede ligada; nada de desligar, reiniciar ou formatar.
- Falso negativo é o erro mais perigoso da varredura.
- MFA exige fatores de tipos diferentes; PIN mais senha não é MFA.
- SIEM correlaciona; SOAR executa playbooks.

Essenciais para a prova (checklist)

- ☐ Sei a ordem das fases de resposta a incidentes.
- ☐ Sei aplicar ordem de volatilidade, cadeia de custódia, legal hold e e-discovery.
- ☐ Sei o ciclo de gestão de vulnerabilidades e como priorizar com CVSS e contexto.
- ☐ Sei diferenciar SIEM, SOAR, XDR, EDR, UEBA e FIM.
- ☐ Sei escolher entre NetFlow, PCAP, logs de proxy, DNS e do SO.
- ☐ Sei diferenciar RBAC, ABAC, MAC e DAC.
- ☐ Sei montar uma combinação válida de MFA e quando usar SSO, federação e OAuth.
- ☐ Sei o papel de SPF, DKIM e DMARC.
- ☐ Sei as portas dos protocolos seguros e suas alternativas inseguras.
- ☐ Sei diferenciar BYOD e COPE e o que o MDM aplica.

Questões de revisão do capítulo

R5.1 · Operações de Segurança

Uma empresa quer que um e-mail que falhe nas verificações SPF e DKIM seja rejeitado e que o dono do domínio receba relatórios. Qual mecanismo define isso?

A. Registro PTR reverso
B. Registro TXT de verificação
C. Política DMARC do domínio
D. Registro MX secundário

R5.2 · Operações de Segurança

Qual é um benefício da automação de tarefas de segurança repetitivas?

A. Resposta mais rápida a incidentes
B. Redução garantida do custo a zero
C. Fim da necessidade de documentação
D. Eliminação de toda a supervisão humana

R5.3 · Operações de Segurança

Uma empresa quer que os administradores usem credenciais temporárias, criadas no momento do acesso e descartadas logo depois. Que conceito é esse?

A. Senhas sem expiração
B. Contas genéricas fixas
C. Chaves gravadas em código
D. Credenciais efêmeras

R5.4 · Operações de Segurança

Uma varredura de vulnerabilidades não detectou uma falha crítica que existia no servidor e foi explorada depois. Como se chama esse erro da ferramenta?

A. Falso negativo da varredura
B. Verdadeiro positivo confirmado
C. Falso positivo da varredura
D. Verdadeiro negativo correto

Respostas comentadas

R5.1. C) Política DMARC do domínio

Por quê: DMARC define a política (none, quarantine, reject) e envia relatórios.

✗ A) Incorreta. Faz resolução reversa.
✗ B) Incorreta. Serve para validar domínio.
✗ D) Incorreta. Define recebimento.

> **Dica de prova:** Rejeitar e receber relatórios: DMARC.

R5.2. A) Resposta mais rápida a incidentes

Por quê: Benefícios: eficiência, aplicação de linhas de base, escala segura, tempo de reação e multiplicação da força de trabalho.

✗ B) Incorreta. Automação tem custo.
✗ C) Incorreta. A documentação continua necessária.
✗ D) Incorreta. A supervisão continua necessária.

> **Dica de prova:** Automação: resposta mais rápida.

R5.3. D) Credenciais efêmeras

Por quê: PAM moderno usa acesso just-in-time, cofres de senhas e credenciais efêmeras.

✗ A) Incorreta. Aumentam o risco.
✗ B) Incorreta. Impedem a rastreabilidade.
✗ C) Incorreta. Podem vazar.

> **Dica de prova:** Criada e descartada no uso: efêmera.

R5.4. A) Falso negativo da varredura

Por quê: Falsos negativos são perigosos porque dão falsa sensação de segurança.

✗ B) Incorreta. Apontaria uma falha real.
✗ C) Incorreta. Apontaria uma falha inexistente.
✗ D) Incorreta. Não haveria falha.

> **Dica de prova:** Não detectou falha real: falso negativo.

DIA DA PROVA

Estratégia de prova

O CompTIA Security+ SY0-701 traz cenários curtos do dia a dia de segurança e pede a melhor ação, ferramenta, controle ou conceito para aquela situação específica. As alternativas erradas costumam ser termos reais do próprio exame que resolvem outro problema (IDS no lugar de IPS, RTO no lugar de RPO, SIEM no lugar de SOAR), além de distratores absurdos ou radicais (desligar o firewall, punir usuários, expor na Internet). Pistas literais no enunciado ('voltar em minutos', 'sem interagir com os sistemas', 'troca o ID na URL') definem a resposta. Há questões de 'Escolha DUAS' e questões baseadas em desempenho (PBQ), em que é preciso aplicar o conceito, não só reconhecê-lo.

Como responder

✓ Planeje o tempo: são até 90 questões em 90 minutos, cerca de um minuto por item; não trave em PBQ, marque e volte no fim.

✓ A aprovação é com 750 numa escala de 100 a 900; foque em acertar com consistência os domínios de maior peso: Operações de Segurança (28%), Ameaças, Vulnerabilidades e Mitigações (22%) e Gestão e Supervisão (20%), sem largar Arquitetura (18%) e Conceitos Gerais (12%).

✓ Grife o requisito do enunciado (tempo, perda de dados, bloquear x alertar, quem decide) antes de ler as alternativas; a resposta certa atende exatamente esse requisito.

✓ Para cada par de termos parecidos nas alternativas, pergunte qual problema cada um resolve; a errada quase sempre é um termo real aplicado ao cenário errado.

✓ Descarte primeiro as alternativas que aumentam a exposição (desligar logs, abrir portas, dar admin a todos, expor na Internet) ou que são punitivas e desproporcionais.

✓ Em 'Escolha DUAS', avalie cada alternativa isoladamente como verdadeira ou falsa para o cenário; normalmente as duas certas se complementam (MFA e bloqueio; isolar e segmentar).

✓ Em questões de cálculo de risco, escreva a fórmula (SLE = AV x EF; ALE = SLE x ARO) e converta a frequência em ARO anual antes de olhar as opções.

✓ Em sequência de processos (resposta a incidentes, gestão de vulnerabilidades, gestão de mudanças), localize em que etapa o cenário parou e avance só uma casa.

Erros que derrubam candidatos

✗ Confundir IDS com IPS, SIEM com SOAR e NetFlow com PCAP por ler rápido demais.

✗ Trocar RTO, RPO e MTD, ou responder a SLE quando a pergunta pede a ALE.

✗ Pular a contenção e ir direto para recuperação, ou desligar e formatar a máquina e destruir evidências.

✗ Classificar controle só pela metade (acertar 'técnico' e errar 'preventivo') ou chamar câmera sem gravação de detectiva.

✗ Achar que hash ou assinatura digital garantem sigilo, ou usar hash onde o dado precisa ser recuperado (tokenização).

✗ Escolher a alternativa mais 'forte' em vez da adequada: bloquear todo o e-mail, punir quem clicou, aplicar todos os patches de uma vez em ICS.

✗ Confundir XSS com CSRF e password spraying com força bruta em uma conta.

Na semana da prova

- ☐ Faça simulados completos cronometrados em 90 minutos e revise cada erro pelo motivo da alternativa errada, não só pela certa.
- ☐ Revise os pares que mais derrubam: IDS x IPS, SIEM x SOAR, RTO x RPO, incremental x diferencial, XSS x CSRF, DAC x MAC, dissuasivo x detectivo.
- ☐ Treine de novo as contas de SLE e ALE com ARO fracionário até sair sem pensar.
- ☐ Memorize a ordem das fases de resposta a incidentes, a ordem de volatilidade e as portas dos protocolos seguros.
- ☐ Na véspera, leia só os blocos 'lembrar' e 'pegadinhas' de cada domínio e durma bem; no dia, chegue cedo e mantenha o ritmo de cerca de um minuto por item.

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 Mitigações

‣ Login em outro país minutos depois de login no Brasil → **Viagem impossível**

‣ '../../etc/passwd' na URL → **Travessia de diretório**

‣ ' OR '1'='1 no campo de login → **Injeção de SQL**

‣ Servidor web busca o serviço de metadados da nuvem → **SSRF**

‣ Trocar o número do ID na URL mostra outro cliente → **IDOR / falha de autorização**

⚠ Ataque offline não gera tentativas de login no sistema. Mesma senha em muitas contas é password spraying.

⚠ Reaproveitar senhas vazadas é credential stuffing; MFA e proibição de reutilização mitigam.

⚠ Typosquatting registra domínio parecido e espera o erro de digitação. Envenenamento altera as respostas de resolução de nomes.

2. Arquitetura de Segurança

‣ Operações voltam em minutos em outro local equipado e sincronizado → **Hot site**

‣ Local com energia, rede e alguns servidores, mas precisa restaurar dados → **Warm site**

‣ Copia apenas o que mudou desde o último backup de qualquer tipo → **Incremental**

‣ Backup que ransomware não altera nem apaga, mesmo com admin comprometido → **Armazenamento imutável ou offline**

‣ Inspecionar HTTPS e identificar aplicações → **NGFW**

⚠ RAID 0 e JBOD não têm redundância. Dois discos gravados ao mesmo tempo é RAID 1.

⚠ O IDS também faz isso. A capacidade exclusiva do IPS em linha é bloquear o ataque.

⚠ Hash não permite recuperar o número. Para cobrar depois, use tokenização.

3. Conceitos Gerais de Segurança

‣ Aprovador não consegue negar depois que aprovou → **Não repúdio (assinatura digital)**

‣ Registrar quais ações o usuário executou depois de entrar → **Contabilização (accounting)**

‣ Usuário autenticado pode apenas ler, sem editar → **Autorização**

‣ Valor aleatório diferente por senha antes do hash → **Salt**

‣ Hash aplicado milhares de vezes para fortalecer senha → **Key stretching (PBKDF2, bcrypt, Argon2)**

⚠ SHA e MD5 são hashes, não cifram; MD5 está quebrado. Simétrico padrão é AES; RSA é assimétrico.

⚠ Cifrar protege o sigilo, não a integridade. Para verificar alteração, compare o hash.

⚠ Assinatura prova autoria e integridade. Sigilo exige criptografia; malware exige outra verificação.

4. Gestão e Supervisão do Programa de Segurança

‣ Perda por evento e quantas vezes por ano ocorre → **ALE = SLE x ARO**

‣ Valor do ativo e percentual que seria destruído → **SLE = AV x EF**

‣ Nível de risco que a empresa está disposta a aceitar para atingir objetivos → **Apetite a risco**

‣ Risco acima de certo valor precisa de aprovação do conselho para ser aceito → **Tolerância a risco com limite de aprovação**

‣ Contratar seguro contra ataques → **Transferir o risco**

⚠ ALE = SLE x ARO, sempre multiplicação: R$ 50 mil x 2 = R$ 100 mil.

⚠ Converta a frequência: ARO = 1/4 = 0,25. Com AV de R$ 400 mil e EF de 25%, a SLE é R$ 100 mil e a ALE é R$ 25 mil.

⚠ Controle técnico ou físico que reduz probabilidade ou impacto é mitigar. Transferir seria contratar seguro; evitar seria deixar de ter o datacenter.

5. Operações de Segurança

‣ Evento 4625 em investigação de força bruta → **Log de segurança do sistema operacional**

‣ Rejeitar e-mail que falha em SPF e DKIM e receber relatórios → **DMARC**

‣ Documento e selfie antes de abrir a conta → **Identity proofing**

‣ Usuário do parceiro entra com as credenciais da própria organização → **Federação de identidades**

▸ App acessa API de terceiro em nome do usuário sem a senha → **OAuth 2.0**

⚠ A próxima fase é contenção. Recuperação só vem depois da erradicação; lições aprendidas fecham o ciclo.

⚠ Desligar perde dados voláteis e formatar destrói evidências. Isole a estação da rede mantendo-a ligada.

⚠ Validação no cliente pode ser contornada; deve ser no servidor. Erros detalhados ajudam o atacante.

GABARITO

Respostas do diagnóstico

D1. A) Escape de máquina virtual → revise o capítulo 1

Por quê: Vulnerabilidades de virtualização incluem VM escape e reutilização de recursos.

✗ B) Incorreta. Expõe dados deixados em memória ou disco.
✗ C) Incorreta. Afeta consultas a bancos.
✗ D) Incorreta. Decorre de ajustes errados.

> **Dica de prova:** Sair da VM para o host: VM escape.

D2. D) Credenciais padrão não alteradas → revise o capítulo 1

Por quê: Trocar credenciais padrão e fechar serviços expostos está entre as primeiras ações de hardening.

✗ A) Incorreta. Não é o problema principal aqui.
✗ B) Incorreta. Não é vulnerabilidade.
✗ C) Incorreta. Não expõe o acesso.

> **Dica de prova:** Senha de fábrica: credencial padrão.

D3. A) Envenenamento de ARP → revise o capítulo 1

Por quê: ARP poisoning permite ataques on-path na rede local; inspeção dinâmica de ARP ajuda a mitigar.

✗ B) Incorreta. Dispara por condição.
✗ C) Incorreta. É ataque físico.
✗ D) Incorreta. Explora funções de hash.

> **Dica de prova:** Tabela ARP alterada: envenenamento de ARP.

D4. D) Exercício de mesa (tabletop) → revise o capítulo 2

Por quê: Testes vão do tabletop à simulação e ao failover completo, com custo e risco crescentes.

✗ A) Incorreta. Busca falhas técnicas.
✗ B) Incorreta. Aciona sistemas reais.
✗ C) Incorreta. Move operações para outro local.

> **Dica de prova:** Discussão sem acionar sistemas: tabletop.

D5. C) Em uma zona desmilitarizada (DMZ) → revise o capítulo 2

Por quê: A DMZ fica entre a Internet e a rede interna, com regras de firewall próprias.

✗ A) Incorreta. Expõe a rede interna.
✗ B) Incorreta. Mistura funções críticas.
✗ D) Incorreta. Não é adequado para serviço público.

> **Dica de prova:** Servidor público separado: DMZ.

D6. C) Jump server → revise o capítulo 2

Por quê: Jump servers concentram e registram o acesso administrativo a redes protegidas.

✗ A) Incorreta. Gerencia impressoras.

✗ B) Incorreta. Envia e recebe mensagens.

✗ D) Incorreta. Distribui endereços IP.

> **Dica de prova:** Acesso administrativo intermediado: jump server.

D7. A) Integridade da informação → revise o capítulo 3

Por quê: Hashes, assinaturas e controles de acesso protegem a integridade.

✗ B) Incorreta. Trata do acesso quando necessário.

✗ C) Incorreta. Trata do sigilo.

✗ D) Incorreta. Trata de permissões.

> **Dica de prova:** Não foi alterada: integridade.

D8. B) Integridade do histórico → revise o capítulo 3

Por quê: O encadeamento de hashes torna o livro-razão resistente a adulteração.

✗ A) Incorreta. Não é a propriedade principal.

✗ C) Incorreta. Os registros podem ser públicos.

✗ D) Incorreta. Não é a propriedade principal.

> **Dica de prova:** Blocos encadeados por hash: integridade.

D9. D) Mudanças sem análise de impacto → revise o capítulo 3

Por quê: Mesmo mudanças emergenciais devem seguir um processo, ainda que acelerado.

✗ A) Incorreta. Não é consequência garantida.

✗ B) Incorreta. Ocorre o contrário.

✗ C) Incorreta. Não é consequência garantida.

> **Dica de prova:** Mudança sem autorização: risco de impacto não previsto.

D10. D) Política de uso aceitável (AUP) → revise o capítulo 4

Por quê: Políticas são obrigatórias e de alto nível; procedimentos detalham como executar tarefas.

✗ A) Incorreta. Não é obrigatório.

✗ B) Incorreta. Detalha passos técnicos específicos.

✗ C) Incorreta. Trata de desempenho de serviços.

> **Dica de prova:** Regras de uso dos recursos: AUP.

D11. D) Comportamento anômalo de risco → revise o capítulo 4

Por quê: Treinamentos ensinam a reconhecer comportamentos arriscados, inesperados ou não intencionais.

✗ A) Incorreta. Não é normal fotografar dados.
✗ B) Incorreta. Não tem relação.
✗ C) Incorreta. Não tem relação.

> **Dica de prova:** Fotografar dados: comportamento anômalo.

D12. B) Registrar o reconhecimento das políticas → revise o capítulo 4

Por quê: Atestação e reconhecimento de políticas fazem parte da conformidade e da conscientização.

✗ A) Incorreta. Não dispensa.
✗ C) Incorreta. Não substitui.
✗ D) Incorreta. Não garante.

> **Dica de prova:** Termo assinado: reconhecimento das políticas.

Agora, treine no formato real

Faça as 6 provas completas do curso CompTIA Security+ SY0-701: 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.