Strecht Simulados · Guia de preparação



Guia de preparação ISC2 CC

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

70%
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 ISC2 CC: 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 70%).

Mapa do exame

Cada prova do curso tem 100 questões e 120 minutos, no formato do exame. Referência de aprovação: 70%.

Domínio (capítulo)	Peso	Neste guia
1. Conceitos de gestão de identidade e acesso (IAM)	20%	18 conceitos · 14 pegadinhas
2. Conceitos de segurança de redes e nuvem	21,3%	18 conceitos · 14 pegadinhas
3. Governança de segurança	17,3%	18 conceitos · 14 pegadinhas
4. Operações de segurança e resposta a incidentes	17,3%	18 conceitos · 14 pegadinhas
5. Princípios de segurança	24%	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 · Conceitos de gestão de identidade e acesso (IAM)

Funcionários entram uma vez com a conta corporativa e acessam e-mail, CRM e portal de RH sem digitar outras senhas. Qual recurso é esse?

A. Logon único (SSO)
B. Rede local virtual
C. Negação implícita
D. Separação de funções

D2 · Conceitos de gestão de identidade e acesso (IAM)

O bloqueio rígido de contas após poucas tentativas passou a ser usado por atacantes para travar contas de propósito. Que alternativa equilibra segurança e disponibilidade?

A. Senhas iguais para facilitar o desbloqueio pelo suporte
B. Bloqueio permanente após a primeira senha digitada errada pelo usuário
C. Bloqueio temporário progressivo e detecção de padrões suspeitos
D. Desativação de qualquer limite de tentativas de login

D3 · Conceitos de gestão de identidade e acesso (IAM)

A empresa quer saber quantas contas privilegiadas existem e quem é responsável por cada uma. Qual é o primeiro passo?

A. Excluir as contas antigas do domínio sem análise
B. Dar a mesma senha às contas privilegiadas
C. Fazer um inventário das contas privilegiadas
D. Publicar as senhas no cofre sem controle de acesso

D4 · Conceitos de segurança de redes e nuvem

Em um data center, cada carga de trabalho só pode falar com as outras de que realmente precisa, com políticas individuais. Que técnica é essa?

A. Tradução de endereços
B. Roteamento estático
C. Rede plana única
D. Microssegmentação

D5 · Conceitos de segurança de redes e nuvem

Um funcionário precisa trabalhar no aeroporto usando o Wi-Fi público. Qual medida protege o tráfego dele?

A. Usar a mesma senha nos serviços acessados
B. Compartilhar a pasta de documentos na rede pública
C. Conectar à VPN corporativa antes de acessar sistemas
D. Desativar o firewall do notebook para conectar melhor

D6 · Conceitos de segurança de redes e nuvem

Os logs mostram um endereço externo testando milhares de portas dos servidores da empresa em poucos minutos. O que isso indica?

A. Varredura de portas para reconhecimento
B. Sincronização de horário por NTP
C. Atualização legítima do antivírus corporativo
D. Backup automático dos servidores

D7 · Governança de segurança

A empresa escolhe um funcionário de cada área para divulgar boas práticas e ser o ponto de contato com a equipe de segurança. Que iniciativa é essa?

A. Teste de intrusão de caixa-preta
B. Rede de embaixadores de segurança
C. Análise de impacto nos negócios
D. Plano de recuperação de desastres

D8 · Governança de segurança

O financeiro recebe um e-mail de um fornecedor conhecido informando nova conta bancária para pagamentos. O que a conscientização orienta?

A. Confirmar a mudança por telefone já cadastrado
B. Atualizar a conta e pagar no mesmo dia, sem consultar ninguém
C. Responder ao e-mail pedindo confirmação
D. Encaminhar o e-mail a todos os colegas

D9 · Governança de segurança

Qual métrica mostra o avanço da proteção das contas de maior risco?

A. Percentual de contas privilegiadas com MFA
B. Quantidade de contas criadas no último ano
C. Número de grupos de e-mail da empresa
D. Total de impressoras ligadas à rede

D10 · Operações de segurança e resposta a incidentes

Qual é o objetivo principal de um exercício de equipe vermelha (red team)?

A. Simular atacantes reais para testar detecção e resposta
B. Atender os chamados de suporte dos usuários
C. Configurar os firewalls e os servidores da empresa toda semana
D. Escrever as políticas de segurança da organização

D11 · Operações de segurança e resposta a incidentes

Uma ferramenta testa a aplicação web em execução, enviando entradas maliciosas como faria um atacante. Que tipo de teste é esse?

A. Análise estática (SAST)
B. Teste de intrusão físico
C. Análise dinâmica (DAST)
D. Revisão de política escrita

D12 · Operações de segurança e resposta a incidentes

Um SIEM recebeu ao mesmo tempo alertas de login falho, de malware e de varredura de portas. O que o analista faz primeiro na triagem?

A. Desliga o SIEM para reduzir o volume de alertas recebidos
B. Fecha todos os alertas para limpar o painel
C. Responde aos alertas na ordem alfabética
D. Prioriza os alertas por gravidade e ativos afetados

01

CAPÍTULO 1 · 20% DA PROVA

Conceitos de gestão de identidade e acesso (IAM)

Este domínio vale 20% e se divide em ciclo de vida de identidades (definição de funções, provisionamento, revisão e desprovisionamento) e controles lógicos de acesso (privilégio mínimo, separação de funções e modelos de controle). A prova adora cenários de RH: funcionário que mudou de setor e manteve acessos, demitido com conta ativa, recontratado com acessos antigos, prestador sem data de expiração. Também cai muito identificar o modelo de acesso (DAC, MAC, RBAC, regras, ABAC), o fator de autenticação e o ataque de senha. Onde mais erro: necessidade de saber x privilégio mínimo, código TOTP como algo que você sabe e pulverização de senhas x força bruta.

Neste capítulo

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

Tópicos-chave

Ciclo de vida da identidade (joiner, mover, leaver)

Definição de funções, provisionamento, revisão e desprovisionamento. Cada evento do RH (entrada, mudança, saída) aciona criação, ajuste ou remoção de acessos; o sistema de RH é a fonte oficial. Mudança de cargo exige revisar e remover acessos antigos, evitando o acúmulo de privilégios (privilege creep).

Comprovação de identidade

Antes de criar a conta, confirmar que a identidade é real: o RH confere documentos e a contratação formal; o banco pede documento e foto do rosto (identity proofing). O NIST SP 800-63 define níveis de garantia. O suporte deve verificar a identidade por método definido antes de redefinir senha, porque atacantes ligam fingindo ser usuários.

Provisionamento

Definir antes a função com os acessos mínimos (ex.: Analista financeiro = ERP + contas a pagar). Provisionamento por grupo ligado à função é previsível e fácil de revisar. Acesso birthright (e-mail, intranet, ponto) deve ser mínimo; extras passam por solicitação aprovada pelo gestor e pelo dono dos dados, em fluxo rastreável.

Revisão e certificação de acessos

Gestores ou donos dos sistemas confirmam periodicamente se cada acesso ainda é necessário; a recertificação documentada serve de evidência em auditorias. A revisão só tem valor se os acessos forem removidos. Contas privilegiadas são revisadas com mais frequência. Revisões também detectam conflitos de separação de funções.

Desprovisionamento

Remover os acessos no momento do desligamento, coordenado com o RH (em casos sensíveis, até antes da comunicação ao funcionário). Inclui recolher crachá, tokens, celulares e notebooks e revogar o acesso físico. Desativar primeiro e excluir depois preserva dados e trilhas para auditoria. Apps fora do SSO, com login próprio, costumam ficar de fora.

Contas órfãs, inativas e conciliação

Conta ativa de quem saiu é órfã e deve ser desativada. Contas sem login há muito tempo de quem ainda trabalha devem ser desativadas ou reconfirmadas com o gestor. Cruzar mensalmente as contas ativas com a lista do RH detecta órfãs e complementa o desprovisionamento automático. Recontratação segue o provisionamento normal para o cargo atual, nunca reativa a conta antiga.

Contas especiais

Prestadores e convidados: data de expiração, patrocinador interno responsável e revisão periódica. Conta de serviço: dono definido, permissões mínimas e revisão. Conta de emergência (break-glass): poucas, senha forte guardada em cofre, uso monitorado e alertas. Conta padrão admin com senha de fábrica: trocar a senha e desativar ou renomear. Contas individuais, nunca genéricas, garantem responsabilização.

Ferramentas de identidade

Serviço de diretório (LDAP, Active Directory) centraliza contas e grupos. IGA centraliza solicitações, aprovações, revisões e desprovisionamento. SCIM automatiza criação e remoção de contas em SaaS. No SSO, o provedor de identidade (IdP) autentica e emite o token; federação (SAML ou OIDC) permite que parceiros entrem com a conta corporativa deles. Autosserviço de senha com segundo fator reduz chamados.

Privilégio mínimo

Conceder só o necessário: estagiário com acesso só às pastas da tarefa, aplicação que lê duas tabelas sem conta de admin do banco, função de nuvem reduzida ao mínimo, crachá que não abre a sala de servidores, campos sensíveis visíveis só à folha. Inclui tirar admin local de usuários, link que expira e escopos OAuth mínimos. Negação implícita aplica o mesmo princípio a regras de firewall.

Necessidade de saber

Foca no acesso ao conteúdo da informação: habilitação para Secreto não basta se a pessoa não trabalha no projeto. Suporte que só vê dados do cliente com chamado aberto aplica necessidade de saber. Privilégio mínimo é mais amplo, sobre permissões em geral.

Gestão de acesso privilegiado (PAM)

Guarda credenciais em cofre com rotação automática, libera acesso temporário e grava sessões para rastrear e auditar ações privilegiadas. Acesso just-in-time concede privilégio só com chamado aprovado e o faz expirar. Contas admin separadas das de e-mail e navegação, estações dedicadas (PAW) e a conta raiz da nuvem com MFA forte e uso raro reduzem a exposição.

Separação de funções e controles correlatos

Quem pede não aprova; quem cadastra fornecedor não aprova pagamento; quem escreve código não publica sozinho; separação entre desenvolvimento e produção. Combinação tóxica é o conjunto de acessos que permite fraude sozinho. Controle duplo exige duas pessoas (regra de duas pessoas, conhecimento dividido). Férias obrigatórias e rodízio de funções revelam fraudes contínuas; sem pessoal, revisão por gestor compensa.

Modelos de controle de acesso

DAC: o dono do recurso decide (pastas compartilhadas), flexível mas com risco de compartilhamento excessivo. MAC: autoridade central define rótulos e habilitações e o sistema impõe; muito seguro, rígido, comum em ambientes militares. RBAC: permissões na função/cargo. Baseado em regras: regras gerais para todos (ACL de firewall). ABAC: atributos do usuário, do recurso e do ambiente (departamento, local, horário).

ACL, matriz e Bell-LaPadula

ACL indica quais usuários podem ler, alterar ou excluir um recurso; aparece em arquivos, roteadores e firewalls. Na matriz de controle de acesso, as linhas formam listas de capacidades e as colunas, ACLs. Bell-LaPadula protege confidencialidade: não ler acima da habilitação e não escrever abaixo.

Fatores de autenticação

Algo que você sabe (senha, PIN), tem (smart card, token, chave de segurança, celular com app autenticador, código TOTP) e é (digital, rosto). MFA de verdade combina categorias diferentes. Localização (onde você está) complementa, não substitui. Crachá + PIN na porta é acesso físico com dois fatores.

MFA forte e autenticação adaptativa

MFA impede o uso de senha roubada por phishing ou credential stuffing. Comece por administradores e acessos remotos. FIDO2 e passkeys resistem a phishing porque a credencial fica ligada à origem do site. Correspondência de números protege contra fadiga de MFA. Autenticação adaptativa pede o segundo fator conforme sinais de risco (país novo, dispositivo desconhecido).

Ataques a credenciais e privilégios

Força bruta testa muitas senhas em uma conta (bloqueio por tentativas ajuda); pulverização testa uma senha comum em muitas contas, evitando o bloqueio (MFA e bloqueio de senhas comuns); credential stuffing usa senhas vazadas de outro site. Escalonamento de privilégios: conta comum vira admin; horizontal: ver dados de outro usuário do mesmo nível trocando um número na URL, por falta de autorização a cada pedido no servidor.

Senhas, sessões e biometria

NIST SP 800-63B: senhas longas, sem trocas periódicas forçadas sem motivo e bloqueio de senhas vazadas. Bloqueio rígido pode ser abusado para travar contas: prefira bloqueio temporário progressivo com detecção. Tempo limite de sessão evita uso de sessão aberta. Biometria: falsa rejeição recusa quem tem direito, falsa aceitação aceita quem não devia; modelos biométricos são dados sensíveis que não podem ser trocados.

Macetes para memorizar

💡 Fatores

Sabe (senha, PIN), Tem (token, cartão, app, chave), É (digital, rosto). MFA = duas caixas diferentes.

💡 Modelos de acesso

DAC = Dono decide. MAC = Mandam os rótulos. RBAC = cargo. Regras = vale para todos. ABAC = Atributos.

💡 Bell-LaPadula

Sigilo: não lê para cima, não escreve para baixo.

💡 Ciclo de vida

Define, provisiona, revisa, desprovisiona; o RH dá o sinal de partida e de chegada.

💡 Ataques de senha

Força bruta = muitas senhas, uma conta. Pulverização = uma senha, muitas contas. Stuffing = senhas vazadas de outro site.

💡 Need to know x privilégio mínimo

Need to know = O QUE posso ver. Privilégio mínimo = O QUE posso fazer.

💡 Biometria

Falsa Aceitação deixa o invasor entrar; falsa Rejeição barra o funcionário.

Tabela de memorização: não confunda

Quando é...	...e quando é
Necessidade de saber Acesso ao conteúdo da informação ligado à tarefa: habilitado, mas fora do projeto, não acessa.	**Privilégio mínimo** Permissões em geral limitadas ao necessário: sem admin local, conta de app sem privilégio de admin no banco.

DAC O dono do recurso concede e retira permissões, como em pastas compartilhadas.	**MAC** Autoridade central define rótulos (Secreto, Confidencial) e habilitações; o sistema impõe, sem decisão do dono.
RBAC Acesso depende do cargo/função; trocar de cargo é trocar a função.	**Baseado em regras** Regras do administrador valem para todos, como ACLs de firewall.
RBAC Permissão por função, sem configurar pessoa por pessoa; risco de explosão de funções.	**ABAC** Políticas que combinam atributos: departamento Financeiro, no escritório, em horário comercial.
Força bruta Muitas senhas contra uma única conta; o bloqueio após erros protege.	**Pulverização de senhas** Uma senha comum (como Empresa@2026) em milhares de contas, evitando o bloqueio; use MFA e bloqueio de senhas comuns.
Falsa aceitação Leitor aceita a digital de quem não está cadastrado; em áreas sensíveis, precisa ser baixa.	**Falsa rejeição** Leitor recusa funcionários cadastrados, que tentam várias vezes; afeta a conveniência.
Separação de funções Etapas de um processo divididas entre pessoas diferentes (cadastrar x aprovar), exigindo conluio para fraude.	**Controle duplo** Duas pessoas juntas para uma mesma ação, cada uma com parte do segredo, como abrir o cofre de chaves.

Números que caem

Item	Valor
Peso médio do domínio na prova	**20%**
Código TOTP típico	**Seis dígitos que mudam a cada 30 segundos (algo que você tem)**
Exemplo de bloqueio contra força bruta	**Conta bloqueada por 15 minutos após cinco senhas erradas seguidas**
Referência do NIST para senhas e identidade	**NIST SP 800-63B (senhas) e NIST SP 800-63 (níveis de garantia)**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Classificar o código de seis dígitos do app autenticador como algo que você sabe.
Como não cair: O código comprova a posse do dispositivo onde o segredo está: algo que você tem. PIN e senha é que são algo que você sabe.

⚠ **Alerta de prova:** Considerar senha + PIN ou senha + pergunta secreta como MFA.
Como não cair: MFA exige categorias diferentes; senha + chave de segurança física é MFA de verdade.

⚠ **Alerta de prova:** Liberar o acesso porque o analista tem habilitação para o nível do documento.
Como não cair: A habilitação não basta: sem necessidade da tarefa, não acessa (need to know).

⚠ **Alerta de prova:** Chamar de escalonamento comum (vertical) o caso do cliente que troca o número da conta na URL.
Como não cair: Ver dados de outro usuário do mesmo nível é escalonamento horizontal; conta comum virando admin é escalonamento de privilégios.

⚠ **Alerta de prova:** Achar que o bloqueio após cinco tentativas resolve a pulverização de senhas.
Como não cair: A pulverização testa uma senha por conta justamente para evitar o bloqueio; MFA, bloqueio de senhas comuns e monitorar falhas espalhadas ajudam.

⚠ **Alerta de prova:** Endurecer o bloqueio rígido de contas quando atacantes passam a travar contas de propósito.
Como não cair: A alternativa equilibrada é bloqueio temporário progressivo e detecção de padrões suspeitos, sem negar serviço.

⚠ **Alerta de prova:** Achar que esconder o botão Excluir na interface é controle de acesso suficiente.
Como não cair: A interface pode ser contornada; a autorização deve ser verificada no servidor a cada pedido.

⚠ **Alerta de prova:** Dizer que no MAC o dono do dado decide quem acessa.
Como não cair: Dono decide é DAC. No MAC, a autoridade central define rótulos e habilitações segundo a política.

⚠ **Alerta de prova:** Chamar ACL de firewall de RBAC.
Como não cair: Regras gerais que valem para todos são controle baseado em regras; RBAC depende do cargo.

⚠ **Alerta de prova:** Considerar a revisão de acessos concluída só porque encontrou as permissões indevidas.
Como não cair: A revisão só tem valor se os acessos forem removidos, com correções registradas como evidência.

⚠ **Alerta de prova:** Achar que desativar a conta do diretório encerra todos os acessos do desligado.
Como não cair: SaaS com login próprio, fora do SSO, fica de fora; inventariar aplicações e integrar ao SSO e ao provisionamento.

⚠ **Alerta de prova:** Reativar a conta antiga do ex-funcionário recontratado.
Como não cair: Os acessos do cargo anterior voltariam sem revisão; seguir o provisionamento normal do cargo atual.

⚠ **Alerta de prova:** Usar a localização como substituta de um fator.
Como não cair: Localização e horário são condições de contexto que complementam os fatores, não os substituem.

⚠ **Alerta de prova:** Em Bell-LaPadula, permitir que o usuário Confidencial leia documento Secreto.
Como não cair: Não se lê acima da habilitação e não se escreve abaixo, para proteger o sigilo.

Como cai na prova

📝 **Como cai:** Cenário de RH (contratação, mudança de setor, demissão, recontratação, temporário) e a pergunta sobre a falha ou a prática correta.
Como resolver: Identifique a etapa do ciclo (provisionar, revisar, desprovisionar) e escolha a ação que remove excesso na hora certa: revisar na mudança, desativar na saída, data de expiração para temporários.

📝 **Como cai:** Descrição de como o acesso é decidido e a pergunta: qual modelo?
Como resolver: Quem decide? Dono = DAC; autoridade central com rótulos = MAC; cargo = RBAC; regras gerais = regras; combinação de atributos e contexto = ABAC.

📝 **Como cai:** Que fator de autenticação é este? ou qual combinação é MFA?
Como resolver: Classifique cada elemento em sabe, tem ou é; só é MFA se houver duas categorias diferentes.

📝 **Como cai:** Princípio aplicado: estagiário com pastas mínimas, habilitado sem projeto, quem pede não aprova.
Como resolver: Permissões limitadas = privilégio mínimo; informação ligada à tarefa = necessidade de saber; etapas divididas entre pessoas = separação de funções; duas pessoas juntas = controle duplo.

📝 **Como cai:** Ataque descrito e a pergunta sobre o controle mais eficaz.
Como resolver: Senha roubada, vazada ou pulverizada: MFA. Força bruta em uma conta: bloqueio por tentativas. Fadiga de MFA: correspondência de números. Phishing de credenciais: FIDO2/passkey.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Mudou de setor e manteve os acessos antigos	**Acúmulo de privilégios; falha na revisão da mudança**
Conta ativa de quem saiu da empresa	**Conta órfã: desativar; conciliar com o RH**
Entrada, mudança e saída de pessoas	**Joiner, mover, leaver**
Criar e remover contas em SaaS a partir do diretório	**SCIM**
Parceiro entra no seu portal com a conta corporativa dele	**Federação (SAML ou OIDC)**
Privilégio liberado por chamado e que expira	**Just-in-time (PAM)**
Gravar sessões de admin, cofre de senhas com rotação	**PAM**
Duas pessoas, cada uma com parte do segredo	**Controle duplo**
Mesma pessoa cria fornecedor, aprova pagamento e concilia	**Combinação tóxica; separação de funções**
Rótulos e habilitação, ambiente militar	**MAC**
Departamento, local e horário avaliados juntos	**ABAC**
Funções demais no RBAC	**Explosão de funções**
Número exibido no autenticador para digitar	**Proteção contra fadiga de MFA**
Autenticação resistente a phishing	**FIDO2 ou passkey**

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

- Código do app autenticador é algo que você tem.
- Revisão de acessos sem remoção não vale nada; contas privilegiadas são revisadas com mais frequência.
- No desligamento, corta-se o acesso na hora, inclusive físico e de apps fora do SSO.
- Autorização é verificada no servidor a cada pedido, não só no login nem na interface.
- MFA primeiro para administradores e acessos remotos.

Essenciais para a prova (checklist)

- ☐ Sei as etapas do ciclo de vida de identidades e o papel do RH como fonte oficial.
- ☐ Sei o que fazer com contas órfãs, inativas, de terceiros, de serviço e de emergência.
- ☐ Sei diferenciar diretório, IGA, SCIM, IdP, SSO, federação e PAM.
- ☐ Sei diferenciar privilégio mínimo e necessidade de saber com exemplos.
- ☐ Sei aplicar separação de funções, controle duplo, férias obrigatórias e rodízio.
- ☐ Sei identificar DAC, MAC, RBAC, baseado em regras e ABAC pelo cenário.
- ☐ Sei classificar fatores de autenticação e reconhecer MFA verdadeira.
- ☐ Sei diferenciar força bruta, pulverização, credential stuffing e escalonamento horizontal.
- ☐ Sei as recomendações atuais do NIST para senhas.
- ☐ Sei diferenciar falsa aceitação e falsa rejeição na biometria.

Questões de revisão do capítulo

R1.1 · Conceitos de gestão de identidade e acesso (IAM)

Um cliente do internet banking muda o número da conta na URL e passa a ver o extrato de outro cliente. Que tipo de falha é essa?

A. Falsa rejeição da biometria
B. Envenenamento de DNS do banco
C. Negação de serviço por inundação
D. Escalonamento horizontal de privilégios

R1.2 · Conceitos de gestão de identidade e acesso (IAM)

O sistema pede um segundo fator só quando o login vem de um país novo ou de um dispositivo desconhecido. Que abordagem é essa?

A. Separação de funções em processos críticos
B. Negação implícita nas regras do firewall
C. Autenticação adaptativa baseada em risco
D. Controle de acesso discricionário do dono

R1.3 · Conceitos de gestão de identidade e acesso (IAM)

Para entrar na sala de servidores, é preciso aproximar o crachá e digitar um PIN. Que tipo de controle é esse?

A. Controle de acesso físico com dois fatores
B. Controle de acesso lógico por senha única
C. Controle de recuperação após desastres
D. Controle administrativo por política escrita

R1.4 · Conceitos de gestão de identidade e acesso (IAM)

Qual é a diferença entre necessidade de saber e privilégio mínimo?

A. Necessidade de saber é opcional; privilégio mínimo é proibido pela maioria das normas
B. Necessidade de saber trata do acesso à informação; privilégio mínimo, das permissões em geral
C. Necessidade de saber é um ataque; privilégio mínimo é uma falha de configuração do sistema
D. Necessidade de saber vale só para redes; privilégio mínimo vale só para papéis impressos no escritório

Respostas comentadas

R1.1. D) Escalonamento horizontal de privilégios

Por quê: A aplicação deve verificar a autorização a cada pedido, não só no login.

✗ A) Incorreta. Recusa usuário válido.
✗ B) Incorreta. Desvia nomes.
✗ C) Incorreta. Derruba serviços.

> **Dica de prova:** Ver dados de outro usuário do mesmo nível: escalonamento horizontal.

R1.2. C) Autenticação adaptativa baseada em risco

Por quê: A autenticação adaptativa equilibra segurança e usabilidade usando sinais de risco.

✗ A) Incorreta. Divide tarefas.
✗ B) Incorreta. Regra de rede.
✗ D) Incorreta. O dono decide.

> **Dica de prova:** MFA conforme o risco: autenticação adaptativa.

R1.3. A) Controle de acesso físico com dois fatores

Por quê: Crachá (algo que você tem) e PIN (algo que você sabe) formam autenticação de dois fatores.

✗ B) Incorreta. Só um fator.
✗ C) Incorreta. Não é o caso.
✗ D) Incorreta. Não é o caso.

> **Dica de prova:** Crachá + PIN na porta: acesso físico com 2 fatores.

R1.4. B) Necessidade de saber trata do acesso à informação; privilégio mínimo, das permissões em geral

Por quê: Ambos limitam o acesso ao necessário, mas a necessidade de saber foca no conteúdo da informação.

✗ A) Incorreta. Não é a diferença.

✗ C) Incorreta. Não é a diferença.

✗ D) Incorreta. Não é a diferença.

> **Dica de prova:** Need to know: informação. Privilégio mínimo: permissões.

02

CAPÍTULO 2 · 21,3% DA PROVA

Conceitos de segurança de redes e nuvem

Este domínio vale 21,3% e mistura três frentes: fundamentos de rede (modelos OSI e TCP/IP, IPv4 e IPv6, portas, firewalls, Wi-Fi, VPN, ICS e IoT), arquitetura segura (segmentação, DMZ, VLAN, microssegmentação, defesa em profundidade e Confiança Zero) e nuvem (cinco características, modelos de serviço e de implantação e responsabilidade compartilhada). Caem muitas perguntas diretas de associação: porta 443, camada 3, SSH no lugar de Telnet, WPA3 com 802.1X. Na nuvem, a pergunta-chave é sempre de quem é a responsabilidade. Onde mais erro: achar que NAT, SSID oculto ou filtro de MAC protegem, confundir modelo de serviço com modelo de implantação e esquecer que dados e acessos são sempre do cliente.

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

Tópicos-chave

Modelo OSI

Camada 1 física (cabo de fibra rompido), 2 enlace (switch comum, endereços MAC), 3 rede (roteador, endereços IP), 4 transporte (portas, TCP e UDP), 7 aplicação (HTTP, SMTP, DNS). Switches de camada 3 também roteiam, mas o switch comum opera na camada 2. Firewalls de aplicação e proxies inspecionam a camada 7.

Modelo TCP/IP

Quatro camadas: acesso à rede, internet (endereçamento IP e roteamento), transporte (TCP e UDP, equivalente à camada 4 do OSI) e aplicação, que reúne sessão, apresentação e aplicação do OSI.

TCP x UDP

TCP é orientado a conexão, garante entrega ordenada e usa o handshake de três vias SYN, SYN-ACK, ACK; a inundação SYN explora conexões abertas pela metade (proteções: SYN cookies, limitação de taxa, anti-DDoS). UDP é mais leve, sem garantia de entrega, preferido para voz e vídeo em tempo real.

IPv4, IPv6 e NAT

IPv4 usa 32 bits e IPv6, 128 bits (espaço muito maior); os dois exigem controles. Privados: 10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16, que saem à internet por NAT. NAT economiza endereços e esconde a estrutura interna, mas não substitui firewall. Loopback 127.0.0.1 (IPv6 ::1). IPv6 ativo sem regras de firewall deixa tráfego sem controle.

Protocolos de infraestrutura e seus ataques

ARP descobre o MAC de um IP na rede local (ARP spoofing: inspeção dinâmica de ARP e criptografia). DHCP distribui IPs (servidor DHCP falso desvia tráfego; proteção de DHCP no switch). DNS resolve nomes, porta 53, UDP para consultas e TCP para respostas grandes (envenenamento de DNS: DNSSEC). ICMP é usado pelo ping e costuma ser limitado vindo da internet.

Protocolos seguros e portas

Telnet e FTP enviam credenciais em texto claro: troque por SSH (22) e SFTP (sobre SSH) ou FTPS (sobre TLS). HTTPS é HTTP com TLS, porta 443, e autentica o servidor pelo certificado. LDAP 389 sem criptografia vira LDAPS 636 ou StartTLS. SNMPv1 vira SNMPv3. RDP (3389) e SMB (445) nunca devem ficar expostos à internet. Servidor SMTP deve exigir autenticação para não virar relay aberto.

Tipos de firewall

Filtro de pacotes sem estado avalia cada pacote por IP e porta (ACLs de roteador). Firewall com inspeção de estado mantém a tabela de conexões. NGFW identifica aplicações e usuários, não só portas (bloqueia app que usa a 443). WAF protege aplicações web contra injeção de SQL e XSS. Proxy web filtra e registra a navegação.

Regras de firewall

As regras são avaliadas de cima para baixo e vale a primeira que corresponder: regras específicas antes das gerais, e a última costuma ser negar tudo. Lista de permissões (allow list) libera só o explicitamente permitido e aplica a negação implícita, mais segura que bloquear só o conhecido. Liberar só as portas necessárias reduz a superfície de ataque.

IDS, IPS e honeypot

IDS detecta e alerta; IPS fica no caminho do tráfego e pode descartar pacotes. Baseado em assinaturas detecta bem ameaças conhecidas; baseado em anomalias acha desvios do normal e ataques novos, com mais falsos positivos. Honeypot é servidor isca sem dados reais: alertas de alta confiança, pois ninguém legítimo deveria acessá-lo.

VPN

Túnel cifrado com IPsec ou TLS que protege confidencialidade e integridade em redes não confiáveis, como Wi-Fi público. Site a site liga matriz e filial entre roteadores, normalmente com IPsec. Split tunneling reduz visibilidade sobre o tráfego direto. A VPN protege o túnel, mas o dispositivo também precisa estar seguro.

Segurança Wi-Fi e Bluetooth

WPA3 é o padrão recomendado. O modo Enterprise com 802.1X e RADIUS dá credenciais individuais, revogáveis e registradas; senha compartilhada exige troca quando alguém sai. Filtro de MAC e SSID oculto são obscuridade. Desative o WPS (PIN vulnerável a força bruta). Evil twin imita o nome da rede; portal cativo não cifra; isolamento de clientes protege visitantes. Bluesnarfing rouba dados por Bluetooth.

ICS, IoT e sistemas embarcados

Costumam ter pouco suporte de segurança, não recebem atualizações com facilidade e usam protocolos sem autenticação nem criptografia. Controles: segmentar e monitorar, isolar ICS, separar OT de TI, firmware em dia, trocar senhas de fábrica e dar ao fornecedor acesso sob demanda por canal controlado e monitorado. Dispositivos médicos, câmeras IP e TVs inteligentes vão para redes separadas.

Segmentação, zonas e DMZ

Zonas de firewall (internet, DMZ, interna, visitantes) aplicam regras conforme o nível de confiança. A DMZ isola o servidor público; deve-se bloquear conexões iniciadas da DMZ para a rede interna. VLANs (marcadas por IEEE 802.1Q nos troncos) separam redes no mesmo switch, mas só são eficazes com regras filtrando o tráfego entre elas. Segmentar o ambiente de cartões reduz o escopo do PCI DSS; air gap é ausência total de conexão.

Microssegmentação e tráfego leste-oeste

Políticas individuais por carga de trabalho permitem que cada uma fale só com as que precisa, limitando a movimentação lateral. Na nuvem, grupos de segurança por VM aplicam esse conceito. Tráfego leste-oeste é o tráfego entre sistemas internos, que fica sem controle quando só a borda é inspecionada.

Defesa em profundidade

Várias camadas (firewall, antivírus, MFA, treinamento, backups, segmentação, monitoramento): se uma falhar, as outras protegem. Inclui a camada física, porque acesso físico contorna controles lógicos. Exemplos: DMZ entre dois firewalls de fabricantes diferentes, rede de gerenciamento separada, jump server para acesso administrativo.

Confiança Zero

Nunca confiar, sempre verificar: verificação explícita, privilégio mínimo e presumir a violação (limitar o raio de dano e monitorar). A identidade de usuários e dispositivos vira o perímetro; o acesso é concedido por sessão, com base no contexto e no estado do dispositivo. O NIST SP 800-207 descreve o ponto de decisão (PDP) e o ponto de aplicação (PEP). ZTNA libera aplicativos, não a rede; NAC verifica o dispositivo antes de entrar.

Características e modelos da nuvem

Cinco características do NIST: autoatendimento sob demanda, amplo acesso à rede, agrupamento de recursos (multilocação), elasticidade rápida e serviço medido. Modelos de serviço: IaaS (VMs, cliente instala o SO), PaaS (banco gerenciado, cliente cuida de código, dados e acessos), SaaS (aplicação pronta) e serverless. Modelos de implantação: pública, privada, híbrida e comunitária.

Responsabilidade compartilhada e ferramentas de nuvem

O provedor cuida do físico e da virtualização; em IaaS, o cliente cuida do SO (patches), firewall virtual, aplicações e dados; em qualquer modelo, dados e identidades são do cliente (bucket público, MFA no SaaS). CSPM detecta configurações inseguras; CASB controla o uso de SaaS e a TI invisível; BYOK dá ao cliente o controle das chaves; crypto-shredding sanitiza apagando a chave. Avalie provedores com SOC 2 tipo II e ISO 27001, escolha a região conforme residência de dados e preveja exportação e exclusão no fim do contrato.

Macetes para memorizar

Camadas OSI cobradas

1 cabo, 2 switch/MAC, 3 roteador/IP, 4 portas/TCP-UDP, 7 HTTP-SMTP-DNS.

Portas

22 SSH, 53 DNS, 389 LDAP, 443 HTTPS, 445 SMB, 636 LDAPS, 3389 RDP.

IPv4 privado

10, 172.16 e 192.168: os três que não saem sem NAT.

Características da nuvem

Autoatendimento, Amplo acesso, Agrupamento, Elasticidade e Medido: três A + E + M.

Responsabilidade compartilhada

Dados e identidades são SEMPRE do cliente; de IaaS para PaaS e SaaS, o cliente gerencia cada vez menos (em IaaS, até os patches do SO).

Confiança Zero

Verifique sempre, dê o mínimo, presuma que já invadiram.

Protocolos inseguros

Telnet vira SSH, FTP vira SFTP, HTTP vira HTTPS, LDAP vira LDAPS, SNMPv1 vira SNMPv3.

Tabela de memorização: não confunda

Quando é...	...e quando é
IDS Detectar e alertar sobre tráfego suspeito sem bloquear (técnico e detectivo).	**IPS** Ficar no caminho do tráfego e descartar pacotes maliciosos (técnico e preventivo).

Filtro de pacotes sem estado Avaliar cada pacote isoladamente por IP de origem, destino e porta.	**Firewall com inspeção de estado** Acompanhar a tabela de conexões e aceitar só respostas a sessões abertas de dentro.
TCP Entrega garantida e ordenada, com handshake de três vias.	**UDP** Voz e vídeo em tempo real, onde reenviar pacotes atrasados não ajuda.
Hub Repete o tráfego para todas as portas; qualquer máquina captura o tráfego das outras.	**Switch** Envia cada quadro à porta certa pelo endereço MAC (camada 2).
VPN tradicional Túnel cifrado que dá acesso à rede interna.	**ZTNA** Libera só os aplicativos de que o usuário precisa após checar identidade e dispositivo, reduzindo a movimentação lateral.
Segmentação com VLAN Separar grupos (visitantes, impressoras, servidores) em segmentos lógicos com regras entre eles.	**Microssegmentação** Política individual por carga de trabalho ou VM, controlando também o tráfego leste-oeste.
IaaS Cliente aluga VMs, instala o SO e aplica os patches dele.	**PaaS** Cliente publica a aplicação sem gerenciar SO, mas continua responsável por código, dados e acessos.

Números que caem

Item	Valor
Peso médio do domínio na prova	**21,3%**
Portas padrão	**SSH 22; DNS 53; LDAP 389; HTTPS 443; SMB 445; LDAPS 636; RDP 3389**
Tamanho do endereço	**IPv4 32 bits; IPv6 128 bits**
Faixas IPv4 privadas	**10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16**
Loopback	**127.0.0.1 no IPv4; ::1 no IPv6**
Camadas do modelo TCP/IP	**4: acesso à rede, internet, transporte e aplicação**
Características essenciais da nuvem (NIST)	**5**
PIN do WPS	**Oito dígitos, vulnerável a força bruta**
Padrões IEEE cobrados	**802.1Q (etiqueta de VLAN no tronco); 802.1X (autenticação de porta e Wi-Fi Enterprise)**
Referência de arquitetura de Confiança Zero	**NIST SP 800-207 (PDP e PEP)**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Achar que o NAT substitui o firewall porque esconde a rede interna.
Como não cair: NAT economiza endereços e esconde a estrutura, mas não filtra tráfego como um firewall.

⚠ **Alerta de prova:** Achar que o portal de boas-vindas da rede de visitantes cifra o tráfego.
Como não cair: O portal cativo só registra aceite e controla o acesso; rede aberta continua sem criptografia.

⚠ **Alerta de prova:** Confiar no SSID oculto ou no filtro de MAC como proteção.
Como não cair: SSID é descoberto com ferramentas simples e MAC é falsificável; use WPA3 e 802.1X.

⚠ **Alerta de prova:** Considerar a rede segmentada só porque foi dividida em VLANs.
Como não cair: Sem ACLs ou firewall filtrando o tráfego entre as VLANs, a segmentação não é eficaz.

⚠ **Alerta de prova:** Achar que a VPN deixa seguro o notebook pessoal infectado.
Como não cair: A VPN protege o túnel; o estado do dispositivo também precisa ser verificado antes do acesso.

⚠ **Alerta de prova:** Culpar o provedor pelo armazenamento deixado público pelo cliente de IaaS.
Como não cair: Configuração é do cliente; configurações incorretas do cliente estão entre as principais causas de vazamentos na nuvem.

⚠ **Alerta de prova:** Dizer que ativar MFA no SaaS é responsabilidade do provedor.
Como não cair: Mesmo no SaaS, contas, permissões, configurações e dados são do cliente.

⚠ **Alerta de prova:** Atribuir ao provedor os patches do SO das VMs em IaaS.
Como não cair: Em IaaS o cliente aplica patches no SO. Em PaaS e serverless, o provedor cuida do SO.

⚠ **Alerta de prova:** Responder nuvem privada quando a pergunta pede o modelo de serviço.
Como não cair: Pública, privada, híbrida e comunitária são modelos de implantação; serviço é IaaS, PaaS ou SaaS.

⚠ **Alerta de prova:** Tentar bloquear um aplicativo que usa a porta 443 com firewall de porta.
Como não cair: Só o NGFW, que identifica aplicações, consegue bloquear sem fechar a 443 para todos.

⚠ **Alerta de prova:** Ignorar a ordem das regras do firewall.
Como não cair: Vale a primeira que corresponde: uma regra ampla no topo libera o que deveria bloquear.

⚠ **Alerta de prova:** Colocar o roteador na camada 2 ou o switch comum na camada 3.
Como não cair: Switch comum e MAC: camada 2. Roteador e IP: camada 3. Portas TCP/UDP: camada 4.

⚠ **Alerta de prova:** Achar que o IDS por assinatura detecta bem ataques novos.
Como não cair: Assinatura pega o conhecido; anomalia acha o novo, com mais falsos positivos.

⚠ **Alerta de prova:** Tratar o air gap como dispensa de qualquer controle.
Como não cair: Mesmo isolado, mídias removíveis e manutenção precisam de controle.

Como cai na prova

📝 **Como cai:** Associação direta: qual porta, qual camada, qual protocolo substitui o inseguro.
Como resolver: Use as tabelas memorizadas (portas, camadas OSI, pares inseguro/seguro) e desconfie de alternativas que trocam camada 2 por 3 ou porta 3389 por 445.

📝 **Como cai:** Cenário de nuvem e a pergunta: qual modelo de serviço ou de implantação?
Como resolver: Primeiro decida se a pergunta é de serviço (o que o cliente gerencia) ou de implantação (quem usa a infraestrutura). Instalar SO = IaaS; banco gerenciado = PaaS; aplicação pronta = SaaS.

📝 **Como cai:** Incidente na nuvem e a pergunta: de quem é a responsabilidade?
Como resolver: Configuração, dados, contas, MFA e patches do SO em IaaS são do cliente; físico, virtualização e, em PaaS/serverless, o SO são do provedor.

📝 **Como cai:** Ataque de rede ou Wi-Fi descrito e a pergunta sobre o nome ou a defesa.
Como resolver: Nomeie pelo mecanismo (ARP falso, DNS adulterado, rede gêmea, handshakes incompletos) e escolha a defesa específica: inspeção de ARP, DNSSEC, VPN, SYN cookies.

📝 **Como cai:** Arquitetura: o que faltou ou qual prática ajudou a conter o atacante.
Como resolver: Atacante circulou livre: faltou defesa em profundidade ou segmentação. Ataque contido no segmento: segmentação. Política por carga: microssegmentação. Acesso por app: ZTNA.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Respostas ARP falsas para se passar pelo gateway	**ARP spoofing**
Endereço certo digitado, site falso aberto	**Envenenamento de DNS; DNSSEC**
Milhares de handshakes incompletos	**Inundação SYN**
Wi-Fi com o mesmo nome da rede oficial	**Evil twin**
Wi-Fi com credencial individual e RADIUS	**WPA2/WPA3 Enterprise com 802.1X**
Porta do switch só libera após autenticar o dispositivo	**IEEE 802.1X**
Notebook checado (antivírus, patches, certificado) antes de entrar na rede	**NAC**
Servidor intermediário para acessar a produção	**Jump server (bastion host)**
Servidor público entre a internet e a rede interna	**DMZ**
Presumir a violação, verificar cada acesso	**Confiança Zero**
Aumentar e reduzir servidores na Black Friday	**Elasticidade rápida**
Data center próprio + nuvem pública para picos	**Nuvem híbrida**
Vários hospitais compartilhando uma nuvem só deles	**Nuvem comunitária**
Alerta de armazenamento público na conta de nuvem	**CSPM**

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

- Dados e identidades são sempre responsabilidade do cliente, em qualquer modelo de nuvem.
- NAT, SSID oculto, filtro de MAC e portal cativo não são proteção de verdade.
- VLAN sem regras entre elas não é segmentação.
- IDS alerta; IPS bloqueia; NGFW enxerga aplicações; WAF protege apps web.
- RDP (3389) e SMB (445) nunca expostos à internet.

Essenciais para a prova (checklist)

- ☐ Sei em que camada OSI atuam cabo, switch, roteador, portas e HTTP/DNS.
- ☐ Sei as quatro camadas do TCP/IP e o handshake TCP.
- ☐ Sei as portas padrão cobradas e os substitutos seguros de Telnet, FTP, LDAP e SNMPv1.
- ☐ Sei diferenciar firewall sem estado, stateful, NGFW, WAF e proxy.
- ☐ Sei configurar Wi-Fi corporativo seguro e reconhecer evil twin e bluesnarfing.
- ☐ Sei proteger ICS e IoT com segmentação e monitoramento.

- ☐ Sei explicar DMZ, VLAN, microssegmentação, tráfego leste-oeste e defesa em profundidade.
- ☐ Sei os três princípios da Confiança Zero e o papel de ZTNA e NAC.
- ☐ Sei as cinco características da nuvem e os modelos de serviço e de implantação.
- ☐ Sei dividir responsabilidades entre cliente e provedor em IaaS, PaaS, SaaS e serverless.

Questões de revisão do capítulo

R2.1 · Conceitos de segurança de redes e nuvem

Uma empresa aluga máquinas virtuais na nuvem e instala nelas seu próprio sistema operacional e banco de dados. Qual é o modelo de serviço?

A. Função como serviço (FaaS)
B. Plataforma como serviço (PaaS)
C. Software como serviço (SaaS)
D. Infraestrutura como serviço (IaaS)

R2.2 · Conceitos de segurança de redes e nuvem

A equipe ainda administra servidores por Telnet, que envia senhas em texto claro. Qual protocolo deve substituí-lo?

A. SSH, na porta 22
B. SNMP, na porta 161
C. FTP, na porta 21
D. HTTP, na porta 80

R2.3 · Conceitos de segurança de redes e nuvem

Um servidor web na DMZ foi invadido. Que regra de firewall impede que ele seja usado para atacar a rede interna?

A. Desligar os logs do firewall para ganhar desempenho
B. Permitir acesso remoto da internet à rede interna
C. Bloquear conexões iniciadas da DMZ para a rede interna
D. Liberar o tráfego entre a DMZ e a rede interna da empresa

R2.4 · Conceitos de segurança de redes e nuvem

A rede de visitantes tem uma página de boas-vindas onde o visitante aceita os termos antes de navegar. Isso substitui a criptografia do Wi-Fi?

A. Não, o portal só controla o acesso, sem cifrar o tráfego
B. Sim, o portal impede que outros capturem o tráfego
C. Sim, o portal cifra o tráfego de cada visitante
D. Sim, o portal transforma a rede em WPA3 Enterprise

Respostas comentadas

R2.1. D) Infraestrutura como serviço (IaaS)

Por quê: No IaaS, o cliente tem mais controle e mais responsabilidade.

✗ A) Incorreta. Só funções, sem servidores.
✗ B) Incorreta. O SO é do provedor.
✗ C) Incorreta. O cliente só usa o app.

> **Dica de prova:** Alugar VMs e instalar o SO: IaaS.

R2.2. A) SSH, na porta 22

Por quê: SSH cifra a sessão e permite autenticação por chaves.

✗ B) Incorreta. É gerenciamento de rede.
✗ C) Incorreta. Também transmite em claro.
✗ D) Incorreta. Não é acesso a terminal.

> **Dica de prova:** Substituir Telnet: SSH.

R2.3. C) Bloquear conexões iniciadas da DMZ para a rede interna

Por quê: A DMZ deve ter o mínimo de comunicação com a rede interna, controlada caso a caso.

✗ A) Incorreta. Perde visibilidade.
✗ B) Incorreta. Aumenta a exposição.
✗ D) Incorreta. Facilita o ataque.

> **Dica de prova:** DMZ invadida: bloquear conexões da DMZ para dentro.

R2.4. A) Não, o portal só controla o acesso, sem cifrar o tráfego

Por quê: Portais cativos registram aceite e acesso, mas redes abertas continuam sem criptografia.

✗ B) Incorreta. Não impede a captura.
✗ C) Incorreta. Não cifra o tráfego.
✗ D) Incorreta. Não altera o padrão.

> **Dica de prova:** Portal de boas-vindas não cifra o tráfego.

03

CAPÍTULO 3 · 17,3% DA PROVA

Governança de segurança

Aqui eu preciso dominar quatro blocos: GRC (governança, risco e conformidade), redundância com continuidade de negócios e recuperação de desastres, conscientização em segurança e métricas de eficácia. A prova traz cenários bem práticos: qual métrica define 15 minutos de perda de dados, que tipo de site alternativo é aquele, que golpe de engenharia social é esse, qual indicador mostrar à diretoria. Os erros mais comuns vêm de trocar RTO por RPO, incremental por diferencial, site quente por morno, KPI por KRI e de achar que conformidade é o mesmo que segurança. Em conscientização, a resposta certa quase sempre é confirmar por outro canal conhecido e avisar a segurança.

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

Tópicos-chave

GRC

Governança, risco e conformidade integrados para alinhar a segurança aos objetivos, riscos e obrigações da empresa. A visão integrada evita silos e retrabalho e permite mapear um controle para vários requisitos ao mesmo tempo (LGPD, ISO 27001, PCI DSS). Plataformas de GRC reúnem riscos, controles, auditorias e evidências em um só lugar.

Governança x gestão

Governança define direção e supervisiona; gestão planeja e executa. Um comitê com executivos de várias áreas que prioriza investimentos e aprova políticas faz governança. A alta direção define o apetite de risco, e o conselho e a alta direção respondem em última instância pelos riscos: a execução pode ser delegada, a responsabilidade final não.

Conformidade

Demonstrar o cumprimento de requisitos legais, regulatórios, contratuais e de políticas internas. Um cliente que exige em contrato MFA e comunicação de incidentes em até 24 horas cria uma obrigação contratual. A conformidade evita multas, sanções e perda de confiança, mas não garante segurança: normas definem um mínimo.

Modelo de três linhas

A primeira linha gerencia riscos na operação, a segunda supervisiona e a terceira, a auditoria interna, dá avaliação independente sobre riscos e controles e reporta à direção. A independência é o que permite uma avaliação objetiva.

Auditoria, evidências e monitoramento contínuo

Auditores verificam políticas e evidências de que são aplicadas: registros de revisões de acesso, relatórios de patches, atas. Autoavaliação é útil no dia a dia; auditoria externa é feita por terceiros independentes e dá garantia a reguladores e clientes. Monitoramento contínuo verifica automaticamente, todo dia, se os controles funcionam.

Ferramentas de governança

Matriz RACI define quem executa, aprova, é consultado e é informado. Registro de riscos guarda riscos com dono, nível, resposta e prazo. Exceção à política passa por processo formal com justificativa, prazo, controles compensatórios e aprovação de quem pode aceitar o risco. Políticas são revisadas periodicamente (por exemplo, uma vez por ano) e após mudanças.

Frameworks de governança

O NIST Cybersecurity Framework 2.0 organiza o programa em Governar, Identificar, Proteger, Detectar, Responder e Recuperar; a versão 2.0 incluiu a função Governar. O COBIT, da ISACA, apoia a governança e a gestão da TI corporativa, alinhando TI aos objetivos de negócio, e é muito usado junto com ISO 27001 e NIST.

Análise de impacto nos negócios (BIA)

Identifica processos críticos, dependências e impactos de parar cada um; é a base para definir RTO e RPO e vem antes do plano de continuidade. A ordem de restauração segue a prioridade da BIA e as dependências: identidade e rede costumam vir antes das aplicações.

RTO, RPO e MTD

RTO é o tempo máximo aceitável para voltar a operar; RPO é quanto de dados se aceita perder e orienta a frequência dos backups; MTD é o tempo máximo que o processo pode ficar parado antes de dano inaceitável. O RTO deve ser menor que o MTD. Para SaaS crítico, o SLA e as regras de recuperação do provedor devem ser compatíveis com RTO e RPO.

Continuidade (BC), recuperação de desastres (DR) e resposta a incidentes

BC mantém o negócio funcionando; DR (DRP) restaura sistemas, dados e infraestrutura de TI dentro do RTO e do RPO e é parte da continuidade. O plano de resposta trata e contém o incidente; um ataque grave pode acionar os dois. Em incêndio, a prioridade número um é a segurança das pessoas; a equipe de gestão de crise aciona o plano por critérios definidos e o plano de comunicação define quem fala com clientes, imprensa e reguladores.

Sites alternativos

Site quente: equipamentos e dados replicados, assume em minutos, custo mais alto, RTO mais baixo. Site morno: servidores e rede instalados, mas precisa de dias para restaurar dados e ajustar. Site frio: só espaço, energia e rede, menor custo e RTO maior. O site de DR deve ficar a distância segura para não ser atingido pelo mesmo desastre regional; voltar ao principal reparado é failback, que também precisa ser planejado e testado.

Testes do plano

Evoluem de checklist (revisão de documentos) e walkthrough (leitura conjunta passo a passo, sem acionar sistemas) para simulações, teste paralelo (ativa o site alternativo sem desligar a produção) e interrupção total (desliga a produção: o mais realista e arriscado). Plano que ninguém conhece não funciona: precisa ser divulgado, treinado e acessível na crise.

Tipos e estratégia de backup

Completo copia tudo. Incremental copia o que mudou desde o último backup de qualquer tipo: rápido de fazer, mas a restauração exige o completo e todos os incrementais. Diferencial copia o que mudou desde o último completo: cresce a cada dia, mas a restauração usa só o completo e o último diferencial. Regra 3-2-1, cópias imutáveis ou offline contra ransomware e restaurações testadas.

Redundância e alta disponibilidade

RAID 1 espelha discos e aumenta a disponibilidade, mas não substitui backup (arquivo apagado some dos dois discos). Failover com dois servidores, clusters e dois provedores de internet reduzem pontos únicos de falha. Nobreak cobre o intervalo até o gerador entrar. Uma só pessoa que sabe restaurar um sistema é ponto único de falha humano: documentar, treinar e ter substitutos. Trabalho remoto também é estratégia de continuidade.

Engenharia social

Explora a confiança e usa urgência, medo, autoridade ou recompensa. Spear phishing usa dados da vítima; whaling mira executivos; vishing é por telefone; smishing por SMS; quishing por QR code; pretexto inventa uma história e um papel; isca (baiting) deixa pendrives; shoulder surfing é olhar a tela. Fraude BEC desvia pagamentos com troca de conta bancária; deepfake de voz exige verificação independente e dupla aprovação.

Cultura e conscientização

Apoio visível da liderança mostra prioridade e dá exemplo; embaixadores (security champions) levam boas práticas às áreas; cultura sem punição para quem relata clique em phishing acelera a contenção. O programa eficaz é contínuo e adaptado a cada função, começa na integração do novato e orienta mesa limpa e tela limpa, gerenciador de senhas, roteador doméstico com senha trocada e cuidado com OSINT nas redes sociais.

Métricas, KPI e KRI

KPI mede desempenho (patches aplicados no prazo); KRI alerta sobre aumento de risco (sistemas críticos com patch atrasado, envelhecimento de vulnerabilidades, exceções vencidas). Indicadores antecedentes (leading, como treinamento em dia) preveem problemas; os de resultado (lagging) mostram o que já ocorreu. Metas SMART têm número, alvo e prazo, e medir antes cria a linha de base.

Métricas de operação e comunicação à diretoria

MTTD é o tempo médio para perceber; tempo médio para conter mede o isolamento; MTTR é o tempo para responder após detectar. Cobertura (% de admins com MFA, % de dispositivos com EDR) revela pontos cegos; % de restaurações testadas mede backup; taxa de cliques em phishing simulado mede conscientização. Diretoria e conselho recebem indicadores de risco e tendências ligados ao negócio, em dashboards e scorecards (indicadores x metas).

Macetes para memorizar

💡 RTO x RPO

RTO = Tempo para voltar a operar. RPO = Ponto no passado até onde se aceita perder dados.

💡 Incremental x diferencial

Incremental = só o que mudou desde o último backup de qualquer tipo (restaura com o completo + todos). Diferencial = o que mudou desde o último completo (restaura com o completo + o último).

💡 Sites

Quente liga em minutos, morno em dias, frio só tem as paredes.

💡 Testes do plano

Conferir documentos (checklist), ler o plano em grupo (walkthrough), simular, ativar o site alternativo junto com a produção (paralelo), desligar a produção (interrupção total).

💡 Engenharia social por canal

V de Voz = vishing; S de SMS = smishing; Q de QR = quishing; isca = pendrive.

💡 KPI x KRI

KPI = Performance (como estou indo). KRI = Risco (onde vai doer).

💡 Três linhas

1 opera, 2 supervisiona, 3 audita com independência.

Tabela de memorização: não confunda

Quando é...	...e quando é

Continuidade de negócios (BC) Manter os processos críticos do negócio funcionando durante a crise (inclui pessoas, comunicação, trabalho remoto).	**Recuperação de desastres (DR)** Restaurar sistemas, dados e infraestrutura de TI afetados, dentro do RTO e do RPO.
RTO Tempo para voltar a operar, como sistemas no ar em até 4 horas.	**RPO** Quantidade máxima de dados que se aceita perder, como 15 minutos; define a frequência de backups ou réplicas.
Backup incremental Copia o que mudou desde o último backup de qualquer tipo; restaurar exige o completo e todos os incrementais.	**Backup diferencial** Copia o que mudou desde o último completo; restaurar usa só o completo e o último diferencial.
Site quente Equipado e com dados replicados, assume em minutos; mais caro.	**Site frio** Só espaço, energia e rede; mais barato e com RTO maior. Equipado mas precisando de dias = site morno.
KPI Medir desempenho de um processo, como percentual de patches aplicados no prazo.	**KRI** Alertar sobre aumento de exposição antes do incidente, como percentual de sistemas críticos com patches atrasados.
Teste paralelo Ativar o site alternativo sem desligar a produção.	**Teste de interrupção total** Desligar a produção para testar de verdade: o mais realista e o mais arriscado.
Governança Definir direção, prioridades, apetite de risco e supervisionar (alta direção, comitê executivo).	**Gestão** Planejar e executar programas e controles que transformam a direção em prática.

Números que caem

Item	Valor
Peso médio do domínio na prova	**17,3%**
Regra de backup resiliente	**3-2-1: três cópias, em duas mídias, uma fora do local**
Relação entre RTO e MTD	**RTO deve ser menor que o MTD**
Exemplo de RPO	**15 minutos de perda aceitável = cópias ou réplicas pelo menos a cada 15 minutos**
Exemplo de meta SMART	**Corrigir 95% das falhas críticas em até 15 dias**
Revisão de políticas	**Periodicamente (por exemplo, uma vez por ano) e após mudanças**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Chamar a perda máxima de 15 minutos de dados de RTO.
Como não cair: Perda de dados é RPO e orienta a frequência dos backups. RTO é o tempo para voltar a operar.

⚠ **Alerta de prova:** Confundir MTD com RPO, MTBF ou MTTD.
Como não cair: MTD é o limite de parada antes do dano inaceitável. MTBF mede confiabilidade, MTTD mede detecção, RPO mede perda de dados.

⚠ **Alerta de prova:** Trocar incremental e diferencial.
Como não cair: Pergunte: desde o último backup de qualquer tipo (incremental) ou desde o último completo (diferencial)?

⚠ **Alerta de prova:** Achar que RAID 1 dispensa backup.
Como não cair: RAID aumenta disponibilidade, mas um arquivo apagado some dos dois discos espelhados.

⚠ **Alerta de prova:** Concluir que quem passou em todas as auditorias está seguro.
Como não cair: Conformidade não garante segurança; normas são o mínimo e a gestão de riscos vai além do checklist.

⚠ **Alerta de prova:** Interpretar o aumento de e-mails suspeitos reportados após a campanha como piora.
Como não cair: Mais relatos é sinal positivo de engajamento e uma fonte valiosa de detecção.

⚠ **Alerta de prova:** Atender o pedido do gerente de não cumprir a política, ou negar sem análise.
Como não cair: Boa governança usa exceção formal: justificativa, prazo, controles compensatórios e aceite de risco por quem tem autoridade.

⚠ **Alerta de prova:** Levar à diretoria métricas técnicas detalhadas.
Como não cair: Diretoria e conselho recebem indicadores de risco e tendências ligados ao negócio, com poucos indicadores e cores de alerta.

⚠ **Alerta de prova:** Chamar de revisão de checklist a leitura conjunta do plano passo a passo.
Como não cair: Ler o plano em grupo, sem acionar sistemas, é walkthrough; checklist só confere documentos.

⚠ **Alerta de prova:** Aprovar os pedidos de MFA de madrugada para que parem de chegar.
Como não cair: Pedidos inesperados indicam senha vazada: recusar, avisar a segurança e trocar a senha.

⚠ **Alerta de prova:** Responder ao próprio e-mail do fornecedor para confirmar a nova conta bancária.
Como não cair: Confirmar por telefone já cadastrado ou outro canal conhecido; é o padrão da fraude BEC.

⚠ **Alerta de prova:** Priorizar servidores e dados em um incêndio.
Como não cair: A segurança das pessoas vem primeiro; a recuperação vem em seguida.

⚠ **Alerta de prova:** Colocar a auditoria interna na segunda linha.
Como não cair: Auditoria interna é a terceira linha, com avaliação independente. A segunda supervisiona.

⚠ **Alerta de prova:** Achar que o problema de um plano pronto que ninguém conhece se resolve escrevendo mais.
Como não cair: Falta divulgar e treinar as pessoas; plano só funciona aprovado, conhecido, testado e acessível.

Como cai na prova

📝 **Como cai:** Cenário com um número de tempo (15 minutos de dados, 4 horas para voltar) e a pergunta sobre a métrica.
Como resolver: Se fala de dados perdidos, é RPO; de tempo para retornar, RTO; de limite antes de dano inaceitável, MTD. Confira se a alternativa explica o que a métrica orienta.

📝 **Como cai:** Descrição de um local alternativo ou de um tipo de backup.
Como resolver: Para sites, veja o que já está instalado e quanto tempo leva. Para backups, veja a referência: último backup qualquer (incremental) ou último completo (diferencial).

📝 **Como cai:** Situação de golpe (telefonema, SMS, QR code, voz do presidente, troca de conta bancária) e a pergunta: o que fazer?
Como resolver: A resposta certa é verificar por outro canal conhecido ou oficial e avisar a segurança; nunca usar o canal que o atacante forneceu.

📝 **Como cai:** Qual métrica usar ou como interpretar um indicador?
Como resolver: Associe o objetivo à métrica: perceber = MTTD; isolar = tempo para conter; resolver = MTTR; cobertura = % com MFA ou EDR; eficácia do treinamento = taxa de cliques; backup = restaurações testadas.

📝 **Como cai:** Pergunta de papéis: quem define, quem responde, quem avalia.
Como resolver: Apetite de risco e responsabilidade final: alta direção e conselho. Avaliação independente: auditoria interna (terceira linha). Acionar o plano: equipe de gestão de crise pelos critérios do plano.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Quanto de dados se aceita perder	**RPO**
Prazo para voltar a operar	**RTO**
Limite antes do dano inaceitável	**MTD (RTO menor que MTD)**
Descobrir processos críticos e impacto de parar	**BIA**
Local pronto em minutos / precisa de dias / só espaço e energia	**Site quente / morno / frio**
Ativar o site alternativo sem parar a produção	**Teste paralelo**
Três cópias, duas mídias, uma fora do local	**Regra 3-2-1**
Quem faz, aprova, é consultado e informado	**Matriz RACI**
Governar, Identificar, Proteger, Detectar, Responder, Recuperar	**NIST CSF 2.0**
Governança de TI alinhada ao negócio, ISACA	**COBIT**
E-mail com nome do gestor e projeto real	**Spear phishing (whaling se mirar executivo)**
Pendrive deixado no estacionamento	**Isca (baiting)**
História inventada fingindo ser auditor	**Pretexto (pretexting)**
Métrica que sinaliza aumento de exposição	**KRI**

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

- RPO é perda de dados e frequência de backup; RTO é tempo de volta; RTO menor que MTD.
- Conformidade não é segurança, e a responsabilidade final pelo risco é do conselho e da alta direção.
- RAID não substitui backup; backup só vale se a restauração for testada.
- Em golpe, confirme por outro canal conhecido e avise a segurança.
- Pessoas primeiro em qualquer crise física.

Essenciais para a prova (checklist)

- ☐ Sei explicar o propósito e o benefício do GRC integrado.
- ☐ Sei diferenciar governança de gestão e os papéis do modelo de três linhas.
- ☐ Sei definir RTO, RPO e MTD e a relação entre eles.
- ☐ Sei que a BIA vem antes do plano e o que ela entrega.
- ☐ Sei diferenciar BC, DR e resposta a incidentes.
- ☐ Sei distinguir sites quente, morno e frio e o que é failback.
- ☐ Sei a ordem dos testes do plano, do checklist à interrupção total.
- ☐ Sei diferenciar backup completo, incremental e diferencial e a regra 3-2-1.
- ☐ Sei nomear cada golpe de engenharia social pelo canal e pela técnica.
- ☐ Sei diferenciar KPI, KRI, indicador antecedente e de resultado, MTTD e MTTR.

Questões de revisão do capítulo

R3.1 · Governança de segurança

Por que uma cultura em que ninguém é punido por relatar um clique em phishing ajuda a segurança?

A. Incentiva relatos rápidos, que permitem conter o ataque cedo
B. Permite que os funcionários ignorem as políticas da empresa
C. Garante que nenhum funcionário vai clicar em phishing de novo
D. Elimina a necessidade de controles técnicos contra phishing

R3.2 · Governança de segurança

Em vez de testar controles uma vez por ano, a empresa usa ferramentas que verificam automaticamente, todo dia, se eles continuam funcionando. Que prática é essa?

A. Análise de impacto nos negócios anual
B. Revisão do plano de marketing da empresa
C. Teste de interrupção total do data center
D. Monitoramento contínuo de controles

R3.3 · Governança de segurança

Onde a empresa registra os riscos identificados, com dono, nível, resposta escolhida e prazo?

A. No inventário de cabos
B. Na tabela de rotas
C. No registro de riscos
D. No log do firewall

R3.4 · Governança de segurança

Em um aeroporto, alguém observa por cima do ombro de um funcionário enquanto ele digita a senha no notebook. Que ataque é esse e o que ajuda a evitá-lo?

A. Injeção de SQL; firewall de aplicação web na rede
B. Negação de serviço; servidores redundantes na nuvem
C. Bisbilhotagem visual; filtro de privacidade na tela
D. Força bruta; bloqueio de conta após muitas tentativas

Respostas comentadas

R3.1. A) Incentiva relatos rápidos, que permitem conter o ataque cedo

Por quê: Quem tem medo de punição esconde o erro, e o atacante ganha tempo.

✗ B) Incorreta. Não é o objetivo.
✗ C) Incorreta. Nada garante isso.
✗ D) Incorreta. Controles continuam.

> **Dica de prova:** Relatar sem medo: resposta mais rápida.

R3.2. D) Monitoramento contínuo de controles

Por quê: O monitoramento contínuo detecta falhas de controle mais cedo e gera evidências para auditorias.

✗ A) Incorreta. Trata de processos críticos.
✗ B) Incorreta. Não tem relação.
✗ C) Incorreta. É teste de recuperação.

> **Dica de prova:** Checar controles todo dia: monitoramento contínuo.

R3.3. C) No registro de riscos

Por quê: O registro de riscos apoia o acompanhamento e a prestação de contas sobre os riscos.

✗ A) Incorreta. Lista cabeamento.
✗ B) Incorreta. Orienta pacotes.
✗ D) Incorreta. Registra tráfego.

> **Dica de prova:** Lista de riscos com dono e resposta: registro de riscos.

R3.4. C) Bisbilhotagem visual; filtro de privacidade na tela

Por quê: Atenção ao ambiente e filtros de privacidade reduzem o shoulder surfing.

✗ A) Incorreta. Não é o ataque descrito.
✗ B) Incorreta. Não é o ataque descrito.
✗ D) Incorreta. Não é o ataque descrito.

> **Dica de prova:** Olhar a tela: shoulder surfing.

04

CAPÍTULO 4 · 17,3% DA PROVA

Operações de segurança e resposta a incidentes

Este domínio vale 17,3% e é o mais operacional: segurança de dados (classificação, rotulagem, mascaramento, sanitização e criptografia), operações de segurança (logs, SIEM, triagem, agentes de ameaça e inteligência), resposta a incidentes (fases, plano, evidências e exercícios), proteção de ativos (inventário, EOL, configuração e mudanças) e testes de segurança (varredura, pentest, equipes, SAST e DAST). As perguntas pedem a fase da resposta, a chave certa na criptografia assimétrica ou o nome da prática descrita. Onde mais erro: contenção x erradicação x recuperação, falso positivo x falso negativo, qual chave usar para sigilo e para assinatura e varredura x teste de intrusão.

Neste capítulo

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

Tópicos-chave

Ciclo de vida e estados dos dados

Criar, armazenar, usar, compartilhar, arquivar e destruir, com controles em cada fase, do rótulo na criação à destruição segura. Os dados precisam de proteção em repouso (criptografia de disco), em trânsito (TLS) e em uso (controles de acesso à memória). Guardar dados além do necessário aumenta o risco e pode violar a LGPD: política de retenção com descarte seguro.

Classificação e rotulagem

Do menos ao mais sensível: público, interno, confidencial e restrito (nomes variam). O proprietário dos dados define a classificação e o acesso; o custodiante aplica os controles no dia a dia. A classificação orienta armazenamento, transmissão, cópia e descarte, inclusive em papel. Rótulos visíveis e metadados informam pessoas e permitem controles automáticos, como DLP.

Mascaramento e tokenização

Mascaramento expõe só parte do dado (os quatro últimos dígitos do cartão) e descaracteriza dados pessoais antes de usar cópia de produção em testes. Tokenização substitui o número do cartão por valor aleatório que só um sistema protegido mapeia; tokens não têm valor fora dele, o que reduz risco e escopo de conformidade.

Sanitização e remanência

Dados apagados ou disco formatado ainda podem ser recuperados (remanência). Sanitizar inclui sobrescrever, apagamento criptográfico ou destruição física. Desmagnetização não funciona em SSD, que usa memória flash: use apagamento criptográfico, comandos de sanitização do fabricante ou destruição física. Desativar servidor: remover acessos, sanitizar mídias e dar baixa no inventário.

Criptografia simétrica x assimétrica

Simétrica (AES) é rápida e usada para grandes volumes; seu problema é distribuir a chave secreta com segurança. Assimétrica permite trocar chaves entre quem nunca se encontrou e fazer assinaturas; depois, a simétrica é usada pelo desempenho. Backups levados para cofre externo devem ser cifrados, porque mídias se perdem no transporte. Computadores quânticos poderão quebrar RSA e ECC; por isso o NIST publicou algoritmos pós-quânticos, como os dos FIPS 203 e 204, enquanto AES e hashes seguem em uso.

Qual chave usar

Para sigilo, cifra-se com a chave pública do destinatário (Ana usa a pública de Bruno). Para assinar, o autor usa a própria chave privada, e qualquer um verifica com a pública dele. Chaves mais críticas são geradas e guardadas em HSM ou cofre de chaves, que controla o uso, registra acessos e dificulta a extração.

Hash

Função de mão única: não se descriptografa. Qualquer mudança no arquivo gera hash diferente, o que verifica integridade (SHA-256). MD5 e SHA-1 têm colisões práticas; SHA-2 e SHA-3 são recomendados. Senhas se guardam como hash com sal único e algoritmo lento (bcrypt, scrypt, Argon2), dificultando ataques de dicionário.

PKI e certificados

A autoridade certificadora (CA) emite e assina certificados, atestando que a chave pública pertence a uma identidade, e pode revogá-los; não guarda chaves privadas dos usuários. O certificado X.509 traz chave pública, identidade do titular, validade, emissor e usos permitidos, assinados pela CA; nunca a chave privada. Inventariar e monitorar validades evita sites fora do ar por certificado vencido.

Logs e monitoramento

Registrar logins bem-sucedidos e falhos com usuário, origem e horário, além de mudanças de privilégio e ações administrativas. Enviar logs a servidor separado e protegido contra alteração impede que invasores apaguem rastros. Sincronizar relógios com NTP e centralizar logs permite montar a sequência dos fatos. Retenção pelo prazo de política, leis e contratos.

SIEM, SOC e automação

O SOC monitora, detecta e responde com SIEM, EDR, triagem e escalonamento. O SIEM normaliza logs de formatos diferentes e correlaciona eventos isolados em um alerta com contexto; a triagem prioriza por gravidade e ativos afetados. Milhares de alertas irrelevantes geram fadiga de alertas. SOAR executa playbooks automaticamente; UEBA aprende o comportamento normal e alerta desvios.

Evento, incidente e qualidade dos alertas

Evento é qualquer ocorrência (login bem-sucedido); incidente viola ou ameaça a segurança (acesso não autorizado confirmado). Falso positivo é alerta sem ataque real (backup legítimo); falso negativo é ataque não detectado; verdadeiro positivo é ataque real alertado; verdadeiro negativo é ausência de alerta sem ataque.

Agentes de ameaça

APT: grupo com muitos recursos, muitas vezes patrocinado por Estado, com acesso escondido por meses para espionagem ou sabotagem. Crime organizado: motivação financeira (ransomware com resgate). Hacktivista: protesto político, busca visibilidade. Script kiddie: ferramentas prontas, pouca habilidade e foco. Ameaça interna maliciosa (funcionário que copia dados) ou não intencional (envio por engano). Espionagem corporativa: rival atrás de segredos comerciais.

Inteligência de ameaças

CTI reúne informações sobre atores, táticas e indicadores para antecipar defesas. IoC: IPs, domínios, hashes ligados a ataques. TTPs são mais difíceis de mudar que IPs e domínios, por isso detectá-las é mais eficaz. ISAC compartilha inteligência entre empresas do setor. Threat hunting busca invasores sem alerta, por hipóteses. MITRE ATT&CK descreve táticas e técnicas; Cyber Kill Chain divide o ataque em etapas e interromper qualquer uma pode impedi-lo.

Fases da resposta a incidentes

Preparação (plano, equipe, ferramentas, contatos, exercícios), detecção e análise (confirmar se o alerta é real e o escopo), contenção (isolar máquinas), erradicação (remover malware, fechar a falha, trocar senhas), recuperação (restaurar de backups limpos e monitorar) e lições aprendidas (atualizar planos, controles e treinamentos). Vários incidentes simultâneos: priorizar por gravidade e impacto no negócio.

Plano de resposta e comunicação

Além dos passos técnicos, define papéis, contatos, escalonamento, comunicação interna e externa e obrigações legais. O coordenador do incidente coordena decisões e tarefas; jurídico e alta direção decidem sobre polícia e reguladores; vazamento relevante de dados pessoais é comunicado à ANPD, além dos titulares. Informações só a quem precisa saber; playbooks detalham a resposta por tipo de incidente; relatório final traz linha do tempo, causa, impacto, ações e melhorias.

Evidências e exercícios

Cadeia de custódia registra quem coletou cada evidência, quando, como e com quem ficou. Ordem de volatilidade: coletar primeiro memória RAM e conexões ativas. Evidências ficam em local protegido, com acesso restrito e registrado. Exercício de mesa (tabletop) discute o cenário em sala; simulação executa as ações. O plano é revisado e testado periodicamente e após mudanças relevantes.

Proteção de ativos, configuração e mudanças

Não se protege o que não se conhece: inventário de ativos e de software, com dono definido. Sistemas EOL ficam com falhas sem correção: substituir, isolar ou compensar. Hardening com linha de base (CIS Benchmarks) e verificação de desvios (drift). Gestão de mudanças registra, avalia impacto, aprova e prevê rollback; mudança emergencial é documentada e revisada depois; patches são testados em homologação.

Testes de segurança

Varredura de vulnerabilidades lista falhas, é automatizada e frequente; a autenticada é mais completa e com menos falsos positivos; o CVSS dá nota de 0 a 10, priorizada junto com exposição e criticidade. Teste de intrusão explora falhas e exige escopo, autorização e regras de engajamento por escrito; depois da correção, retestar. Caixa-preta, cinza e branca variam o conhecimento dado ao testador. Red team ataca, blue defende, purple une os dois e white arbitra. SAST analisa código parado, DAST testa a aplicação rodando, modelagem de ameaças (STRIDE) vem no projeto e bug bounty paga pesquisadores externos.

Macetes para memorizar

💡 Fases da resposta

Prepara, Detecta, Contém, Erradica, Recupera, Aprende: isolar = conter, limpar = erradicar, restaurar = recuperar.

💡 Chaves assimétricas

Segredo para alguém: pública DELE. Assinatura minha: privada MINHA.

💡 Hash

Hash é impressão digital do arquivo: só confere, nunca volta.

💡 Cores das equipes

Vermelho ataca, azul defende, roxo mistura os dois, branco apita o jogo.

💡 SAST x DAST

S de Static/Stopped (código parado); D de Dynamic (rodando).

💡 Caixas

Preta = nada sabe; cinza = sabe um pouco; branca = vê tudo, até o código.

Ordem de volatilidade

Colete primeiro o que evapora: RAM antes do disco.

Varredura x pentest

Varredura LISTA, pentest EXPLORA.

Tabela de memorização: não confunda

Quando é...	...e quando é
Evento Qualquer ocorrência observável, como um login bem-sucedido.	**Incidente** Ocorrência que viola ou ameaça a segurança, como acesso não autorizado confirmado.
Criptografia simétrica Cifrar grandes volumes com rapidez (AES); exige distribuir a chave secreta.	**Criptografia assimétrica** Trocar chaves entre quem nunca se encontrou e assinar; cifrar com a pública do destinatário.
Mascaramento Mostrar só parte do dado na tela ou descaracterizar dados para testes.	**Tokenização** Substituir o dado por valor aleatório que só um sistema protegido mapeia de volta.
Varredura de vulnerabilidades Listar falhas de forma automatizada e frequente, sem explorá-las.	**Teste de intrusão** Simular ataque real explorando as falhas, com escopo, autorização e regras de engajamento.
SAST Analisar o código-fonte sem executar, cedo no desenvolvimento.	**DAST** Testar a aplicação em execução enviando entradas maliciosas como um atacante externo.
Contenção Limitar a propagação: isolar da rede as máquinas infectadas.	**Erradicação** Remover a causa: apagar o malware, fechar a falha explorada, trocar senhas. Depois vem a recuperação.
Exercício de mesa Discutir em sala, passo a passo, um cenário hipotético, sem afetar sistemas.	**Simulação completa** Executar de fato as ações do plano, com mais realismo e custo.

Números que caem

Item	Valor
Peso médio do domínio na prova	**17,3%**
Escala do CVSS	**Nota de 0 a 10 conforme a gravidade técnica**
Padrões pós-quânticos do NIST	**FIPS 203 e FIPS 204**
Hashes	**MD5 e SHA-1 com colisões práticas; SHA-2 e SHA-3 recomendados**

Estados dos dados	**3: em repouso, em trânsito e em uso**
Ciclo de vida dos dados	**6 fases: criar, armazenar, usar, compartilhar, arquivar e destruir**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Achar que é possível descriptografar o hash de uma senha.
Como não cair: Hash é mão única; atacantes só tentam adivinhar entradas que gerem o mesmo hash, por isso sal e algoritmo lento.

⚠ **Alerta de prova:** Cifrar a mensagem para Bruno com a chave privada de Ana ou de Bruno.
Como não cair: Sigilo usa a chave pública do destinatário; a privada de Ana serviria para assinar e a de Bruno ela nem deve ter.

⚠ **Alerta de prova:** Assinar o documento com a chave pública do leitor.
Como não cair: Assinatura usa a chave privada do próprio autor; a pública do leitor serve para cifrar para ele.

⚠ **Alerta de prova:** Usar AES para verificar se o arquivo baixado foi alterado.
Como não cair: AES protege o sigilo; integridade se verifica comparando o hash (SHA-256).

⚠ **Alerta de prova:** Desmagnetizar SSDs antes do descarte.
Como não cair: SSD usa memória flash; use apagamento criptográfico, sanitização do fabricante ou destruição física.

⚠ **Alerta de prova:** Dizer que a varredura explora as falhas e o pentest só as lista.
Como não cair: É o contrário: varredura lista, pentest explora. E ambos exigem autorização.

⚠ **Alerta de prova:** Achar que a varredura autenticada dispensa autorização dos donos.
Como não cair: A vantagem é ser mais completa e com menos falsos positivos; a autorização continua necessária.

⚠ **Alerta de prova:** Chamar de falso negativo o alerta disparado por um backup legítimo.
Como não cair: Alerta sem ataque real é falso positivo; falso negativo é deixar de alertar um ataque.

⚠ **Alerta de prova:** Classificar o isolamento das máquinas infectadas como erradicação.
Como não cair: Isolar é contenção; remover malware e fechar a falha é erradicação; restaurar e monitorar é recuperação.

⚠ **Alerta de prova:** Restaurar qualquer backup na recuperação.
Como não cair: Backup infectado traz o atacante de volta: usar backups limpos e monitorar o retorno.

⚠ **Alerta de prova:** Coletar primeiro o disco rígido do computador comprometido.
Como não cair: Ordem de volatilidade: primeiro o que se perde mais rápido, como a memória RAM e conexões ativas.

⚠ **Alerta de prova:** Confundir equipe roxa com equipe branca.
Como não cair: Purple une ataque e defesa compartilhando em tempo real; white define regras, acompanha e arbitra.

⚠ **Alerta de prova:** Aplicar a correção urgente sem registro para ganhar tempo, ou esperar o comitê semanal.
Como não cair: Mudança emergencial: aprovação rápida, documentada e revisada depois.

⚠ **Alerta de prova:** Achar que bloquear os IPs do atacante é a defesa mais duradoura.
Como não cair: IPs, domínios e hashes mudam rápido; TTPs são mais difíceis de mudar e detectá-las é mais eficaz.

Como cai na prova

📝 **Como cai:** A equipe fez tal ação durante o incidente. Em que fase ela está?
Como resolver: Mapeie o verbo: confirmar alerta e escopo = detecção e análise; isolar = contenção; remover malware, fechar falha, trocar senhas = erradicação; restaurar e monitorar = recuperação; reunião pós = lições aprendidas; plano e treino = preparação.

📝 **Como cai:** Cenário de criptografia com duas pessoas e a pergunta sobre qual chave usar.
Como resolver: Pergunte o objetivo: sigilo = pública do destinatário; assinatura/não repúdio = privada do remetente. Verificar alteração = hash; problema da simétrica = distribuir chaves.

📝 **Como cai:** Descrição de uma ferramenta ou função de operações (SIEM, SOAR, UEBA, CTI).
Como resolver: Padronizar = normalização; ligar eventos = correlação; resposta automática por playbook = SOAR; comportamento fora do normal = UEBA; indicadores compartilhados no setor = ISAC.

📝 **Como cai:** Tipo de teste descrito pela informação dada ao testador ou pelo alvo.
Como resolver: Pela informação: caixa-preta, cinza ou branca. Pelo alvo: código parado (SAST), aplicação rodando (DAST), prédio (pentest físico). Pelo objetivo: listar (varredura) ou explorar (pentest).

📝 **Como cai:** Agente de ameaça descrito por recursos e motivação.
Como resolver: Estado e espionagem longa = APT; resgate e dinheiro = crime organizado; protesto = hacktivista; ferramentas prontas sem foco = script kiddie; funcionário = ameaça interna (maliciosa ou não intencional); rival = espionagem corporativa.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Mostrar só os quatro últimos dígitos do cartão	**Mascaramento**
Número do cartão trocado por valor aleatório mapeado por sistema protegido	**Tokenização**
Dados recuperáveis após formatar	**Remanência; sanitização**
Logs de formatos diferentes convertidos para um padrão	**Normalização no SIEM**
Várias falhas de login + login com sucesso + cópia grande pela mesma conta	**Correlação de eventos**
Plataforma bloqueia o remetente e abre chamado sozinha	**SOAR**
Usuário baixando volume incomum de madrugada	**UEBA**
IP de comando e controle nos logs	**Indicador de comprometimento (IoC)**
Buscar invasores sem alerta, a partir de hipóteses	**Threat hunting**
Quem coletou a evidência, quando e com quem ficou	**Cadeia de custódia**
Gestores discutem um ataque hipotético em sala	**Exercício de mesa (tabletop)**
Servidores afastados da linha de base aprovada	**Desvio de configuração (drift)**
Testador recebe só conta comum e lista de endereços	**Caixa-cinza**
Entrar no prédio logo atrás de quem passou o crachá	**Tailgating (pentest físico)**

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

- Sigilo = chave pública do destinatário; assinatura = chave privada do autor; integridade = hash.
- Isolar é contenção; limpar é erradicação; restaurar de backup limpo e monitorar é recuperação.
- Varredura lista, pentest explora, e todo teste precisa de autorização por escrito.
- SSD não se desmagnetiza; use apagamento criptográfico ou destruição física.
- Evidência exige cadeia de custódia e coleta do mais volátil primeiro.

Essenciais para a prova (checklist)

- ☐ Sei as fases do ciclo de vida dos dados, os três estados e quem classifica os dados.
- ☐ Sei diferenciar mascaramento, tokenização, sanitização e remanência.
- ☐ Sei qual chave usar para sigilo e para assinatura e o que um certificado X.509 contém.
- ☐ Sei por que hash não se reverte, como guardar senhas e quais algoritmos estão quebrados.
- ☐ Sei o que o SIEM faz (normalização, correlação, triagem) e o papel de SOC, SOAR e UEBA.
- ☐ Sei diferenciar evento de incidente e os quatro resultados de alerta.
- ☐ Sei identificar agentes de ameaça pela motivação e usar IoC, TTP, MITRE ATT&CK e Kill Chain.
- ☐ Sei as seis fases da resposta a incidentes e o que o plano deve definir.
- ☐ Sei aplicar inventário, EOL, linha de base, drift, gestão de mudanças e rollback.
- ☐ Sei diferenciar varredura, pentest, caixas, equipes coloridas, SAST, DAST e modelagem de ameaças.

Questões de revisão do capítulo

R4.1 · Operações de segurança e resposta a incidentes

Uma empresa paga recompensas a pesquisadores externos que encontram e relatam falhas em seus sistemas, seguindo regras publicadas. Que programa é esse?

A. Programa de conscientização em segurança para funcionários
B. Plano de continuidade de negócios
C. Programa de recompensa por bugs (bug bounty)
D. Política de uso aceitável dos recursos

R4.2 · Operações de segurança e resposta a incidentes

A política diz que documentos confidenciais impressos devem ser destruídos em fragmentadora ao fim do uso. O que define essa regra?

A. A marca da fragmentadora utilizada
B. O tipo de papel comprado pela empresa
C. O tratamento exigido pela classificação
D. A velocidade de impressão do escritório

R4.3 · Operações de segurança e resposta a incidentes

Qual algoritmo de hash não deve mais ser usado para segurança, por ter colisões conhecidas?

A. O algoritmo SHA-256
B. O algoritmo MD5
C. O algoritmo SHA-384
D. O algoritmo SHA3-256

R4.4 · Operações de segurança e resposta a incidentes

Um servidor roda um sistema operacional que não recebe mais atualizações do fabricante. Qual é o principal risco?

A. Vulnerabilidades novas ficam sem correção
B. A licença passa a ser gratuita para sempre
C. Os backups deixam de ser necessários
D. O servidor fica mais rápido sem atualizações

Respostas comentadas

R4.1. C) Programa de recompensa por bugs (bug bounty)

Por quê: Regras claras definem escopo e conduta, tornando a pesquisa autorizada.

✗ A) Incorreta. Treina funcionários.
✗ B) Incorreta. Mantém operações.
✗ D) Incorreta. Regras de uso.

> **Dica de prova:** Pagar por falhas encontradas: bug bounty.

R4.2. C) O tratamento exigido pela classificação

Por quê: A classificação orienta armazenamento, transmissão, cópia e descarte, inclusive em papel.

✗ A) Incorreta. Não tem relação.
✗ B) Incorreta. Não tem relação.
✗ D) Incorreta. Não tem relação.

> **Dica de prova:** Destruir confidencial impresso: regra da classificação.

R4.3. B) O algoritmo MD5

Por quê: MD5 e SHA-1 têm colisões práticas; SHA-2 e SHA-3 são recomendados.

✗ A) Incorreta. Ainda considerado seguro.
✗ C) Incorreta. Ainda considerado seguro.
✗ D) Incorreta. Ainda considerado seguro.

> **Dica de prova:** Hash quebrado: MD5.

R4.4. A) Vulnerabilidades novas ficam sem correção

Por quê: Sistemas em fim de vida (EOL) devem ser substituídos, isolados ou protegidos por controles compensatórios.

✗ B) Incorreta. Não é o risco.
✗ C) Incorreta. Não é o risco.
✗ D) Incorreta. Não é o risco.

> **Dica de prova:** Sistema sem atualização: falhas sem correção.

05

CAPÍTULO 5 · 24% DA PROVA

Princípios de segurança

Este é o domínio de maior peso (24%) e a base de todo o resto. Preciso reconhecer na hora qual propriedade foi afetada (confidencialidade, integridade, disponibilidade, não repúdio, autenticidade, privacidade), separar identificação, autenticação, autorização e contabilização e dominar o vocabulário de risco: ameaça, vulnerabilidade, risco inerente e residual, apetite e as quatro respostas. As perguntas são cenários curtos (planilha enviada ao fornecedor errado, site fora do ar, valor alterado, seguro contratado) que pedem o nome do conceito, além de cálculo de SLE e ALE, a hierarquia política, norma, procedimento e diretriz, leis e frameworks e o Código de Ética da ISC2 com a ordem dos cânones. Onde mais erro: confundir confidencialidade com privacidade, norma com diretriz, transferir com aceitar e classificar controles, que sempre têm duas dimensões (técnico, administrativo ou físico + preventivo, detectivo, corretivo, dissuasivo, diretivo ou compensatório).

Neste capítulo

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

Tópicos-chave

Tríade CIA

Confidencialidade: só pessoas autorizadas acessam a informação. Integridade: os dados não são alterados de forma indevida ou não autorizada. Disponibilidade: acesso oportuno e confiável para quem precisa. Ransomware que bloqueia arquivos afeta a disponibilidade; se o atacante também copiar os dados (dupla extorsão), afeta a confidencialidade.

Conflitos e prioridades na CIA

Controles equilibram os três objetivos: liberar a pasta de contratos para todos aumenta a disponibilidade e reduz a confidencialidade. Cifrar backups e perder a única cópia da chave mostra que sigilo sem gestão de chaves derruba a disponibilidade. Em sistemas de controle industrial, a disponibilidade costuma ter a maior prioridade.

Identificação e AAA

O nome de usuário identifica; a senha autentica (comprova a identidade alegada). Depois vem a autorização (o que pode fazer, como ler sem alterar) e a contabilização (accounting: registra o que fez, para auditoria). RADIUS e TACACS+ centralizam o AAA de roteadores e acesso remoto.

Não repúdio

Impede que alguém negue ter realizado uma ação; o mecanismo típico é a assinatura digital com a chave privada do autor. Depende de a chave privada estar sob controle exclusivo do titular: se o diretor empresta o token à assistente, o não repúdio fica comprometido. A assinatura também comprova integridade e origem, mas não dá sigilo.

Autenticidade e autenticação de dispositivos

O navegador verifica o certificado do site emitido por autoridade confiável, o que garante a autenticidade do servidor. Certificados emitidos pela empresa em notebooks autenticam dispositivos, apoiando a Confiança Zero. No TLS mútuo (mTLS), cliente e servidor apresentam e verificam certificados.

Responsabilização (accountability)

Ligar cada ação a uma pessoa, com usuário, data e hora. Depende de contas individuais, relógios sincronizados e logs protegidos. Vários técnicos usando a mesma conta admin destroem a responsabilização individual; controle de versões e trilhas de auditoria também apoiam a integridade.

Privacidade e princípios da LGPD

Privacidade envolve finalidade, transparência e controle do titular sobre seus dados pessoais. Princípios cobrados: limitação da finalidade (usar dados só para o fim informado), minimização (coletar só o necessário), transparência (aviso de privacidade) e qualidade (correção de dados inexatos). Privacy by design inclui requisitos de privacidade desde o início do projeto.

Direitos do titular e papéis na LGPD

O titular pode confirmar o tratamento, acessar, corrigir, pedir eliminação e portabilidade; a revogação do consentimento deve ser fácil e gratuita e os tratamentos já realizados continuam válidos. Controlador decide sobre o tratamento; operador trata em nome dele (ex.: provedor de folha); encarregado (DPO) é o canal com titulares e ANPD. Compartilhar com terceiro exige base legal, finalidade clara e contrato com o operador.

Dados sensíveis, crianças, pseudonimização e anonimização

Dados sensíveis pela LGPD: saúde, religião, origem racial e biometria, com bases legais e cuidados mais rígidos. Dados de crianças exigem consentimento específico de um dos pais ou responsável. Pseudonimizado (código com tabela de volta guardada à parte) continua sendo dado pessoal; anonimizado de forma eficaz e irreversível, em regra, deixa de ser.

Ameaça, vulnerabilidade, exploit e risco

Vulnerabilidade é a fraqueza (falta de patch, senha de quatro dígitos permitida); ameaça é o agente ou evento que pode explorá-la (grupo criminoso, enchente, funcionário que apaga tabela sem querer); exploit é o código que aproveita a falha. Risco é a combinação de probabilidade e impacto. Exposição à internet, exploit público e inteligência de ataques ao setor aumentam a probabilidade.

Ciclo de gestão de riscos

Identificar, avaliar, tratar e monitorar, de forma contínua. O primeiro passo da avaliação é identificar os ativos e seu valor; priorizar por valor e criticidade para o negócio. Migração para nuvem, fornecedores novos, técnica de ataque nova ou uso de IA generativa pública exigem reavaliar e atualizar o registro de riscos, que é um documento vivo.

Respostas ao risco

Mitigar: aplicar controles (patch, MFA). Transferir: seguro cibernético passa o impacto financeiro, mas a empresa continua responsável pela proteção e pela reputação. Evitar: deixar de oferecer o serviço. Aceitar: seguir sem controle novo, de forma consciente, dentro do apetite, com registro formal, assinatura de quem tem autoridade e prazo. Ignorar não é resposta válida.

Risco inerente, residual, apetite e KRI

Inerente é o risco antes de qualquer controle; residual é o que sobra depois. Apetite de risco, definido pela direção, é quanto risco a organização aceita. Residual acima do apetite exige controles adicionais ou decisão da direção; KRI acima do limite de tolerância exige escalar e acionar o tratamento. O dono do risco é o gestor do processo afetado.

Análise quantitativa x qualitativa

Quantitativa usa valores: SLE = valor do ativo x fator de exposição (EF); ALE = SLE x ARO (vezes por ano). Permite comparar com o custo do controle: controle mais caro que a perda anual esperada não se justifica, salvo exigência legal ou de reputação. Qualitativa usa escalas alto/médio/baixo e matriz de calor; sua limitação é depender do julgamento de quem avalia.

Política, norma, procedimento e diretriz

Política define o que fazer, é obrigatória e aprovada pela alta direção. Norma (padrão) define requisitos obrigatórios e mensuráveis (ex.: AES com chave de 256 bits). Procedimento é o passo a passo (como criar uma conta). Diretriz recomenda sem obrigar (frases longas como senha). Política sem fiscalização e sanções não é eficaz, e a lei prevalece sobre a política interna.

Leis, regulações e frameworks

Leis são obrigatórias: LGPD, GDPR (vale para quem trata dados de residentes da UE), HIPAA (saúde nos EUA), SOX (controles sobre relatórios financeiros), Marco Civil da Internet (guarda de registros de acesso) e Resolução CMN nº 4.893 (bancos). PCI DSS é imposto por contrato pelas bandeiras. Frameworks são orientação voluntária e devem ser adaptados ao porte da empresa: ISO/IEC 27001 (SGSI certificável, Declaração de Aplicabilidade), ISO/IEC 27002 (implementação dos controles), NIST SP 800-53 (catálogo de controles), CIS Benchmarks (configuração segura) e Controles CIS (lista priorizada).

Tipos e funções de controles

Categorias: técnico (hardware/software: firewall, criptografia, DLP), administrativo (política, treinamento, verificação de antecedentes, termo de confidencialidade) e físico (crachá, câmera, cerca, vigilante, mantrap). Funções: preventivo, detectivo, corretivo, de recuperação, dissuasivo, diretivo e compensatório (proteção equivalente quando o controle principal não pode ser aplicado).

Código de Ética da ISC2 e conduta profissional

Cânones aplicados em ordem: proteger a sociedade, o bem comum e a infraestrutura; agir com honra, honestidade e justiça (o que inclui agir com legalidade); prestar serviço diligente e competente aos contratantes; promover e proteger a profissão. Devido cuidado é fazer o que uma pessoa prudente faria; devida diligência é investigar e verificar continuamente. A ISC2 exige CPE e mantém processo de queixas que pode levar à perda da certificação.

Macetes para memorizar

💡 Tríade CIA

Vazou = C. Mudou = I. Parou = D.

💡 AAA

Quem é (autenticação), o que pode (autorização), o que fez (contabilização). O nome de usuário só identifica.

💡 Cálculo de risco

SLE (Single = uma ocorrência) = Valor x EF. ALE (Annual = por ano) = SLE x ARO.

💡 Documentos

Política diz O QUÊ; norma diz o REQUISITO obrigatório; procedimento diz COMO; diretriz só SUGERE.

💡 Respostas ao risco

Mitigar = controle. Transferir = seguro. Evitar = parar. Aceitar = assinar com prazo.

💡 Cânones da ISC2

Ordem fixa: Sociedade, Honra, Contratantes, Profissão. Em conflito, vale o que vem primeiro.

💡 Devido cuidado x diligência

Cuidado FAZ; diligência CONFERE.

💡 Classificar controles

Sempre duas palavras: categoria (técnico, administrativo, físico) + função (preventivo, detectivo, corretivo...).

Tabela de memorização: não confunda

Quando é...	...e quando é
Confidencialidade Proteger a informação contra acesso não autorizado: arquivo cifrado, impressão com PIN, planilha enviada à pessoa errada.	**Privacidade** Direitos do titular sobre dados pessoais: finalidade, consentimento, transparência, acesso, correção e eliminação.

Pseudonimização Nomes trocados por códigos com tabela de correspondência guardada à parte; ainda é dado pessoal.	**Anonimização** Publicar estatísticas sem que ninguém possa ser identificado, nem com dados extras; de forma eficaz, deixa de ser dado pessoal.
Norma (padrão) Requisito obrigatório e mensurável que detalha a política, como o algoritmo e o tamanho de chave exigidos.	**Diretriz** Recomendação de boa prática sem obrigar, com flexibilidade, como sugerir frases longas como senha.
Risco inerente Nível de risco antes de aplicar qualquer controle.	**Risco residual** O que sobra depois de firewall, MFA e treinamento; deve ficar dentro do apetite ou ser aceito formalmente.
Transferir o risco Contratar seguro cibernético ou passar o impacto a terceiros; a responsabilidade pela proteção e reputação continua.	**Aceitar o risco** Seguir sem controle novo porque o custo supera a perda esperada e o risco está dentro do apetite, com registro, aprovação e prazo.
Devido cuidado Agir como uma empresa prudente: definir políticas, aplicar o patch disponível de uma falha conhecida.	**Devida diligência** Investigar e verificar: checar se as políticas são cumpridas, avaliar certificações, contratos e incidentes do fornecedor antes de contratar.
Autenticação Comprovar quem é, com senha, código no celular ou biometria.	**Autorização** Definir o que a pessoa já autenticada pode fazer, como abrir relatórios de vendas sem poder alterá-los.

Números que caem

Item	Valor
Peso médio do domínio na prova	**24% (o maior)**
Perda esperada em um evento	**SLE = valor do ativo x fator de exposição**
Perda anual esperada	**ALE = SLE x ARO**
Exemplo de ALE	**R$ 50 mil x 40% = SLE R$ 20 mil; uma vez a cada 10 anos (ARO 0,1) = R$ 2.000 por ano**
Exemplo de SLE	**EF de 25% sobre R$ 2 milhões = R$ 500 mil**
Marco Civil da Internet	**Provedores de aplicações guardam registros de acesso por seis meses**
Bancos no Brasil	**Resolução CMN nº 4.893 exige política de segurança cibernética**
Cânones do Código de Ética da ISC2	**4, aplicados em ordem (sociedade primeiro)**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Marcar confidencialidade quando o ransomware cifra os arquivos e a empresa fica sem acesso.
Como não cair: Sem acesso é disponibilidade. Só entra confidencialidade se o enunciado disser que o atacante copiou os dados (dupla extorsão).

⚠ **Alerta de prova:** Achar que a assinatura digital garante o sigilo da mensagem.
Como não cair: Assinatura (hash + chave privada do autor) comprova integridade, origem e não repúdio. Para sigilo é preciso cifrar.

⚠ **Alerta de prova:** Chamar o seguro cibernético de aceitar ou evitar o risco.
Como não cair: Seguro é transferir. Evitar exige parar a atividade; aceitar é não fazer nada novo de forma consciente.

⚠ **Alerta de prova:** Escolher ignorar o risco como uma resposta possível.
Como não cair: As respostas válidas são mitigar, transferir, evitar e aceitar. Ignorar não é resposta.

⚠ **Alerta de prova:** Classificar a senha de quatro dígitos permitida pelo sistema como ameaça.
Como não cair: Fraqueza é vulnerabilidade. Ameaça é o agente ou evento que explora (o grupo criminoso, a enchente).

⚠ **Alerta de prova:** Classificar o IPS como detectivo porque ele também detecta.
Como não cair: A função principal do IPS é impedir o tráfego malicioso: técnico e preventivo. O IDS só alerta: técnico e detectivo.

⚠ **Alerta de prova:** Chamar o alarme da porta da sala de servidores de preventivo.
Como não cair: Alarme detecta e alerta: físico e detectivo. Fechaduras e catracas previnem; vigilante que barra é físico e preventivo.

⚠ **Alerta de prova:** Classificar a revisão semanal de relatórios de acesso como controle técnico.
Como não cair: A revisão é processo humano: administrativo e detectivo. Técnica é a ferramenta que gera o relatório.

⚠ **Alerta de prova:** Marcar dissuasivo para a placa Acesso permitido somente a pessoal autorizado.
Como não cair: Placa que diz o que fazer é diretiva (pode também dissuadir). A placa Área monitorada por câmeras, feita para desencorajar, é dissuasiva.

⚠ **Alerta de prova:** Chamar de controle de recuperação o isolamento de um sistema legado que não aceita MFA.
Como não cair: Controle que substitui o principal impossível de aplicar é compensatório. Recuperação restaura após um evento.

⚠ **Alerta de prova:** Dizer que dados pseudonimizados deixam de ser dados pessoais.
Como não cair: Se existe a tabela que permite voltar ao nome, continua dado pessoal. Só a anonimização eficaz e irreversível tira esse status.

⚠ **Alerta de prova:** Seguir a política interna quando ela permite guardar dados por mais tempo que a lei.
Como não cair: Leis e regulamentos estão acima das políticas; a política deve ser corrigida.

⚠ **Alerta de prova:** Tratar o PCI DSS ou um framework como lei.
Como não cair: Framework é orientação voluntária; PCI DSS é imposto por contrato. Ambos podem virar obrigatórios por contrato ou regulação setorial.

⚠ **Alerta de prova:** Obedecer ao gestor que pede para apagar logs e esconder uma falha do auditor.
Como não cair: Seguir ordens não justifica conduta desonesta ou ilegal: recusar. Em conflito entre cânones, a sociedade vem primeiro.

Como cai na prova

📝 **Como cai:** Cenário de um fato ocorrido e a pergunta: qual propriedade foi violada ou protegida?
Como resolver: Ache o verbo central: vazou/expôs = confidencialidade; alterou = integridade; ficou indisponível = disponibilidade; não pode negar = não repúdio; finalidade/consentimento = privacidade.

📝 **Como cai:** Cálculo com valor do ativo, percentual destruído e frequência em anos.
Como resolver: SLE = valor x EF. Converta a frequência em ARO (uma vez a cada 10 anos = 0,1). ALE = SLE x ARO. Ex.: R$ 50 mil x 40% = R$ 20 mil; x 0,1 = R$ 2.000 por ano.

📝 **Como cai:** Como classificar este controle? com alternativas em pares (Técnico e preventivo, Físico e detectivo...).
Como resolver: Decida primeiro a categoria (tecnologia, processo/pessoa ou barreira física) e depois a função principal (impede, descobre, corrige, desencoraja, orienta ou substitui).

📝 **Como cai:** Empresa toma uma decisão sobre um risco: qual resposta foi escolhida?
Como resolver: Seguro = transferir; parar o serviço = evitar; aplicar patches/MFA = mitigar; seguir sem controle novo de forma consciente = aceitar.

📝 **Como cai:** Dilema ético de um profissional (presente, conflito de interesses, ordem do chefe, falha em software de terceiro).
Como resolver: Escolha a alternativa honesta, legal e transparente: declarar, recusar, relatar pelos canais, divulgação coordenada com o fabricante. Em conflito, siga a ordem dos cânones.

📝 **Como cai:** Qual documento ou referência usar? (passo a passo, requisito, recomendação, SGSI certificável, catálogo de controles).
Como resolver: Passo a passo = procedimento; requisito obrigatório = norma; recomendação = diretriz; SGSI certificável = ISO 27001; implementar controles = ISO 27002; catálogo do governo dos EUA = NIST SP 800-53; configuração segura = CIS Benchmarks.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Dado enviado por engano a quem não devia ver	**Confidencialidade**
Valor alterado sem autorização, dose trocada no prontuário, hash comparado ao abrir o arquivo	**Integridade**
Site fora do ar, arquivos inacessíveis	**Disponibilidade**
Não pode negar que assinou ou aprovou	**Não repúdio (chave privada exclusiva)**
Registrar o que o usuário fez depois de entrar	**Contabilização (accounting)**
Coleta de dados além do necessário para o serviço	**Minimização de dados**
Dados usados para outro fim sem avisar o titular	**Limitação da finalidade**
Percentual do ativo perdido em um evento	**Fator de exposição (EF)**
Quantas vezes por ano o evento ocorre	**ARO; ALE = SLE x ARO**
Diretoria declara quanto risco aceita	**Apetite de risco**
Controle substituto quando o principal não pode ser aplicado	**Controle compensatório**
Recomendação sem obrigar	**Diretriz**
Controles do Anexo A aplicados e excluídos com justificativa	**Declaração de Aplicabilidade (ISO 27001)**

Conflito de interesses, presente de fornecedor, mentir sobre certificação	**Agir com honra e honestidade: declarar, recusar, afastar-se**

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

- Controle sempre tem categoria e função; o IPS é preventivo e o IDS é detectivo.
- Seguro transfere o impacto financeiro, mas nunca a responsabilidade pela proteção e pela reputação.
- A lei prevalece sobre a política interna; framework orienta, lei obriga, PCI DSS vem por contrato.
- Não repúdio exige chave privada sob controle exclusivo do titular.
- Em dilema ético, a sociedade vem primeiro e ordens do chefe não justificam desonestidade.

Essenciais para a prova (checklist)

- ☐ Sei identificar qual propriedade da CIA foi afetada em um cenário, inclusive o caso da dupla extorsão.
- ☐ Sei a ordem identificação, autenticação, autorização e contabilização e o que cada uma faz.
- ☐ Sei calcular SLE e ALE e converter frequência em ARO.
- ☐ Sei distinguir ameaça, vulnerabilidade, exploit e risco.
- ☐ Sei as quatro respostas ao risco e o que deve acompanhar a aceitação formal.
- ☐ Sei diferenciar política, norma, procedimento e diretriz e quem aprova a política.
- ☐ Sei classificar controles por categoria e por função, incluindo diretivo, dissuasivo e compensatório.
- ☐ Sei os papéis da LGPD (controlador, operador, encarregado) e os direitos do titular.
- ☐ Sei a ordem dos quatro cânones da ISC2 e a diferença entre devido cuidado e devida diligência.
- ☐ Sei para que servem ISO 27001, ISO 27002, NIST SP 800-53, CIS Benchmarks, Controles CIS, PCI DSS, HIPAA e SOX.

Questões de revisão do capítulo

R5.1 · Princípios de segurança

Qual sequência representa o ciclo de gestão de riscos?

A. Planejar, codificar, testar e publicar software
B. Comprar, instalar, esquecer e substituir controles
C. Identificar, avaliar, tratar e monitorar os riscos
D. Detectar, conter, erradicar e recuperar sistemas

R5.2 · Princípios de segurança

Um funcionário apagou sem querer uma tabela importante do banco de dados. Como classificar essa ameaça?

A. Ameaça humana acidental
B. Ameaça persistente avançada
C. Ameaça natural ambiental
D. Ameaça de hacktivista

R5.3 · Princípios de segurança

A empresa migrou sistemas para a nuvem e passou a trabalhar com fornecedores novos. O que deve acontecer com a avaliação de riscos?

A. Ficar como está até a próxima década
B. Ser descartada, pois a nuvem é segura
C. Ser entregue ao provedor de nuvem
D. Ser revisada, pois o ambiente mudou

R5.4 · Princípios de segurança

Um sistema de prevenção de intrusão (IPS) descarta automaticamente pacotes de ataque conhecidos. Como classificar esse controle?

A. Físico e compensatório
B. Administrativo e diretivo
C. Físico e detectivo
D. Técnico e preventivo

Respostas comentadas

R5.1. C) Identificar, avaliar, tratar e monitorar os riscos

Por quê: Riscos mudam com o tempo, por isso o ciclo é contínuo e inclui monitoramento e revisão.

✗ A) Incorreta. É desenvolvimento.
✗ B) Incorreta. Não é gestão de riscos.
✗ D) Incorreta. É resposta a incidentes.

> **Dica de prova:** Ciclo de riscos: identificar, avaliar, tratar, monitorar.

R5.2. A) Ameaça humana acidental

Por quê: Erros humanos estão entre as causas mais comuns de incidentes; backups e controles de acesso ajudam.

✗ B) Incorreta. Não é ataque sofisticado.
✗ C) Incorreta. Não é evento natural.
✗ D) Incorreta. Não há motivação política.

> **Dica de prova:** Apagou sem querer: ameaça humana acidental.

R5.3. D) Ser revisada, pois o ambiente mudou

Por quê: Mudanças relevantes exigem reavaliar ameaças, vulnerabilidades e controles.

✗ A) Incorreta. Riscos mudam com o ambiente.
✗ B) Incorreta. A responsabilidade é compartilhada.
✗ C) Incorreta. O cliente continua responsável.

> **Dica de prova:** Ambiente mudou: revisar os riscos.

R5.4. D) Técnico e preventivo

Por quê: O IPS também detecta, mas sua função principal é impedir o tráfego malicioso.

✗ A) Incorreta. Barreira que substitui outra.
✗ B) Incorreta. Política que orienta.
✗ C) Incorreta. Barreira física que identifica.

> **Dica de prova:** IPS: técnico e preventivo.

DIA DA PROVA

Estratégia de prova

A prova ISC2 CC é adaptativa (CAT), com 100 a 125 itens de múltipla escolha e tipos avançados em 2 horas, e aprovação com 700 de 1000 pontos. É uma certificação de nível de entrada: cada item costuma trazer um cenário curto e cobrar um único conceito, pedindo o nome da prática, a fase, o tipo de controle ou a melhor ação. As alternativas erradas costumam ser conceitos vizinhos do mesmo tema (RTO no lugar de RPO, contenção no lugar de erradicação, DAC no lugar de MAC) ou ações claramente irresponsáveis, como fechar alertas, publicar senhas ou agir sem registro. A prova premia a resposta prudente, documentada e baseada em risco, com pessoas e sociedade em primeiro lugar.

Como responder

✓ Distribua o estudo pelos pesos: Princípios de segurança (24%) e Redes e nuvem (21,3%) primeiro, depois IAM (20%), Governança (17,3%) e Operações e resposta a incidentes (17,3%).

✓ Com 2 horas para até 125 itens, mantenha ritmo de cerca de um minuto por item e não trave em nenhum.

✓ Antes de olhar as alternativas, nomeie o conceito descrito no cenário com suas palavras; depois procure a alternativa que bate com ele.

✓ Elimine primeiro as alternativas absurdas ou irresponsáveis (desligar o SIEM, apagar logs, agir sem autorização) e depois decida entre os dois conceitos vizinhos que sobrarem.

✓ Em perguntas de classificação de controle, responda nas duas dimensões: categoria (técnico, administrativo, físico) e função (preventivo, detectivo, corretivo, dissuasivo, diretivo, compensatório).

✓ Em perguntas de escolha múltipla (Escolha DUAS), avalie cada alternativa isoladamente como verdadeira ou falsa antes de marcar.

✓ Quando o enunciado pedir o que fazer primeiro, prefira a ação que reduz o risco imediato ou que confirma os fatos: verificar a identidade, confirmar por outro canal, priorizar por gravidade, inventariar.

✓ Em dilemas éticos, aplique os cânones da ISC2 em ordem e escolha a conduta honesta, legal e transparente.

Erros que derrubam candidatos

✗ Trocar pares vizinhos: RTO x RPO, incremental x diferencial, IDS x IPS, contenção x erradicação, DAC x MAC.

✗ Classificar controles pela função secundária (chamar IPS de detectivo ou placa diretiva de dissuasiva).

✗ Atribuir ao provedor de nuvem responsabilidades do cliente, como dados, MFA, configuração de acesso e patches do SO em IaaS.

✗ Inverter as chaves na criptografia assimétrica ou achar que hash pode ser revertido.

✗ Confiar em falsas proteções: NAT, SSID oculto, filtro de MAC, portal cativo e VLAN sem regras.

✗ Achar que conformidade, revisão sem remoção ou plano não testado bastam para estar seguro.

✗ Escolher a alternativa mais técnica quando o cenário pede pessoas primeiro ou comunicação pelo canal definido.

Na semana da prova

- ☐ Revise as tabelas de memorização: portas, camadas OSI, fórmulas SLE e ALE, fases da resposta a incidentes e ordem dos cânones.
- ☐ Refaça os pares que mais confunde (RTO x RPO, DAC x MAC x RBAC x ABAC, varredura x pentest, modelos de nuvem) até acertar sem hesitar.
- ☐ Faça ao menos uma prova completa cronometrada em 2 horas para calibrar o ritmo de cerca de um minuto por item.
- ☐ Revise as pegadinhas de cada domínio e anote em uma folha os erros que repetiu nas provas de treino.
- ☐ Na véspera, só revisão leve dos itens de lembrar e checklist; durma bem e chegue cedo ao centro de testes.

REVISÃO FINAL

Folha de cola

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

1. Conceitos de gestão de identidade e acesso (IAM)

‣ Mudou de setor e manteve os acessos antigos → **Acúmulo de privilégios; falha na revisão da mudança**

‣ Conta ativa de quem saiu da empresa → **Conta órfã: desativar; conciliar com o RH**

‣ Entrada, mudança e saída de pessoas → **Joiner, mover, leaver**

‣ Criar e remover contas em SaaS a partir do diretório → **SCIM**

‣ Parceiro entra no seu portal com a conta corporativa dele → **Federação (SAML ou OIDC)**

⚠ O código comprova a posse do dispositivo onde o segredo está: algo que você tem. PIN e senha é que são algo que você sabe.

⚠ MFA exige categorias diferentes; senha + chave de segurança física é MFA de verdade.

⚠ A habilitação não basta: sem necessidade da tarefa, não acessa (need to know).

2. Conceitos de segurança de redes e nuvem

‣ Respostas ARP falsas para se passar pelo gateway → **ARP spoofing**

‣ Endereço certo digitado, site falso aberto → **Envenenamento de DNS; DNSSEC**

‣ Milhares de handshakes incompletos → **Inundação SYN**

‣ Wi-Fi com o mesmo nome da rede oficial → **Evil twin**

‣ Wi-Fi com credencial individual e RADIUS → **WPA2/WPA3 Enterprise com 802.1X**

⚠ NAT economiza endereços e esconde a estrutura, mas não filtra tráfego como um firewall.

⚠ O portal cativo só registra aceite e controla o acesso; rede aberta continua sem criptografia.

⚠ SSID é descoberto com ferramentas simples e MAC é falsificável; use WPA3 e 802.1X.

3. Governança de segurança

‣ Quanto de dados se aceita perder → **RPO**

‣ Prazo para voltar a operar → **RTO**

‣ Limite antes do dano inaceitável → **MTD (RTO menor que MTD)**

‣ Descobrir processos críticos e impacto de parar → **BIA**

‣ Local pronto em minutos / precisa de dias / só espaço e energia → **Site quente / morno / frio**

⚠ Perda de dados é RPO e orienta a frequência dos backups. RTO é o tempo para voltar a operar.

⚠ MTD é o limite de parada antes do dano inaceitável. MTBF mede confiabilidade, MTTD mede detecção, RPO mede perda de dados.

⚠ Pergunte: desde o último backup de qualquer tipo (incremental) ou desde o último completo (diferencial)?

4. Operações de segurança e resposta a incidentes

‣ Mostrar só os quatro últimos dígitos do cartão → **Mascaramento**

‣ Número do cartão trocado por valor aleatório mapeado por sistema protegido → **Tokenização**

‣ Dados recuperáveis após formatar → **Remanência; sanitização**

‣ Logs de formatos diferentes convertidos para um padrão → **Normalização no SIEM**

‣ Várias falhas de login + login com sucesso + cópia grande pela mesma conta → **Correlação de eventos**

⚠ Hash é mão única; atacantes só tentam adivinhar entradas que gerem o mesmo hash, por isso sal e algoritmo lento.

⚠ Sigilo usa a chave pública do destinatário; a privada de Ana serviria para assinar e a de Bruno ela nem deve ter.

⚠ Assinatura usa a chave privada do próprio autor; a pública do leitor serve para cifrar para ele.

5. Princípios de segurança

‣ Dado enviado por engano a quem não devia ver → **Confidencialidade**

‣ Valor alterado sem autorização, dose trocada no prontuário, hash comparado ao abrir o arquivo → **Integridade**

‣ Site fora do ar, arquivos inacessíveis → **Disponibilidade**

‣ Não pode negar que assinou ou aprovou → **Não repúdio (chave privada exclusiva)**

‣ Registrar o que o usuário fez depois de entrar → **Contabilização (accounting)**

⚠ Sem acesso é disponibilidade. Só entra confidencialidade se o enunciado disser que o atacante copiou os dados (dupla extorsão).

⚠ Assinatura (hash + chave privada do autor) comprova integridade, origem e não repúdio. Para sigilo é preciso cifrar.

⚠ Seguro é transferir. Evitar exige parar a atividade; aceitar é não fazer nada novo de forma consciente.

GABARITO

Respostas do diagnóstico

D1. A) Logon único (SSO) → revise o capítulo 1

Por quê: O SSO reduz o número de senhas e centraliza o controle de acesso, o que exige proteger bem essa conta.

✗ B) Incorreta. Segmenta a rede.

✗ C) Incorreta. Bloqueia o não liberado.

✗ D) Incorreta. Divide tarefas críticas.

> **Dica de prova:** Uma entrada para vários sistemas: SSO.

D2. C) Bloqueio temporário progressivo e detecção de padrões suspeitos → revise o capítulo 1

Por quê: Limitar tentativas com atraso crescente e MFA reduz ataques sem negar serviço aos usuários.

✗ A) Incorreta. Aumenta o risco.

✗ B) Incorreta. Trava usuários legítimos.

✗ D) Incorreta. Facilita a força bruta.

> **Dica de prova:** Bloqueio abusado: bloqueio progressivo e detecção.

D3. C) Fazer um inventário das contas privilegiadas → revise o capítulo 1

Por quê: Sem inventário, contas esquecidas ficam fora do controle e da revisão.

✗ A) Incorreta. Interrompe o negócio.

✗ B) Incorreta. Aumenta o risco.

✗ D) Incorreta. Expõe as contas.

> **Dica de prova:** Controlar contas privilegiadas: inventariar primeiro.

D4. D) Microssegmentação → revise o capítulo 2

Por quê: A microssegmentação limita a movimentação lateral e apoia a Confiança Zero.

✗ A) Incorreta. Não segmenta cargas.

✗ B) Incorreta. Não controla acesso.

✗ C) Incorreta. Sem separação.

> **Dica de prova:** Política por carga de trabalho: microssegmentação.

D5. C) Conectar à VPN corporativa antes de acessar sistemas → revise o capítulo 2

Por quê: Em redes não confiáveis, a VPN protege contra interceptação.

✗ A) Incorreta. Aumenta o risco.

✗ B) Incorreta. Expõe arquivos.

✗ D) Incorreta. Aumenta o risco.

> **Dica de prova:** Wi-Fi público: usar VPN.

D6. A) Varredura de portas para reconhecimento → revise o capítulo 2

Por quê: A varredura costuma preceder ataques; reduzir serviços expostos limita o que o atacante encontra.

✗ B) Incorreta. Não é o comportamento.

✗ C) Incorreta. Não é o comportamento.

✗ D) Incorreta. Não é o comportamento.

> **Dica de prova:** Muitas portas testadas: varredura de portas.

D7. B) Rede de embaixadores de segurança → revise o capítulo 3

Por quê: Embaixadores (security champions) ajudam a criar cultura e a adaptar orientações a cada área.

✗ A) Incorreta. Testa sistemas.

✗ C) Incorreta. Trata de processos críticos.

✗ D) Incorreta. Trata de restaurar a TI.

> **Dica de prova:** Pessoas de referência nas áreas: embaixadores.

D8. A) Confirmar a mudança por telefone já cadastrado → revise o capítulo 3

Por quê: A fraude de e-mail corporativo (BEC) usa contas invadidas ou falsas para desviar pagamentos.

✗ B) Incorreta. Facilita a fraude.

✗ C) Incorreta. O golpista responde.

✗ D) Incorreta. Não verifica a fraude.

> **Dica de prova:** Troca de conta bancária por e-mail: confirmar por outro canal.

D9. A) Percentual de contas privilegiadas com MFA → revise o capítulo 3

Por quê: Métricas de cobertura em ativos críticos mostram onde o risco ainda está alto.

✗ B) Incorreta. Não mede proteção.

✗ C) Incorreta. Não mede proteção.

✗ D) Incorreta. Não mede proteção.

> **Dica de prova:** Proteção das contas críticas: % de admins com MFA.

D10. A) Simular atacantes reais para testar detecção e resposta → revise o capítulo 4

Por quê: O red team usa táticas reais com objetivos definidos; o blue team defende.

✗ B) Incorreta. É tarefa de suporte.

✗ C) Incorreta. É tarefa operacional.

✗ D) Incorreta. É tarefa de governança.

> **Dica de prova:** Red team: simular atacantes reais.

D11. C) Análise dinâmica (DAST) → revise o capítulo 4

Por quê: O DAST encontra falhas visíveis em execução, como injeção e configurações inseguras.

✗ A) Incorreta. Examina o código parado.
✗ B) Incorreta. Testa o ambiente físico.
✗ D) Incorreta. Não testa a aplicação.

> **Dica de prova:** Aplicação rodando: DAST.

D12. D) Prioriza os alertas por gravidade e ativos afetados → revise o capítulo 4

Por quê: A triagem classifica, correlaciona e prioriza eventos para decidir quais viram incidentes.

✗ A) Incorreta. Perde a visibilidade.
✗ B) Incorreta. Ignora possíveis incidentes.
✗ C) Incorreta. Não considera o risco.

> **Dica de prova:** Muitos alertas: priorizar por gravidade e ativo.

Agora, treine no formato real

Faça as 6 provas completas do curso ISC2 CC: 600 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 ISC2. As questões são inéditas e não reproduzem a prova real.