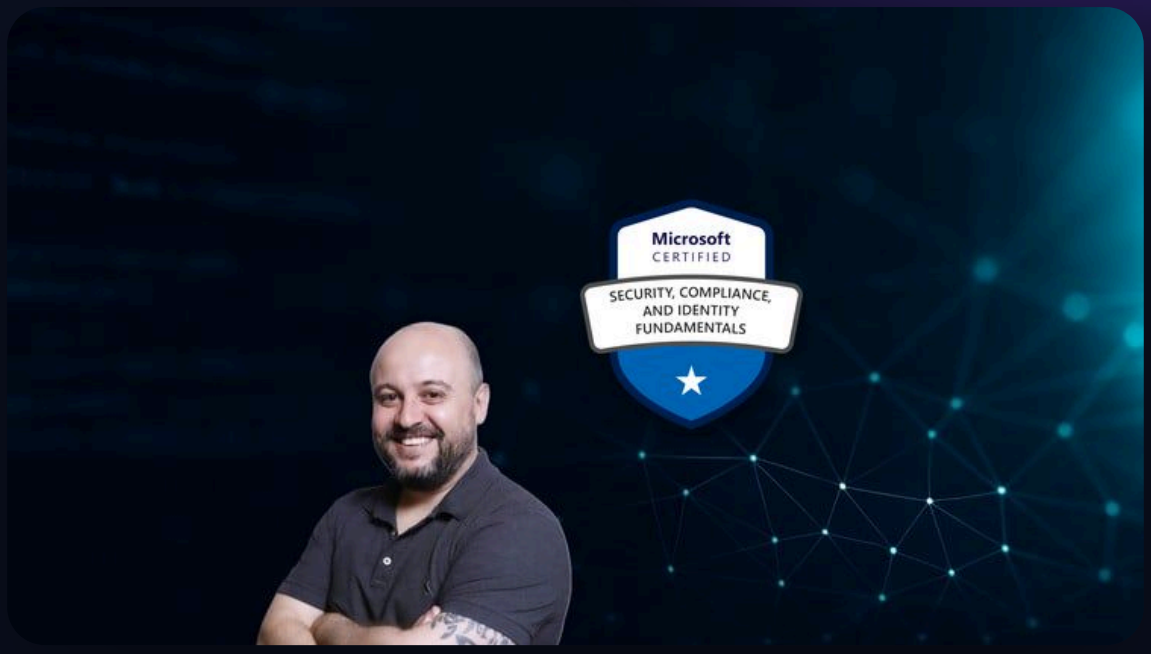


Guia de preparação SC-900

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.

4 capítulos por domínio	**28** 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 SC-900: 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 50 questões e 45 minutos, no formato do exame. Referência de aprovação: 70%.

Domínio (capítulo)	Peso	Neste guia
1. Conceitos de segurança, conformidade e identidade	10-15%	17 conceitos · 12 pegadinhas
2. Recursos das soluções de conformidade da Microsoft	35-40%	18 conceitos · 14 pegadinhas
3. Recursos das soluções de segurança da Microsoft	35-40%	18 conceitos · 14 pegadinhas
4. Recursos do Microsoft Entra	25-30%	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 segurança, conformidade e identidade

No contexto de GRC, qual conceito se refere a cumprir leis, regulamentos e normas aplicáveis à organização?

A. Gestão de risco
B. Conformidade
C. Autenticação
D. Governança

D2 · Conceitos de segurança, conformidade e identidade

Como se chama o serviço que cria, mantém e gerencia identidades e oferece autenticação a aplicativos, como o Microsoft Entra ID?

A. Um firewall de aplicativo
B. Um agente de acesso SaaS
C. Um cofre de chaves
D. Um provedor de identidade

D3 · Conceitos de segurança, conformidade e identidade

Por que a identidade passou a ser considerada o principal perímetro de segurança?

A. Todos os funcionários trabalham na rede interna do escritório
B. As aplicações de nuvem não exigem mais login dos usuários
C. Os usuários acessam recursos de qualquer lugar e de qualquer dispositivo
D. Os firewalls de borda ficaram mais baratos que as licenças

D4 · Recursos das soluções de conformidade da Microsoft

Uma política deve manter documentos por três anos e, depois, apagá-los automaticamente. Qual configuração de retenção atende?

A. Excluir após o uso
B. Reter sem prazo definido
C. Reter e depois excluir
D. Reter indefinidamente

D5 · Recursos das soluções de conformidade da Microsoft

Qual recurso do Purview reconhece padrões como números de CPF e de cartão de crédito para classificar dados e disparar políticas?

A. Fluxos de ciclo de vida do Entra
B. Classificadores treináveis com ML
C. Tipos de informações confidenciais
D. Barreiras de informações do Teams

D6 · Recursos das soluções de conformidade da Microsoft

A empresa quer que times do Teams e sites do SharePoint classificados como Restrito não permitam convidados externos. Como aplicar isso?

A. Política de retenção aplicada ao site
B. Rótulo de confidencialidade no site
C. Revisão de descarte ao fim da retenção
D. Tipo de informação confidencial do site

D7 · Recursos das soluções de segurança da Microsoft

Em uma arquitetura hub e spoke, a empresa quer inspecionar e controlar de forma central o tráfego entre as redes virtuais e para a internet. Qual serviço fica no hub?

A. Microsoft Purview
B. Azure Key Vault
C. Microsoft Priva
D. Azure Firewall

D8 · Recursos das soluções de segurança da Microsoft

Uma arquitetura separa servidores web, de aplicação e de banco em sub-redes diferentes, com regras controlando o tráfego entre elas. Qual prática de segurança é essa?

A. Criptografia em repouso
B. Autenticação multifator
C. Retenção de dados
D. Segmentação de rede

D9 · Recursos das soluções de segurança da Microsoft

A equipe cria no AD uma conta falsa, que ninguém deve usar, para gerar alerta se um invasor tentar autenticar com ela. Como o Defender para Identidade chama esse tipo de conta?

A. Conta de serviço
B. Conta honeytoken
C. Conta de emergência
D. Conta de convidado

D10 · Recursos do Microsoft Entra

Uma empresa quer sincronizar os usuários do Active Directory local com o Microsoft Entra ID, para que usem a mesma identidade em apps na nuvem. Qual ferramenta atende?

A. Microsoft Entra Verified ID
B. Microsoft Purview Data Map
C. Microsoft Defender para Identidade
D. Microsoft Entra Connect

D11 · Recursos do Microsoft Entra

Computadores Windows da empresa continuam no domínio do AD local, mas também precisam ser reconhecidos pelo Microsoft Entra ID para o Acesso Condicional. Como são identificados?

A. Registrados como dispositivos pessoais
B. Ingressados só no Entra
C. Ingressados de forma híbrida
D. Convidados do locatário

D12 · Recursos do Microsoft Entra

A equipe quer acompanhar a saúde da sincronização do Entra Connect e receber alertas quando ela falhar. Qual recurso atende?

A. Microsoft Purview Data Map
B. Microsoft Entra Verified ID
C. Microsoft Entra Connect Health
D. Microsoft Defender EASM

01

CAPÍTULO 1 · 10-15% DA PROVA

Conceitos de segurança, conformidade e identidade

É o menor domínio (10% a 15%), mas é a base de tudo e costuma ter questões diretas, de definição. Preciso dominar responsabilidade compartilhada (IaaS, PaaS, SaaS), defesa em profundidade e suas camadas, Zero Trust (três princípios e seis pilares), tríade CIA, criptografia (simétrica, assimétrica, hash, salt, assinatura digital, em trânsito e em repouso), GRC e conceitos de identidade (pilares, autenticação x autorização, fatores de MFA, provedor de identidade, tokens, SSO, federação e protocolos). As pegadinhas aqui são de ordem e de troca: chave pública x privada, autenticação x autorização, governança x conformidade x risco, camada de rede x perímetro. Se eu decorar as listas e as definições curtas, este domínio vira ponto garantido.

Neste capítulo
17 tópicos-chave · 12 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Modelo de responsabilidade compartilhada

Em IaaS, o provedor cuida de datacenter, rede física e hosts; o cliente cuida de SO (inclusive patches), aplicações, rede virtual, identidades e dados. A responsabilidade do cliente diminui de IaaS para PaaS e SaaS, mas dados, dispositivos, contas e identidades sempre ficam com ele. Segurança física é sempre do provedor; identidade e diretório são compartilhados em PaaS e SaaS.

Defesa em profundidade

Camadas: física, identidade e acesso, perímetro, rede, computação, aplicação e dados (no centro). Cada camada tem controles próprios: física protege prédios e hardware; identidade exige MFA e controla acesso; perímetro trata da borda (ex.: DDoS); rede segmenta e nega por padrão; computação cuida de patches e antimalware nas VMs; aplicação trata de código seguro; dados usam criptografia, classificação e DLP.

Zero Trust: princípios

Verificar explicitamente (decidir o acesso com todos os sinais, de forma contínua), usar o acesso com privilégio mínimo (JIT, JEA, políticas adaptativas por risco) e presumir a violação (segmentar, criptografar e monitorar como se o invasor já estivesse dentro). O Zero Trust não confia na rede interna, na VPN nem na localização.

Zero Trust: pilares

Seis pilares protegidos: identidades, pontos de extremidade, aplicativos, dados, infraestrutura e rede. Itens de negócio como orçamento, folha de pagamento ou marketing não são pilares.

Tríade CIA

Confidencialidade (impedir acesso indevido ao conteúdo), integridade (dados sem alteração indevida, ex.: hash publicado de um instalador) e disponibilidade (serviço acessível quando necessário, ex.: afetada por DDoS). Autenticidade não faz parte da tríade.

Criptografia simétrica e assimétrica

Simétrica usa a mesma chave para cifrar e decifrar e é rápida (ex.: AES). Assimétrica usa par de chaves (ex.: RSA): para sigilo, cifra-se com a chave pública do destinatário e só a privada dele decifra. As duas são reversíveis com a chave certa.

Assinatura digital

Usa criptografia assimétrica para garantir autoria e integridade: assina-se com a chave privada do remetente e qualquer pessoa verifica com a chave pública dele.

Hash e salt

Hash é de mão única, irreversível, usado para guardar senhas e comparar no login. Salt faz senhas iguais terem hashes diferentes, dificultando ataques com tabelas pré-calculadas (rainbow tables). Base64 é só codificação, facilmente revertida.

Criptografia em trânsito e em repouso

Em trânsito protege dados na rede (TLS, IPsec, HTTPS) contra interceptação. Em repouso protege dados armazenados em discos, bancos e arquivos, para que quem obtenha o disco não consiga ler; no Azure é habilitada por padrão em muitos serviços.

GRC

Governança é o conjunto de regras, políticas e processos internos que orientam como a organização é dirigida. Gestão de risco identifica ameaças, avalia probabilidade e impacto e decide mitigar, transferir, aceitar ou evitar. Conformidade é cumprir leis, regulamentos e normas externas.

Residência, soberania e privacidade de dados

Residência de dados trata de onde os dados ficam guardados (ex.: dentro das fronteiras de um país). Soberania de dados trata de quais leis se aplicam a eles. Privacidade de dados é o terceiro conceito de conformidade dessa família.

Identidade como perímetro

Como usuários acessam recursos de qualquer lugar e de qualquer dispositivo, com dados fora da rede corporativa, a identidade virou o principal perímetro de segurança. Proteger identidades com autenticação forte e controle de acesso passou a ser a base.

Pilares da identidade

Quatro pilares: administração (criar, manter e desativar identidades), autenticação (comprovar quem é), autorização (definir o que pode fazer) e auditoria (registrar quem fez o quê, quando e onde). Autenticação vem antes da autorização.

Fatores de autenticação e MFA

A MFA combina pelo menos dois fatores de categorias diferentes: algo que você sabe (senha, PIN), algo que você tem (celular, chave de segurança) e algo que você é (biometria, como impressão digital). Algo que você faz não é um dos três fatores clássicos.

Provedor de identidade e tokens

O provedor de identidade (ex.: Microsoft Entra ID) cria, mantém e gerencia identidades e autentica usuários para os aplicativos. Na autenticação moderna, o app recebe um token com informações (declarações) sobre o usuário, nunca a senha nem o diretório, o que permite o logon único (SSO).

Federação e protocolos

Na federação, um provedor de identidade confia na autenticação feita por outro, permitindo que funcionários de uma empresa usem as próprias credenciais nos apps da parceira. Protocolos modernos: SAML (padrão aberto baseado em XML para SSO federado), OAuth 2.0 e OpenID Connect.

Serviços de diretório

O Active Directory Domain Services (AD DS) é o diretório local tradicional, com Kerberos, LDAP e Políticas de Grupo para usuários e computadores do domínio. O Microsoft Entra ID é o serviço de identidade na nuvem, e os dois se integram em cenários híbridos.

Macetes para memorizar

Camadas da defesa em profundidade

Na ordem: Física, Identidade, Perímetro, Rede, Computação, Aplicação, Dados (dados no centro).

Zero Trust

Três verbos: Verificar, Limitar, Presumir. Seis pilares: identidades, endpoints, apps, dados, infraestrutura e rede.

Chaves assimétricas

Para esconder, use a pública DELE; para assinar, use a privada SUA.

Pilares da identidade

Os 4 A: Administração, Autenticação, Autorização, Auditoria.

Fatores de MFA

Sabe, tem, é: senha, celular, digital.

Responsabilidade compartilhada

Sempre meu: dados, dispositivos, contas e identidades. Sempre do provedor: o prédio (física).

GRC

Governança manda (regras internas), Risco mede (probabilidade e impacto), Conformidade obedece (leis externas).

Tabela de memorização: não confunda

Quando é...	...e quando é
Criptografia simétrica Mesma chave compartilhada para cifrar e decifrar, com rapidez.	**Criptografia assimétrica** Par de chaves: pública do destinatário cifra para sigilo; privada do remetente assina, pública verifica.
Criptografia Proteger dados que precisarão ser lidos de novo com a chave certa.	**Hash** Guardar senhas ou verificar integridade sem possibilidade de voltar ao original (com salt para senhas).
Criptografia em trânsito Dados trafegando na rede, como HTTPS com TLS, contra interceptação de pacotes.	**Criptografia em repouso** Dados armazenados em disco ou banco, contra quem obtém o disco.
Autenticação Comprovar quem é o usuário (senha, MFA). Vem primeiro.	**Autorização** Definir o que ele pode fazer depois de autenticado (ex.: só ler o relatório).
Governança Regras, políticas e processos internos que dirigem a organização.	**Conformidade** Atender a leis, regulamentos e normas externas. Identificar e tratar ameaças é gestão de risco.

IaaS Cliente cuida de SO, patches, aplicações, rede virtual, identidades e dados.	**SaaS** Provedor cuida até da aplicação; cliente continua com dados, dispositivos, contas e identidades.
Camada de rede Segmentar e negar tráfego por padrão entre recursos, limitando a movimentação do invasor.	**Camada de perímetro** Proteger a borda contra ataques como DDoS.

Números que caem

Item	Valor
Peso do domínio na prova	**10% a 15%**
Princípios do Zero Trust	**3**
Pilares do Zero Trust	**6**
Pilares da identidade	**4**
Camadas da defesa em profundidade	**7**
Fatores mínimos na MFA	**pelo menos 2, de categorias diferentes**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Cifrar com a chave privada do remetente para que só o destinatário leia.
Como não cair: A privada do remetente assina. Sigilo para o destinatário = chave pública do destinatário.

⚠ **Alerta de prova:** Verificar assinatura digital com a chave privada ou assinar com a pública.
Como não cair: Assina com a privada do remetente; verifica com a pública dele.

⚠ **Alerta de prova:** Achar que o salt serve para recuperar a senha original ou acelerar o login.
Como não cair: O hash continua irreversível. O salt existe para que senhas iguais tenham hashes distintos.

⚠ **Alerta de prova:** Escolher AES, RSA ou Base64 para guardar senhas de forma irrecuperável.
Como não cair: AES e RSA são reversíveis com a chave e Base64 é só codificação. Irreversível é hash com salt.

⚠ **Alerta de prova:** Achar que a Microsoft aplica os patches do SO de uma VM em IaaS.
Como não cair: Em IaaS, o patch do SO é do cliente; a Microsoft cuida da camada física e da virtualização.

⚠ **Alerta de prova:** Achar que, em SaaS, o cliente não tem mais nenhuma responsabilidade de segurança.
Como não cair: Dados, dispositivos, contas e identidades são sempre do cliente, em qualquer modelo.

⚠ **Alerta de prova:** Inverter a ordem: autorização antes da autenticação.
Como não cair: Primeiro quem é (autenticação), depois o que pode (autorização).

⚠ **Alerta de prova:** Chamar de conformidade as regras e processos internos da organização.
Como não cair: Regras internas = governança. Conformidade = leis e normas externas.

⚠ **Alerta de prova:** Achar que verificar explicitamente é confiar em quem está na rede corporativa ou usou VPN, ou verificar só no primeiro acesso do dia.
Como não cair: Zero Trust não confia em localização nem VPN; a verificação é contínua e usa todos os sinais.

⚠ **Alerta de prova:** Colocar autenticidade na tríade CIA ou classificar DDoS como ataque à integridade.
Como não cair: CIA = confidencialidade, integridade e disponibilidade. Serviço fora do ar = disponibilidade; nenhum dado foi alterado nem exposto.

⚠ **Alerta de prova:** Considerar algo que você faz como fator de MFA.
Como não cair: Os três fatores clássicos são sabe, tem e é. Biometria = algo que você é.

⚠ **Alerta de prova:** Achar que o aplicativo recebe a senha ou o hash do usuário na autenticação moderna.
Como não cair: O app recebe um token com informações sobre o usuário e confia no provedor de identidade.

Como cai na prova

📝 **Como cai:** Definição direta: Qual conceito se refere a...?, com quatro termos da mesma família.
Como resolver: Lembre a definição curta de cada termo da família (governança, risco, conformidade; ou confidencialidade, integridade, disponibilidade) e case com a palavra-chave do enunciado: regras internas, ameaças, leis, alteração, fora do ar.

📝 **Como cai:** Em qual camada da defesa em profundidade fica o controle X?
Como resolver: Associe o controle ao alvo: MFA e acesso = identidade; DDoS na borda = perímetro; segmentação e negar por padrão = rede; patch e antimalware em VM = computação; criptografia do que está guardado = dados.

📝 **Como cai:** Responsabilidade compartilhada: quem cuida de Y em IaaS, PaaS ou SaaS?
Como resolver: Física é sempre do provedor; dados, dispositivos, contas e identidades sempre do cliente. Em IaaS, SO é do cliente; em PaaS e SaaS, SO é do provedor. Identidade e diretório são compartilhados em PaaS e SaaS.

📝 **Como cai:** Qual chave usar ou qual técnica de criptografia aplicar?
Como resolver: Defina o objetivo: sigilo (pública do destinatário), assinatura (privada do remetente), guardar senha (hash com salt), mesma chave nos dois lados (simétrica). Descarte codificações como Base64.

📝 **Como cai:** Princípio do Zero Trust por cenário.
Como resolver: Todos os sinais = verificar explicitamente; mínimo de permissões e só quando precisa = privilégio mínimo; segmentar e monitorar como se já houvesse invasão = presumir a violação. Qualquer alternativa que confie em rede interna ou VPN está errada.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
mesma chave nos dois lados	**Criptografia simétrica**
hash publicado para conferir o arquivo baixado	**Integridade**
site fora do ar por ataque de negação de serviço	**Disponibilidade**
HTTPS, TLS, dados trafegando	**Criptografia em trânsito**
disco roubado, dados ilegíveis	**Criptografia em repouso**
dados devem ficar dentro das fronteiras do país	**Residência de dados**
segmentar, criptografar e monitorar como se já houvesse invasão	**Presumir a violação**
acesso só quando precisa, pelo tempo necessário, mínimo de permissões	**Privilégio mínimo (JIT e JEA)**
decidir o acesso com base em todos os sinais	**Verificar explicitamente**
entrar uma vez e usar vários aplicativos	**SSO com provedor de identidade**

funcionários da parceira usam as próprias credenciais nos nossos apps	**Federação**
padrão aberto baseado em XML para SSO federado	**SAML**
patches e antimalware nas VMs	**Camada de computação da defesa em profundidade**
identificar ameaças, avaliar probabilidade e impacto	**Gestão de risco**

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

- Sigilo: cifre com a pública do destinatário. Assinatura: assine com a privada do remetente.
- Hash é irreversível; salt faz senhas iguais terem hashes diferentes.
- Dados, dispositivos, contas e identidades são sempre do cliente; segurança física é sempre do provedor.
- Zero Trust: verificar explicitamente, privilégio mínimo e presumir a violação; nunca confiar na rede interna.
- Autenticação (quem é) vem antes da autorização (o que pode).

Essenciais para a prova (checklist)

- ☐ Sei dizer o que é do cliente e o que é do provedor em IaaS, PaaS e SaaS.
- ☐ Sei as sete camadas da defesa em profundidade e um controle de cada.
- ☐ Sei os três princípios e os seis pilares do Zero Trust.
- ☐ Sei classificar um cenário em confidencialidade, integridade ou disponibilidade.
- ☐ Sei qual chave usar para sigilo e para assinatura digital.
- ☐ Sei a diferença entre criptografia, hash, salt e codificação.
- ☐ Sei diferenciar governança, gestão de risco e conformidade, e residência x soberania de dados.
- ☐ Sei os quatro pilares da identidade e os três fatores de autenticação.
- ☐ Sei o que são provedor de identidade, token, SSO, federação e SAML.
- ☐ Sei por que a identidade é o principal perímetro de segurança.

Questões de revisão do capítulo

R1.1 · Conceitos de segurança, conformidade e identidade

Em uma VM do Azure (IaaS), quem é responsável por aplicar as atualizações de segurança do sistema operacional?

A. A Microsoft
B. O provedor de internet
C. O fabricante do hardware
D. O cliente

R1.2 · Conceitos de segurança, conformidade e identidade

Entre os pilares da identidade, qual trata da criação, manutenção e desativação das identidades ao longo do tempo?

A. Auditoria
B. Autenticação
C. Administração
D. Autorização de acesso

R1.3 · Conceitos de segurança, conformidade e identidade

Uma empresa publica o hash de um instalador para que os usuários confirmem que o arquivo baixado não foi alterado. Qual princípio de segurança está sendo protegido?

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

R1.4 · Conceitos de segurança, conformidade e identidade

Na criptografia assimétrica, qual chave o remetente usa para cifrar uma mensagem que só o destinatário poderá ler?

A. A chave pública do destinatário
B. A chave privada do próprio remetente
C. A mesma chave compartilhada por ambos
D. A chave privada do destinatário

Respostas comentadas

R1.1. D) O cliente

Por quê: Em IaaS, o provedor cuida de datacenter, rede física e hosts. O cliente cuida de SO, aplicações, rede virtual, identidades e dados.

✗ A) Incorreta. A Microsoft cuida da camada física e da virtualização.
✗ B) Incorreta. O provedor de internet só fornece conectividade.
✗ C) Incorreta. O fabricante não atualiza o SO do cliente.

> **Dica de prova:** IaaS: patch do SO é do cliente.

R1.2. C) Administração

Por quê: Os quatro pilares da identidade são administração, autenticação, autorização e auditoria.

✗ A) Incorreta. Auditoria registra o que foi feito.
✗ B) Incorreta. Autenticação comprova quem é.
✗ D) Incorreta. Autorização define o que pode fazer.

> **Dica de prova:** Criar e desativar identidades: administração.

R1.3. D) Integridade

Por quê: A tríade CIA reúne confidencialidade (sigilo), integridade (dados sem alteração indevida) e disponibilidade (acesso quando necessário).

✗ A) Incorreta. Autorização define permissões.
✗ B) Incorreta. Disponibilidade é manter o serviço acessível.
✗ C) Incorreta. Confidencialidade é impedir acesso indevido ao conteúdo.

> **Dica de prova:** Dado não foi alterado: integridade.

R1.4. A) A chave pública do destinatário

Por quê: Na criptografia assimétrica, a chave pública cifra e a privada decifra. Em assinaturas digitais, a privada assina e a pública verifica.

✗ B) Incorreta. A chave privada do remetente é usada para assinar, não para garantir sigilo ao destinatário.
✗ C) Incorreta. Chave compartilhada é característica da criptografia simétrica.
✗ D) Incorreta. A chave privada do destinatário fica só com ele.

> **Dica de prova:** Sigilo para o destinatário: cifre com a pública dele.

02

CAPÍTULO 2 · 35-40% DA PROVA

Recursos das soluções de conformidade da Microsoft

Este domínio (20% a 25%) é todo Microsoft Purview, mais os compromissos de privacidade da Microsoft: Service Trust Portal, Compliance Manager, classificação de dados, rótulos de confidencialidade, DLP, retenção e gerenciamento de registros, Insider Risk, conformidade de comunicações, barreiras de informações, eDiscovery, auditoria e governança de dados. As questões trazem um requisito de negócio ou jurídico (manter X anos, impedir vazamento, preservar para processo, saber quem fez o quê) e pedem o recurso certo. Onde mais erro: rótulo de confidencialidade x rótulo de retenção, política de retenção x rótulo de retenção, retenção legal (eDiscovery) x política de retenção, Compliance Manager x Service Trust Portal, e tipos de informações confidenciais x classificadores treináveis x EDM. Minha regra: confidencialidade protege quem acessa, retenção define quanto tempo fica, DLP impede que saia.

Neste capítulo

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

Tópicos-chave

Princípios de privacidade da Microsoft

Quatro áreas: o cliente controla os próprios dados, sabe onde eles ficam, os dados são protegidos em repouso e em trânsito e a Microsoft defende os dados contra acessos indevidos. A Microsoft não usa os dados para anúncios nem os vende. Pedidos governamentais são redirecionados ao cliente, pedidos sem base legal são contestados e, quando a lei permite, o cliente é avisado com cópia do pedido.

Service Trust Portal e Customer Lockbox

O Service Trust Portal reúne relatórios de auditoria independentes e certificações (como ISO 27001 e SOC 2) e materiais sobre como a Microsoft protege os dados dos clientes. O Customer Lockbox (Sistema de Proteção de Dados do Cliente) garante que engenheiros da Microsoft só acessem conteúdo do cliente com aprovação explícita, com registro das ações.

Portal do Microsoft Purview e funções

Centraliza Compliance Manager, proteção de informações, DLP, ciclo de vida de dados, eDiscovery, auditoria e governança. Usa funções e grupos de funções do Purview para delegar tarefas de conformidade (DLP, retenção, eDiscovery) com menor privilégio, sem precisar de Administrador Global.

Compliance Manager

Traz avaliações criadas a partir de modelos para centenas de regulamentos (ISO 27001, LGPD), com controles, ações de melhoria e pontuação de conformidade. Ações gerenciadas pela Microsoft já vêm implementadas e testadas; ações gerenciadas pelo cliente dependem da empresa, refletindo a responsabilidade compartilhada. Cada ação tem responsável, status, evidências e testes, e o Compliance Manager também avalia Azure, AWS e Google Cloud com conectores.

Pontuação de conformidade

Soma os pontos das ações de melhoria concluídas, com pesos pelo tipo de ação e pelo risco: preventivas obrigatórias valem mais que detectivas e corretivas, e discricionárias valem menos que obrigatórias. Serve para entender a postura e priorizar ações por risco; não substitui auditorias externas nem garante que a empresa cumpre toda a legislação.

Classificação de dados

Tipos de informações confidenciais reconhecem padrões (CPF, cartão de crédito), com centenas prontos e possibilidade de personalizados. Classificadores treináveis usam aprendizado de máquina para reconhecer categorias de documentos sem padrão fixo (contratos, currículos). A correspondência exata de dados (EDM) usa um hash dos valores reais da organização para detectar com precisão e menos falsos positivos.

Content explorer e activity explorer

O content explorer mostra onde estão os itens classificados e rotulados e quantos contêm dados sensíveis. O activity explorer mostra o que foi feito com eles, como rótulos removidos e arquivos copiados para USB.

Rótulos de confidencialidade

Classificam e protegem conteúdo com criptografia baseada em identidade e marcação de conteúdo (cabeçalho, rodapé, marca-d'água); a proteção viaja com o arquivo. Também protegem contêineres: times do Teams, grupos do Microsoft 365 e sites do SharePoint (ex.: bloquear convidados). Valem no Power BI e no Microsoft Fabric e, com o scanner do Purview, em compartilhamentos de rede locais.

Políticas de rótulos e rotulagem automática

Rótulos criados só aparecem no Word e no Outlook depois de publicados por uma política de rótulos, que pode definir rótulo padrão, rótulo obrigatório e justificativa para rebaixar a classificação. Rótulos têm ordem de prioridade. Podem ser aplicados manualmente, recomendados ao usuário ou aplicados automaticamente com base em tipos de informações confidenciais.

Prevenção contra perda de dados (DLP)

Usa tipos de informações confidenciais para proteger dados em Exchange, SharePoint, OneDrive, Teams, dispositivos Windows e macOS (DLP de ponto de extremidade, ex.: bloquear cópia para USB) e no Microsoft 365 Copilot. Ações: dicas de política, auditar, alertar, bloquear com ou sem substituição (com justificativa do usuário) e quarentena para dados em repouso. Pode rodar em modo de simulação, e os alertas são investigados no painel de alertas de DLP ou como incidentes no portal do Defender.

Retenção: políticas e rótulos

Políticas de retenção cobrem locais inteiros (Exchange, SharePoint, Teams) sem ação do usuário; rótulos de retenção aplicam regras diferentes por item, de forma manual, padrão no local ou automática (informações confidenciais, palavras-chave, classificadores). Configurações: reter por um período, reter e depois excluir, ou só excluir após o período. No Teams há políticas separadas para mensagens de canal, chats e canais compartilhados.

Recursos avançados de retenção

Retenção baseada em eventos começa a contar a partir de um evento (fim do contrato, desligamento). Escopos adaptáveis atualizam a política pelos atributos de usuários, grupos e sites (ex.: todo o Jurídico). Bloqueio de preservação impede que alguém, inclusive administradores, desative ou reduza a política. No SharePoint e no OneDrive, itens retidos alterados ou excluídos ficam na biblioteca de retenção de preservação.

Gerenciamento de registros

Usa rótulos de retenção para declarar itens como registros, que não podem ser editados nem excluídos até o fim do período. A revisão de descarte exige que um responsável aprove a exclusão no fim da retenção, com prova de quem aprovou. O plano de arquivos organiza os rótulos de retenção com categorias, referências e autoridades legais e permite exportar essa estrutura.

Insider Risk Management

Detecta riscos internos, como roubo de dados por funcionários que estão saindo, usando modelos de política. O conector de dados de RH importa datas de demissão e mudanças de cargo como gatilhos. Tem privacidade por projeto (pseudonimização de usuários, controle por funções, auditoria) e casos com alertas, atividades em sequência e encaminhamento para eDiscovery ou RH. A proteção adaptável endurece DLP, Acesso Condicional e outras políticas conforme o risco do usuário.

Conformidade de comunicações e barreiras de informações

A conformidade de comunicações analisa e-mail, Teams e outros canais em busca de conteúdo ofensivo, assédio e conflitos de interesse. As barreiras de informações restringem comunicação e compartilhamento no Teams, SharePoint e OneDrive entre segmentos de usuários (ex.: pesquisa x investimentos).

eDiscovery

Permite criar casos, aplicar retenção legal (hold) para preservar conteúdo mesmo que o usuário tente apagar, pesquisar e exportar resultados. O conjunto de revisão traz análise, agrupamento por tema, identificação de duplicados e marcação de itens relevantes antes da exportação.

Auditoria do Purview

Registra eventos de muitos serviços para responder quem fez o quê e quando, apoiando investigações forenses, de conformidade e jurídicas. A Auditoria Standard retém registros por 180 dias. A Auditoria Premium tem retenção mais longa (um ano, ou até dez anos com complemento), eventos de investigação (como quais e-mails foram acessados) e maior largura de banda de acesso à API.

DSPM e governança de dados

O Gerenciamento de Postura de Segurança de Dados (DSPM) combina classificação, atividades e riscos para recomendar proteções, inclusive em prompts para o Copilot e outros apps e agentes de IA; a versão antiga focada só em IA agora se chama DSPM para IA (clássico). Na governança, o Data Map escaneia fontes (Azure SQL, Data Lake, Amazon S3) e registra metadados, linhagem e classificação, e o Unified Catalog permite descobrir dados com descrições, responsáveis e glossário.

Macetes para memorizar

💡 Três verbos do Purview

Rótulo de confidencialidade PROTEGE, retenção GUARDA, DLP SEGURA na porta.

💡 Classificação

Padrão = tipo de informação confidencial; Parecido = classificador treinável; Exato = EDM.

💡 Exploradores

Content = onde está (conteúdo); Activity = o que fizeram (atividade).

💡 Retenção

Política = local inteiro; Rótulo = item a item; Evento = relógio começa depois; Bloqueio de preservação = cadeado sem chave.

💡 Compliance Manager x Service Trust Portal

Compliance Manager olha para dentro (sua empresa); Service Trust Portal olha para a Microsoft.

💡 Auditoria

Standard = 180 dias. Premium = mais tempo e mais eventos para investigar.

💡 Privacidade da Microsoft

Controle, localização, segurança e defesa: o dado é do cliente, sem anúncios e sem venda.

Tabela de memorização: não confunda

Quando é...	...e quando é
Rótulo de confidencialidade Proteger quem acessa: criptografia, marca-d'água, restrição de ações, controle de convidados em sites e times.	**Rótulo de retenção** Definir quanto tempo o item fica e o que acontece depois, inclusive declarar como registro. Um item pode ter os dois.
Política de retenção Reter tudo de um local inteiro (todas as caixas de correio, um site, mensagens de canal do Teams) sem o usuário classificar nada.	**Rótulo de retenção** Regras diferentes por item ou documento, aplicadas manual ou automaticamente (ex.: dados de saúde por dez anos).
Compliance Manager Avaliar a conformidade da própria empresa contra um regulamento, com ações de melhoria e pontuação.	**Service Trust Portal** Ler relatórios de auditoria e certificações dos serviços de nuvem da Microsoft.
Tipos de informações confidenciais Dados com padrão fixo, como CPF e número de cartão. Se for preciso detectar valores reais da própria base com menos falsos positivos, use EDM.	**Classificadores treináveis** Categorias de documentos sem padrão fixo, como contratos e currículos, reconhecidas por aprendizado de máquina.
Content explorer Onde estão os itens rotulados e quantos têm dados sensíveis.	**Activity explorer** O que foi feito com os itens: rótulo removido, cópia para USB.
Auditoria Standard Saber quem acessou ou excluiu um arquivo, com registros mantidos por 180 dias.	**Auditoria Premium** Retenção mais longa e eventos de investigação, como quais e-mails um invasor acessou.

Retenção legal (eDiscovery) Preservar caixas de correio de pessoas específicas durante um processo judicial, mesmo que tentem apagar.	**Bloqueio de preservação** Impedir que uma política de retenção seja desativada ou reduzida, nem mesmo por administradores.

Números que caem

Item	Valor
Peso do domínio na prova	**20% a 25%**
Retenção padrão da Auditoria Standard	**180 dias**
Retenção da Auditoria Premium	**um ano, ou até dez anos com complemento**
Áreas dos compromissos de privacidade da Microsoft	**4: controle, localização, segurança e defesa dos dados**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Achar que o rótulo de confidencialidade define o tempo de guarda e o de retenção protege o acesso.
Como não cair: Os papéis estão invertidos: confidencialidade = quem acessa; retenção = quanto tempo fica. Os dois são do Purview, não do Defender nem do Sentinel.

⚠ **Alerta de prova:** Escolher Reter indefinidamente ou Excluir após o uso para guardar por três anos e depois apagar.
Como não cair: Guardar X anos e apagar depois é reter e depois excluir.

⚠ **Alerta de prova:** Usar rótulo de retenção item a item quando o requisito é manter todas as caixas de correio sem ação do usuário.
Como não cair: Local inteiro = política de retenção. Rótulo de retenção é para regras por item.

⚠ **Alerta de prova:** Escolher o Compliance Manager para ler relatórios SOC 2 e ISO 27001 da Microsoft.
Como não cair: O Compliance Manager avalia a própria empresa. Relatórios de auditoria da Microsoft ficam no Service Trust Portal.

⚠ **Alerta de prova:** Escolher tipos de informações confidenciais para reconhecer contratos e currículos.
Como não cair: Tipos de informações confidenciais reconhecem padrões como CPF e cartão. Documentos sem padrão fixo pedem classificadores treináveis.

⚠ **Alerta de prova:** Usar tipo genérico de número de cartão quando o cenário pede detectar CPFs reais da base de clientes com menos falsos positivos.
Como não cair: Valores reais da própria base = correspondência exata de dados (EDM), baseada em hash dos valores.

⚠ **Alerta de prova:** Mover para a quarentena do EOP um e-mail que viola regra de DLP, ou bloquear sem substituição quando o usuário pode enviar com justificativa.
Como não cair: A quarentena do EOP é para spam e malware. Enviar após informar justificativa = bloquear com substituição.

⚠ **Alerta de prova:** Escolher a política de retenção do Teams ou barreira de informações para impedir número de cartão no chat.
Como não cair: Retenção define tempo de guarda e barreira restringe quem conversa com quem. Impedir dado sensível no chat é DLP para o Teams.

⚠ **Alerta de prova:** Achar que, com política de retenção ativa, um arquivo excluído no SharePoint some na hora ou vira registro regulatório.
Como não cair: Uma cópia fica na biblioteca de retenção de preservação. Registro exige rótulo de retenção específico.

⚠ **Alerta de prova:** Achar que rótulos criados já aparecem para os usuários, ou que um grupo dinâmico os publica.
Como não cair: Rótulo só aparece no Word e no Outlook depois de publicado por uma política de rótulos.

⚠ **Alerta de prova:** Achar que a pontuação de conformidade garante cumprir toda a legislação ou substitui auditoria externa.
Como não cair: Ela mede o progresso nas ações de melhoria e ajuda a priorizar por risco; cabe à empresa validar seus controles.

⚠ **Alerta de prova:** Achar que a Microsoft entrega dados ao governo sem avisar o cliente ou dá acesso direto às agências.
Como não cair: A Microsoft redireciona o pedido ao cliente, contesta pedidos sem base legal e, quando permitido, avisa o cliente.

⚠ **Alerta de prova:** Escolher marcação de conteúdo para impedir que pessoas de fora abram um documento encaminhado.
Como não cair: Marcação só mostra a classificação. Controlar quem abre, onde o arquivo estiver, é criptografia do rótulo com permissões.

⚠ **Alerta de prova:** Escolher Auditoria Standard para saber quais e-mails um invasor acessou com retenção longa.
Como não cair: A Standard tem retenção menor e menos eventos de investigação. Cenário de investigação de acesso a e-mails = Auditoria Premium.

Como cai na prova

📝 **Como cai:** Requisito de tempo: manter X anos, excluir depois, contar a partir de um evento.
Como resolver: Tempo de guarda é sempre retenção, nunca DLP nem rótulo de confidencialidade. Depois escolha a variação: local inteiro = política; por item = rótulo; a partir de evento = baseada em eventos; ninguém pode reduzir = bloqueio de preservação; aprovar antes de apagar = revisão de descarte.

📝 **Como cai:** Requisito de proteção: impedir vazamento, criptografar, marcar, impedir que externos abram.
Como resolver: Impedir que o dado saia por e-mail, Teams, USB ou Copilot = DLP. Classificar e proteger o próprio arquivo onde ele estiver = rótulo de confidencialidade (criptografia ou marcação).

📝 **Como cai:** Cenário jurídico ou de investigação: processo judicial, quem fez o quê, funcionário saindo.
Como resolver: Processo judicial = eDiscovery (hold, conjunto de revisão). Quem acessou ou excluiu = Auditoria (Premium se precisar de retenção longa ou eventos de leitura de e-mail). Comportamento arriscado de funcionário = Insider Risk Management.

📝 **Como cai:** Pergunta sobre o Compliance Manager: como a pontuação é calculada, quem implementa a ação, o que ela garante.
Como resolver: Pontuação = pontos das ações de melhoria concluídas, com peso por risco. Ações da Microsoft x do cliente = responsabilidade compartilhada. A pontuação ajuda a priorizar, mas não garante conformidade nem substitui auditoria.

📝 **Como cai:** Qual é a diferença entre dois rótulos, dois exploradores ou dois níveis de auditoria?
Como resolver: Use as âncoras: confidencialidade = acesso, retenção = tempo; content = onde, activity = o que fizeram; Standard = 180 dias, Premium = mais tempo e mais eventos. Descarte a alternativa que inverte os papéis.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
relatórios ISO 27001 e SOC 2 dos serviços da Microsoft	**Service Trust Portal**

pontuação de conformidade com LGPD ou ISO e ações de melhoria	**Compliance Manager (avaliação a partir de modelo)**
aprovar acesso de engenheiros da Microsoft ao conteúdo	**Customer Lockbox (Sistema de Proteção de Dados do Cliente)**
impedir envio de cartão de crédito para fora	**DLP do Purview**
aviso no Outlook explicando a regra na hora de enviar	**Dica de política de DLP**
testar a DLP sem bloquear ninguém	**Modo de simulação**
cabeçalho e marca-d'água com a classificação	**Marcação de conteúdo do rótulo de confidencialidade**
funcionário que pediu demissão baixando muitos arquivos	**Insider Risk Management (com conector de RH)**
mensagens ofensivas ou de assédio no Teams	**Conformidade de comunicações**
duas áreas não podem conversar por conflito de interesses	**Barreiras de informações**
localizar, preservar e exportar conteúdo para processo judicial	**eDiscovery (retenção legal e conjunto de revisão)**
contar o prazo a partir do fim do contrato	**Retenção baseada em eventos**
política que nem administradores podem afrouxar	**Bloqueio de preservação**
dados sensíveis em prompts do Copilot ou de apps de IA	**DSPM do Purview (e DLP para o Microsoft 365 Copilot para bloquear uso de conteúdo rotulado)**

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

- Rótulo de confidencialidade = quem acessa (viaja com o arquivo); rótulo de retenção = quanto tempo fica; DLP = impede que o dado sensível saia.
- Rótulos só aparecem para os usuários depois de publicados em uma política de rótulos.
- Service Trust Portal = documentos da Microsoft; Compliance Manager = avaliação da sua empresa.
- Auditoria Standard guarda 180 dias; Premium guarda mais e tem eventos de investigação.
- Retenção legal (hold) é do eDiscovery e preserva conteúdo para processos; bloqueio de preservação trava a política de retenção.

Essenciais para a prova (checklist)

- ☐ Sei os quatro compromissos de privacidade da Microsoft e como ela trata pedidos governamentais.
- ☐ Sei o que encontro no Service Trust Portal e para que serve o Customer Lockbox.
- ☐ Sei como o Compliance Manager organiza avaliações, ações de melhoria e a pontuação de conformidade.
- ☐ Sei diferenciar tipos de informações confidenciais, classificadores treináveis e EDM.
- ☐ Sei o que rótulos de confidencialidade fazem (criptografia, marcação, contêineres) e como são publicados e aplicados automaticamente.
- ☐ Sei os locais e as ações de uma política de DLP, incluindo dicas de política, substituição e modo de simulação.
- ☐ Sei escolher entre política de retenção, rótulo de retenção, retenção baseada em eventos, escopos adaptáveis e bloqueio de preservação.
- ☐ Sei o que são registros, revisão de descarte e plano de arquivos.
- ☐ Sei separar Insider Risk Management, conformidade de comunicações, barreiras de informações e eDiscovery.
- ☐ Sei a diferença entre Auditoria Standard e Premium e o papel de DSPM, Data Map e Unified Catalog.

Questões de revisão do capítulo

R2.1 · Recursos das soluções de conformidade da Microsoft

No Compliance Manager, algumas ações de melhoria aparecem como já implementadas e testadas pela Microsoft. Como essas ações são classificadas?

A. Ações gerenciadas pelo cliente
B. Ações gerenciadas pela Microsoft
C. Ações de resposta a incidentes
D. Ações de revisão de acesso

R2.2 · Recursos das soluções de conformidade da Microsoft

A empresa quer que as regras de DLP fiquem mais rígidas automaticamente para usuários que o Insider Risk Management classificou como de alto risco. Qual recurso atende?

A. Proteção adaptável
B. Busca de ameaças
C. Rotulagem manual
D. Retenção legal

R2.3 · Recursos das soluções de conformidade da Microsoft

Uma agência governamental pede à Microsoft dados que um cliente corporativo guarda na nuvem. Segundo os compromissos de privacidade da Microsoft, qual é a conduta padrão?

A. Excluir os dados antes de responder
B. Redirecionar o pedido para o próprio cliente
C. Dar acesso direto e irrestrito à agência
D. Entregar os dados sem avisar o cliente

R2.4 · Recursos das soluções de conformidade da Microsoft

A equipe de governança quer escanear fontes como Azure SQL, Data Lake e Amazon S3 para registrar metadados e classificar dados automaticamente. Qual recurso do Purview atende?

A. Data Map do Microsoft Purview
B. Barreiras de informações do Teams
C. Auditoria Premium do Microsoft 365
D. Compliance Manager do Purview

Respostas comentadas

R2.1. B) Ações gerenciadas pela Microsoft

Por quê: O Compliance Manager separa ações da Microsoft e do cliente, refletindo a responsabilidade compartilhada na pontuação de conformidade.

✗ A) Incorreta. Ações do cliente dependem da configuração e dos processos da empresa.
✗ C) Incorreta. Resposta a incidentes é outro processo.
✗ D) Incorreta. Revisões de acesso são do Entra.

> **Dica de prova:** Controle feito pela plataforma: ação gerenciada pela Microsoft.

R2.2. A) Proteção adaptável

Por quê: A proteção adaptável integra o Insider Risk Management à DLP, ao Acesso Condicional e a outras políticas, aplicando controles conforme o risco.

✗ B) Incorreta. A busca de ameaças é do Sentinel e do Defender.
✗ C) Incorreta. A rotulagem manual depende dos usuários.
✗ D) Incorreta. A retenção legal preserva conteúdo.

> **Dica de prova:** Controle que endurece com o risco: proteção adaptável.

R2.3. B) Redirecionar o pedido para o próprio cliente

Por quê: Pelo compromisso de defender os dados, a Microsoft direciona pedidos governamentais ao cliente, contesta na Justiça pedidos sem base legal e, quando a lei permite, avisa o cliente.

✗ A) Incorreta. Excluir dados não faz parte da resposta a pedidos legais.

✗ C) Incorreta. A Microsoft não dá a nenhum governo acesso direto ou irrestrito aos dados dos clientes.

✗ D) Incorreta. A Microsoft só divulga dados quando o cliente orienta ou a lei exige e, quando permitido, avisa o cliente e envia cópia do pedido.

> **Dica de prova:** Governo pediu dados do cliente: a Microsoft redireciona ao cliente.

R2.4. A) Data Map do Microsoft Purview

Por quê: O Data Map é a base da governança de dados do Purview, alimentando o catálogo com metadados, linhagem e classificação.

✗ B) Incorreta. Barreiras restringem comunicação.

✗ C) Incorreta. A auditoria registra atividades de usuários.

✗ D) Incorreta. O Compliance Manager trata de conformidade regulatória.

> **Dica de prova:** Escanear fontes e mapear metadados: Data Map.

03

CAPÍTULO 3 · 35-40% DA PROVA

Recursos das soluções de segurança da Microsoft

Este é o domínio mais pesado (35% a 40%) e o mais largo: segurança de rede do Azure (NSG, Azure Firewall, WAF, DDoS Protection, Bastion, Key Vault), Microsoft Defender for Cloud (CSPM e planos CWP), Microsoft Sentinel (SIEM e SOAR) e Microsoft Defender XDR com seus produtos (Ponto de Extremidade, Office 365, Identidade e Cloud Apps). A prova descreve um problema técnico e pede o produto ou recurso certo, e as alternativas erradas costumam ser produtos reais de outra área. Onde mais erro: NSG x Azure Firewall x WAF, regras de automação x playbooks no Sentinel, CSPM básico gratuito x Defender CSPM, Secure Score do Microsoft 365 x classificação de segurança do Defender for Cloud, e qual Defender protege o quê. Minha regra é amarrar cada produto ao seu alvo: e-mail, endpoint, AD local, apps SaaS, cargas de nuvem ou logs de tudo.

Neste capítulo

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

Tópicos-chave

Grupo de segurança de rede (NSG) e grupos de segurança de aplicativo

O NSG tem regras de permissão e negação por IP, porta e protocolo, aplicadas a sub-redes e interfaces de rede. Sem regras personalizadas, a entrada vinda da internet é negada pela regra padrão (só o tráfego da rede virtual e do balanceador é permitido). Grupos de segurança de aplicativo deixam as regras se referirem à função das VMs (ex.: servidores web) em vez de IPs. NSG não inspeciona HTTP, não usa FQDN nem inteligência de ameaças.

Azure Firewall

Firewall de rede gerenciado e com estado, com regras de rede e de aplicativo, filtragem por FQDN e inteligência de ameaças para alertar ou negar tráfego de IPs e domínios maliciosos conhecidos. Fica no hub da topologia hub e spoke, controlando de forma central o tráfego entre redes virtuais e para a internet. O Azure Firewall Premium acrescenta IDPS com assinaturas, inspeção de TLS e filtragem de URL.

Firewall de Aplicativo Web (WAF)

Inspeciona requisições HTTP e HTTPS e bloqueia ataques do OWASP Top 10, como injeção de SQL e cross-site scripting. Roda no Application Gateway (aplicações regionais) ou no Azure Front Door (aplicações globais, na borda da rede da Microsoft).

Azure DDoS Protection

Toda a infraestrutura do Azure já tem proteção básica contra DDoS sem configuração. O Azure DDoS Protection acrescenta aprendizado do padrão de tráfego da aplicação, mitigação automática, métricas, alertas, relatórios e suporte durante ataques.

Azure Bastion e segmentação

O Bastion dá acesso RDP e SSH às VMs pelo portal sem expor portas de gerenciamento à internet. Segmentação de rede separa camadas (web, aplicação, banco) em sub-redes com regras entre elas, aplicando o princípio de presumir a violação.

Azure Key Vault

Centraliza segredos, chaves de criptografia e certificados, com acesso controlado por Azure RBAC, identidades gerenciadas e logs das operações. Guarda chaves gerenciadas pelo cliente, com controle de rotação e revogação. Exclusão reversível vem habilitada e a proteção contra limpeza é recomendada; o HSM Gerenciado oferece HSM dedicado, de locatário único, validado no FIPS 140 nível 3.

Microsoft Defender for Cloud

Plataforma de proteção de aplicações nativas de nuvem (CNAPP) para Azure, AWS, GCP e ambientes locais. Une gerenciamento de postura (CSPM), com recomendações e classificação de segurança, e proteção de cargas de trabalho (CWP), que detecta ameaças em tempo real. O Microsoft Cloud Security Benchmark (MCSB) é a iniciativa padrão e a base das recomendações; normas como PCI DSS e ISO 27001 podem ser adicionadas ao painel de conformidade regulatória.

CSPM básico x Defender CSPM

O CSPM básico é gratuito e entrega recomendações e classificação de segurança (Secure Score). O plano Defender CSPM acrescenta mapa de segurança de nuvem, análise de caminho de ataque (rota do invasor até o dado crítico) e cloud security explorer (consultas ao grafo de recursos). A classificação sobe corrigindo recomendações: resolver todas as de um controle soma os pontos dele.

Planos de proteção de cargas de trabalho (CWP)

Defender para Servidores (VMs Windows e Linux, EDR, acesso just-in-time às portas de gerenciamento), Storage (malware nos uploads, dados sensíveis), Bancos de Dados (acessos anômalos e injeção de SQL), Contêineres (AKS, EKS, GKE, imagens e tempo de execução), App Service, Key Vault (acessos incomuns aos cofres) e Resource Manager (operações de gerenciamento suspeitas pelo portal, API, CLI ou PowerShell). Há ainda verificação sem agente, automação de fluxo de trabalho e segurança de DevOps para repositórios do GitHub e Azure DevOps.

Microsoft Sentinel

SIEM e SOAR nativo de nuvem: coletar, detectar, investigar e responder. Os dados ficam em um workspace do Log Analytics, consultados com KQL, e o custo depende principalmente do volume ingerido e da retenção. Recebe dados por conectores (Azure, Microsoft 365, AWS, GCP, Syslog, CEF, terceiros) e instala soluções prontas pelo hub de conteúdo.

Detecção no Sentinel

Regras de análise geram alertas e incidentes: agendadas, quase em tempo real (NRT, a cada minuto), de anomalias, de Fusion (correlaciona alertas de baixa fidelidade em ataques de vários estágios) e de segurança da Microsoft. UEBA cria perfis de comportamento normal; indicadores de inteligência de ameaças cruzam IPs e domínios maliciosos com os logs; o painel MITRE ATT&CK mostra a cobertura por tática e técnica.

Investigação e resposta no Sentinel

Regras de automação fazem triagem simples (atribuir, ajustar severidade); playbooks com Aplicativos Lógicos executam respostas complexas, como bloquear usuário no Entra. Busca de ameaças (hunting) procura ataques antes do alerta; notebooks usam Python e ML; pastas de trabalho são painéis; watchlists guardam listas como VIPs; grafo de investigação e páginas de entidade mostram conexões e histórico.

Microsoft Defender XDR e portal do Defender

Correlaciona sinais de Ponto de Extremidade, Office 365, Identidade e Cloud Apps em incidentes unificados. Oferece busca avançada com KQL (até 30 dias de dados), investigação e resposta automatizadas, central de ações e interrupção automática de ataques (desativa conta e contém dispositivos em ransomware). O portal do Defender une SIEM e XDR; após 31 de março de 2027, o Sentinel fica só no portal do Defender.

Microsoft Defender para Ponto de Extremidade

Protege Windows, macOS, Linux, Android e iOS com proteção de última geração do Defender Antivírus, regras de redução da superfície de ataque (ASR), EDR com linha do tempo, investigação e correção automatizadas, proteção de rede (sites maliciosos em qualquer app), controle de dispositivo (USB) e proteção contra adulteração. Ações de resposta: isolar, restringir apps, coletar pacote de investigação e verificar com antivírus.

Microsoft Defender para Office 365 e EOP

O Exchange Online Protection dá a proteção básica antispam e antimalware. O Defender para Office 365 protege e-mail, Teams, SharePoint e OneDrive: plano 1 com Links Seguros, Anexos Seguros e anti-phishing (proteção contra representação, spoofing); plano 2 acrescenta Explorador de Ameaças, investigação automatizada e treinamento de simulação de ataque. ZAP remove e-mail malicioso já entregue; quarentena guarda o suspeito; contas prioritárias protegem executivos.

Microsoft Defender para Identidade

Usa sensores nos controladores de domínio para detectar ataques ao AD local: reconhecimento, Kerberoasting, pass-the-hash, golden ticket e movimentação lateral. Contas honeytoken servem de isca; caminhos de movimentação lateral mostram rotas até contas sensíveis; avaliações de postura de identidade apontam senhas que nunca expiram e protocolos inseguros, refletidas no Microsoft Secure Score.

Microsoft Defender para Cloud Apps (CASB)

Agente de segurança de acesso à nuvem com quatro pilares: visibilidade, segurança de dados, proteção contra ameaças e conformidade. Descobre shadow IT, avalia apps no catálogo por mais de 90 fatores de risco, bloqueia apps marcados como não sancionados via Defender para Ponto de Extremidade e tem governança de aplicativos OAuth. Políticas de arquivos, detecção de anomalias, conectores de aplicativos via API e controle de sessão integrado ao Acesso Condicional (ver sim, baixar não).

Postura, exposição e IA

Microsoft Secure Score mede a postura em identidades, dispositivos e apps do Microsoft 365. Security Exposure Management dá visão unificada de exposição e caminhos de ataque; Defender EASM mapeia ativos expostos na internet; Defender Vulnerability Management faz inventário e priorização de vulnerabilidades. Security Copilot usa IA generativa para resumir incidentes e explicar scripts; Microsoft Threat Intelligence aparece em Visão geral, Intel explorer, análise de ameaças e páginas de entidade.

Macetes para memorizar

💡 Os quatro Defenders do XDR

PIOC: Ponto de extremidade (dispositivos), Identidade (AD local), Office 365 (e-mail e colaboração), Cloud Apps (SaaS).

💡 Rede no Azure

NSG = porteiro de porta e IP; Firewall = guarda central do hub; WAF = leitor de HTTP; DDoS = para-choque de volume; Bastion = porta dos fundos segura para RDP/SSH.

💡 SIEM x SOAR

SIEM enxerga (coleta, correlaciona, detecta); SOAR age (orquestra e automatiza a resposta). Sentinel faz os dois.

💡 Sentinel: quem faz o quê

Conector traz, regra de análise detecta, pasta de trabalho mostra, regra de automação tria, playbook reage, hunting procura antes do alerta.

💡 Defender for Cloud

CSPM = postura (como está configurado); CWP = proteção (quem está atacando agora). Grátis só recomendações e Secure Score.

💡 Defender para Office 365

EOP é o básico; P1 protege (Links e Anexos Seguros); P2 investiga e treina (Explorador, AIR, simulação).

Secure Scores

Microsoft Secure Score = Microsoft 365; classificação de segurança do Defender for Cloud = nuvem; pontuação de conformidade = Compliance Manager (Purview).

Tabela de memorização: não confunda

Quando é...	...e quando é
Grupo de segurança de rede (NSG) Permitir só a porta 1433 vinda da sub-rede da aplicação: regra simples por IP, porta e protocolo em sub-rede ou interface.	**Azure Firewall** Controle central no hub, com estado, filtragem por FQDN e inteligência de ameaças para várias redes virtuais.
Azure Firewall Filtrar tráfego de rede entre redes virtuais e para a internet.	**Firewall de Aplicativo Web (WAF)** Inspecionar requisições HTTP contra injeção de SQL, XSS e OWASP Top 10, no Application Gateway ou no Front Door.
Regras de automação (Sentinel) Triagem simples e centralizada de incidentes: atribuir analista, ajustar severidade.	**Playbooks (Sentinel)** Fluxos complexos com Aplicativos Lógicos: bloquear usuário no Entra, isolar máquina, abrir chamado.
CSPM básico (gratuito) Recomendações e classificação de segurança sem custo adicional.	**Defender CSPM e planos CWP** Análise de caminho de ataque e cloud security explorer (Defender CSPM) ou detecção de ameaças em servidores, bancos e contêineres (planos CWP).
Microsoft Secure Score Postura em identidades, dispositivos e aplicativos do Microsoft 365, com ações recomendadas para melhorar.	**Classificação de segurança do Defender for Cloud** Postura dos recursos de nuvem (Azure e outras nuvens), medida pelas recomendações baseadas no MCSB.
Defender para Office 365 plano 1 Proteção contra ameaças, como Links Seguros e Anexos Seguros.	**Defender para Office 365 plano 2** Explorador de Ameaças, investigação automatizada, busca e treinamento de simulação de ataque.
Busca de ameaças (hunting) no Sentinel Procurar proativamente sinais de ataques que ainda não geraram alertas.	**Regras de análise no Sentinel** Detectar padrões suspeitos de forma contínua e gerar alertas e incidentes.

Números que caem

Item	Valor
Peso do domínio na prova	**35% a 40%**

Dados consultáveis pela busca avançada do Defender XDR	**até 30 dias**
Frequência das regras NRT do Sentinel	**a cada minuto**
Fatores de risco usados pelo catálogo do Defender para Cloud Apps	**mais de 90**
Validação do HSM Gerenciado do Azure Key Vault	**FIPS 140 nível 3**
Fim do suporte ao Sentinel no portal do Azure	**após 31 de março de 2027 (fica só no portal do Defender)**
Aposentadoria do portal autônomo do Defender Threat Intelligence	**1 de agosto de 2026**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Escolher o NSG para bloquear injeção de SQL ou XSS porque ele filtra tráfego.
Como não cair: O NSG filtra por IP, porta e protocolo e não inspeciona HTTP. Ataques de aplicação web pedem WAF.

⚠ **Alerta de prova:** Escolher o Azure Firewall Premium para ataques volumétricos de negação de serviço.
Como não cair: O Azure Firewall filtra tráfego, mas a proteção dedicada contra DDoS volumétrico é o Azure DDoS Protection.

⚠ **Alerta de prova:** Achar que o Azure não tem nenhuma proteção contra DDoS sem contratar plano, ou que a básica já traz relatórios por aplicação.
Como não cair: A proteção básica de infraestrutura vem por padrão; métricas, alertas e ajuste por aplicação vêm só com o Azure DDoS Protection.

⚠ **Alerta de prova:** Escolher conectores de dados ou pastas de trabalho quando o cenário pede detectar e gerar incidentes no Sentinel.
Como não cair: Conectores trazem dados, pastas de trabalho visualizam, regras de automação tratam incidentes existentes. Quem detecta são as regras de análise.

⚠ **Alerta de prova:** Marcar Coletar e armazenar logs de várias fontes como a capacidade SOAR do Sentinel.
Como não cair: Coletar, correlacionar e detectar é SIEM. SOAR é orquestrar e automatizar respostas.

⚠ **Alerta de prova:** Achar que o custo do Sentinel depende de analistas, regras ou pastas de trabalho.
Como não cair: O fator principal é o volume de dados ingeridos e analisados (mais a retenção).

⚠ **Alerta de prova:** Escolher Defender para Ponto de Extremidade para descobrir shadow IT, já que ele fornece sinais de uso.
Como não cair: Descobrir e controlar apps SaaS é o Defender para Cloud Apps; o Ponto de Extremidade só ajuda a bloquear o app marcado como não sancionado.

⚠ **Alerta de prova:** Atribuir ao Defender para Office 365 recursos de outros Defenders: sensores em controladores de domínio, regras de ASR ou descoberta de shadow IT.
Como não cair: Sensores em DCs = Defender para Identidade; ASR = Ponto de Extremidade; shadow IT = Cloud Apps. Office 365 = Links e Anexos Seguros, anti-phishing e simulação.

⚠ **Alerta de prova:** Colocar análise de caminho de ataque ou detecção de ameaças no CSPM básico gratuito.
Como não cair: O gratuito tem só recomendações e classificação. Caminho de ataque é do Defender CSPM; detecção de ameaças é dos planos CWP; malware em storage é do Defender para Storage.

⚠ **Alerta de prova:** Achar que o PCI DSS ou a ISO 27001 é a iniciativa padrão do Defender for Cloud.
Como não cair: O padrão é o MCSB; PCI DSS e ISO 27001 podem ser adicionados ao painel de conformidade regulatória.

⚠ **Alerta de prova:** Usar Links Seguros para bloquear sites maliciosos em qualquer navegador ou aplicativo do dispositivo.
Como não cair: Links Seguros atuam em links de e-mail e documentos do Office. Em qualquer app do dispositivo é a proteção de rede do Defender para Ponto de Extremidade.

⚠ **Alerta de prova:** Confundir o catálogo de apps do Defender para Cloud Apps com Compliance Manager ou Service Trust Portal para avaliar um app SaaS de terceiro.
Como não cair: Compliance Manager avalia a própria empresa e o Service Trust Portal trata dos serviços da Microsoft. Risco de app SaaS de terceiro é o catálogo do Defender para Cloud Apps.

⚠ **Alerta de prova:** Achar que o Defender for Cloud sempre exige agente na VM ou só avalia VMs Windows.
Como não cair: A verificação sem agente usa instantâneos de disco para achar vulnerabilidades, segredos e malware em Windows e Linux.

⚠ **Alerta de prova:** Achar que o Sentinel só coleta logs do Azure ou precisa de exportação manual para a AWS.
Como não cair: O Sentinel é multinuvem: conectores de dados coletam de Azure, Microsoft 365, AWS, GCP, ambientes locais e terceiros.

Como cai na prova

📝 **Como cai:** A empresa quer [proteger alvo X contra ameaça Y]. Qual solução atende?, com quatro produtos de áreas diferentes.
Como resolver: Identifique o alvo: e-mail = Defender para Office 365; notebooks e servidores = Ponto de Extremidade; AD local = Identidade; apps SaaS = Cloud Apps; cargas de nuvem = Defender for Cloud; logs de várias fontes = Sentinel. Depois elimine produtos de conformidade (Purview) e de identidade (Entra).

📝 **Como cai:** No Microsoft Sentinel, qual recurso [ação]?, com alternativas que são todas recursos do Sentinel.
Como resolver: Mapeie o verbo: trazer dados = conectores; detectar = regras de análise; visualizar = pastas de trabalho; triagem simples = regras de automação; resposta complexa = playbook; procurar antes do alerta = hunting; comportamento anômalo = UEBA; lista de referência = watchlist.

📝 **Como cai:** Qual plano do Defender for Cloud atende?, com Defender para Servidores, Storage, Key Vault, App Service, Contêineres e similares.
Como resolver: Leia qual recurso está sendo atacado: VM = Servidores; upload em conta de armazenamento = Storage; SQL = Bancos de Dados; Kubernetes = Contêineres; site no Serviço de Aplicativos = App Service; cofre = Key Vault; operações pelo portal ou CLI = Resource Manager.

📝 **Como cai:** Escolha DUAS: produtos do Defender XDR, capacidades do Sentinel, ações de resposta no endpoint ou serviços de filtragem de rede.
Como resolver: Elimine o que é backup, licenças, sincronização de identidade ou retenção de documentos. Fique com as duas que pertencem ao mesmo produto citado (ex.: XDR = busca avançada e incidentes correlacionados; rede = NSG e Azure Firewall).

📝 **Como cai:** Qual afirmação diferencia X de Y?, com uma alternativa com os papéis invertidos.
Como resolver: Fixe um dos lados (Azure Firewall = rede; WAF = HTTP) e descarte a alternativa que troca os papéis ou atribui funções de outro serviço (segredos e certificados são do Key Vault).

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Kerberoasting, pass-the-hash, golden ticket, controladores de domínio	**Microsoft Defender para Identidade**
conta falsa isca no AD	**Conta honeytoken (Defender para Identidade)**
shadow IT, apps SaaS sem aprovação, CASB	**Microsoft Defender para Cloud Apps**

ver documentos sim, baixar não, em dispositivo não gerenciado	**Controle de sessão do Defender para Cloud Apps com Acesso Condicional**
e-mail malicioso já entregue precisa ser removido	**Limpeza automática de hora zero (ZAP)**
e-mail fingindo ser o presidente com nome parecido	**Proteção contra representação (anti-phishing do Defender para Office 365)**
macros criando processos filhos, scripts ofuscados	**Regras de redução da superfície de ataque (ASR)**
malware tenta desligar o antivírus	**Proteção contra adulteração**
portas de gerenciamento abertas só quando o admin pedir	**Acesso just-in-time às VMs (Defender para Servidores)**
RDP e SSH sem expor portas à internet	**Azure Bastion**
IDPS e inspeção de TLS no firewall	**Azure Firewall Premium**
Azure, AWS e Google Cloud com postura avaliada em um só lugar	**Microsoft Defender for Cloud**
ataque em vários estágios correlacionado a partir de alertas de baixa fidelidade	**Fusion no Sentinel**
lista de executivos ou IPs confiáveis para correlacionar no Sentinel	**Watchlist (lista de observação)**

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

- Cada Defender tem um alvo: Office 365 = e-mail e colaboração; Ponto de Extremidade = dispositivos; Identidade = AD local; Cloud Apps = SaaS; Defender for Cloud = cargas de nuvem e multinuvem.
- Sentinel = SIEM + SOAR, dados no workspace do Log Analytics, custo por volume ingerido.
- NSG filtra porta e IP; Azure Firewall é central com FQDN e threat intel; WAF inspeciona HTTP; DDoS Protection trata volume.
- CSPM básico é gratuito (recomendações e Secure Score); caminho de ataque e cloud security explorer são do Defender CSPM.
- MCSB é a iniciativa padrão do Defender for Cloud.

Essenciais para a prova (checklist)

☐ Sei qual serviço de rede do Azure usar entre NSG, grupos de segurança de aplicativo, Azure Firewall (e Premium), WAF, DDoS Protection e Bastion.

☐ Sei o que o Key Vault guarda e como recuperar um segredo excluído.

☐ Sei separar CSPM básico, Defender CSPM e cada plano CWP do Defender for Cloud.

☐ Sei o que é SIEM e o que é SOAR e onde o Sentinel guarda os dados.

☐ Sei a função de conectores, regras de análise, NRT, Fusion, UEBA, watchlists, pastas de trabalho, regras de automação, playbooks, hunting e notebooks.

☐ Sei quais produtos compõem o Defender XDR e o que são incidentes, busca avançada e interrupção automática de ataques.

☐ Sei os recursos do Defender para Ponto de Extremidade: última geração, ASR, EDR, AIR, proteção de rede, controle de dispositivo e adulteração.

☐ Sei diferenciar EOP, Defender para Office 365 plano 1 e plano 2, e o que fazem ZAP e quarentena.

☐ Sei o que o Defender para Identidade detecta e o que são honeytoken e caminhos de movimentação lateral.

☐ Sei os pilares de um CASB e os recursos do Defender para Cloud Apps.

Questões de revisão do capítulo

R3.1 · Recursos das soluções de segurança da Microsoft

Um aplicativo OAuth de terceiros recebeu permissões amplas no Microsoft 365 e passou a acessar muitos e-mails. Qual recurso do Defender para Cloud Apps ajuda a detectar e controlar isso?

A. Barreira de informações
B. Revisão de descarte
C. Governança de aplicativos
D. Busca avançada de e-mails

R3.2 · Recursos das soluções de segurança da Microsoft

No Microsoft Sentinel, qual capacidade corresponde ao SOAR?

A. Orquestrar e automatizar respostas
B. Classificar documentos com rótulos de sigilo
C. Coletar e armazenar logs de várias fontes
D. Sincronizar identidades do AD com a nuvem

R3.3 · Recursos das soluções de segurança da Microsoft

Quando o Defender for Cloud gerar um alerta de alta severidade, a equipe quer abrir automaticamente um chamado e avisar no Teams. Qual recurso atende?

A. Painel de conformidade
B. Classificação de segurança da nuvem
C. Análise de caminho de ataque
D. Automação de fluxo de trabalho

R3.4 · Recursos das soluções de segurança da Microsoft

O Microsoft Sentinel recebe listas de IPs e domínios maliciosos conhecidos e cruza com os logs coletados. Como esses dados são chamados?

A. Indicadores de inteligência de ameaças
B. Rótulos de retenção de registros
C. Pacotes de acesso com aprovação
D. Tipos de informações confidenciais

Respostas comentadas

R3.1. C) Governança de aplicativos

Por quê: A governança de aplicativos do Defender para Cloud Apps dá visibilidade e controle sobre apps que usam APIs do Microsoft Graph.

✗ A) Incorreta. Barreiras restringem comunicação entre grupos.
✗ B) Incorreta. A revisão de descarte é do Purview.
✗ D) Incorreta. A busca avançada consulta dados, sem governar apps.

> **Dica de prova:** Apps OAuth com permissão demais: governança de aplicativos.

R3.2. A) Orquestrar e automatizar respostas

Por quê: O SIEM coleta, correlaciona e detecta; o SOAR automatiza e orquestra respostas. O Sentinel oferece os dois.

✗ B) Incorreta. Rótulos são do Purview.
✗ C) Incorreta. Coletar e armazenar logs é parte do SIEM.
✗ D) Incorreta. Sincronização é do Entra Connect.

> **Dica de prova:** SOAR: automatizar a resposta.

R3.3. D) Automação de fluxo de trabalho

Por quê: A automação de fluxo de trabalho do Defender for Cloud executa aplicativos lógicos quando surgem alertas, recomendações ou mudanças de conformidade.

✗ A) Incorreta. O painel avalia normas.
✗ B) Incorreta. A classificação mede a postura.
✗ C) Incorreta. A análise mostra rotas de ataque.

> **Dica de prova:** Alerta do Defender for Cloud dispara ação: automação de fluxo.

R3.4. A) Indicadores de inteligência de ameaças

Por quê: O Sentinel importa indicadores de inteligência de ameaças de feeds e plataformas, e regras de análise detectam correspondências nos dados.

✗ B) Incorreta. Rótulos de retenção definem tempo de guarda.

✗ C) Incorreta. Pacotes de acesso concedem permissões.

✗ D) Incorreta. Tipos de informações confidenciais detectam dados sensíveis.

> **Dica de prova:** IPs e domínios maliciosos conhecidos: indicadores de ameaça.

04

CAPÍTULO 4 · 25-30% DA PROVA

Recursos do Microsoft Entra

Aqui eu preciso reconhecer, pelo cenário, qual recurso do Microsoft Entra resolve o problema: Entra ID, Acesso Condicional, ID Protection, PIM, ID Governance (revisões de acesso, gerenciamento de direitos, fluxos de ciclo de vida), External ID, identidade híbrida e métodos de autenticação. O domínio pesa de 25% a 30% e quase toda pergunta é um cenário curto com quatro recursos parecidos nas alternativas. Quando a alternativa errada é do Purview ou do Defender, eu descarto rápido; o difícil é quando as quatro são do próprio Entra. Onde mais erro: revisão de acesso x PIM, colaboração B2B x conexão direta B2B, hash de senha x passagem x federação, dispositivo registrado x ingressado x ingressado híbrido, e conceitos invertidos (risco de entrada x risco de usuário, atribuição qualificada x ativa). Também preciso saber que ID Protection e PIM ficam no Entra ID P2 e que o Acesso Condicional só decide bloquear ou conceder, com ou sem controles.

Neste capítulo

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

Tópicos-chave

Microsoft Entra ID

Serviço de identidade e acesso na nuvem: autentica usuários, dispositivos e aplicativos e oferece SSO, MFA e Acesso Condicional. Usa OAuth 2.0, OpenID Connect e SAML, enquanto o AD DS local usa Kerberos e LDAP. É administrado no centro de administração do Microsoft Entra, que reúne Entra ID, ID Governance, External ID, Verified ID e Global Secure Access.

Licenças do Entra ID (Free, P1, P2)

O Free traz recursos básicos. O P1 acrescenta Acesso Condicional e identidade híbrida avançada. O P2 acrescenta ID Protection e Privileged Identity Management (PIM); o Microsoft 365 Basic não inclui esses recursos.

Acesso Condicional

Motor de políticas se-então, avaliado depois da primeira etapa de autenticação e a cada acesso. Sinais: usuário ou grupo, local, dispositivo (inclusive plataforma), aplicativo, risco de entrada e risco de usuário. Decisões: bloquear, conceder ou conceder exigindo controles como MFA, dispositivo em conformidade, dispositivo ingressado de forma híbrida ou aplicativo aprovado. Políticas podem ficar desativadas, ativadas ou em modo somente relatório, que mede o impacto sem bloquear ninguém.

Controles de sessão, força de autenticação e CAE

Controles de sessão incluem frequência de entrada (pedir login de novo a cada X horas), sessão persistente do navegador e controle de apps pelo Defender para Cloud Apps. A força de autenticação exige combinações específicas, como MFA resistente a phishing (FIDO2). A avaliação contínua de acesso (CAE) faz Exchange Online e SharePoint Online reagirem quase em tempo real a desativação de conta, troca de senha e mudança de local, sem esperar o token expirar.

Padrões de segurança

Opção para quem não tem licença premium: exigem registro de MFA, protegem administradores e bloqueiam autenticação herdada para todos de uma vez. Quem tem licença premium costuma usar o Acesso Condicional. Bloquear autenticação herdada é essencial porque esses protocolos não suportam MFA e a maioria dos ataques de spray de senha os usa.

Microsoft Entra ID Protection

Calcula risco de entrada (aquele login: IP anônimo, viagem atípica) e risco de usuário (a conta como um todo: credenciais vazadas) e pode acionar o Acesso Condicional. Na autocorreção, o risco de entrada é resolvido com MFA e o risco de usuário com troca segura de senha. Também avalia o risco de entidades de serviço; com Workload ID Premium há detalhes completos e Acesso Condicional baseado em risco para elas.

Privileged Identity Management (PIM)

Acesso privilegiado just-in-time: a atribuição qualificada exige ativação sob demanda, com MFA, justificativa e aprovação; a atribuição ativa já vale. Controla funções do Entra, funções do Azure RBAC e grupos com privilégios. Tem alertas de segurança (excesso de Administradores Globais, funções atribuídas fora do PIM, ativações sem MFA), histórico de auditoria (quem ativou e com qual justificativa) e revisões de acesso das funções.

Funções do Entra x Azure RBAC

Funções do Microsoft Entra gerenciam objetos do diretório (usuários, senhas, grupos); o Azure RBAC gerencia recursos do Azure, como VMs e contas de armazenamento. Há funções internas e personalizadas, atribuídas em escopos como locatário, unidade administrativa ou aplicativo. Exemplos de menor privilégio: Administrador de Assistência Técnica só redefine senhas; Leitor de Segurança e Leitor Global só leem.

Unidades administrativas e contas de emergência

Unidades administrativas delimitam a administração: permitem delegar funções, como Administrador de Usuários, só para uma filial ou parte da organização. Contas de acesso de emergência são pelo menos duas, só na nuvem, excluídas das políticas de Acesso Condicional, fortemente protegidas e monitoradas. Administradores Globais devem ser poucos, com PIM, MFA resistente a phishing e contas separadas do uso diário.

Microsoft Entra ID Governance

Revisões de acesso confirmam periodicamente quem ainda precisa de acesso (podem ser recorrentes, mostrar recomendações baseadas em uso e aplicar resultados automaticamente). Gerenciamento de direitos entrega pacotes de acesso (grupos, apps, sites) agrupados em catálogos, com solicitação, aprovação, expiração e separação de funções por pacotes incompatíveis. Fluxos de trabalho de ciclo de vida automatizam entrada, mudança e saída por atributos como data de contratação; termos de uso registram quem aceitou, quando e qual versão.

Microsoft Entra External ID

Atende parceiros (B2B) e consumidores (CIAM, com cadastro, entrada com e-mail ou contas sociais e marca personalizada). Na colaboração B2B, o parceiro entra como convidado usando a própria identidade; na conexão direta B2B há confiança mútua sem conta de convidado, usada nos canais compartilhados do Teams. As configurações de acesso entre locatários controlam B2B de entrada e saída e a confiança em declarações de MFA e de dispositivo do parceiro.

Identidade híbrida: sincronização

O Entra Connect Sync ou o Entra Cloud Sync sincroniza usuários e grupos do AD local com o Entra ID; o Cloud Sync usa agentes leves configurados pela nuvem e atende várias florestas desconectadas. O Entra Connect Health mostra alertas, desempenho e erros da sincronização e de serviços como o AD FS.

Identidade híbrida: autenticação

Três opções: sincronização de hash de senha (autenticação na nuvem, guarda um hash do hash e habilita a detecção de credenciais vazadas), autenticação de passagem (valida a senha no AD local, sem hash na nuvem) e federação (autenticação no AD FS ou outro provedor local, mais controle e mais infraestrutura). A Microsoft recomenda considerar o hash pela simplicidade. O Seamless SSO funciona com hash ou passagem; o write-back de senha faz o SSPR valer no AD local.

Identidades de carga de trabalho

Aplicativos, entidades de serviço e identidades gerenciadas: identidades de software que se autenticam. O objeto de aplicativo é o modelo global e a entidade de serviço é a instância dele em cada locatário. Não conseguem fazer MFA e dependem de segredos ou certificados, por isso precisam de controles próprios. A federação de identidade de carga de trabalho deixa GitHub e Kubernetes acessarem recursos sem credenciais armazenadas.

Identidades gerenciadas e Acesso Condicional para workloads

Identidade gerenciada é um tipo especial de entidade de serviço que dispensa gerenciar credenciais (ex.: VM lendo o Key Vault sem senha no código). A atribuída pelo sistema segue o ciclo de vida do recurso e é excluída com ele; a atribuída pelo usuário é independente e compartilhável. Com Workload ID Premium, o Acesso Condicional vale para entidades de serviço de locatário único, com o único controle de bloquear, por local ou risco; identidades gerenciadas não são cobertas.

Identidades de dispositivo

Registrado no Entra: dispositivo pessoal (BYOD), conhecido pelo Entra sem a empresa assumir controle total. Ingressado no Entra: dispositivo da organização que entra direto com conta do Entra, sem domínio local. Ingressado de forma híbrida: continua no domínio do AD local e também é reconhecido pelo Entra para o Acesso Condicional.

Métodos de autenticação

Sem senha: Windows Hello para Empresas, chaves FIDO2 (passkeys), Microsoft Authenticator e autenticação baseada em certificado (CBA, com cartão inteligente e sem AD FS). Passkeys resistem a phishing porque a chave pública é vinculada ao site. Token de hardware OATH gera códigos TOTP sem celular; SMS é mais fraco (troca de chip). Correspondência de números combate fadiga de MFA; o Passe de Acesso Temporário (TAP) permite o primeiro registro de método forte; a política de métodos de autenticação habilita ou desabilita métodos por usuários e grupos.

Senhas: SSPR, proteção de senha e bloqueio inteligente

A redefinição de senha self-service (SSPR) deixa o usuário trocar a própria senha e reduz chamados. A proteção de senha bloqueia senhas fracas conhecidas (lista global) e termos da empresa (lista personalizada), também no AD local com agentes nos controladores. O bloqueio inteligente barra força bruta e spray de senha sem travar o usuário legítimo. Orientação atual: sem expiração periódica forçada, com MFA e troca só quando houver indício de comprometimento.

Macetes para memorizar

Licenças

P1 = Política (Acesso Condicional). P2 = Proteção e Privilégio (ID Protection e PIM).

Risco no ID Protection

Entrada é o evento, usuário é a pessoa: entrada se resolve com MFA, usuário se resolve trocando a senha.

Autenticação híbrida

HPF: Hash (nuvem autentica), Passagem (AD local confere), Federação (AD FS manda).

Dispositivos

Registrado = meu (BYOD). Ingressado = da empresa só no Entra. Híbrido = da empresa no domínio e no Entra.

Acesso Condicional

Sinal entra, decisão sai: quem, onde, qual dispositivo, qual app, qual risco -> bloquear ou conceder (com MFA, conformidade...).

PIM

Qualificada = qualifica para ativar depois. Ativa = já está ativa.

Identidade gerenciada

Sistema morre com o recurso; Usuário vive sozinha e se compartilha.

Sem senha

Hello, FIDO2, Authenticator e certificado: nenhum deles pede senha; SMS e pergunta de segurança não entram nessa lista.

Tabela de memorização: não confunda

Quando é...	...e quando é
Revisões de acesso Confirmar periodicamente (ex.: a cada trimestre) se membros, convidados ou titulares de funções ainda precisam do acesso, removendo o que sobrou.	**Privileged Identity Management (PIM)** Dar a função privilegiada só quando precisa, por tempo limitado, com MFA, justificativa e aprovação (just-in-time).
Sincronização de hash de senha Autenticação feita na nuvem, simples e resiliente, com bônus de detectar credenciais vazadas no ID Protection.	**Autenticação de passagem** A senha precisa ser validada no AD local no momento do login, sem guardar hash na nuvem. Se a exigência é usar o AD FS local com regras próprias, é federação.
Colaboração B2B Parceiro acessa um site ou app como convidado no diretório, usando a própria conta corporativa.	**Conexão direta B2B** Usuários do parceiro participam de canais compartilhados do Teams sem que a empresa crie contas de convidado.
Dispositivo registrado Celular ou notebook pessoal (BYOD) que precisa ser conhecido pelo Entra sem ser da empresa.	**Dispositivo ingressado de forma híbrida** Computador corporativo que continua no domínio do AD local e também precisa ser reconhecido pelo Entra. Se não há domínio local, é ingressado no Entra.

Funções do Microsoft Entra Gerenciar objetos do diretório: redefinir senhas, administrar usuários e grupos.	**Azure RBAC** Ver ou alterar recursos do Azure, como VMs e contas de armazenamento (ex.: auditor que só lê a assinatura).
Identidade gerenciada atribuída pelo sistema Identidade ligada a um único recurso, criada e excluída junto com ele.	**Identidade gerenciada atribuída pelo usuário** Identidade compartilhada por várias VMs, que continua existindo mesmo se uma delas for excluída.
Padrões de segurança Empresa sem licença premium que quer MFA e bloqueio de autenticação herdada rápido para todos.	**Acesso Condicional** Regras granulares por sinal (local, dispositivo, risco, app), como exigir MFA quando o risco de entrada for médio ou alto.

Números que caem

Item	Valor
Peso do domínio na prova	**25% a 30%**
Contas de acesso de emergência recomendadas	**pelo menos duas, só na nuvem**
Licença com ID Protection e PIM	**Microsoft Entra ID P2**
Opções de autenticação híbrida	**3: hash de senha, passagem e federação**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Dar a função de Administrador de Segurança (ou Global) a quem só precisa redefinir senhas de usuários comuns.
Como não cair: Menor privilégio: Administrador de Assistência Técnica. Administrador de Segurança mexe em configurações de segurança e Global tem acesso total.

⚠ **Alerta de prova:** Escolher a proteção de senha quando o cenário pede que o usuário troque a própria senha esquecida.
Como não cair: Proteção de senha só bloqueia senhas fracas; quem redefine é o SSPR. E FIDO2 elimina a senha, mas não bloqueia termos em quem ainda usa senha.

⚠ **Alerta de prova:** Usar um grupo dinâmico por país para bloquear entradas vindas de fora de uma lista aprovada.
Como não cair: Grupo dinâmico só organiza membros, sem avaliar a origem do login. Bloquear por país é Acesso Condicional com locais nomeados.

⚠ **Alerta de prova:** Marcar endereço IP público como controle de concessão do Acesso Condicional.
Como não cair: IP e local são sinais. Controles de concessão são exigir MFA, dispositivo em conformidade, ingressado híbrido ou aplicativo aprovado.

⚠ **Alerta de prova:** Achar que uma revisão de acesso trimestral resolve revogação imediata ou bloqueio na hora do login.
Como não cair: Revisões validam acessos periodicamente e não agem no momento. Revogar quase em tempo real é CAE; decidir no login é Acesso Condicional.

⚠ **Alerta de prova:** Cair em conceitos invertidos: risco de entrada avalia a conta; atribuição qualificada já vale; AD DS usa OAuth e Entra usa Kerberos.
Como não cair: Risco de entrada = aquele login; risco de usuário = a conta. Qualificada = precisa ativar; ativa = já vale. AD DS = Kerberos e LDAP; Entra ID = OAuth, OIDC e SAML.

⚠ **Alerta de prova:** Escolher Microsoft Defender para Identidade ou Verified ID para sincronizar usuários do AD local com o Entra ID.
Como não cair: Defender para Identidade monitora ameaças no AD e Verified ID emite credenciais verificáveis. Sincronizar é Entra Connect (ou Cloud Sync).

⚠ **Alerta de prova:** Achar que os padrões de segurança do locatário parceiro fazem sua empresa aceitar a MFA dos usuários dele.
Como não cair: A confiança na MFA e no dispositivo do parceiro é definida nas configurações de acesso entre locatários do seu locatário.

⚠ **Alerta de prova:** Escolher identidade gerenciada atribuída pelo sistema quando várias VMs precisam compartilhar a mesma identidade.
Como não cair: A atribuída pelo sistema é ligada a um único recurso e excluída com ele. Compartilhada e independente é a atribuída pelo usuário.

⚠ **Alerta de prova:** Considerar pontuação de conformidade, rótulo de retenção ou tamanho da caixa de correio como sinais do Acesso Condicional.
Como não cair: Sinais são quem, onde, qual dispositivo, qual app e qual risco. Pontuação de conformidade é do Compliance Manager e rótulos são do Purview.

⚠ **Alerta de prova:** Achar que o SMS é fraco por funcionar só em iOS ou não receber códigos no exterior.
Como não cair: O problema do SMS é poder ser desviado por troca de chip; a Microsoft recomenda métodos mais fortes, como Authenticator com correspondência de números, passkeys, FIDO2 e Windows Hello. Para fadiga de MFA, a resposta é correspondência de números, não SMS nem pergunta de segurança.

⚠ **Alerta de prova:** Resolver falta de função adequada atribuindo Administrador Global, grupo do Microsoft 365 ou pacote de acesso.
Como não cair: Pacotes de acesso concedem recursos e grupos do Microsoft 365 servem para colaboração, sem permissões administrativas. Nenhuma função interna serve: crie uma função personalizada do Entra.

⚠ **Alerta de prova:** Delegar a administração de uma filial com termos de uso, TAP ou grupos do Microsoft 365.
Como não cair: Administração restrita a uma parte da organização é unidade administrativa.

⚠ **Alerta de prova:** Achar que a sincronização de hash de senha dispensa MFA ou o AD local para login no domínio.
Como não cair: O benefício extra do hash é detectar credenciais vazadas no ID Protection. A MFA continua recomendada e o login no domínio local continua no AD.

Como cai na prova

📝 **Como cai:** Cenário de negócio curto seguido de Qual recurso do Microsoft Entra atende?, com quatro recursos do próprio Entra.
Como resolver: Grife o verbo do cenário (sincronizar, revisar, ativar sob demanda, bloquear no login, delegar, convidar). Associe o verbo ao recurso: sincronizar = Connect; revisar = revisões de acesso; ativar sob demanda = PIM; bloquear no login = Acesso Condicional; delegar parte = unidade administrativa.

📝 **Como cai:** Qual é a diferença entre X e Y?, com uma alternativa certa e uma com os conceitos invertidos.
Como resolver: Lembre a definição de um dos lados (ex.: risco de entrada = aquele login) e confira se a alternativa coloca cada termo no lado certo. A invertida é a armadilha mais frequente.

📝 **Como cai:** Escolha DUAS: sinais, decisões, métodos sem senha ou opções híbridas.
Como resolver: Elimine primeiro o que é de outro produto (rótulos e pontuação de conformidade são do Purview) e o que continua sendo senha. Sobram as duas do mesmo grupo: sinais (dispositivo, risco), decisões (bloquear, conceder com MFA), sem senha (FIDO2, Windows Hello), híbrido (hash, passagem).

📝 **Como cai:** Qual função ou atribuição segue o menor privilégio?
Como resolver: Descarte Administrador Global e Proprietário da assinatura de cara. Escolha a função mais restrita que ainda cumpre a tarefa: redefinir senha = Assistência Técnica; só ver segurança = Leitor de Segurança; recursos do Azure = Azure RBAC.

📝 **Como cai:** Cenário de identidade híbrida com exigência específica (sem hash na nuvem, AD FS, senha valendo no local, sem digitar senha de novo).
Como resolver: Sem hash na nuvem = passagem; AD FS com regras próprias = federação; SSPR atualizando o AD = write-back; computador no domínio sem novo prompt = Seamless SSO; saúde da sincronização = Connect Health.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
consumidores criam conta com e-mail ou conta social	**Microsoft Entra External ID para clientes (CIAM)**
admin só quando precisa, por tempo limitado, com aprovação	**PIM (atribuição qualificada)**
gestores confirmam a cada trimestre se ainda precisam do acesso	**Revisões de acesso**
pacote com grupos, apps e sites, aprovação do gestor e expiração	**Gerenciamento de direitos com pacotes de acesso (recursos ficam em catálogos)**
primeiro dia do funcionário, tarefas automáticas de admissão ou desligamento	**Fluxos de trabalho de ciclo de vida**
app no Azure lê o Key Vault sem senha no código	**Identidade gerenciada**
pipeline do GitHub Actions sem segredos no repositório	**Federação de identidade de carga de trabalho**
substituir a VPN por acesso Zero Trust a aplicações internas	**Microsoft Entra Private Access (Global Secure Access)**
apps legados precisam de LDAP, Kerberos e Política de Grupo sem controladores próprios	**Microsoft Entra Domain Services**
fábrica sem celular precisa de MFA	**Token de hardware OATH**
novo funcionário sem método precisa registrar FIDO2 no primeiro acesso	**Passe de Acesso Temporário (TAP)**
senhas com o nome da empresa, como Contoso2026	**Proteção de senha com lista personalizada (agentes no AD para valer no local)**
testar política sem bloquear ninguém	**Modo somente relatório do Acesso Condicional**

de onde e com qual método o usuário entrou na última semana	**Logs de entrada do Microsoft Entra (alterações no diretório ficam nos logs de auditoria)**

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

- Acesso Condicional age depois do primeiro fator e só bloqueia ou concede (com ou sem controles); não cria grupos, não exclui contas, não aplica rótulos.
- ID Protection e PIM exigem Entra ID P2; Acesso Condicional exige P1; sem licença premium, use padrões de segurança.
- Identidades de carga de trabalho (apps, entidades de serviço, identidades gerenciadas) não fazem MFA e precisam de controles próprios.
- Revisão de acesso é periódica; PIM é just-in-time; CAE é quase em tempo real.
- Orientação de senha atual: sem expiração forçada, com MFA, proteção de senha e troca só quando houver indício de comprometimento.

Essenciais para a prova (checklist)

☐ Sei listar os sinais, as decisões e os controles de concessão e de sessão do Acesso Condicional.

☐ Sei diferenciar risco de entrada e risco de usuário e a autocorreção de cada um.

☐ Sei o que o PIM controla (funções do Entra, do Azure e grupos) e a diferença entre atribuição qualificada e ativa.

☐ Sei separar revisões de acesso, gerenciamento de direitos, fluxos de ciclo de vida e termos de uso dentro do ID Governance.

☐ Sei escolher entre hash de senha, passagem e federação, e quando usar Seamless SSO e write-back.

☐ Sei diferenciar colaboração B2B, conexão direta B2B, CIAM e configurações de acesso entre locatários.

☐ Sei classificar dispositivos como registrados, ingressados ou ingressados de forma híbrida.

☐ Sei quais são as identidades de carga de trabalho e a diferença entre identidade gerenciada do sistema e do usuário.

☐ Sei quais métodos são sem senha, quais resistem a phishing e por que o SMS é mais fraco.

☐ Sei o que cada licença (Free, P1, P2) acrescenta.

Questões de revisão do capítulo

R4.1 · Recursos do Microsoft Entra

Uma empresa quer aceitar a MFA já feita pelos usuários de um locatário parceiro, para que eles não repitam a MFA ao acessar os recursos dela. Qual recurso atende?

A. Grupo dinâmico com os usuários parceiros
B. Proteção de senha com lista personalizada
C. Configurações de acesso entre locatários do Entra
D. Padrões de segurança do locatário parceiro

R4.2 · Recursos do Microsoft Entra

Um aplicativo em uma VM do Azure precisa ler segredos do Azure Key Vault sem guardar senhas ou chaves no código. Qual tipo de identidade atende?

A. Grupo de segurança dinâmico
B. Conta local da própria VM
C. Conta de usuário convidado
D. Identidade gerenciada

R4.3 · Recursos do Microsoft Entra

A cada trimestre, os gestores devem confirmar se os membros de um grupo e os convidados ainda precisam de acesso a um aplicativo. Qual recurso atende?

A. Identidade gerenciada
B. Revisões de acesso do Entra
C. Proteção de senha
D. Padrões de segurança

R4.4 · Recursos do Microsoft Entra

Aplicações legadas migradas para VMs do Azure precisam de LDAP, Kerberos e Política de Grupo, sem a empresa manter controladores de domínio. Qual serviço atende?

A. Microsoft Entra Internet Access
B. Microsoft Entra Verified ID
C. Microsoft Entra Domain Services
D. Microsoft Entra ID Protection

Respostas comentadas

R4.1. C) Configurações de acesso entre locatários do Entra

Por quê: As configurações de acesso entre locatários controlam a colaboração B2B de entrada e saída e a confiança em declarações de MFA e de dispositivos.

✗ A) Incorreta. Grupos dinâmicos organizam usuários.
✗ B) Incorreta. A proteção de senha bloqueia senhas fracas.
✗ D) Incorreta. Os padrões de segurança do parceiro não definem a confiança no seu locatário.

> **Dica de prova:** Confiar na MFA do parceiro: acesso entre locatários.

R4.2. D) Identidade gerenciada

Por quê: No Microsoft Entra, as identidades de carga de trabalho são aplicativos, entidades de serviço e identidades gerenciadas. A identidade gerenciada é um tipo especial de entidade de serviço que dispensa o gerenciamento de credenciais.

✗ A) Incorreta. Grupos agrupam identidades, mas não autenticam o aplicativo.
✗ B) Incorreta. Contas locais da VM não autenticam no Key Vault.
✗ C) Incorreta. Convidados são pessoas de outras organizações.

> **Dica de prova:** App no Azure sem senha no código: identidade gerenciada.

R4.3. B) Revisões de acesso do Entra

Por quê: As revisões de acesso do Microsoft Entra ID Governance ajudam a manter o menor privilégio, removendo acessos que não são mais necessários.

✗ A) Incorreta. Identidades gerenciadas são para aplicativos.
✗ C) Incorreta. A proteção de senha bloqueia senhas fracas.
✗ D) Incorreta. Os padrões de segurança ativam proteções básicas.

> **Dica de prova:** Confirmar periodicamente quem ainda precisa: revisões de acesso.

R4.4. C) Microsoft Entra Domain Services

Por quê: O Microsoft Entra Domain Services fornece serviços de domínio gerenciados, compatíveis com o AD DS, para cargas legadas na nuvem.

✗ A) Incorreta. O Internet Access protege o tráfego de internet.
✗ B) Incorreta. O Verified ID emite credenciais verificáveis.
✗ D) Incorreta. O ID Protection detecta riscos de identidade.

> **Dica de prova:** Domínio gerenciado para apps legados: Entra Domain Services.

DIA DA PROVA

Estratégia de prova

O SC-900 é uma prova de fundamentos que testa se você reconhece o produto ou recurso Microsoft certo para um cenário curto de negócio. A maioria das perguntas tem quatro alternativas que são produtos reais, quase sempre de áreas diferentes (Entra, Defender, Sentinel, Purview), e a errada mais tentadora é um recurso vizinho do mesmo produto. Há também questões de múltipla resposta (Escolha DUAS) e perguntas de diferença entre conceitos em que uma alternativa tem os papéis invertidos. O peso maior está em soluções de segurança (35% a 40%) e no Microsoft Entra (25% a 30%), então reconhecer rapidamente qual Defender, qual recurso do Sentinel e qual recurso do Entra se aplica decide a nota.

Como responder

✓ Leia o enunciado procurando o alvo (e-mail, dispositivo, AD local, app SaaS, nuvem, dados, identidade) e o verbo (detectar, bloquear, reter, revisar, sincronizar); esses dois juntos apontam o produto.

✓ Elimine primeiro as alternativas de outra família: se o cenário é identidade, descarte Purview e Defender; se é retenção ou vazamento de dados, descarte Entra e Sentinel.

✓ Em Escolha DUAS, confirme que as duas marcadas pertencem ao mesmo produto ou à mesma lista (sinais do Acesso Condicional, produtos do Defender XDR, opções híbridas); elimine antes o que é de outro produto.

✓ Em perguntas de diferença entre X e Y, fixe a definição de um dos lados e descarte a alternativa com os papéis invertidos.

✓ Quando o cenário pede menor privilégio, descarte Administrador Global e Proprietário da assinatura e escolha a função mais restrita que cumpre a tarefa.

✓ Divida o tempo: a Microsoft não divulga o número exato (de 40 a 60 questões, cerca de 50) e são 45 minutos; não fique preso em uma; marque para revisão e volte no fim.

✓ Distribua o estudo pelos pesos: segurança (35-40%) e Entra (25-30%) somam a maior parte da nota, mas conceitos (10-15%) são definições rápidas que não se pode errar.

✓ Desconfie de alternativas com palavras absolutas (sempre exige agente, só coleta do Azure, nenhuma proteção existe) e confira contra o que você sabe do recurso: o Defender for Cloud tem verificação sem agente, o Sentinel coleta de AWS e GCP e o Azure tem proteção básica contra DDoS. Mas algumas limitações são reais: o Acesso Condicional só bloqueia ou concede e o CSPM básico só traz recomendações e classificação de segurança.

Erros que derrubam candidatos

✗ Confundir recursos vizinhos: revisões de acesso x PIM, regras de automação x playbooks, política x rótulo de retenção, NSG x Azure Firewall x WAF.

✗ Trocar Microsoft Secure Score (Microsoft 365), classificação de segurança do Defender for Cloud e pontuação de conformidade do Compliance Manager.

✗ Marcar a alternativa com conceitos invertidos por ler rápido (risco de entrada x usuário, qualificada x ativa, chave pública x privada, confidencialidade x retenção).

✗ Atribuir a um Defender o recurso de outro: sensores em controladores de domínio são do Defender para Identidade, ASR é do Ponto de Extremidade, shadow IT é do Cloud Apps.

✗ Achar que o Compliance Manager mostra os relatórios de auditoria da Microsoft, que ficam no Service Trust Portal.

✗ Esquecer licenças e planos: ID Protection e PIM no P2; análise de caminho de ataque no Defender CSPM; Explorador de Ameaças no Defender para Office 365 plano 2.

✗ Escolher revisões ou retenções periódicas quando o cenário pede ação imediata no login (Acesso Condicional) ou revogação quase em tempo real (CAE).

Na semana da prova

- ☐ Refaça as provas práticas e, em cada erro, anote o par de recursos que você confundiu; revise só esses pares.
- ☐ Monte uma tabela de uma página com produto, alvo e recursos-chave: Entra, Defender XDR (Ponto de Extremidade, Office 365, Identidade, Cloud Apps), Defender for Cloud, Sentinel e Purview.
- ☐ Revise as listas que caem como definição: camadas da defesa em profundidade, princípios e pilares do Zero Trust, pilares da identidade, tríade CIA e GRC.

☐ Releia os números que aparecem nas alternativas: Auditoria Standard 180 dias, busca avançada até 30 dias, regras NRT a cada minuto, licença P2 para ID Protection e PIM.

☐ Na véspera, só revisão leve dos macetes e das pegadinhas; chegue sabendo que são de 40 a 60 questões (cerca de 50) em 45 minutos, com pontuação de 1 a 1000 e mínimo de 700.

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 segurança, conformidade e identidade

‣ mesma chave nos dois lados → **Criptografia simétrica**

‣ hash publicado para conferir o arquivo baixado → **Integridade**

‣ site fora do ar por ataque de negação de serviço → **Disponibilidade**

‣ HTTPS, TLS, dados trafegando → **Criptografia em trânsito**

‣ disco roubado, dados ilegíveis → **Criptografia em repouso**

⚠ A privada do remetente assina. Sigilo para o destinatário = chave pública do destinatário.

⚠ Assina com a privada do remetente; verifica com a pública dele.

⚠ O hash continua irreversível. O salt existe para que senhas iguais tenham hashes distintos.

2. Recursos das soluções de conformidade da Microsoft

‣ relatórios ISO 27001 e SOC 2 dos serviços da Microsoft → **Service Trust Portal**

‣ pontuação de conformidade com LGPD ou ISO e ações de melhoria → **Compliance Manager (avaliação a partir de modelo)**

‣ aprovar acesso de engenheiros da Microsoft ao conteúdo → **Customer Lockbox (Sistema de Proteção de Dados do Cliente)**

‣ impedir envio de cartão de crédito para fora → **DLP do Purview**

‣ aviso no Outlook explicando a regra na hora de enviar → **Dica de política de DLP**

⚠ Os papéis estão invertidos: confidencialidade = quem acessa; retenção = quanto tempo fica. Os dois são do Purview, não do Defender nem do Sentinel.

⚠ Guardar X anos e apagar depois é reter e depois excluir.

⚠ Local inteiro = política de retenção. Rótulo de retenção é para regras por item.

3. Recursos das soluções de segurança da Microsoft

‣ Kerberoasting, pass-the-hash, golden ticket, controladores de domínio → **Microsoft Defender para Identidade**

‣ conta falsa isca no AD → **Conta honeytoken (Defender para Identidade)**

‣ shadow IT, apps SaaS sem aprovação, CASB → **Microsoft Defender para Cloud Apps**

‣ ver documentos sim, baixar não, em dispositivo não gerenciado → **Controle de sessão do Defender para Cloud Apps com Acesso Condicional**

‣ e-mail malicioso já entregue precisa ser removido → **Limpeza automática de hora zero (ZAP)**

⚠ O NSG filtra por IP, porta e protocolo e não inspeciona HTTP. Ataques de aplicação web pedem WAF.

⚠ O Azure Firewall filtra tráfego, mas a proteção dedicada contra DDoS volumétrico é o Azure DDoS Protection.

⚠ A proteção básica de infraestrutura vem por padrão; métricas, alertas e ajuste por aplicação vêm só com o Azure DDoS Protection.

4. Recursos do Microsoft Entra

‣ consumidores criam conta com e-mail ou conta social → **Microsoft Entra External ID para clientes (CIAM)**

‣ admin só quando precisa, por tempo limitado, com aprovação → **PIM (atribuição qualificada)**

‣ gestores confirmam a cada trimestre se ainda precisam do acesso → **Revisões de acesso**

‣ pacote com grupos, apps e sites, aprovação do gestor e expiração → **Gerenciamento de direitos com pacotes de acesso (recursos ficam em catálogos)**

‣ primeiro dia do funcionário, tarefas automáticas de admissão ou desligamento → **Fluxos de trabalho de ciclo de vida**

⚠ Menor privilégio: Administrador de Assistência Técnica. Administrador de Segurança mexe em configurações de segurança e Global tem acesso total.

⚠ Proteção de senha só bloqueia senhas fracas; quem redefine é o SSPR. E FIDO2 elimina a senha, mas não bloqueia termos em quem ainda usa senha.

⚠ Grupo dinâmico só organiza membros, sem avaliar a origem do login. Bloquear por país é Acesso Condicional com locais nomeados.

GABARITO

Respostas do diagnóstico

D1. B) Conformidade → revise o capítulo 1

Por quê: GRC reúne governança (regras e processos internos), risco (identificar e tratar ameaças) e conformidade (atender a leis e normas).

✗ A) Incorreta. Gestão de risco identifica e trata ameaças ao negócio.

✗ C) Incorreta. Autenticação comprova identidades.

✗ D) Incorreta. Governança são as regras e processos internos para dirigir a organização.

> **Dica de prova:** Seguir leis e normas: conformidade.

D2. D) Um provedor de identidade → revise o capítulo 1

Por quê: Na autenticação moderna, os aplicativos confiam em um provedor de identidade central, que autentica o usuário e emite tokens.

✗ A) Incorreta. O firewall de aplicativo protege aplicações web.

✗ B) Incorreta. O agente de acesso (CASB) protege o uso de apps de nuvem.

✗ C) Incorreta. O cofre guarda segredos e chaves.

> **Dica de prova:** Gerencia identidades e autentica: provedor de identidade.

D3. C) Os usuários acessam recursos de qualquer lugar e de qualquer dispositivo → revise o capítulo 1

Por quê: Com usuários e dados fora da rede corporativa, proteger identidades com autenticação forte e controle de acesso passou a ser a base da segurança.

✗ A) Incorreta. O trabalho acontece dentro e fora da rede.

✗ B) Incorreta. Aplicações de nuvem exigem autenticação.

✗ D) Incorreta. Custos de firewall não explicam a mudança.

> **Dica de prova:** Acesso de qualquer lugar: a identidade é o novo perímetro.

D4. C) Reter e depois excluir → revise o capítulo 2

Por quê: Configurações de retenção podem reter por um período, reter e excluir, ou apenas excluir após um período.

✗ A) Incorreta. Só excluir não garante a retenção de três anos.

✗ B) Incorreta. Reter sem prazo não atende ao requisito de exclusão.

✗ D) Incorreta. Reter para sempre não exclui depois.

> **Dica de prova:** Guardar X anos e apagar: reter e depois excluir.

D5. C) Tipos de informações confidenciais → revise o capítulo 2

Por quê: O Purview tem centenas de tipos de informações confidenciais prontos, incluindo documentos brasileiros, e permite criar tipos personalizados.

✗ A) Incorreta. Fluxos de ciclo de vida são do Entra.
✗ B) Incorreta. Classificadores treináveis reconhecem categorias de documentos.
✗ D) Incorreta. Barreiras restringem comunicação.

> **Dica de prova:** Padrão como CPF: tipo de informação confidencial.

D6. B) Rótulo de confidencialidade no site → revise o capítulo 2

Por quê: Além de arquivos e e-mails, rótulos de confidencialidade podem proteger contêineres: times do Teams, grupos do Microsoft 365 e sites do SharePoint.

✗ A) Incorreta. Retenção define tempo de guarda.
✗ C) Incorreta. Revisão de descarte trata do fim da retenção.
✗ D) Incorreta. Tipos de informações confidenciais detectam padrões em conteúdo.

> **Dica de prova:** Controlar convidados em times e sites: rótulo para contêiner.

D7. D) Azure Firewall → revise o capítulo 3

Por quê: Na topologia hub e spoke, serviços compartilhados como o Azure Firewall ficam no hub e as cargas de trabalho ficam nos spokes.

✗ A) Incorreta. O Purview trata de conformidade e dados.
✗ B) Incorreta. O Key Vault guarda segredos.
✗ C) Incorreta. O Priva trata de privacidade.

> **Dica de prova:** Controle central de tráfego no hub: Azure Firewall.

D8. D) Segmentação de rede → revise o capítulo 3

Por quê: Redes virtuais, sub-redes e NSGs permitem segmentar ambientes, aplicando o princípio de presumir a violação.

✗ A) Incorreta. Criptografia em repouso protege dados armazenados.
✗ B) Incorreta. MFA protege identidades.
✗ C) Incorreta. Retenção define tempo de guarda.

> **Dica de prova:** Separar camadas por sub-rede: segmentação.

D9. B) Conta honeytoken → revise o capítulo 3

Por quê: No Defender para Identidade, marcar contas como honeytoken ajuda a detectar invasores que tentam usar credenciais encontradas no ambiente.

✗ A) Incorreta. Contas de serviço executam aplicativos.
✗ C) Incorreta. Contas de emergência são usadas em falhas de acesso.
✗ D) Incorreta. Convidados são usuários externos.

> **Dica de prova:** Conta isca: honeytoken.

D10. D) Microsoft Entra Connect → revise o capítulo 4

Por quê: Na identidade híbrida, o Entra Connect Sync ou o Entra Cloud Sync sincroniza usuários e grupos do AD local com o Entra ID.

✗ A) Incorreta. O Verified ID emite credenciais verificáveis.
✗ B) Incorreta. O Data Map cataloga dados.
✗ C) Incorreta. O Defender para Identidade monitora ameaças no AD.

> **Dica de prova:** AD local para o Entra ID: Entra Connect.

D11. C) Ingressados de forma híbrida → revise o capítulo 4

Por quê: O ingresso híbrido no Microsoft Entra permite manter a gestão pelo AD local e, ao mesmo tempo, usar recursos de nuvem como o Acesso Condicional.

✗ A) Incorreta. Registro é para dispositivos pessoais.
✗ B) Incorreta. Esses dispositivos continuam no domínio local.
✗ D) Incorreta. Convidados são usuários externos.

> **Dica de prova:** Domínio local + Entra: ingresso híbrido.

D12. C) Microsoft Entra Connect Health → revise o capítulo 4

Por quê: O Microsoft Entra Connect Health mostra alertas, desempenho e erros de sincronização e de serviços como o AD FS.

✗ A) Incorreta. O Data Map cataloga dados.
✗ B) Incorreta. O Verified ID trata de credenciais verificáveis.
✗ D) Incorreta. O EASM mapeia ativos expostos.

> **Dica de prova:** Saúde da sincronização híbrida: Connect Health.

Agora, treine no formato real

Faça as 6 provas completas do curso SC-900: 300 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 Microsoft. As questões são inéditas e não reproduzem a prova real.