Strecht Simulados · Guia de preparação



Guia de preparação AB-650

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.

3 capítulos por domínio	**21** 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 AB-650: 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 100 minutos, no formato do exame. Referência de aprovação: 70%.

Domínio (capítulo)	Peso	Neste guia
1. Configurar e gerenciar locatários e cargas de trabalho do Microsoft 365	20-25%	18 conceitos · 14 pegadinhas
2. Gerenciar e proteger serviços de IA no Microsoft 365	35-40%	18 conceitos · 14 pegadinhas
3. Governar e proteger locatários e cargas de trabalho do Microsoft 365	40-45%	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 9 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 · Configurar e gerenciar locatários e cargas de trabalho do Microsoft 365

Ao adicionar o domínio fabrikamtextil.com.br no Microsoft 365 admin center, o administrador percebe que o registrador do domínio é compatível com Domain Connect. Que benefício esse suporte traz durante o assistente de configuração?

A. O registro MX é ignorado e o e-mail continua chegando ao provedor anterior por padrão
B. O assistente abre o registrador para autorizar a criação dos registros DNS
C. O domínio passa a ser verificado pelo histórico de cobrança da assinatura, sem consultar o DNS
D. A Microsoft transfere o domínio para o seu próprio registrador e assume a renovação anual

D2 · Configurar e gerenciar locatários e cargas de trabalho do Microsoft 365

A Concessionária Rodovia Sul comprou o domínio rodoviasul.com.br pelo Microsoft 365, que gerencia o DNS. Agora o marketing quer adicionar o subdomínio ofertas.rodoviasul.com.br ao locatário. O que impede essa configuração?

A. Subdomínios só são aceitos depois que o domínio principal completa um ano de registro
B. Subdomínios precisam de uma assinatura do Microsoft 365 separada, com outro locatário
C. Subdomínios exigem uma licença adicional de Exchange Online para cada endereço criado
D. Subdomínios só podem ser adicionados quando a organização gerencia o próprio DNS no registrador

D3 · Configurar e gerenciar locatários e cargas de trabalho do Microsoft 365

A Rede de Lojas Bela Casa quer usar o Windows Location Services para identificar automaticamente as lojas em Health > Network connectivity, sem cadastrar sub-redes. Qual requisito o administrador precisa garantir?

A. Ativar o recurso nas configurações de local, que vem desligado, e ter dois computadores em Wi-Fi por loja
B. Instalar o Microsoft Edge em todos os computadores e cadastrar o endereço postal de cada loja no admin center
C. Ligar os computadores de cada loja por cabo de rede para que a localização tenha precisão de 300 metros
D. Instalar em cada loja um servidor dedicado que envia os testes de rede uma vez por hora ao admin center

D4 · Gerenciar e proteger serviços de IA no Microsoft 365

O gerente de TI da Prefeitura de Lagoa Bonita quer que alguns administradores usem o Microsoft 365 Admin agent, uma experiência agêntica que ajuda a operar o Microsoft 365, o Copilot e os agentes. Onde ele controla se administradores qualificados podem usar o Copilot nos centros de administração?

A. Em Agents > Settings > Agent and plugin access, liberando agentes da Microsoft
B. Em Copilot > Settings > User access > Microsoft Copilot in admin centers
C. Em Health > Service health > Customize, ativando as notificações do Copilot
D. Em Settings > Org settings > Organization profile > Custom themes do locatário

D5 · Gerenciar e proteger serviços de IA no Microsoft 365

Por política de marca, a Agência de Publicidade Contraste não quer que os funcionários gerem imagens com o Microsoft Copilot. Onde o administrador encontra o controle para impedir as experiências de geração de imagem?

A. Em Copilot > Settings > User access > Pin Microsoft Copilot Chat
B. Em Copilot > Settings > Copilot actions > Copilot image generation
C. Em Copilot > Settings > Other settings > Copilot custom dictionary
D. Em Copilot > Settings > Data access > AI providers operating as independent processors

D6 · Gerenciar e proteger serviços de IA no Microsoft 365

A administradora da Agência de Turismo Destino Certo habilitou a pesquisa na web no Microsoft Copilot para todos. Um gerente que trabalha com dados sigilosos pergunta se pode desligar a pesquisa na web só para ele. Qual é a resposta?

A. Não, porque a escolha do administrador não pode ser alterada pelo usuário final
B. Não, porque a pesquisa na web só pode ser desligada por política de grupo do Windows
C. Sim, desligando as experiências conectadas opcionais na privacidade do Word
D. Sim, pelo botão Web search em Personalization > Advanced nas configurações do app

D7 · Governar e proteger locatários e cargas de trabalho do Microsoft 365

Um professor da Escola Técnica Engenho digitou a mesma senha errada cinco vezes seguidas, mas a conta não foi bloqueada pelo bloqueio inteligente. O analista de suporte achou que o recurso estava desligado. Como o comportamento se explica?

A. O bloqueio inteligente precisa ser ativado pela Proteção de Senha no modo Enforced antes de valer na nuvem
B. O bloqueio inteligente guarda os três últimos hashes de senha errada e não conta repetições da mesma senha
C. O bloqueio inteligente só funciona para contas de administradores e não protege contas de usuários comuns
D. O bloqueio inteligente só age depois de 50 tentativas com falha em locatários comerciais com mais de mil usuários

D8 · Governar e proteger locatários e cargas de trabalho do Microsoft 365

A equipe de compliance da Operadora Logística Tucano criou um tipo de informação confidencial personalizado para o número de contrato, que tem nove dígitos. Muitos números de telefone geram falsos positivos. O que a equipe deve acrescentar ao padrão para aumentar a confiança das detecções?

A. Um rótulo de confidencialidade com criptografia aplicado aos contratos
B. Uma política de expiração de grupos para as bibliotecas com contratos
C. Um elemento de suporte com palavras-chave próximas, como contrato ou nº do contrato
D. Um rótulo de retenção que exclua os documentos com números de telefone dos clientes

D9 · Governar e proteger locatários e cargas de trabalho do Microsoft 365

O administrador da Têxtil Paraná configurou o SSPR exigindo um método de autenticação e testou com a própria conta de Global Administrator. O sistema pediu dois métodos e não aceitou perguntas de segurança. Ele concluiu que a política estava errada. Como o comportamento se explica?

A. Contas com funções administrativas seguem a política de duas etapas, que não pode ser alterada
B. A política de um método só passa a valer depois de 30 dias da primeira configuração
C. O SSPR ignora a política do locatário até que a Proteção de Senha seja ativada no local
D. O Global Administrator precisa de licença P2 para usar a mesma política dos usuários

01

CAPÍTULO 1 · 20-25% DA PROVA

Configurar e gerenciar locatários e cargas de trabalho do Microsoft 365

Este domínio (20-25%) é o mais operacional: domínios e DNS, temas, configurações da organização, licenças, Microsoft 365 Backup, conectividade de rede, Service health, caixas compartilhadas, Teams com Copilot em reuniões e SharePoint. A prova cobra limites exatos (temas, tamanho de logotipo, caixas compartilhadas, janelas do Backup) e sequências corretas (converter a caixa antes de tirar a licença, entrar no novo grupo licenciado antes de sair do antigo). Também cai muito a política de Copilot nas reuniões do Teams, com seus valores e padrões. Onde mais erro é confundir padrão com exceção: o que vem por padrão na política de reunião, o que só o tema padrão aceita e o que vale para a organização inteira sem poder ser direcionado a grupos.

Neste capítulo

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

Tópicos-chave

Domínios e DNS

Se já existe SPF, acrescentam-se os valores do Microsoft 365 ao registro existente; nunca se cria um segundo SPF. No MX, número de preferência menor significa prioridade maior, e trocar o MX leva todo o e-mail do domínio ao Microsoft 365. Domain Connect abre o registrador para autorizar a criação dos registros, sem transferir o domínio nem dispensar a verificação por DNS.

Subdomínios, domínio padrão e onmicrosoft.com

Subdomínio só pode ser adicionado quando a organização gerencia o próprio DNS no registrador, e é verificado automaticamente pelo domínio pai. Trocar o domínio padrão afeta só contas novas. Domínios onmicrosoft.com não podem ser excluídos nem renomeados; cria-se outro e define-se como fallback.

Temas da organização

Há um tema padrão e até quatro temas de grupo, cada um associado a no máximo cinco grupos do Microsoft 365 (não grupos de segurança nem listas de distribuição). Só o tema padrão aceita upload direto de logotipo, abaixo de 10 KB; temas de grupo usam URL. A aba General impede que usuários substituam o tema e a aba Logos aceita logotipo alternativo para temas escuros.

Cor de destaque e rodapé do Copilot Chat

A cor de destaque aparece em alguns links e botões sobre fundo claro, como na caixa de entrada; fundo e textos da barra superior usam outras cores. O logotipo no rodapé do app Microsoft 365 Copilot, com o rótulo Managed by, vem da aba Copilot Chat do tema padrão e vale para todos, sem direcionamento a grupos.

Tempo limite de sessão ociosa

Fica em Org Settings > Security & privacy, e a ativação inicial exige Global Administrator. Vale para a organização inteira, só nos apps web (Outlook na Web, OneDrive, SharePoint e Office na Web), sem afetar apps de desktop e móveis e sem direcionamento a grupos ou unidades administrativas. Para limitar só dispositivos não gerenciados, usa-se Acesso Condicional com Use app enforced restrictions (P1 ou P2).

Licenciamento baseado em grupo

License Administrator é a função mínima para atribuir licenças a grupos. Grupos aninhados não recebem a licença; só membros de primeiro nível. Falhas aparecem em Billing > Licenses > produto > Errors & issues, e para trocar de licença o usuário entra no novo grupo, confirma a licença e só depois sai do antigo.

Planos e licenças de IA

Microsoft 365 E7 inclui E5, Copilot, Agent 365 e Microsoft Entra Suite. Copilot Business é complemento pago para até 300 usuários com licenças Business. Agent 365 é licenciado por usuário e habilitá-lo exige pelo menos um usuário licenciado. Copilot Studio usa licença de locatário mais Copilot Studio User License só para quem cria, ou pay-as-you-go por política de cobrança no Power Platform admin center.

Microsoft 365 Backup: cobrança e janelas

Antes de criar políticas é preciso configurar o pay-as-you-go no nó Billing com assinatura do Azure, grupo de recursos e região. Custa US$ 0,15 por GB por mês do que é protegido e restaurar é grátis. A janela de recuperação tem opções fixas de 3 meses, 6 meses, 1 ano e 2 anos.

Backup: pontos e restauração

Caixas do Exchange têm pontos de 10 minutos; sites e OneDrive passam a semanais depois de duas semanas. Express restore point no mesmo URL é o mais rápido (sobrescreve); restaurar em novo URL preserva o conteúdo atual. Suporta caixas de usuário e compartilhadas, não de sala nem de grupo.

Backup: funções e usuários excluídos

Microsoft 365 Backup Administrator gerencia tudo; Exchange Administrator gerencia só o Exchange; SharePoint Backup Admin é exigida para restauração granular de arquivos e pastas. Usuário excluído há menos de 30 dias: restaura-se a conta e depois o OneDrive pelo Backup; o backup é retido por um ano. Caixa inativa usa Recover an inactive mailbox, não Restore. A Backup Notification List avisa sobre pausas e remoções.

Conectividade de rede

Em Health > Network connectivity, locais são cadastrados com sub-redes LAN (obrigatórias); IPs públicos de saída são só diferenciador. Windows Location Services vem desligado, exige Wi-Fi e pelo menos dois computadores por local e agrupa por cidade. O teste manual de conectividade dá resultado em 2 a 3 minutos; Service Support Administrator configura e Reports Reader lê.

Service health e Message center

Advisory afeta alguns usuários com o serviço disponível; incident indica serviço ou função principal indisponível. Notificações por e-mail ficam em Customize > Email, com até dois endereços. Manutenções e mudanças planejadas ficam no Message center, categoria Plan for change.

Preferências de versão

Deferred release atrasa as atualizações principais cerca de 30 dias; um piloto pode ficar em Standard release (Assign users or groups for standard release). No Message center essas atualizações têm as marcas Major update e Deferred feature. Targeted release não aceita alterações a partir de novembro de 2026 e será aposentado em janeiro de 2027; Frontier é prévia antes da disponibilidade geral.

Caixas de correio compartilhadas

Sem licença vão até 50 GB; com Exchange Online Plan 2 vão a 100 GB. Suportam no máximo 25 usuários simultâneos, não impedem exclusão de mensagens e não aceitam pessoas de fora. Retenção de litígio e arquivo morto ampliado exigem Plan 2 ou Plan 1 com Exchange Online Archiving; para manter a caixa de ex-funcionário: converter ainda licenciada, remover a licença e manter a conta.

Canais do Teams

Só o proprietário do canal privado adiciona membros a ele, nem mesmo o proprietário do time. Só proprietários do time criam canais compartilhados; externos entram pelo B2B direct connect, e convidados não podem ser adicionados a canais compartilhados.

Copilot nas reuniões do Teams

O padrão da política é On with saved transcript required (EnabledWithTranscript), que fixa During and after the meeting sem permitir mudança. Enabled deixa Only during the meeting como padrão e o organizador muda; EnabledWithTranscriptDefaultOn põe During and after como padrão e o organizador muda. Off desliga também gravação e transcrição; reuniões com criptografia de ponta a ponta não têm Copilot.

Permissões e pesquisa no SharePoint

Site de equipe ligado a grupo do Microsoft 365 recebe permissões pelo grupo, que não tem somente leitura; leitura vai no grupo Visitors do site. Para tirar um site da pesquisa sem mexer em acesso, marca-se No em Allow this site to appear in Search results. Restricted Content Discovery impede a descoberta em experiências de toda a organização, sem mudar permissões nem índice, e não vale para OneDrive.

SharePoint Advanced Management e Microsoft 365 Archive

As políticas de ciclo de vida de sites tratam sites inativos, propriedade (número mínimo de proprietários) e atestado. Relatórios de governança de acesso a dados como Sharing links activity e Everyone except external users (EEEU) mostram compartilhamento amplo recente. Sites inativos que precisam ser preservados vão para o Microsoft 365 Archive, que mantém conteúdo, permissões e metadados e libera a cota ativa.

Macetes para memorizar

Temas

1 + 4 x 5: um padrão, quatro de grupo, cinco grupos do Microsoft 365 por tema; logotipo enviado só no padrão e menor que 10 KB.

MX

No MX, quem tem número menor fala primeiro.

Caixa compartilhada

50 de graça, 100 com Plan 2, 25 pessoas no máximo, ninguém de fora.

Janela do Backup

3-6-12-24 meses, nada no meio.

Pontos do Backup

Exchange de 10 em 10 minutos; sites e OneDrive viram semanais depois de duas semanas.

Política de Copilot em reuniões

Sem mexer = transcrição obrigatória e organizador sem escolha. DefaultOn = transcrição por padrão, organizador livre. Off = sem Copilot, sem gravação, sem transcrição.

Troca de licença por grupo

Entra no novo antes de sair do velho.

Tabela de memorização: não confunda

Quando é...	...e quando é
Express restore point no mesmo URL Ransomware: devolver o site ao estado saudável no menor tempo, aceitando sobrescrever.	**Restaurar em novo URL** Recuperar sem sobrescrever conteúdo novo e saudável criado depois do incidente.

Recover an inactive mailbox Caixa inativa protegida pelo Backup cujos dados de backup precisam ser preservados.	**Restore an inactive mailbox** Não preserva os dados de backup da caixa antiga; não serve ao cenário do Backup.
Advisory Impacto limitado a alguns usuários, com o serviço disponível.	**Incident** Serviço ou função principal indisponível.
Sub-redes LAN Separar escritórios na mesma cidade, inclusive com computadores por cabo.	**Windows Location Services** Detectar locais automaticamente por cidade, com Wi-Fi e pelo menos dois computadores por local.
EnabledWithTranscript (padrão) Copilot fica fixo em During and after the meeting, sem escolha do organizador.	**EnabledWithTranscriptDefaultOn** During and after vem por padrão, mas o organizador pode mudar para Only during the meeting.
Tempo limite de sessão ociosa Desconectar apps web de toda a organização após inatividade.	**Acesso Condicional com Use app enforced restrictions** Aplicar a restrição só a dispositivos não gerenciados ou a um conjunto de usuários.
Pay-as-you-go do nó Billing Microsoft 365 Backup e armazenamento adicional do SharePoint.	**Política de cobrança no Power Platform admin center** Copilot Studio sem compromisso, pagando Copilot Credits consumidos.

Números que caem

Item	Valor
Temas	**1 padrão + até 4 temas de grupo, cada um com até 5 grupos do Microsoft 365**
Upload direto de logotipo no tema padrão	**abaixo de 10 KB (JPG, PNG, GIF ou SVG)**
Caixa compartilhada sem licença	**até 50 GB; 100 GB com Exchange Online Plan 2**
Usuários de uma caixa compartilhada	**máximo de 25**
Custo do Microsoft 365 Backup	**US$ 0,15 por GB por mês protegido; restauração gratuita**
Janela de recuperação do Backup	**3 meses, 6 meses, 1 ano ou 2 anos**
Pontos de restauração do Backup	**Exchange: RPO de 10 minutos; sites e OneDrive: 10 minutos nas 2 semanas mais recentes e semanais de 2 a 52 semanas**
Backup de OneDrive e caixa de usuário excluído	**retido por 1 ano**
Copilot Business	**até 300 usuários**

Copilot em reuniões e eventos do Teams	**até 1.000 participantes**
Deferred release	**cerca de 30 dias após a disponibilidade geral**
Targeted release	**alterações bloqueadas em novembro de 2026; aposentado em janeiro de 2027**
Teste manual de conectividade de rede	**resultado em 2 a 3 minutos**
Notificações por e-mail do Service health	**até 2 endereços**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Criar um segundo registro TXT de SPF só com os valores do Microsoft 365.
Como não cair: Dois SPF é o que a documentação manda evitar; acrescente os valores ao existente.

⚠ **Alerta de prova:** Dar ao MX do Exchange Online o maior número de preferência para priorizá-lo.
Como não cair: Número menor = prioridade maior.

⚠ **Alerta de prova:** Achar que trocar o domínio padrão renomeia as contas existentes.
Como não cair: Só contas novas usam o domínio padrão; credenciais e acesso não mudam.

⚠ **Alerta de prova:** Associar um tema de grupo a grupo de segurança ou lista de distribuição.
Como não cair: Temas de grupo aceitam só grupos do Microsoft 365.

⚠ **Alerta de prova:** Subir logotipo de 35 KB num tema de grupo.
Como não cair: Upload direto só no tema padrão e abaixo de 10 KB; temas de grupo usam URL.

⚠ **Alerta de prova:** Direcionar o tempo limite de sessão ociosa a um grupo ou esperar que desconecte o Outlook de desktop.
Como não cair: Vale para a organização inteira e só para apps web.

⚠ **Alerta de prova:** Colocar grupos dentro do grupo licenciado para simplificar.
Como não cair: Licenciamento por grupo não suporta aninhamento; membros dos grupos internos ficam sem licença.

⚠ **Alerta de prova:** Remover o usuário do grupo da licença antiga antes de incluí-lo no novo.
Como não cair: Entre no novo grupo, confirme a licença e só então saia do antigo para não haver intervalo sem acesso.

⚠ **Alerta de prova:** Remover a licença ou excluir a conta antes de converter a caixa do ex-funcionário em compartilhada.
Como não cair: Sem licença a conversão não aparece, e a conta ancora a caixa: converta, tire a licença e mantenha a conta.

⚠ **Alerta de prova:** Licenciar a caixa compartilhada com Plan 2 para aceitar 40 usuários simultâneos.
Como não cair: Plan 2 amplia o armazenamento para 100 GB; o limite de usuários é 25 e exclusões não podem ser bloqueadas.

⚠ **Alerta de prova:** Proteger caixa de sala ou de grupo no Microsoft 365 Backup.
Como não cair: O backup suporta caixas de usuário e compartilhadas, não de sala nem de grupo.

⚠ **Alerta de prova:** Escolher 18 meses ou 5 anos de janela de recuperação no Backup.
Como não cair: As opções são fixas: 3 meses, 6 meses, 1 ano e 2 anos.

⚠ **Alerta de prova:** Achar que o proprietário do time adiciona pessoas a qualquer canal privado.
Como não cair: Só o proprietário do canal privado adiciona membros.

⚠ **Alerta de prova:** Supor que Copilot em Off na reunião ainda permite gravar e transcrever.
Como não cair: Off desliga também gravação e transcrição.

Como cai na prova

📝 **Como cai:** Sequência de passos (converter caixa, trocar licença, restaurar usuário excluído).
Como resolver: Procure a ordem que nunca deixa o usuário sem acesso ou sem âncora: converter com licença, entrar no novo grupo primeiro, restaurar a conta antes do OneDrive.

📝 **Como cai:** Limite numérico disfarçado em alternativa plausível (18 meses, 35 KB, 40 usuários, 10 temas).
Como resolver: Compare com os limites decorados: 3/6/12/24 meses, menos de 10 KB, 25 usuários, quatro temas de grupo com cinco grupos.

📝 **Como cai:** Qual função mínima configura ou lê (licenças, rede, Backup).
Como resolver: License Administrator para licenças; Service Support Administrator configura e Reports Reader lê a rede; Backup Administrator para tudo do Backup, Exchange Administrator só Exchange, SharePoint Backup Admin para restauração granular.

📝 **Como cai:** Valor da política de reunião do Teams e comportamento resultante.
Como resolver: Identifique se o organizador pode mudar e qual o modo padrão; lembre que During and after depende de transcrição e que alguém com permissão pode ativá-la.

📝 **Como cai:** Escolha DUAS sobre Restricted Content Discovery, SAM ou caixas compartilhadas.
Como resolver: Marque as afirmações que preservam permissões e descrevem limites reais; descarte as que estendem o recurso ao OneDrive, removem do índice ou aumentam usuários com licença.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Registrador compatível com Domain Connect	**Assistente abre o registrador para autorizar a criação dos registros DNS.**
Domínio comprado pelo Microsoft 365 com DNS gerenciado pela Microsoft e pedido de subdomínio	**Não é possível: subdomínio exige DNS gerenciado pela organização.**
Usuários trocam o tema e logotipo some no modo escuro	**Aba General impede substituir; logotipo alternativo para temas escuros na aba Logos.**
Licença por grupo não chegou a alguns usuários	**Billing > Licenses > produto > Errors & issues (e verificar aninhamento).**
Backup não deixa criar política	**Configurar pay-as-you-go com assinatura do Azure, grupo de recursos e região.**
Restaurar só alguns arquivos de um site protegido	**Função SharePoint Backup Admin.**
Avisar vários responsáveis se alguém pausar política do Backup	**Backup Notification List.**
Escola nova sem computadores suficientes para medições automáticas	**Teste manual de conectividade de rede, resultado em 2 a 3 minutos.**
Manutenção planejada com antecedência	**Message center, categoria Plan for change.**
Piloto recebe na disponibilidade geral e o restante cerca de 30 dias depois	**Deferred release para a organização e o piloto em Standard release.**
Caixa compartilhada chegando a 50 GB	**Exchange Online Plan 2 na caixa.**

Copilot não aparece na reunião do conselho	**Criptografia de ponta a ponta não tem Copilot.**
Sites do RH em revisão antes de ampliar o Copilot	**Restricted Content Discovery: muda a descoberta, não as permissões.**
Milhares de sites encerrados que o jurídico não deixa excluir	**Microsoft 365 Archive.**

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

- Domínios onmicrosoft.com não são excluídos nem renomeados: crie outro e defina como fallback.
- Só o proprietário do time cria canal compartilhado e convidados não entram em canais compartilhados (externos usam B2B direct connect).
- Copilot Studio: quem só conversa com agentes publicados não precisa de licença; licença por usuário é só para quem cria.

Essenciais para a prova (checklist)

☐ Sei conectar domínio com SPF existente, priorizar MX e explicar Domain Connect, subdomínios e domínio padrão.

☐ Sei os limites de temas, logotipo, cor de destaque e rodapé do Copilot Chat.

☐ Sei quem ativa o tempo limite de sessão ociosa, onde ele vale e quando usar Use app enforced restrictions.

☐ Sei atribuir e trocar licenças por grupo e achar os erros em Errors & issues.

☐ Sei configurar, cobrar e restaurar no Microsoft 365 Backup, com as funções certas e os tipos de caixa suportados.

☐ Sei cadastrar locais de rede por sub-rede LAN ou Windows Location Services e rodar o teste manual.

☐ Sei diferenciar advisory, incident, Plan for change e configurar notificações do Service health.

☐ Sei usar Deferred release, Standard release, Frontier e o cronograma de aposentadoria do Targeted release.

☐ Sei os valores da política de Copilot nas reuniões do Teams e seus efeitos.

☐ Sei aplicar Restricted Content Discovery, ocultar site da pesquisa, usar relatórios de governança e o Microsoft 365 Archive.

Questões de revisão do capítulo

R1.1 · Configurar e gerenciar locatários e cargas de trabalho do Microsoft 365

A coordenadora de suporte da Universidade Comunitária Saber quer que dois analistas atribuam licenças do Microsoft 365 a grupos no admin center, seguindo o menor privilégio. Qual função mínima a documentação aceita para essa tarefa?

A. Global Administrator
B. License Administrator
C. Exchange Administrator
D. Reports Reader

R1.2 · Configurar e gerenciar locatários e cargas de trabalho do Microsoft 365

Na Exportadora Café do Vale, um funcionário apagou pastas importantes do OneDrive há três dias, mas criou documentos novos e saudáveis desde então. A conta está no Microsoft 365 Backup. O administrador quer recuperar o conteúdo antigo sem sobrescrever o que foi criado depois. Que destino ele deve escolher na restauração completa da conta?

A. Replace accounts with backups com express restore point
B. Create new SharePoint sites and restore to them
C. Replace accounts with backups e depois Restore
D. Restore to the original location com versões

R1.3 · Configurar e gerenciar locatários e cargas de trabalho do Microsoft 365

Na Indústria Ferreira, o administrador do Teams não alterou a configuração Copilot nas políticas de reunião. Um organizador tenta mudar o Copilot da reunião para Only during the meeting nas opções da reunião, mas a opção não está disponível. O que explica esse comportamento?

A. O valor padrão On deixa a decisão com o primeiro participante que entrar na reunião
B. O valor padrão Off bloqueia o Copilot até que um participante licenciado ative a transcrição
C. O valor padrão On with saved transcript required obriga o modo During and after the meeting
D. O valor padrão On with transcript saved by default exige licença do Teams Premium

R1.4 · Configurar e gerenciar locatários e cargas de trabalho do Microsoft 365

Depois de uma auditoria, a Indústria de Plásticos Brilho quer que vários responsáveis sejam avisados por e-mail se alguém pausar uma política do Microsoft 365 Backup ou remover sites da proteção, para que essas ações não passem despercebidas. O que o administrador deve configurar?

A. As notificações por e-mail do Backup, com a Backup Notification List
B. Uma regra de transporte que copie os e-mails do administrador do Backup
C. Uma política de alerta do Defender para exclusão de arquivos em massa
D. As notificações do Service health para o serviço SharePoint Online

Respostas comentadas

R1.1. B) License Administrator

Por quê: Para atribuir ou remover licenças de grupos no Microsoft 365 admin center, é preciso ser pelo menos Groups Administrator, License Administrator ou User Administrator. Também é possível usar o Set-MgGroupLicense do Microsoft Graph PowerShell, e o admin center atribui licenças a até 20 grupos por vez.

✗ A) Incorreta. Atende, mas é privilegiada demais para a tarefa.
✗ C) Incorreta. Essa função gerencia o Exchange Online, não a atribuição de licenças.
✗ D) Incorreta. Essa função só lê relatórios de uso.

> **Dica de prova:** Licença por grupo com menor privilégio: License Administrator.

R1.2. B) Create new SharePoint sites and restore to them

Por quê: Na restauração completa de OneDrive ou SharePoint, Replace accounts with backups (ou Replace sites with backups) reverte tudo ao ponto escolhido. Create new SharePoint sites and restore to them restaura em um novo URL, com R e um número no final, permitindo recuperar sem sobrescrever dados atuais.

✗ A) Incorreta. O ponto expresso acelera a restauração, mas a substituição ainda sobrescreve os dados atuais.
✗ C) Incorreta. Substituir a conta reverte todo o OneDrive ao ponto escolhido e sobrescreve o conteúdo criado depois.
✗ D) Incorreta. Esse é um destino da restauração granular de arquivos, e no local original os itens são restaurados no lugar.

> **Dica de prova:** Recuperar sem sobrescrever: restaurar em novo URL.

R1.3. C) O valor padrão On with saved transcript required obriga o modo During and after the meeting

Por quê: A configuração Copilot fica em Meetings > Meeting policies > Recording & transcription. O padrão é On with saved transcript required: o organizador recebe During and after the meeting e não pode mudar. Com On, Only during the meeting é o padrão e pode ser alterado.

✗ A) Incorreta. Com On, o padrão é Only during the meeting e o organizador pode mudar, o contrário do caso descrito.
✗ B) Incorreta. Off não é o valor padrão; além disso, com Off o organizador ainda pode alterar a opção.
✗ D) Incorreta. Esse valor permite que o organizador mude a opção e não é o padrão da política.

> **Dica de prova:** Política sem ajuste: Copilot com transcrição salva e organizador sem escolha.

R1.4. A) As notificações por e-mail do Backup, com a Backup Notification List

Por quê: Com as notificações por e-mail do Microsoft 365 Backup, a Backup Notification List (até 20 pessoas, mais listas de distribuição e grupos de segurança com e-mail) recebe resumos diários de eventos potencialmente nocivos, como desabilitar o backup, pausar uma política, remover unidades de proteção ou excluir backups. Eventos rotineiros são opcionais.

✗ B) Incorreta. Uma regra de transporte não gera avisos sobre eventos do Backup.
✗ C) Incorreta. Essa política trata de atividades de usuários, não de mudanças nas políticas de backup.
✗ D) Incorreta. O Service health avisa sobre incidentes da Microsoft, não sobre ações no Backup.

> **Dica de prova:** Avisar sobre pausas e remoções no Backup: Backup Notification List.

02

CAPÍTULO 2 · 35-40% DA PROVA

Gerenciar e proteger serviços de IA no Microsoft 365

Este domínio (35-40%) cobra o administrador do Copilot e dos agentes: onde fica cada configuração no Microsoft 365 admin center, como o Copilot Cowork é cobrado e liberado, como governar o registro de agentes e como o Microsoft Entra Agent ID protege as identidades de agente. A prova adora o caminho exato (Copilot > Settings > Copilot actions, Agents > Settings > Sharing) e a diferença entre controles parecidos: Sharing, User access, Agent and plugin access e Agent feedback sharing. Também caem muito os modelos da Anthropic, a pesquisa na web com o Bing e os conectores do Copilot. Meus erros vêm de achar que um controle cobre mais do que cobre: Sharing só vale para o Agent Builder, a descoberta do Cowork não dá acesso e a precedência das políticas de gastos não decide quem usa.

Neste capítulo

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

Tópicos-chave

Relatório de prontidão do Copilot

Fica em Reports > Usage e pode levar até 72 horas para aparecer, com dados de até 72 horas de atraso. A coluna Suggested candidate for Copilot marca, toda semana, os 25% de usuários sem licença com uso mais intenso de apps nos 28 dias anteriores. O indicador de canal considera Current Channel ou Monthly Enterprise Channel, e ver as recomendações de licenciamento exige permissão para gerenciar licenças.

Pesquisa na web no Copilot

Controlada pela política Allow web search in Copilot no Cloud Policy, que vale para Microsoft 365 Copilot e Copilot Chat. Desabilitar a web só no modo Work também a desliga no Researcher e no Cowork. Sem essa política configurada, desabilitar as experiências conectadas opcionais desliga a web; no comercial ela fica disponível por padrão e o usuário pode desligá-la para si em Personalization > Advanced.

Consultas enviadas ao Bing

A consulta gerada tem poucas palavras e não inclui nome de usuário, domínio nem ID do locatário. A DPA, o EU Data Boundary e a HIPAA não se aplicam a essas consultas, que não treinam modelos de base. As citações das consultas aparecem só no Copilot Chat e ficam na conversa por 24 horas.

Configurações do Copilot no admin center

Copilot actions traz Copilot image generation e Screen and camera sharing (desligar não desliga a voz). User access traz Microsoft Copilot in admin centers (Admin agent) e Pin Microsoft Copilot Chat, cuja mudança pode levar até 48 horas. Other settings traz Copilot diagnostics logs; também existem Copilot Frontier (prévia para um grupo), Copilot Release preferences e Microsoft Copilot self-service purchases (permitir só trials).

Aviso de IA (Copilot AI disclaimer)

Ativá-lo cria a política de locatário Copilot AI Disclaimer no Microsoft 365 Apps admin center. Aparece nos apps do Office (como Excel e OneNote) e no app Copilot, não no SharePoint, OneDrive, Whiteboard ou Forms. Não cria regra de transporte, DLP nem Acesso Condicional.

Copilot Search

Não exige configuração inicial; quem não tem licença recebe a experiência do Microsoft Search. O conteúdo indexado por conectores entra automaticamente. Acrônimos podem ser importados por CSV com Acronym, Stands For e State, e os que estão em Draft não aparecem; marcadores com data e hora futura ficam no estado Scheduled.

Conectores do Copilot

Conector federado busca dados em tempo real por MCP, não indexa no Microsoft Graph e é somente leitura. Conector sincronizado indexa no Graph; o personalizado com configuração de locatário serve fonte sem conector pronto para toda a organização, e o de autoatendimento indexa por usuário e remove o conteúdo quando ele desconecta. Todos respeitam as permissões da origem.

Modelos da Anthropic e provedores de IA

A Anthropic atua como subprocessador da Microsoft e é ligada ou desligada em AI providers operating as Microsoft subprocessors. Na UE, EFTA e Reino Unido o padrão é No users, os modelos ficam fora do EU Data Boundary e não existem no GCC High. Os modelos Anthropic models with Data Retention ficam desligados por padrão e exigem opt-in separado, com a Anthropic como processador independente; a atribuição de acesso é por provedor, aceita grupos aninhados e até 999 atribuições.

Copilot Cowork e Cost Management

Com cobrança baseada em uso, estar em uma política de gastos que seleciona o Cowork já concede acesso; a configuração de descoberta controla só a visibilidade e as configurações de modelo só o seletor. Com várias políticas para o mesmo serviço vence o maior limite por usuário, depois o maior limite total da política e, por fim, a mais recente; a escolhida vale por inteiro. Com orçamento limitado esgotado, o acesso volta no dia 1º, e créditos pré-pagos são usados antes do pay-as-you-go.

Perfis de modelo e funções da cobrança

Perfis de modelo valem hoje só para o Cowork e exigem pelo menos dois modelos, de um ou mais provedores; modelos de provedores desabilitados não aparecem. Global Administrator e Billing Administrator definem métodos de cobrança; AI Administrator edita limites e alertas, mas não cria políticas de gastos; funções de leitura só veem consumo, na aba Consumption do Cost Management.

Registro de agentes

Um agente do Copilot Studio pode aparecer duas vezes (Shared by creator e Published by your org) por design. Upload de agente usa Add agent: Publish define quem pode instalar e Deploy quem já recebe instalado. Atualizações ficam em Pending update até o administrador selecionar Update in store, e agentes excluídos podem ser restaurados em All agents > Deleted em até 30 dias.

Configurações de agentes

Sharing vale só para agentes do Agent Builder (No users ainda permite compartilhar com pessoas específicas). User access define quem usa agentes; Agent and plugin access define as categorias permitidas (Microsoft, organização, editores externos); Agent feedback sharing com Selected agents envia avaliações aos desenvolvedores; Tags só organizam. Aprovar solicitações e atribuir proprietário exige AI Administrator ou Global Administrator.

Fixação, bloqueio e ferramentas

O administrador fixa no máximo três agentes, apenas implantados e desbloqueados, com até seis horas para aparecer. Bloquear um agente do SharePoint ou Foundry afeta só o Copilot Chat. Plug-ins têm disponibilidade por usuário em Agents > Tools > Plugins e pedidos em Tools > Requests; conectores do Power Platform usados por agentes são bloqueados no Power Platform admin center, e servidores MCP próprios são registrados pela CLI do Agent 365 e aprovados no admin center.

Microsoft Entra Agent ID: patrocinador, proprietário e manager

Toda identidade de agente exige pelo menos um patrocinador, que decide o ciclo de vida e pode desabilitar, mas não reabilitar; como grupo, aceita grupo dinâmico ou grupo do Microsoft 365 com associação atribuída, nunca grupo atribuível a funções nem grupo de segurança com associação atribuída. Proprietários são opcionais (usuários, inclusive convidados, e entidades de serviço, nunca grupos) e fazem as mudanças técnicas. O manager só pede pacotes de acesso, sem alterar nem excluir.

Blueprints e Acesso Condicional para agentes

Blueprints de identidade de agente servem de modelo com relação pai e filho; selecionar o blueprint na política cobre os agentes atuais e futuros no acesso só de aplicativo. Contas de usuário de agente só são cobertas por políticas direcionadas a Agent Users, sem inclusão por grupo. No fluxo delegado, o usuário é o sujeito do token e a política deve mirar o usuário.

Governança de identidades para agentes

Pacotes de acesso para agentes usam a política For users, service principals, and agent identities com escopo All agents e aceitam grupos, funções do Entra e permissões de API com prazo, mas não funções de site do SharePoint. Perto do vencimento, o patrocinador é notificado e pode pedir extensão; Lifecycle Workflows de mudança transferem patrocínios. Exige E7, ou Agent 365 com Entra ID P1 ou Microsoft 365 E3.

Risky agents no ID Protection

Confirm compromise eleva o risco para alto e aciona políticas que bloqueiam agentes de alto risco; Confirm safe zera o risco; Disable impede todas as entradas do agente; Dismiss descarta o risco atual. Security Reader vê o relatório e Conditional Access Administrator cria a política baseada em risco.

Agent 365: dados e Defender

Instância de agente nova é auditada, tem dados sensíveis classificados e entra nas avaliações de IA do Compliance Manager; para DLP e retenção precisa ser incluída como usuário ou por grupo, e conteúdo novo não herda rótulo. Arquivo criptografado exige VIEW e EXTRACT explícitos para a instância. No Defender, a regra Default da proteção em tempo real audita; regras personalizadas bloqueiam no escopo; a coleta de evidências de prompt vem ligada, só com trechos e redação de segredos; Advanced Hunting usa AgentsInfo e CloudAppEvents.

Macetes para memorizar

Cowork

Descoberta = vitrine, modelo = cardápio, política de gastos = catraca. Só a catraca dá acesso.

Pessoas do Agent ID

Patrocinador decide (obrigatório), Proprietário mexe (opcional), Manager pede (só pacote de acesso).

Conectores

Federado = ao vivo e só leitura. Sincronizado = copia para o índice.

Risky agents

Compromise sobe para alto, Safe zera, Disable tranca a porta, Dismiss descarta.

Fixar agentes

Regra do 3-6: no máximo três agentes, até seis horas para aparecer, só implantados e desbloqueados.

Pilares do Copilot Control System

SGM: Segurança e governança, Gerenciamento (controles), Medição e relatórios.

Prontidão do Copilot

72 horas para aparecer, 25% sugeridos por semana, 28 dias de uso, Current ou Monthly Enterprise.

Anthropic

Europa começa desligada e fora do EU Data Boundary; With Data Retention sempre pede opt-in separado.

Tabela de memorização: não confunda

Quando é...	...e quando é
Conector federado Dado ao vivo que não pode ser copiado para o índice; leitura em tempo real por MCP, sem gravação.	**Conector sincronizado** Conteúdo precisa ser indexado no Microsoft Graph para Copilot e Microsoft Search, inclusive fonte sem conector pronto (personalizado).
Sharing (Agents > Settings) Limitar o compartilhamento de agentes criados no Agent Builder.	**User access** Definir quais usuários ou grupos podem usar agentes e plug-ins, como um piloto.
Publish Definir quem pode instalar o agente enviado.	**Deploy** Pré-instalar o agente para o grupo; só agentes implantados podem ser fixados.
Patrocinador do agente Responsável obrigatório pelo ciclo de vida: pede extensões, desabilita, recebe avisos de vencimento.	**Proprietário do agente** Opcional; faz mudanças técnicas como credenciais e propriedades de autenticação e pode reabilitar.
Confirm compromise Elevar o risco do agente para alto e deixar o Acesso Condicional baseado em risco agir.	**Disable** Impedir todas as entradas do agente no Entra ID e nos apps conectados.
Copilot Analytics (Copilot Dashboard) Medir adoção por aplicativo, impacto nos hábitos de trabalho e retorno; o AI Administrator habilita e delega o acesso.	**DSPM para IA** Avaliar riscos de segurança de dados e interações com IA.

Pay-as-you-go do Copilot Chat
Agentes medidos no Copilot Chat para usuários sem licença: criar a política de cobrança e conectá-la ao serviço no admin center.

Política de gastos do Cost Management
Liberar e limitar experiências como o Copilot Cowork com Copilot Credits.

Números que caem

Item	Valor
Relatório de prontidão do Copilot	**até 72 horas para aparecer e até 72 horas de atraso nos dados**
Suggested candidate for Copilot	**25% dos usuários sem licença, reavaliado toda semana, com base nos 28 dias anteriores**
Mudança em Pin Microsoft Copilot Chat	**até 48 horas**
Citações das consultas ao Bing	**só no Copilot Chat, por 24 horas**
Agentes fixados pelo administrador	**máximo de 3; até 6 horas para aparecer**
Restaurar agente excluído no admin center	**até 30 dias, em All agents > Deleted**
Atribuições de acesso por provedor de IA	**até 999 (usuários e grupos combinados)**
Perfil de modelo do Cowork	**mínimo de 2 modelos**
Métricas de agentes de terceiros no Agent overview	**começam na ativação das licenças do Agent 365; janela chega a 30 dias**
Restricted SharePoint Search (aposentando)	**limitado a 100 sites**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Achar que Sharing = No users bloqueia também agentes do Copilot Studio.
Como não cair: Sharing só se aplica ao Agent Builder e ainda permite compartilhar com pessoas específicas.

⚠ **Alerta de prova:** Desmarcar a descoberta do Cowork ou bloquear a entrada do agente Cowork esperando tirar o acesso.
Como não cair: Descoberta é só visibilidade e a entrada do agente não controla mais o acesso; quem está numa política de gastos que seleciona o Cowork tem acesso.

⚠ **Alerta de prova:** Diminuir o limite de uma política de gastos para que ela vença a outra e restrinja o piloto.
Como não cair: A precedência só escolhe o limite de quem está em várias políticas (vence o maior por usuário); ela não decide quem tem acesso.

⚠ **Alerta de prova:** Supor que a entrada duplicada de um agente do Copilot Studio no registro é corrupção.
Como não cair: Shared by creator e Published by your org são registros separados do mesmo agente, por design.

⚠ **Alerta de prova:** Inverter Publish e Deploy ao enviar um agente .zip.
Como não cair: Publish = quem pode instalar; Deploy = quem já recebe instalado.

⚠ **Alerta de prova:** Desligar Screen and camera sharing achando que a voz também some.
Como não cair: A documentação informa que desligar essa configuração não desliga a voz.

⚠ **Alerta de prova:** Pensar que conector federado grava dados se o administrador configurar ou o usuário tiver licença.
Como não cair: Conector federado é somente leitura, sempre.

⚠ **Alerta de prova:** Colocar contas de usuário de agente num grupo de segurança incluído nas políticas de Acesso Condicional atuais.
Como não cair: Inclusão por grupo não é suportada; crie política direcionada a Agent Users.

⚠ **Alerta de prova:** Selecionar a identidade do agente quando ele age em nome do usuário logado.
Como não cair: No fluxo delegado o usuário é o sujeito do token; a política deve mirar o usuário.

⚠ **Alerta de prova:** Definir um grupo de segurança com associação atribuída ou um grupo atribuível a funções como patrocinador, ou um grupo como proprietário.
Como não cair: Patrocinador aceita grupo dinâmico (de segurança ou do Microsoft 365) ou grupo do Microsoft 365 com associação atribuída; proprietário só usuário (inclusive convidado) ou entidade de serviço.

⚠ **Alerta de prova:** Reaproveitar pacote de acesso com função de membro de site do SharePoint para agentes.
Como não cair: Identidades de agente não recebem funções de site do SharePoint por pacotes de acesso.

⚠ **Alerta de prova:** Desativar o EU Data Boundary ou mover o locatário para liberar os modelos da Anthropic na Europa.
Como não cair: O próprio administrador faz o opt-in em AI providers operating as Microsoft subprocessors.

⚠ **Alerta de prova:** Esperar que Apply template rode toda semana sobre agentes novos.
Como não cair: Apply template é uma operação única em massa, não uma regra agendada.

⚠ **Alerta de prova:** Desligar a regra Default da proteção em tempo real achando que ela bloqueia tudo.
Como não cair: A regra Default audita; desligá-la tira a visibilidade. Bloqueio vem de regras personalizadas com escopo.

Como cai na prova

📝 **Como cai:** Administrador mudou uma configuração e o efeito não foi o esperado.
Como resolver: Pergunte o que aquele controle realmente cobre (Agent Builder x Copilot Studio, visibilidade x acesso, limite x acesso) e quanto tempo leva (48 horas para fixação do Copilot Chat, 72 horas para o relatório).

📝 **Como cai:** Onde configurar: quatro caminhos de menu parecidos.
Como resolver: Mapeie o tema para a seção: Copilot actions (imagem, tela e câmera), User access (admin centers, fixação), Data access (provedores de IA), Other settings (diagnóstico, dicionário), Agents > Settings (Sharing, User access, Agent and plugin access, feedback).

📝 **Como cai:** Escolha DUAS sobre patrocinadores, proprietários, Risky agents ou Bing.
Como resolver: Verifique quem é obrigatório, quem pode ser grupo e o efeito exato de cada ação; descarte afirmações que excluem, apagam histórico ou tornam algo automático.

📝 **Como cai:** Política de Acesso Condicional não cobre certos agentes.
Como resolver: Identifique o padrão: identidade de agente (blueprint ou identidade), conta de usuário de agente (Agent Users) ou acesso delegado (usuário).

📝 **Como cai:** Usuário em várias políticas de gastos ou orçamento esgotado.
Como resolver: Vale uma política inteira: a de maior limite por usuário, depois a de maior limite total e, por fim, a mais recente; orçamento limitado esgotado suspende até o dia 1º e o pré-pago é consumido antes do pay-as-you-go.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Impedir geração de imagens com o Copilot	**Copilot > Settings > Copilot actions > Copilot image generation.**
Grupo testando recursos antes da disponibilidade geral	**Copilot Frontier.**
Funcionários experimentam o Copilot sem comprar por conta própria	**Microsoft Copilot self-service purchases permitindo apenas trials.**
Recursos do Copilot não aparecem para um usuário licenciado	**Copilot Service Plan Diagnostic em Support > Help and support.**
Usuários não podem enviar feedback e a Microsoft precisa investigar	**Copilot diagnostics logs em Other settings.**
Visão gráfica dos agentes por plataforma, com filtro de sem proprietário	**Agent Map em Agents > All agents > Map (GA ou AI Administrator).**
Agentes do Agent Builder sem dono para os gestores	**Regra Reassign ownerless agents created with Agent Builder to manager.**
Pedido de agente da Microsoft bloqueado	**Requests com Allow user to install; desbloquear e aprovar.**
Listar agentes do registro por Graph PowerShell	**CopilotPackages.Read.All e copilot/admin/catalog/packages.**
Agente novo acessando dados do Microsoft 365 por MCP	**Work IQ MCP (servidores por carga são legados).**
Políticas iguais para dezenas de agentes, inclusive futuros	**Blueprint de identidade de agente.**
Custo da tarefa do Cowork durante a execução	**Comando /cost; consumo no Cost Management.**
Pedidos de créditos pelo fluxo do ServiceNow	**Política de solicitação em Credit requests; aparece como Handled externally.**
Auditar interações com o Copilot com menor privilégio	**Audit Reader filtrando as cargas AIApp e Copilot.**

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

- Global Reader vê as configurações e o Agent overview, mas aprovar solicitações e atribuir proprietários exige AI Administrator ou Global Administrator.
- Restricted SharePoint Search está sendo aposentado e a nova ativação está bloqueada; a orientação é o Restricted Content Discovery.
- Tarefas automatizadas do Cowork rodam com as permissões do usuário, pedem aprovação antes de enviar e-mail salvo autorização prévia, têm proteção contra loop e ficam no log de auditoria unificado.
- Agent ID está disponível para os clientes do Entra; estender os recursos de segurança aos agentes exige o Agent 365.
- Modelo de política personalizado de agente exige política de Acesso Condicional criada antes no Entra com pelo menos uma identidade de agente e a função Attribute Assignment Administrator além do AI Administrator.

Essenciais para a prova (checklist)

☐ Sei ler o relatório de prontidão (72 horas, candidatos sugeridos, canais elegíveis, Total Prerequisite Licenses) e calcular o Active users rate.

☐ Sei controlar a pesquisa na web pelo Cloud Policy e explicar o que vai para o Bing e o que não se aplica.

☐ Sei localizar geração de imagem, Frontier, preferências de versão, self-service purchases, diagnóstico e aviso de IA nas configurações do Copilot.

☐ Sei liberar, desligar e restringir modelos da Anthropic e provedores de IA, inclusive na UE.

☐ Sei como o acesso ao Cowork é concedido, como as políticas de gastos competem e o que acontece quando o orçamento acaba.

☐ Sei diferenciar Sharing, User access, Agent and plugin access, Agent feedback sharing e Tags.

☐ Sei publicar, implantar, fixar, bloquear, atualizar, restaurar e reatribuir agentes no registro.

☐ Sei os papéis de patrocinador, proprietário e manager e quais tipos de grupo cada um aceita.

☐ Sei montar Acesso Condicional para identidades de agente, blueprints, Agent Users e acesso delegado.

☐ Sei o que o Agent 365 faz automaticamente no Purview e o que exige inclusão manual em DLP e retenção.

Questões de revisão do capítulo

R2.1 · Gerenciar e proteger serviços de IA no Microsoft 365

A equipe de desenvolvimento da Rede Óptica Visão entregou ao administrador o arquivo .zip de um agente feito no Copilot Studio. Ele quer que o agente possa ser instalado por toda a área comercial, mas que já apareça instalado apenas para os 15 gerentes. Como fazer isso no upload pelo Microsoft 365 admin center?

A. Enviar o .zip pelo Agent Store, que distribui o agente para quem tiver licença
B. Fixar o agente para os gerentes sem publicá-lo, para que a área possa instalar
C. Usar Add agent, pôr os gerentes em Publish e o grupo comercial em Deploy
D. Usar Add agent, escolher o grupo comercial em Publish e os gerentes em Deploy

R2.2 · Gerenciar e proteger serviços de IA no Microsoft 365

Um agente de cobrança da Financeira Crédito Fácil recebeu, por um pacote de acesso com prazo de 90 dias, a associação a um grupo que dá acesso a uma API interna. Faltando poucos dias para o vencimento, o agente ainda é necessário. O que acontece e quem age?

A. O agente perde a identidade no Entra e precisa ser criado de novo pelo proprietário
B. O patrocinador do agente é notificado e pode pedir uma extensão, se a política permitir
C. O Global Administrator recebe um chamado automático para recriar o pacote do zero
D. O pacote é renovado sozinho por mais 90 dias, porque o agente teve atividade recente na API

R2.3 · Gerenciar e proteger serviços de IA no Microsoft 365

O administrador de busca da Cooperativa de Saúde Bem Viver tem uma planilha com 300 acrônimos internos e quer carregá-los de uma vez no Copilot Search, deixando alguns em revisão. Como deve proceder?

A. Criar um conector federado que leia a planilha e publique os acrônimos em tempo real
B. Enviar a planilha ao suporte da Microsoft para que os acrônimos sejam publicados pelo backend
C. Importar um CSV com Acronym, Stands For e State, usando Draft para os que ficam em revisão
D. Cadastrar os acrônimos como marcadores, já que acrônimos não aceitam importação em massa

R2.4 · Gerenciar e proteger serviços de IA no Microsoft 365

A Rede de Livrarias Página Certa liberou plug-ins de editores externos na organização, mas quer que o plug-in de uma plataforma de pagamentos fique disponível só para o time financeiro. Funcionários de outras áreas que encontrarem o plug-in devem poder pedir acesso. Como configurar isso?

A. Em Billing > Licenses, atribuir uma licença do plug-in só ao grupo financeiro e bloquear os demais no Entra
B. Em Agents > Settings > Sharing, escolher Specific users com o grupo financeiro e aprovar os pedidos no Agent Map
C. Em Copilot > Settings > Data access, desabilitar o provedor do plug-in e liberar o grupo financeiro por exceção
D. Em Agents > Tools > Plugins, abrir Users do plug-in, escolher o grupo financeiro e revisar os pedidos em Agents > Tools > Requests

Respostas comentadas

R2.1. D) Usar Add agent, escolher o grupo comercial em Publish e os gerentes em Deploy

Por quê: Em Agents > All agents > Add agent, o administrador envia o .zip (validado), confere nome e produtos, define em Publish quem pode instalar e, opcionalmente, em Deploy quem recebe o agente pré-instalado; depois escolhe o modelo de política, revisa permissões e conclui com Finish deployment.

✗ A) Incorreta. O upload de agentes personalizados para gerenciamento é feito no registro do admin center.
✗ B) Incorreta. Só agentes implantados podem ser fixados, e fixar não define quem pode instalar.
✗ C) Incorreta. A ordem está invertida: Deploy pré-instala para o grupo inteiro e Publish limitaria a instalação aos gerentes.

> **Dica de prova:** Upload de agente: Publish = quem pode instalar; Deploy = quem já recebe instalado.

R2.2. B) O patrocinador do agente é notificado e pode pedir uma extensão, se a política permitir

Por quê: Atribuições de pacotes de acesso a agentes têm início e fim. Se a identidade tem patrocinador, ele é avisado perto do vencimento e pode pedir extensão (se a política permitir), o que pode iniciar nova aprovação, ou deixar expirar; sem ação, a atribuição vence e o agente perde o acesso aos recursos.

✗ A) Incorreta. A expiração remove o acesso aos recursos, não a identidade do agente.
✗ C) Incorreta. O fluxo previsto é a notificação ao patrocinador, que pode pedir extensão.
✗ D) Incorreta. Não há renovação automática por atividade; sem ação, a atribuição expira.

> **Dica de prova:** Pacote de acesso do agente vencendo: o patrocinador pede extensão.

R2.3. C) Importar um CSV com Acronym, Stands For e State, usando Draft para os que ficam em revisão

Por quê: Em Copilot > Search > Acronyms, os acrônimos podem ser adicionados um a um ou importados por CSV. Os campos obrigatórios são Acronym, Stands For e State (Published, Draft ou Excluded); incluir o ID de um acrônimo existente faz a importação substituí-lo.

✗ A) Incorreta. Acrônimos são curados no Copilot Search, não por conector.

✗ B) Incorreta. O próprio administrador importa os acrônimos no admin center.

✗ D) Incorreta. Acrônimos podem ser importados em massa por CSV.

> **Dica de prova:** Acrônimos em massa: CSV com Acronym, Stands For e State.

R2.4. D) Em Agents > Tools > Plugins, abrir Users do plug-in, escolher o grupo financeiro e revisar os pedidos em Agents > Tools > Requests

Por quê: Em Agents > Tools > Plugins, o administrador escolhe All users, No users ou Specific users and groups para cada plug-in. Quem estiver fora da disponibilidade vê o plug-in como bloqueado pela política e pode selecionar Request access; os pedidos são aprovados ou rejeitados em Agents > Tools > Requests.

✗ A) Incorreta. A disponibilidade do plug-in é definida nas configurações de ferramentas, não por licença.

✗ B) Incorreta. Sharing trata do compartilhamento de agentes do Agent Builder, e pedidos não são aprovados no Agent Map.

✗ C) Incorreta. As configurações de provedores de IA não controlam a disponibilidade de plug-ins por usuário.

> **Dica de prova:** Plug-in só para um time: disponibilidade por usuário e pedidos em Tools > Requests.

03

CAPÍTULO 3 · 40-45% DA PROVA

Governar e proteger locatários e cargas de trabalho do Microsoft 365

Este é o maior domínio da prova (40-45%) e mistura três mundos: identidade no Microsoft Entra, proteção de e-mail e colaboração no Defender for Office 365 e proteção de dados no Microsoft Purview. Preciso saber qual função atende com menor privilégio, qual licença cada recurso exige (Free, P1, P2, Plan 1, Plan 2, E5) e qual recurso resolve exatamente o cenário descrito. O enunciado quase sempre traz um detalhe que elimina três alternativas: associação dinâmica, convite já resgatado, usuário sem senha, método exigido no SSPR, anexo detectado pelo Safe Attachments. Onde mais erro é em regras finas: precedência de retenção, comportamento padrão das listas de convite, o que o bloqueio inteligente conta e o que cada força de autenticação aceita. Também caem muito as integrações com o Copilot: DLP no local do Copilot, herança de rótulo e direitos VIEW e EXTRACT.

Neste capítulo

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

Tópicos-chave

Unidade administrativa e licenças

Criar unidades administrativas é possível no Microsoft Entra ID Free, mas cada administrador com função no escopo da unidade precisa de P1. Membros de unidade com associação atribuída ficam no Free; se a unidade usar regras de associação dinâmica, cada membro também precisa de P1. Funções com escopo de unidade não exigem P2 nem PIM.

Unidade administrativa de gerenciamento restrito

Protege objetos sensíveis (como contas de executivos) contra administradores com escopo no locatário inteiro, inclusive o Global Administrator, que só altera esses objetos se receber uma função no escopo da unidade, ação registrada na auditoria. Aceita usuários, grupos de segurança e dispositivos, mas não aceita grupos do Microsoft 365. Uma unidade comum não impede administradores do locatário inteiro.

Funções de menor privilégio no Entra

Helpdesk Administrator redefine senha de usuários não administradores; User Administrator cria e gerencia usuários e grupos e é o mínimo para o Bulk create; Privileged Role Administrator (ou Global Administrator) gerencia atribuições de outros administradores no PIM. External Identity Provider Administrator configura a colaboração externa sem Global Administrator, e Global Reader só lê, inclusive as configurações do Copilot.

Contato de e-mail x usuário de e-mail x convidado

Contato de e-mail representa pessoa externa no catálogo de endereços, pode estar em lista de distribuição e não tem credenciais; cria-se no EAC em Recipients > Contacts. Usuário de e-mail entra no locatário, mas recebe e-mail no endereço externo. Convidado B2B tem conta no Entra ID, pode receber Acesso Condicional e MFA e participa de times e canais.

Bloqueio inteligente

Funciona por padrão e não depende da Proteção de Senha. Guarda os três últimos hashes de senha errada e não conta repetições da mesma senha errada. O limite padrão é de 10 tentativas com falha nos locatários públicos, e o código AADSTS50053 indica conta bloqueada por ele.

Proteção de Senha do Microsoft Entra

A lista personalizada de senhas banidas impede termos como nome da marca e produtos, mas só é verificada quando o usuário troca ou redefine a senha; senhas atuais não são bloqueadas. No AD local exige o serviço proxy e os agentes nos controladores de domínio, e a implantação recomendada começa no modo Audit e depois passa a Enforced.

SSPR

Exige um ou dois métodos; quando a política exige um método, o Authenticator não pode ser o único disponível. Contas com funções administrativas seguem a política de duas etapas fixa, que exige dois métodos e proíbe perguntas de segurança. Perguntas de segurança servem só para redefinir senha, nunca como fator de entrada; senha redefinida na nuvem só chega ao AD local com o write-back (Entra Connect Sync ou Cloud Sync).

Política de métodos de autenticação

Desde 30 de setembro de 2025 os métodos não podem mais ser gerenciados nas políticas legadas de MFA e SSPR; o caminho é Entra ID > Authentication methods > Policies, com o controle de migração manual. Ali se habilitam Temporary Access Pass, chaves de acesso (com perfis de chave por grupo, vinculadas ao dispositivo ou sincronizadas) e campanha de registro (adiamento de 0 a 14 dias).

Temporary Access Pass

Código temporário para o primeiro acesso sem senha, por exemplo para registrar uma chave de acesso. O tempo de vida é configurável de 10 minutos a 30 dias (43.200 minutos), com padrão de 1 hora e máximo padrão de 8 horas; com One-time use desligado (o padrão), o código pode ser usado mais de uma vez. Só usuários incluídos na política entram com ele, e configurar a política exige Authentication Policy Administrator.

Forças de autenticação

Multifactor authentication strength aceita MFA comum; Phishing-resistant MFA strength aceita só métodos resistentes a phishing. As forças internas não podem ser modificadas por ninguém (a Microsoft as atualiza); para combinações sob medida cria-se uma força personalizada. Habilitar a chave de acesso na política de métodos não obriga seu uso: é preciso exigir uma força no Acesso Condicional.

Acesso Condicional baseado em risco (ID Protection)

Exige Microsoft Entra ID P2. Sign-in risk avalia cada entrada; User risk avalia o usuário. Require risk remediation e Require password change deixam o usuário se autorremediar; Block access depende do administrador. Para usuário sem senha, a remediação revoga as sessões e pede nova entrada, sem troca de senha.

Report-only, What If e logs de entrada

Report-only mede o impacto real de uma política sem afetar ninguém, e o resultado aparece nos logs de entrada do Entra. What If simula uma entrada específica (usuário, país, app) para descobrir quais políticas se aplicam. Aplicativo com identidade própria aparece em Service principal sign-ins, e a experiência legada de logs mostra só entradas interativas de usuário.

Configurações de colaboração externa

Por padrão, qualquer usuário, inclusive convidados, pode convidar externos. Guest user access restrito aos próprios objetos impede ver outros usuários e grupos; o padrão é acesso limitado. Só existe uma política de domínios, com lista de permissão ou de bloqueio, e trocar o tipo descarta a lista anterior; a lista atinge convites novos e pendentes, não quem já resgatou.

B2B direct connect e confiança de MFA

Por padrão, a colaboração B2B com outras organizações do Entra é permitida e o B2B direct connect é bloqueado; ele precisa ser liberado nas duas organizações e não cria conta de convidado. Para evitar MFA duplicada de parceiros, configura-se nas configurações de entrada a confiança nas declarações de MFA do locatário deles. External user leave settings só fica disponível com as informações de privacidade da organização preenchidas.

PIM: elegível x ativo

Atribuição elegível exige ativar a função antes de usar; ativa já está valendo. Atribuições podem ter início e fim, aprovação, justificativa e contexto de autenticação do Acesso Condicional na ativação; Activation maximum duration vai de 1 a 24 horas. O PIM oferece revisões de acesso e histórico de auditoria e impede remover a última atribuição ativa de Global Administrator e Privileged Role Administrator.

Defender for Office 365: políticas e precedência

Sem políticas personalizadas, a Built-in protection aplica Safe Links e Safe Attachments básicos, inclusive Safe Links no Teams e nos apps do Office. Quem está em várias políticas recebe Strict, que vence Standard, que vence personalizada; não há soma. A política antiphishing padrão traz proteção contra falsificação e inteligência de caixa de correio, mas a proteção contra representação de usuários exige cadastrar os remetentes protegidos.

Investigação e resposta no Defender

Plan 1 oferece Real-time detections; Plan 2 traz o Threat Explorer, investigação automatizada (AIR) com ações aprovadas no Action center e Attack simulation training (também no E5). ZAP remove ameaças descobertas depois da entrega. No Threat Explorer é possível selecionar mensagens já entregues e iniciar correção, como exclusão reversível, acompanhada no Action center.

Retenção no Purview

Com várias retenções, vale o período mais longo; para exclusão, o explícito vence o implícito (rótulo vence política) e a política com escopo específico vence a que vale para todos; data de criação nunca decide. Um item tem um único rótulo de retenção, mas várias políticas podem atingi-lo. Canais compartilhados herdam a retenção do time pai, e Preservation Lock impede desligar, excluir ou afrouxar a política.

Macetes para memorizar

💡 Licença de unidade administrativa

Admin com escopo = P1. Membro atribuído = Free. Membro dinâmico = P1. P2 nunca entra nessa conta.

💡 Precedência no Defender

S antes de S antes de P: Strict > Standard > Personalizada. Não soma, escolhe uma.

💡 Retenção

Guardar: ganha o mais longo. Apagar: ganha o explícito (rótulo) e o mais específico. Data de criação nunca decide.

💡 Temporary Access Pass

1 hora de padrão, 30 dias de teto (43.200 minutos), uso único desligado por padrão.

💡 Bloqueio inteligente

Dez erros diferentes derrubam; o mesmo erro repetido não conta (três últimos hashes).

💡 Listas de convite B2B

Lista só olha para frente: barra convites novos e pendentes, não expulsa quem já entrou.

PIM

Elegível = ativar para usar. Ativo = já valendo. Duração de ativação de 1 a 24 horas.

Plan 1 x Plan 2

P1 vê em tempo real (Real-time detections); P2 explora, simula e investiga (Threat Explorer, Attack simulation training, AIR).

Tabela de memorização: não confunda

Quando é...	...e quando é
Contato de e-mail Externo só precisa aparecer no catálogo e receber e-mail da lista de distribuição, sem entrar em nada.	**Usuário de e-mail** Externo precisa entrar no locatário e acessar recursos, mas o e-mail continua indo para o endereço externo dele.
Helpdesk Administrator Redefinir senha de usuários comuns com menor privilégio, sem mexer em administradores.	**User Administrator** Criar e gerenciar usuários e grupos, inclusive criação em massa pelo Bulk create.
Atribuição elegível no PIM Uso eventual ou por projeto, com ativação, aprovação, justificativa, duração máxima e datas de início e fim.	**Atribuição ativa no PIM** Função precisa valer o tempo todo, sem ativação; não atende pedidos de just-in-time.
Sign-in risk Reagir à entrada suspeita naquele momento, por exemplo exigindo MFA em risco médio e alto.	**User risk** Tratar a conta considerada comprometida, com Require risk remediation ou troca segura de senha.
Real-time detections (Plan 1) Investigar e-mails mal-intencionados quase em tempo real com o Plan 1.	**Threat Explorer (Plan 2)** Mais exibições, filtros e ações de correção em massa sobre mensagens já entregues.
Safe Links Link que vira armadilha depois da entrega: verificação no momento do clique, inclusive no Teams e nos apps do Office.	**Safe Attachments com Dynamic Delivery** Anexo precisa ser verificado sem atrasar o e-mail: entrega o corpo com espaços reservados até terminar a análise.
Rótulo de retenção Exclusão explícita no item; vence a política na exclusão e só existe um por item.	**Política de retenção** Retenção aplicada a um local inteiro; várias podem atingir o mesmo item e vale o período mais longo.

Números que caem

Item	Valor
Limite padrão do bloqueio inteligente nos locatários públicos	**10 tentativas com falha**
Hashes de senha errada guardados pelo bloqueio inteligente	**3 últimos**

Restaurar usuário excluído em Deleted users	**até 30 dias**
Adiamento na campanha de registro do Authenticator	**0 a 14 dias**
Temporary Access Pass	**configurável de 10 minutos a 30 dias (43.200 minutos); padrão de 1 hora; máximo padrão de 8 horas**
Métodos exigidos no SSPR	**1 ou 2**
Fim da gestão de métodos nas políticas legadas de MFA e SSPR	**30 de setembro de 2025**
Activation maximum duration no PIM	**1 a 24 horas**
Expiração de grupos: seleção de grupos específicos	**máximo de 500 grupos; tempo de vida mínimo de 30 dias; uma política por organização**
Construtor de regras de grupo dinâmico	**até 5 expressões**
Retenção de spam na quarentena (políticas padrão e personalizadas)	**1 a 30 dias**
Entrada de permissão criada via Submissions	**vale em até 5 minutos**
Bloqueios de arquivos, URLs, domínios e endereços na Lista de Permissões/Bloqueios	**expiram em 30 dias por padrão; podem ir até 90 dias ou nunca expirar, conforme a escolha**
Avaliação padrão do DSPM para IA	**semanal, dos 100 sites mais usados**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Achar que membros de unidades administrativas sempre ficam no Free.
Como não cair: Isso vale só para associação atribuída; com regras de associação dinâmica, cada membro também precisa de P1.

⚠ **Alerta de prova:** Supor que funções com escopo de unidade administrativa exigem P2 porque usariam o PIM.
Como não cair: Escopo de unidade administrativa exige P1 para o administrador, sem P2 nem PIM.

⚠ **Alerta de prova:** Concluir que o bloqueio inteligente está desligado porque a mesma senha errada repetida cinco vezes não bloqueou.
Como não cair: Ele guarda os três últimos hashes de senha errada e não conta a repetição da mesma senha; o limite padrão é 10 tentativas.

⚠ **Alerta de prova:** Acreditar que a lista de senhas banidas bloqueia na hora as contas com senhas que contêm os termos.
Como não cair: A verificação acontece só na troca ou redefinição de senha; não há bloqueio de contas existentes.

⚠ **Alerta de prova:** Pensar que o usuário libera o próprio e-mail com malware porque a política de quarentena permite liberação.
Como não cair: Para malware ou phishing detectados pelo Safe Attachments, o usuário só consegue solicitar a liberação; administradores revisam e liberam.

⚠ **Alerta de prova:** Escolher Require multifactor authentication quando o requisito é método resistente a phishing.
Como não cair: Essa concessão aceita qualquer MFA, inclusive SMS; use a força Phishing-resistant MFA strength.

⚠ **Alerta de prova:** Tentar editar uma força de autenticação interna para remover um método.
Como não cair: Forças internas não são editáveis por nenhuma função; crie uma força personalizada.

⚠ **Alerta de prova:** Bloquear um domínio na lista de colaboração e esperar que convidados que já resgataram percam o acesso.
Como não cair: A lista vale para convites novos e pendentes (o resgate pendente falha); quem já entrou precisa ser removido manualmente.

⚠ **Alerta de prova:** Imaginar que convidados não conseguem convidar outros externos num locatário novo.
Como não cair: O padrão do Entra permite que qualquer usuário, inclusive convidados, convide; restrinja com Only users assigned to specific admin roles.

⚠ **Alerta de prova:** Usar o estado Off com What If para medir o impacto de uma política em milhares de usuários.
Como não cair: What If simula uma entrada por vez; para impacto real sem afetar ninguém, use Report-only e leia os logs de entrada.

⚠ **Alerta de prova:** Achar que o usuário que entra só com chave de acesso será forçado a criar senha nova pela remediação de risco.
Como não cair: Para usuário sem senha, a remediação revoga as sessões e exige nova entrada, sem troca de senha.

⚠ **Alerta de prova:** Considerar que, com duas políticas de retenção de cinco e sete anos, prevalece a menor ou que os períodos se somam.
Como não cair: Vale o período de retenção mais longo; os períodos não se acumulam e a data de criação não decide.

⚠ **Alerta de prova:** Escolher a DLP no local Microsoft 365 Copilot and Copilot Chat para impedir colagem de dados em sites de IA de terceiros no navegador.
Como não cair: Esse local protege só Copilot e Copilot Chat; dados colados em IA de terceiros no navegador pedem DLP de endpoint.

⚠ **Alerta de prova:** Colocar a condição de SIT e a de rótulo na mesma regra da DLP do Copilot, ou achar que precisam de locatários diferentes.
Como não cair: As condições não podem ficar na mesma regra; use uma regra para cada condição dentro da mesma política.

Como cai na prova

📝 **Como cai:** Cenário pede a função adequada com menor privilégio para uma tarefa específica.
Como resolver: Descarte Global Administrator logo de cara; identifique a tarefa exata (redefinir senha, criar em massa, gerenciar atribuições, criar alerta, só ler) e escolha a função mais estreita que a cumpre.

📝 **Como cai:** Diretor financeiro pergunta quantas licenças P1 ou P2 são necessárias.
Como resolver: Veja se há associação dinâmica (membros precisam de P1), se há escopo de unidade (admin precisa de P1) e se a política é baseada em risco (P2). Dispositivos em grupos dinâmicos não exigem licença.

📝 **Como cai:** Política mudou e o enunciado pergunta o que acontece com quem já estava em outra situação.
Como resolver: Separe o estado atual: convite resgatado x pendente, senha existente x nova senha, usuário com um método x política que passou a exigir dois. A mudança costuma valer só para eventos futuros.

📝 **Como cai:** Escolha DUAS sobre PIM, ID Protection, TAP ou Attack simulation training.
Como resolver: Procure as duas afirmações literalmente verdadeiras e descarte as que trocam o responsável (Security Reader criando atribuição), o limite (365 dias) ou a ferramenta.

📝 **Como cai:** Usuário está em várias políticas (retenção, antiphishing, rótulos) e o enunciado pede qual vale.
Como resolver: Aplique a regra de precedência própria de cada recurso: maior retenção, explícito vence implícito, Strict vence Standard, rótulo de maior prioridade na herança do Copilot.

📝 **Como cai:** Copilot interagindo com conteúdo rotulado ou sensível.
Como resolver: O Copilot respeita permissões e direitos de uso: precisa de VIEW e EXTRACT, herda o rótulo de maior prioridade e, sob DLP por rótulo, pode citar o item sem usar o conteúdo.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Gerentes regionais administram só usuários da própria região	**Unidade administrativa por região com a função no escopo da unidade (P1 para quem administra).**
Proteger contas VIP do Helpdesk sem tirar a função dele	**Unidade administrativa de gerenciamento restrito.**
Funcionários aprovaram notificações do Authenticator que não pediram	**Correspondência de números.**
Primeiro acesso sem nunca receber senha	**Temporary Access Pass habilitado na política de métodos de autenticação.**
Senha redefinida na nuvem e a antiga continua valendo no domínio	**Write-back de senha pelo Entra Connect Sync ou Cloud Sync.**
Ataques de pulverização de senha usando POP e IMAP	**Acesso Condicional com Client apps em Exchange ActiveSync clients e Other clients + Block access.**
Nome da marca usado nas senhas	**Lista personalizada de senhas banidas da Proteção de Senha.**
Ameaça reconhecida depois que a mensagem já foi entregue	**ZAP (limpeza automática de zero hora).**
E-mail legítimo caindo na quarentena e reanálise pela Microsoft	**Submissions como Should not have been blocked; a entrada de permissão vale em até 5 minutos.**
Boletins promocionais para Lixo Eletrônico sem tratar como spam comum	**Veredito Bulk e limite de BCL na política antispam.**
Muitos falsos positivos em tipo de informação confidencial personalizado	**Elementos de suporte com palavras-chave próximas.**
Conteúdo sem padrão fixo, como currículos	**Classificador treinável.**
Nenhum administrador pode afrouxar a retenção	**Preservation Lock.**

Alertas de DLP antigos sumiram do painel	**Retenção do log de auditoria define quanto tempo o alerta fica visível.**

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

- Habilitar um método não obriga ninguém a usá-lo: exigir chave de acesso ou método resistente a phishing é trabalho de força de autenticação no Acesso Condicional.
- Remetentes falsificados e endereços IP bloqueados na Lista de Permissões/Bloqueios nunca expiram.
- Licença por Graph PowerShell falha em conta nova sem UsageLocation; o par é Get-MgSubscribedSku + Set-MgUserLicense (-AddLicenses e -RemoveLicenses).
- Interações com o Copilot já entram no Audit (Standard) com a auditoria ligada; pay-as-you-go de auditoria é para apps de IA que não são da Microsoft.
- Rótulos com criptografia no SharePoint e OneDrive precisam ser habilitados para coautoria, pesquisa e DLP funcionarem.

Essenciais para a prova (checklist)

☐ Sei calcular licenças P1 para unidades administrativas atribuídas e dinâmicas e para grupos dinâmicos de usuários.

☐ Sei escolher entre Helpdesk Administrator, User Administrator, Privileged Role Administrator, External Identity Provider Administrator e Global Reader.

☐ Sei diferenciar contato de e-mail, usuário de e-mail e convidado B2B.

☐ Sei as regras do SSPR: um ou dois métodos, política de duas etapas dos administradores, perguntas de segurança e write-back.

☐ Sei quando usar TAP, perfis de chave de acesso, correspondência de números e forças de autenticação internas ou personalizadas.

☐ Sei configurar Acesso Condicional em report-only, usar What If e bloquear autenticação herdada por Client apps.

☐ Sei o comportamento padrão de convites, listas de permissão e bloqueio, B2B direct connect e confiança de MFA de entrada.

☐ Sei montar atribuições elegíveis no PIM com prazo, aprovação, justificativa e contexto de autenticação.

☐ Sei a precedência Strict > Standard > personalizada e o que Built-in protection, ZAP, Safe Links e Dynamic Delivery fazem.

☐ Sei aplicar os princípios de retenção e configurar DLP para Copilot, endpoint e sites de IA de terceiros.

Questões de revisão do capítulo

R3.1 · Governar e proteger locatários e cargas de trabalho do Microsoft 365

A conta de uma gerente da Imobiliária Lar Feliz foi excluída por engano há 12 dias. Ela tinha licenças do Microsoft 365 E5 e várias associações de grupo. O que o administrador consegue fazer?

A. Pedir ao suporte da Microsoft que restaure a conta a partir do backup
B. Recriar a conta com o mesmo nome, porque a exclusão é sempre permanente
C. Aguardar a sincronização noturna, que devolve a conta excluída sozinha
D. Restaurar a conta em Deleted users com as propriedades e as licenças

R3.2 · Governar e proteger locatários e cargas de trabalho do Microsoft 365

A Indústria Têxtil Bordado Fino quer incentivar os funcionários a registrar o Microsoft Authenticator durante a entrada, permitindo que cada um adie o registro por alguns dias antes de ser obrigado. O administrador escolheu o estado Enabled na campanha de registro. Qual intervalo ele pode definir para o adiamento?

A. De 7 a 90 dias
B. De 0 a 14 dias
C. De 15 a 60 dias
D. De 1 a 30 dias

R3.3 · Governar e proteger locatários e cargas de trabalho do Microsoft 365

Os advogados do Escritório Moura & Lima reclamam que os e-mails com anexos chegam com atraso por causa da verificação do Safe Attachments. A segurança não aceita entregar anexos sem verificação. Qual ação do Safe Attachments equilibra os dois lados?

A. Monitor, que entrega a mensagem e o anexo na hora e só registra o resultado da verificação nos relatórios do portal
B. Dynamic Delivery, que entrega a mensagem com espaços reservados no lugar dos anexos até o fim da verificação
C. Block, que retém a mensagem inteira até concluir a verificação e só então entrega ao destinatário
D. Off, que desliga a verificação para os advogados e mantém a proteção antimalware padrão nas caixas

R3.4 · Governar e proteger locatários e cargas de trabalho do Microsoft 365

A Cooperativa Elétrica Luz do Campo decidiu estender a Proteção de Senha do Microsoft Entra ao Active Directory local. O administrador quer saber quais componentes precisam ser instalados e registrados no ambiente local antes de habilitar o recurso no Microsoft Entra admin center. Qual é a resposta?

A. O Microsoft Entra Connect Health e o agente de autenticação de passagem do domínio
B. O agente do Microsoft Defender for Identity em cada estação de trabalho
C. O conector de rede privada do Global Secure Access em cada filial
D. O serviço proxy da Proteção de Senha e os agentes nos controladores de domínio

Respostas comentadas

R3.1. D) Restaurar a conta em Deleted users com as propriedades e as licenças

Por quê: Depois de excluída, a conta fica suspensa por 30 dias e pode ser restaurada em Entra ID > Users > Deleted users, com todas as propriedades. As licenças atribuídas no momento da exclusão também voltam, mesmo que não haja licenças livres. Uma exclusão permanente não pode ser revertida por ninguém.

✗ A) Incorreta. O próprio administrador restaura em Deleted users dentro dos 30 dias.
✗ B) Incorreta. A exclusão de usuário é reversível por 30 dias; recriar perderia as propriedades.
✗ C) Incorreta. Só usuários sincronizados do AD local podem voltar pela sincronização; não é o caso descrito.

> **Dica de prova:** Usuário excluído há menos de 30 dias: Deleted users > Restore user.

R3.2. B) De 0 a 14 dias

Por quê: A campanha de registro incentiva o registro de métodos mais fortes durante a entrada. No estado Microsoft managed, a Microsoft define o método e o adiamento; no estado Enabled, o administrador escolhe chave de acesso ou Authenticator, de 0 a 14 dias de adiamento e se os adiamentos são limitados.

✗ A) Incorreta. Não existe esse intervalo na campanha de registro.
✗ C) Incorreta. O máximo é de 14 dias.
✗ D) Incorreta. O intervalo configurável vai de 0 a 14 dias.

> **Dica de prova:** Campanha de registro no estado Enabled: adiamento de 0 a 14 dias.

R3.3. B) Dynamic Delivery, que entrega a mensagem com espaços reservados no lugar dos anexos até o fim da verificação

Por quê: No Safe Attachments, o Dynamic Delivery entrega as mensagens imediatamente, mas troca os anexos por espaços reservados até a verificação terminar; anexos mal-intencionados vão para a quarentena. É a opção indicada para evitar atrasos sem abrir mão da análise.

✗ A) Incorreta. Entregar o anexo antes da verificação contraria a exigência da segurança.
✗ C) Incorreta. Reter a mensagem inteira é justamente o que causa o atraso reclamado.
✗ D) Incorreta. Desligar a verificação viola a exigência de não entregar anexos sem análise.

> **Dica de prova:** Anexo verificado sem atrasar o e-mail: Dynamic Delivery.

R3.4. D) O serviço proxy da Proteção de Senha e os agentes nos controladores de domínio

Por quê: Para proteger o AD DS local, o administrador instala e registra o serviço proxy da Proteção de Senha e os agentes nos controladores de domínio. Depois, em Authentication methods > Password protection, ativa a proteção no Windows Server Active Directory e escolhe o modo Audit ou Enforced.

✗ A) Incorreta. Esses componentes não são os da Proteção de Senha local.

✗ B) Incorreta. O Defender for Identity é outro produto e não aplica a lista de senhas banidas.

✗ C) Incorreta. Esse conector não tem relação com a validação de senhas no AD local.

> **Dica de prova:** Proteção de Senha no AD local: serviço proxy e agentes nos controladores.

DIA DA PROVA

Estratégia de prova

O AB-650 é um exame de nível Associate, em beta, com questões de múltipla escolha e múltipla resposta baseadas em cenários de administração do Microsoft 365 e de IA. Quase toda questão descreve uma empresa, um requisito e uma restrição (menor privilégio, sem afetar usuários, sem mudar permissões, sem compras fora da TI), e a resposta certa é o recurso que cumpre o requisito sem violar a restrição. As alternativas erradas costumam ser recursos reais aplicados ao problema errado: retenção onde se pede DLP, Service health onde se pede Message center, Global Administrator onde basta uma função estreita. O peso maior está em governança e proteção (40-45%) e em IA (35-40%), por isso Entra, Defender, Purview, Copilot e agentes dominam a prova. Nomes de configurações aparecem em inglês, como no admin center.

Como responder

✓ Leia primeiro a pergunta final e a restrição do cenário (menor privilégio, sem interromper, sem licença extra) antes de olhar as alternativas.

✓ Nas questões de função, elimine Global Administrator quando houver função específica que atenda; ele só é certo quando a tarefa exige, como a primeira ativação da sessão ociosa.

✓ Nas questões de licença, procure a palavra que muda tudo: dinâmica, risco, simulação de ataque, Threat Explorer, Agent 365.

✓ Em Escolha DUAS, avalie cada afirmação isoladamente como verdadeira ou falsa; não procure a dupla que combina.

✓ Quando duas alternativas parecem certas, prefira a que resolve o requisito inteiro com o controle nativo, sem depender de ação manual ou de lembrete.

✓ Domine os nomes exatos dos menus e opções em inglês, porque a prova está disponível só em inglês e as alternativas trocam caminhos parecidos.

✓ Administre os 100 minutos: marque para revisão os cenários longos de Cowork e Agent ID e volte a eles depois de garantir as questões diretas.

✓ Use os pesos para revisar: governança e proteção, depois IA, depois locatário e cargas de trabalho.

Erros que derrubam candidatos

✗ Escolher o recurso que avisa ou registra quando o cenário pede impedir (alerta no lugar de Preservation Lock, Monitor no lugar de Dynamic Delivery).

✗ Achar que mudanças de política afetam o passado: listas de convite, senhas banidas e exigência de dois métodos no SSPR valem para eventos futuros.

✗ Confundir visibilidade com acesso no Copilot Cowork e nos agentes (descoberta, Tags, Sharing).

✗ Trocar ferramentas parecidas de monitoramento: Service health, Message center, relatório de uso, relatório de prontidão, Agent Map e Copilot Dashboard.

✗ Esquecer que forças de autenticação internas não se editam e que habilitar um método não obriga o uso.

✗ Errar a ordem de operações em caixas compartilhadas, licenças por grupo e restauração de usuários excluídos.

✗ Aplicar DLP do Copilot onde o problema é IA de terceiros no navegador, que pede DLP de endpoint.

Na semana da prova

- ☐ Refaça os simulados priorizando os temas em que errou e reescreva a regra que faltou em uma frase curta.
- ☐ Revise as tabelas de números de cada capítulo: TAP, bloqueio inteligente, temas, caixas compartilhadas, Backup, fixação de agentes e prontidão.
- ☐ Repasse as comparações de pares (elegível x ativo, federado x sincronizado, Publish x Deploy, patrocinador x proprietário) até responder sem hesitar.
- ☐ Se o inglês não for seu idioma nativo, peça os 30 minutos adicionais ao agendar a prova.
- ☐ Lembre que exames beta não são pontuados imediatamente; a nota mínima é 700 numa escala de 1 a 1000.
- ☐ Na véspera, revise só os itens de lembrar e o checklist de cada capítulo e durma bem.

REVISÃO FINAL

Folha de cola

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

1. Configurar e gerenciar locatários e cargas de trabalho do Microsoft 365

‣ Registrador compatível com Domain Connect → **Assistente abre o registrador para autorizar a criação dos registros DNS.**

‣ Domínio comprado pelo Microsoft 365 com DNS gerenciado pela Microsoft e pedido de subdomínio → **Não é possível: subdomínio exige DNS gerenciado pela organização.**

‣ Usuários trocam o tema e logotipo some no modo escuro → **Aba General impede substituir; logotipo alternativo para temas escuros na aba Logos.**

‣ Licença por grupo não chegou a alguns usuários → **Billing > Licenses > produto > Errors & issues (e verificar aninhamento).**

‣ Backup não deixa criar política → **Configurar pay-as-you-go com assinatura do Azure, grupo de recursos e região.**

⚠ Dois SPF é o que a documentação manda evitar; acrescente os valores ao existente.

⚠ Número menor = prioridade maior.

⚠ Só contas novas usam o domínio padrão; credenciais e acesso não mudam.

2. Gerenciar e proteger serviços de IA no Microsoft 365

‣ Impedir geração de imagens com o Copilot → **Copilot > Settings > Copilot actions > Copilot image generation.**

‣ Grupo testando recursos antes da disponibilidade geral → **Copilot Frontier.**

‣ Funcionários experimentam o Copilot sem comprar por conta própria → **Microsoft Copilot self-service purchases permitindo apenas trials.**

‣ Recursos do Copilot não aparecem para um usuário licenciado → **Copilot Service Plan Diagnostic em Support > Help and support.**

‣ Usuários não podem enviar feedback e a Microsoft precisa investigar → **Copilot diagnostics logs em Other settings.**

⚠ Sharing só se aplica ao Agent Builder e ainda permite compartilhar com pessoas específicas.

⚠ Descoberta é só visibilidade e a entrada do agente não controla mais o acesso; quem está numa política de gastos que seleciona o Cowork tem acesso.

⚠ A precedência só escolhe o limite de quem está em várias políticas (vence o maior por usuário); ela não decide quem tem acesso.

3. Governar e proteger locatários e cargas de trabalho do Microsoft 365

‣ Gerentes regionais administram só usuários da própria região → **Unidade administrativa por região com a função no escopo da unidade (P1 para quem administra).**

‣ Proteger contas VIP do Helpdesk sem tirar a função dele → **Unidade administrativa de gerenciamento restrito.**

‣ Funcionários aprovaram notificações do Authenticator que não pediram → **Correspondência de números.**

‣ Primeiro acesso sem nunca receber senha → **Temporary Access Pass habilitado na política de métodos de autenticação.**

‣ Senha redefinida na nuvem e a antiga continua valendo no domínio → **Write-back de senha pelo Entra Connect Sync ou Cloud Sync.**

⚠ Isso vale só para associação atribuída; com regras de associação dinâmica, cada membro também precisa de P1.

⚠ Escopo de unidade administrativa exige P1 para o administrador, sem P2 nem PIM.

⚠ Ele guarda os três últimos hashes de senha errada e não conta a repetição da mesma senha; o limite padrão é 10 tentativas.

GABARITO

Respostas do diagnóstico

D1. B) O assistente abre o registrador para autorizar a criação dos registros DNS → revise o capítulo 1

Por quê: Quando o registrador oferece Domain Connect, o assistente abre uma janela do registrador para o administrador entrar e autorizar o registro TXT de verificação e os registros DNS dos serviços do Microsoft 365. Sem esse suporte, a verificação e os registros são feitos à mão.

✗ A) Incorreta. O assistente adiciona os registros dos serviços escolhidos, como o MX, quando o administrador autoriza.

✗ C) Incorreta. A posse continua sendo verificada por DNS; o Domain Connect só automatiza a criação dos registros.

✗ D) Incorreta. O Domain Connect não transfere o domínio de registrador.

> **Dica de prova:** Domain Connect automatiza registros DNS com autorização no registrador.

D2. D) Subdomínios só podem ser adicionados quando a organização gerencia o próprio DNS no registrador → revise o capítulo 1

Por quê: Para adicionar subdomínios, a organização precisa gerenciar as próprias configurações de DNS no registrador. Quando o DNS é gerenciado pela Microsoft por registros NS, ou o domínio foi comprado da Microsoft, não é possível adicionar subdomínios. Um subdomínio adicionado é verificado automaticamente pelo domínio pai.

✗ A) Incorreta. Não há tempo mínimo de registro para adicionar subdomínios.

✗ B) Incorreta. Subdomínios podem ficar no mesmo locatário quando a organização gerencia o DNS.

✗ C) Incorreta. Adicionar subdomínio não depende de licença por endereço.

> **Dica de prova:** DNS gerenciado pela Microsoft: sem subdomínios.

D3. A) Ativar o recurso nas configurações de local, que vem desligado, e ter dois computadores em Wi-Fi por loja → revise o capítulo 1

Por quê: Para usar o Windows Location Services, o administrador ativa a opção nas configurações de local da conectividade de rede (desligada por padrão) e garante pelo menos dois computadores por local com OneDrive atualizado, consentimento de localização e Wi-Fi. Os locais são agrupados por cidade e as amostras aparecem em cerca de 24 horas.

✗ B) Incorreta. O método detecta os locais pela cidade; não depende do endereço postal cadastrado.

✗ C) Incorreta. Computadores ligados por cabo não têm localização precisa; o método pede Wi-Fi.

✗ D) Incorreta. Os testes rodam nos computadores dos usuários, no máximo uma vez por dia.

> **Dica de prova:** Windows Location Services: opt-in, Wi-Fi e dois computadores por local.

D4. B) Em Copilot > Settings > User access > Microsoft Copilot in admin centers → revise o capítulo 2

Por quê: Em Copilot > Settings > User access, a configuração Microsoft Copilot in admin centers controla se administradores qualificados podem usar o Copilot nos centros de administração suportados. O Microsoft 365 Admin agent é a experiência assistiva e agêntica que ajuda a operar o Microsoft 365, o Copilot e os agentes.

✗ A) Incorreta. Essa configuração define quais categorias de agentes e plug-ins os usuários instalam.
✗ C) Incorreta. O Service health trata de incidentes e notificações dos serviços.
✗ D) Incorreta. Temas tratam da identidade visual, não do uso do Copilot por administradores.

> **Dica de prova:** Copilot para administradores: Microsoft Copilot in admin centers.

D5. B) Em Copilot > Settings > Copilot actions > Copilot image generation → revise o capítulo 2

Por quê: Em Copilot > Settings, a categoria Copilot actions reúne Copilot image generation (permitir ou impedir as experiências de geração de imagem), Screen and camera sharing (visão no Copilot, sem desligar voz) e Copilot in Teams meetings, que leva ao Teams admin center.

✗ A) Incorreta. A fixação do Copilot Chat não controla a geração de imagens.
✗ C) Incorreta. O dicionário personalizado trata do vocabulário usado em experiências do Teams.
✗ D) Incorreta. Essa configuração trata do acesso a modelos de terceiros, não da geração de imagens em si.

> **Dica de prova:** Bloquear geração de imagem: Copilot actions > Copilot image generation.

D6. D) Sim, pelo botão Web search em Personalization > Advanced nas configurações do app → revise o capítulo 2

Por quê: Com a pesquisa na web habilitada pelo administrador, o botão Web content vem ligado e o usuário pode desligá-lo (no app, em Settings > Personalization > Advanced > Web search); a preferência vale entre sessões e clientes. Se o administrador desabilita a web, o botão fica indisponível.

✗ A) Incorreta. Com a web habilitada, o usuário pode desligá-la para si.
✗ B) Incorreta. Há um botão de Web content para o usuário quando o administrador habilita a web.
✗ C) Incorreta. Essa configuração de privacidade nos apps não afeta a pesquisa na web do Copilot.

> **Dica de prova:** Usuário quer o Copilot sem web: desligar o botão nas configurações do app.

D7. B) O bloqueio inteligente guarda os três últimos hashes de senha errada e não conta repetições da mesma senha → revise o capítulo 3

Por quê: O bloqueio inteligente bloqueia a conta por um minuto após 10 tentativas com falha nos locatários públicos (3 nos do governo dos Estados Unidos), por mais tempo a cada nova falha. Ele acompanha os três últimos hashes de senha errada, para não aumentar o contador quando a mesma senha incorreta é repetida.

✗ A) Incorreta. O bloqueio inteligente funciona por padrão e não depende do modo da Proteção de Senha.
✗ C) Incorreta. O bloqueio inteligente protege as contas em geral, não só as de administradores.
✗ D) Incorreta. O limite padrão é de 10 tentativas com falha nos locatários públicos.

> **Dica de prova:** Mesma senha errada repetida não conta no bloqueio inteligente.

D8. C) Um elemento de suporte com palavras-chave próximas, como contrato ou nº do contrato

→ revise o capítulo 3

Por quê: Um tipo de informação confidencial combina elemento principal (expressão regular, com ou sem checksum, lista ou dicionário de palavras-chave ou função), elementos de suporte, nível de confiança e proximidade. Encontrar elementos de suporte perto do principal aumenta a confiança da detecção.

✗ A) Incorreta. O rótulo protege o conteúdo, mas não melhora a detecção do padrão.

✗ B) Incorreta. A expiração de grupos não altera a precisão de um tipo de informação confidencial.

✗ D) Incorreta. Retenção controla por quanto tempo o conteúdo é guardado, não a detecção do SIT.

> **Dica de prova:** Muitos falsos positivos no SIT: adicione elementos de suporte próximos.

D9. A) Contas com funções administrativas seguem a política de duas etapas, que não pode ser alterada → revise o capítulo 3

Por quê: Para contas com funções administrativas, o Microsoft Entra aplica uma política de duas etapas no SSPR: exige dois dados de autenticação, como e-mail, aplicativo ou telefone, e proíbe perguntas de segurança. Essa política não pode ser alterada; por isso a recomendação é testar o SSPR com um usuário sem função administrativa.

✗ B) Incorreta. Não existe esse prazo; a diferença acontece porque a conta é administrativa.

✗ C) Incorreta. A Proteção de Senha não tem relação com o número de métodos exigido no SSPR.

✗ D) Incorreta. A diferença não é de licença; a política de duas etapas vale para funções administrativas.

> **Dica de prova:** Testou SSPR com conta admin e viu dois métodos: é a política de duas etapas fixa.

Agora, treine no formato real

Faça as 6 provas completas do curso AB-650: 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.