

Guia de preparação AB-900

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

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-900: o guia explica o que cai e onde estão as armadilhas; as provas treinam o ritmo e mostram o que você ainda não domina.

Quando	O que fazer
Semana 1	Faça o teste diagnóstico (página seguinte) e leia os capítulos 1 e 2. No fim da semana, faça a Prova 1 do curso no tempo do exame.
Semana 2	Leia os demais capítulos, começando pelos domínios em que você errou mais no diagnóstico. Faça as provas 2 e 3.
Semana 3	Releia os alertas de pegadinha e as tabelas de comparação. Faça as provas 4 e 5 e revise cada erro pela explicação.
Semana 4	Estude a folha de cola, faça a Prova 6 e refaça as provas abaixo de 80%. Agende o exame quando estiver acima de 80% em todas (a nota de corte é 70%).

Mapa do exame

Cada prova do curso tem 50 questões e 45 minutos, no formato do exame. Referência de aprovação: 70%.

Domínio (capítulo)	Peso	Neste guia
1. Entender a proteção e a governança de dados para o Microsoft 365 e o Copilot	35-40%	18 conceitos · 14 pegadinhas
2. Executar tarefas administrativas básicas para o Copilot e os agentes	25-30%	18 conceitos · 12 pegadinhas
3. Identificar os principais recursos e objetos dos serviços do Microsoft 365	30-35%	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 · Entender a proteção e a governança de dados para o Microsoft 365 e o Copilot

Antes de liberar o Copilot, a empresa quer avaliar quais sites têm dados sensíveis expostos a muita gente. Qual recurso do DSPM para IA ajuda?

A. Caixas de recurso do Exchange
B. Avaliações de risco de dados
C. Registros DNS do domínio
D. Políticas de reunião do Teams

D2 · Entender a proteção e a governança de dados para o Microsoft 365 e o Copilot

Um arquivo com política de retenção de cinco anos é excluído por um usuário em um site do SharePoint. O que acontece?

A. O arquivo é perdido de imediato e para sempre
B. O usuário perde o acesso ao site inteiro
C. Uma cópia é mantida na biblioteca de retenção
D. O arquivo é enviado ao e-mail do administrador

D3 · Entender a proteção e a governança de dados para o Microsoft 365 e o Copilot

Um site de RH tem permissões antigas e confusas. O administrador quer que só membros de um grupo específico acessem o site, inclusive pelo Copilot. O que usar?

A. Rótulo de retenção aplicado aos arquivos do site
B. Caixa de correio compartilhada do RH
C. Política de reunião do Teams
D. Política de controle de acesso restrito do site

D4 · Executar tarefas administrativas básicas para o Copilot e os agentes

Um usuário quer encontrar um prompt que ele mesmo salvou semanas atrás para reutilizá-lo. Onde procurar?

A. Na galeria de prompts do Copilot
B. No log de auditoria do Purview
C. Nas regras de fluxo do Exchange
D. No relatório de uso do centro de administração

D5 · Executar tarefas administrativas básicas para o Copilot e os agentes

No centro de administração, o que os insights de um agente ajudam o administrador a acompanhar?

A. Os registros DNS usados pelo domínio
B. O conteúdo privado das caixas de correio
C. Usuários ativos, sessões e tendências de uso do agente
D. As senhas e os métodos de MFA dos criadores dos agentes

D6 · Executar tarefas administrativas básicas para o Copilot e os agentes

No Outlook, qual tarefa é um bom exemplo de uso do Copilot integrado?

A. Configurar a retenção de chats do Teams
B. Atribuir licenças a um grupo dinâmico
C. Resumir uma conversa longa de e-mails
D. Criar uma política de acesso condicional

D7 · Identificar os principais recursos e objetos dos serviços do Microsoft 365

A empresa quer que os funcionários reservem a sala de reuniões pelo calendário do Outlook. O que criar no centro de administração do Exchange?

A. Uma caixa de correio de recurso para a sala
B. Um site de comunicação no SharePoint
C. Um usuário com licença completa para a sala
D. Uma política de mensagens no Teams

D8 · Identificar os principais recursos e objetos dos serviços do Microsoft 365

Um usuário novo consegue entrar no Microsoft 365, mas não tem caixa de correio no Outlook. Qual é a causa mais provável?

A. A senha dele tem caracteres especiais demais
B. A licença dele não inclui o Exchange Online
C. Ele ainda não entrou em nenhum canal do Teams
D. O site do SharePoint dele está vazio

D9 · Identificar os principais recursos e objetos dos serviços do Microsoft 365

Qual opção é um exemplo de autorização, e não de autenticação?

A. Exigir a senha do usuário na tela de entrada
B. Conceder a um usuário a permissão de editar um site
C. Verificar a digital do usuário no Windows Hello
D. Pedir ao usuário um código no Microsoft Authenticator

01

CAPÍTULO 1 · 35-40% DA PROVA

Entender a proteção e a governança de dados para o Microsoft 365 e o Copilot

É o domínio de maior peso (35 a 40%), então é onde mais pontos se ganham ou se perdem. Preciso entender que o Copilot só enxerga o que o usuário já pode acessar e que o grande risco é o compartilhamento excessivo que já existe; daí vêm as ferramentas do SharePoint Advanced Management e do Purview para corrigir. As questões descrevem uma necessidade (classificar, bloquear vazamento, guardar, achar, investigar, medir conformidade) e pedem a solução exata do Purview, com alternativas vizinhas que fazem coisas parecidas. Onde mais erro: Gerenciador de conteúdo x Gerenciador de atividades, DLP x Conformidade de Comunicações x Risco Interno, política x rótulo de retenção, Descoberta de Conteúdo Restrita x acesso restrito x Pesquisa Restrita e os seis princípios de IA responsável.

Neste capítulo

18 tópicos-chave · 14 pegadinhas · 7 macetes · 15 gatilhos · 4 questões comentadas

Tópicos-chave

Como o Copilot acessa dados

O Copilot age com as permissões do usuário e só usa o conteúdo que ele pode acessar no momento do prompt; se perdeu acesso ontem, o arquivo não é usado. Ele não cria permissões: torna fácil achar o que já estava acessível, por isso pode expor um arquivo confidencial que o usuário nunca abriu. A principal implicação de segurança é o compartilhamento excessivo existente, e revisar permissões é o passo inicial.

Microsoft Graph e índice semântico

O Microsoft Graph reúne pessoas, relacionamentos, e-mails, reuniões e arquivos e dá o contexto dos dados de trabalho (é ele que sabe quem é o gestor do usuário). O índice semântico entende relações entre conteúdos e ajuda o Copilot a recuperar informações relevantes, sempre dentro dos limites de acesso do usuário. Conectores do Copilot levam conteúdo externo (como um sistema de chamados) ao Graph com listas de controle de acesso.

Compromissos de dados do Copilot

Prompts e respostas ficam no limite de serviço do Microsoft 365 e não treinam os modelos de base; o Copilot herda os compromissos de segurança, privacidade e conformidade do Microsoft 365, inclusive o Limite de Dados da UE quando aplicável. No Copilot Chat com conta corporativa, o ícone de escudo indica proteção de dados empresariais. As interações ficam em uma pasta oculta da caixa de correio do usuário, o que permite aplicar retenção, auditoria e Descoberta Eletrônica.

Rótulos de confidencialidade

Classificam e protegem itens (arquivos e e-mails), reuniões e contêineres (grupos, equipes e sites), com marca d'água e criptografia que acompanham o arquivo fora do site original. Rótulos são criados uma vez e publicados por políticas de rótulos, que definem quem os vê, o rótulo padrão e se é preciso justificar a remoção. Rótulo de contêiner controla privacidade, acesso de convidados e compartilhamento externo (equipe Confidencial sem convidados); a opção Não Encaminhar impede encaminhar, copiar e imprimir, mas permite ler e responder.

Rótulos e o Copilot

Conteúdo gerado pelo Copilot a partir de itens rotulados herda o rótulo de maior prioridade (Interno + Confidencial = Confidencial), e a origem não muda. Se a criptografia não concede ao usuário o direito de exibição ou de extrair conteúdo, o Copilot não usa o arquivo para aquele usuário e não remove a proteção. A prioridade é a ordem dos rótulos, com o mais restritivo no topo; ela também decide quando dois rótulos se aplicam na rotulagem automática.

Rotulagem automática e rótulo recomendado

A política de rotulagem automática no Purview aplica rótulos a arquivos e e-mails existentes com base em tipos de informações confidenciais, sem ação dos usuários (milhares de arquivos antigos). A rotulagem no cliente com rótulo recomendado sugere o rótulo no aplicativo quando detecta conteúdo sensível e deixa o usuário decidir. Rótulo padrão na política de rótulos marca automaticamente todo documento novo, e o usuário pode mudar.

Classificação de dados

Tipos de informações confidenciais combinam padrões, palavras-chave e checagens para achar dados como CPF ou cartão. Classificadores treináveis usam aprendizado de máquina e reconhecem categorias de formato variado a partir de exemplos (contratos, currículos). A classificação por correspondência exata de dados (EDM) usa uma tabela de valores reais para detectar valores exatos com alta precisão e poucos falsos positivos.

Data Explorer: conteúdo x atividades

O Gerenciador de conteúdo mostra quantidade e localização de itens com tipos de informação sensível e rótulos (em quais sites e caixas se concentram); exige funções específicas, como Visualizador de Conteúdo, porque mostra o conteúdo dos itens. O Gerenciador de atividades (explorador de atividades) mostra o que foi feito: aplicar, alterar ou remover rótulo, copiar para mídia removível, imprimir.

Prevenção contra Perda de Dados (DLP)

Inspeciona conteúdo em Exchange, SharePoint, OneDrive, Teams, dispositivos e outros locais e pode auditar, bloquear ou bloquear com substituição registrando a justificativa do usuário. Dicas de política orientam o usuário no Outlook, no Teams e nos apps do Office; o modo de simulação mostra o impacto antes de ligar a política. Os alertas ficam no painel de alertas de DLP do Purview (política, usuário, local, conteúdo detectado; atribuir, comentar, resolver) e também podem ser investigados no Defender XDR.

DLP para o Copilot e DLP de ponto de extremidade

Uma política de DLP para o Microsoft 365 Copilot pode usar rótulos como condição para impedir que o Copilot use certos itens nas respostas (não resumir Altamente confidencial). A DLP de ponto de extremidade monitora e bloqueia ações no dispositivo, como copiar para USB, imprimir, enviar para a nuvem e colar dados em sites de IA de terceiros pelo navegador. Rótulos com criptografia e DLP para o Copilot complementam a revisão de permissões no SharePoint.

Gerenciamento de Risco Interno

Usa sinais como data de desligamento (por exemplo, do conector de RH) e downloads em massa para identificar riscos de usuários internos. Modelos de política que mais aparecem: roubo de dados por usuários que estão saindo e uso arriscado de aplicativos de IA (prompts com dados sensíveis ou respostas sensíveis). Pseudonimiza nomes por padrão e restringe o acesso por funções; o fluxo é alerta, triagem, caso e ação. A Proteção Adaptável usa os níveis de risco para aplicar controles de DLP mais rígidos a quem tem risco maior.

Conformidade de Comunicações

Analisa conduta em e-mails, chats do Teams e interações com IA, incluindo prompts e respostas do Copilot: assédio, linguagem ofensiva, informações sensíveis compartilhadas de forma inadequada e conflitos regulatórios. Os revisores analisam as mensagens sinalizadas e podem resolver, marcar como falso positivo, notificar o usuário ou escalar.

DSPM para IA

Gestão de postura de segurança de dados para IA: descobre quais apps de IA são usados, mostra relatórios e gerenciador de atividades com interações e tipos de informação sensível, faz avaliações de risco de dados (itens sensíveis com acesso amplo) e oferece políticas com um clique (DLP, risco interno, auditoria). Depende da auditoria ativa: sem ela, as atividades de IA não aparecem nos relatórios. Com extensões do navegador e dispositivos integrados, mostra acessos a sites de IA de terceiros e dados sensíveis enviados.

Retenção (Gerenciamento do Ciclo de Vida de Dados)

Política de retenção vale para locais inteiros (caixas, sites, chats e canais do Teams, interações do Copilot); rótulo de retenção vale para itens específicos e é publicado para aplicação manual ou aplicado automaticamente por informações sensíveis, palavras-chave ou classificadores treináveis. Ambos podem reter, excluir ou reter e depois excluir. Pelos princípios de retenção, reter vence excluir e o prazo de retenção mais longo vence; rótulo que declara registro impede editar e excluir.

Preservação de conteúdo

No SharePoint e OneDrive, a biblioteca de retenção para preservação guarda cópias de itens retidos que foram excluídos ou alterados. Conta excluída com caixa sob retenção vira caixa inativa, preservada enquanto a retenção valer. Escopo adaptável usa consultas sobre atributos (departamento) e se atualiza sozinho; escopo estático exige atualização manual.

Descoberta Eletrônica e auditoria

A pesquisa de conteúdo busca por palavras e condições em caixas, sites, conversas do Teams e interações com o Copilot, e permite preservar (hold, mesmo que o usuário tente apagar) e exportar com cadeia de custódia. Chats do Teams ficam nas caixas dos participantes; mensagens de canais, na caixa do grupo. O acesso exige função de Descoberta Eletrônica no Purview (Gerente de Descoberta Eletrônica); os logs de auditoria do Purview registram interações com o Copilot e os recursos acessados.

Gerenciador de Conformidade

Usa modelos de regulamentações, inclusive normas de IA, para gerar avaliações com ações de melhoria, que podem ser atribuídas a responsáveis, documentadas com evidências e testadas. A pontuação de conformidade mede o progresso. Ações gerenciadas pela Microsoft já vêm pontuadas por causa da responsabilidade compartilhada na nuvem; as do cliente precisam ser implementadas e comprovadas.

SharePoint Advanced Management e restrições temporárias

O SAM reúne relatórios de governança de acesso a dados (links 'Todas as pessoas da organização', sites com 'Todos, exceto usuários externos', permissões por site com contagem de usuários), revisão de acesso ao site pelos proprietários, controle de acesso restrito (só membros do grupo definido acessam, mesmo com permissão no arquivo) e políticas de ciclo de vida para sites inativos. Descoberta de Conteúdo Restrita esconde um site da pesquisa e do Copilot, e a Pesquisa Restrita do SharePoint limita pesquisa e Copilot a até 100 sites aprovados; ambas são temporárias, e a correção definitiva é ajustar as permissões.

Macetes para memorizar

Princípios de IA responsável

Transparência = explica (notas, avisos, fontes); Responsabilidade = responde (comitê, revisar antes de decidir); Confiabilidade e segurança = não causa dano (recusa uso nocivo, filtros, Prompt Shields); Privacidade e segurança = protege dados (só o que pode acessar, não treina); Imparcialidade = trata igual; Inclusão = alcança todos (leitor de tela, idiomas).

Data Explorer

Conteúdo = ONDE está; Atividades = QUEM fez.

DLP x Comunicações x Risco Interno

DLP protege o DADO; Comunicações vigia a CONDUTA; Risco Interno vigia a PESSOA (quem sai, quem abusa da IA).

Retenção

Política = LOCAL inteiro; Rótulo = ITEM. Em conflito: guardar ganha de apagar, o mais longo ganha.

Restrições do SharePoint

Descoberta restrita ESCONDE; acesso restrito TRANCA; Pesquisa Restrita FILTRA (até 100 sites). Nenhuma substitui corrigir permissão.

Copilot e permissões

O Copilot vê o que você vê, agora. Não cria acesso, só revela o que estava aberto demais.

Classificação

Padrão fixo = tipo de informação; Exemplo variado = classificador treinável; Valor exato da base = EDM.

Tabela de memorização: não confunda

Quando é...	...e quando é
Gerenciador de conteúdo Saber onde estão e quantos são os itens com dados sensíveis ou rótulos.	**Gerenciador de atividades** Saber quem aplicou, alterou ou removeu rótulo, copiou para pendrive ou imprimiu.
DLP Impedir vazamento de dados sensíveis (cartão no Teams, e-mail para externo).	**Conformidade de Comunicações** Detectar conduta nas mensagens e prompts: assédio, linguagem ofensiva, conflito regulatório.
Política de retenção Regra para locais inteiros, como todos os chats do Teams ou as interações do Copilot.	**Rótulo de retenção** Regra por item (documento ou e-mail), aplicada manualmente ou automaticamente, inclusive declarando registro.

Descoberta de Conteúdo Restrita Esconder um site da pesquisa e do Copilot enquanto as permissões não são corrigidas.	**Controle de acesso restrito** Limitar quem pode abrir o site a um grupo definido, mesmo que alguém tenha link ou permissão no arquivo.
Tipos de informações confidenciais Dados com padrão fixo, como CPF ou cartão (e EDM para valores exatos da base).	**Classificadores treináveis** Documentos de formato variado, como contratos, aprendidos a partir de exemplos.
Rotulagem automática no Purview Rotular em massa arquivos existentes sem ação do usuário.	**Rótulo recomendado no cliente** Sugerir o rótulo no Word quando detectar dado sensível e deixar o usuário decidir.
Roubo de dados por usuários que saem Funcionário em desligamento baixando ou levando dados.	**Uso arriscado de aplicativos de IA** Usuário colocando dados sensíveis em prompts de IA ou obtendo respostas sensíveis.

Números que caem

Item	Valor
Pesquisa Restrita do SharePoint	**até 100 sites aprovados, além do conteúdo do próprio usuário**
Peso do domínio na prova	**35 a 40%, o maior peso da prova**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** O Copilot expôs um arquivo confidencial porque usa conta de serviço com acesso total ou ignora rótulos.
Como não cair: Ele age com as permissões do usuário e respeita rótulos; o usuário já tinha permissão, mesmo sem saber.

⚠ **Alerta de prova:** Site de RH aberto a todos: desativar o Copilot só para o RH ou criar lista de distribuição.
Como não cair: A primeira ação é corrigir as permissões e remover acessos amplos; recursos de restrição são temporários.

⚠ **Alerta de prova:** Para revisar interações do Copilot com informação sensível compartilhada indevidamente, escolher Gerenciador de Conformidade.
Como não cair: Gerenciador de Conformidade avalia controles regulatórios; quem analisa prompts e respostas é a Conformidade de Comunicações.

⚠ **Alerta de prova:** Linguagem ofensiva nas mensagens como modelo do Gerenciamento de Risco Interno.
Como não cair: Linguagem ofensiva é Conformidade de Comunicações; Risco Interno trata exfiltração por quem sai e uso arriscado de IA.

⚠ **Alerta de prova:** Para ver onde estão os números de cartão, escolher Gerenciador de atividades.
Como não cair: Atividades mostra ações sobre os itens; localização e quantidade é Gerenciador de conteúdo.

⚠ **Alerta de prova:** Conteúdo gerado de arquivos Interno e Confidencial fica sem rótulo ou com o de menor prioridade.
Como não cair: Herda automaticamente o de maior prioridade (Confidencial); o Copilot não cria rótulos nem altera a origem.

⚠ **Alerta de prova:** Contratos de formato variado: usar tipos de informações confidenciais.
Como não cair: Tipos usam padrões fixos; formato variado aprendido por exemplos é classificador treinável.

⚠ **Alerta de prova:** Números exatos de contrato da base: usar um tipo genérico de 10 dígitos.
Como não cair: Tipo genérico sem validação gera muitos falsos positivos; valores exatos da base é EDM.

⚠ **Alerta de prova:** Política manda excluir em 3 anos e outra reter por 7: a exclusão vence.
Como não cair: Reter tem prioridade sobre excluir e o prazo mais longo de retenção vence: fica 7 anos.

⚠ **Alerta de prova:** Rótulo de confidencialidade com marca d'água para excluir após sete anos ou para impedir exclusão.
Como não cair: Rótulo de confidencialidade protege, mas não exclui nem retém; prazo e registro são rótulos de retenção. Criptografia é de rótulos de confidencialidade, não de retenção.

⚠ **Alerta de prova:** Para aplicar retenção só ao Jurídico atualizando sozinha, usar escopo estático com lista de nomes.
Como não cair: Escopo estático exige atualização manual; escopo adaptável por atributo acompanha entradas e saídas.

⚠ **Alerta de prova:** Na Descoberta Eletrônica, procurar chats do Teams no site da equipe ou no computador do usuário.
Como não cair: Chats ficam nas caixas de correio dos participantes; mensagens de canais, na caixa do grupo.

⚠ **Alerta de prova:** Para pesquisar na Descoberta Eletrônica basta ser proprietário de sites ou ter licença do Copilot.
Como não cair: O acesso é por grupo de funções do Purview, como Gerente de Descoberta Eletrônica.

⚠ **Alerta de prova:** Desativar a auditoria para reduzir registros ou porque não afeta nada.
Como não cair: Sem auditoria, as atividades de IA não aparecem nos relatórios do DSPM para IA e se perde a evidência.

Como cai na prova

📝 **Como cai:** Necessidade de proteção descrita em uma frase, com quatro soluções do Purview como alternativas.
Como resolver: Classifique o verbo: identificar dado (classificação), marcar e proteger (rótulo), impedir saída (DLP), guardar ou apagar por prazo (retenção), achar para processo (Descoberta), conduta (Comunicações), pessoa de risco (Risco Interno), medir norma (Gerenciador de Conformidade).

📝 **Como cai:** Comportamento do Copilot diante de permissões, rótulos ou criptografia.
Como resolver: Aplique a regra: usa só o que o usuário acessa agora; respeita rótulos; sem direito de exibição ou extração não usa; conteúdo novo herda o rótulo de maior prioridade. Descarte qualquer alternativa em que o Copilot remove proteção ou cria acesso.

📝 **Como cai:** Compartilhamento excessivo antes de liberar o Copilot.
Como resolver: Identifique a etapa: achar (relatórios de governança de acesso, avaliações de risco de dados), corrigir (revisão de acesso pelos proprietários, link padrão para pessoas específicas, ciclo de vida de sites inativos) ou conter temporariamente (Descoberta restrita, Pesquisa Restrita, acesso restrito).

📝 **Como cai:** Ação da Microsoft ou do Copilot pedindo o princípio de IA responsável.
Como resolver: Associe a ação à palavra-chave: explicar limites e mostrar fontes (transparência), supervisão humana e revisão (responsabilidade), bloquear conteúdo nocivo (confiabilidade e segurança), proteger dados (privacidade), grupos prejudicados (imparcialidade), acessibilidade (inclusão).

📝 **Como cai:** Prazo de guarda ou exclusão com conflito entre políticas ou com conta excluída.
Como resolver: Reter vence excluir e o prazo mais longo vence; item excluído vai para a biblioteca de retenção; caixa de conta excluída sob retenção vira caixa inativa.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em

funcionário em desligamento levando dados	**Risco Interno: roubo de dados por usuários que estão saindo**
quais apps de IA são usados e dados sensíveis em prompts	**DSPM para IA**
esconder um site do Copilot por enquanto	**Descoberta de Conteúdo Restrita**
só um grupo acessa o site, mesmo com link	**Controle de acesso restrito (SAM)**
Copilot só com sites aprovados enquanto revisa permissões	**Pesquisa Restrita do SharePoint**
sites com muitos links 'Todas as pessoas da organização'	**Relatório de governança de acesso a dados**
proprietários confirmam se o acesso ainda é necessário	**Revisão de acesso ao site**
marca d'água e criptografia que acompanham o arquivo	**Rótulo de confidencialidade**
deixar o usuário seguir informando motivo de negócio	**DLP com substituição e justificativa**
ver o que a DLP detectaria sem afetar usuários	**Modo de simulação**
quanto maior o risco, mais rígida a DLP	**Proteção Adaptável**
preservar e-mails de funcionário em processo, mesmo que ele apague	**Hold da Descoberta Eletrônica**
nível de conformidade com uma regulamentação e ações de melhoria	**Gerenciador de Conformidade (pontuação de conformidade)**
texto colado que tenta fazer o Copilot ignorar as regras de segurança	**Injeção de prompt (filtros e Prompt Shields bloqueiam)**
copiar para pendrive arquivos sensíveis	**DLP de ponto de extremidade (bloquear) / Gerenciador de atividades (ver quem fez)**

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

- O Copilot não cria acesso: o risco é o compartilhamento excessivo que já existe, e a correção definitiva é ajustar permissões.
- Prompts e respostas não treinam os modelos de base e ficam na caixa de correio do usuário, sujeitos a retenção, auditoria e Descoberta.
- Conteúdo gerado herda o rótulo de maior prioridade; sem direito de uso, o Copilot não lê o arquivo.
- Reter vence excluir e o prazo mais longo vence.
- DSPM para IA depende da auditoria ativa.

Essenciais para a prova (checklist)

☐ Sei explicar por que o Copilot pode expor arquivos que o usuário nunca abriu.
☐ Sei o papel do Microsoft Graph, do índice semântico e dos conectores do Copilot.
☐ Sei os escopos dos rótulos de confidencialidade, a prioridade e a herança no Copilot.
☐ Sei diferenciar tipos de informações confidenciais, classificadores treináveis e EDM.
☐ Sei quando usar Gerenciador de conteúdo e Gerenciador de atividades.
☐ Sei as ações de uma regra de DLP, dicas de política, modo de simulação e onde investigar alertas.
☐ Sei separar DLP, Conformidade de Comunicações, Risco Interno e Proteção Adaptável.
☐ Sei o que o DSPM para IA oferece e por que depende da auditoria.
☐ Sei as regras de retenção, caixas inativas, escopos adaptáveis e rótulos de registro.
☐ Sei quando usar relatórios de governança, revisão de acesso, acesso restrito, Descoberta restrita e Pesquisa Restrita.

Questões de revisão do capítulo

R1.1 · Entender a proteção e a governança de dados para o Microsoft 365 e o Copilot

Para quais tipos de itens os rótulos de confidencialidade podem ser configurados no Purview?

A. Arquivos, e-mails, reuniões, grupos e sites
B. Registros DNS, apps e locais nomeados
C. Senhas, chaves de BitLocker e certificados
D. Licenças, domínios e caixas de recurso

R1.2 · Entender a proteção e a governança de dados para o Microsoft 365 e o Copilot

Um funcionário saiu da empresa e sua conta foi excluída, mas a caixa estava sob retenção. O que acontece com o conteúdo?

A. É apagado em definitivo na mesma hora
B. Vira uma caixa inativa e fica preservado
C. É publicado no site da equipe do usuário
D. É movido para a caixa do gestor do usuário

R1.3 · Entender a proteção e a governança de dados para o Microsoft 365 e o Copilot

Onde ficam guardados os prompts e as respostas do Microsoft 365 Copilot de um usuário, para fins de conformidade?

A. No computador do usuário, em uma pasta temporária
B. Em uma pasta oculta da caixa de correio do usuário
C. Em uma lista de distribuição criada pelo sistema
D. Em um site público do SharePoint da organização inteira

R1.4 · Entender a proteção e a governança de dados para o Microsoft 365 e o Copilot

Por que o Copilot é capaz de expor um arquivo confidencial a um usuário que nunca o abriu?

A. Porque o arquivo foi copiado para a internet pela Microsoft
B. Porque o usuário já tinha permissão no arquivo, mesmo sem saber
C. Porque o Copilot usa uma conta de serviço com acesso total aos sites
D. Porque o Copilot ignora os rótulos de confidencialidade

Respostas comentadas

R1.1. A) Arquivos, e-mails, reuniões, grupos e sites

Por quê: Rótulos podem proteger itens (arquivos e e-mails), reuniões e contêineres (grupos, equipes e sites).

✗ B) Incorreta. Não são escopos de rótulos.
✗ C) Incorreta. Não são escopos de rótulos.
✗ D) Incorreta. Não são escopos de rótulos.

> **Dica de prova:** Escopo do rótulo: itens, reuniões e contêineres.

R1.2. B) Vira uma caixa inativa e fica preservado

Por quê: Caixas inativas preservam o conteúdo de ex-funcionários enquanto a retenção estiver em vigor.

✗ A) Incorreta. A retenção impede a perda.

✗ C) Incorreta. Não é o efeito.

✗ D) Incorreta. Não é o efeito padrão.

> **Dica de prova:** Conta excluída com retenção: caixa inativa.

R1.3. B) Em uma pasta oculta da caixa de correio do usuário

Por quê: Guardar as interações na caixa do usuário permite aplicar retenção, auditoria e Descoberta Eletrônica.

✗ A) Incorreta. Não é onde ficam.

✗ C) Incorreta. Não é onde ficam.

✗ D) Incorreta. Não é onde ficam.

> **Dica de prova:** Interações do Copilot: caixa do usuário.

R1.4. B) Porque o usuário já tinha permissão no arquivo, mesmo sem saber

Por quê: O Copilot não cria acesso; ele torna fácil achar o que já é acessível, por isso a revisão de permissões é essencial.

✗ A) Incorreta. Os dados ficam no limite do serviço.

✗ C) Incorreta. Ele age com as permissões do usuário.

✗ D) Incorreta. Ele respeita os rótulos.

> **Dica de prova:** Exposição pelo Copilot: permissão que já existia.

02

CAPÍTULO 2 · 25-30% DA PROVA

Executar tarefas administrativas básicas para o Copilot e os agentes

Aqui preciso saber o que o administrador faz no dia a dia com o Copilot e os agentes: licenças e cobrança conforme o uso, ligar e desligar recursos, acompanhar adoção, gerenciar prompts e cuidar do ciclo de vida dos agentes (criar, compartilhar, aprovar, disponibilizar, monitorar, bloquear, remover). A prova também pede para escolher entre Copilot integrado, Researcher (Pesquisador), Analyst (Analista) e agente personalizado a partir do cenário. As alternativas erradas costumam mandar para o portal errado (Exchange, Purview, Entra, DNS) ou propor medidas desproporcionais, como excluir contas. Onde mais erro: Copilot Chat sem licença x licenciado, quando o uso por agentes exige cobrança por uso, e qual relatório ou centro de administração mostra cada informação.

Neste capítulo

18 tópicos-chave · 12 pegadinhas · 6 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Microsoft 365 Copilot Chat

Disponível para usuários do Microsoft 365 sem licença do Copilot, com conversas fundamentadas na web e proteção de dados empresariais, usando a conta corporativa (não exige assinatura do Azure). Pode usar agentes cobrados por consumo. Recursos com dados de trabalho dentro dos aplicativos exigem a licença do Microsoft 365 Copilot.

Licença do Microsoft 365 Copilot

É um complemento de planos qualificados, como Microsoft 365 E3, E5 e Business Standard, com preço fixo mensal por usuário. Traz o Copilot dentro dos aplicativos (Word, Excel, PowerPoint, Outlook, Teams) trabalhando com os dados de trabalho. Quem perde a licença perde os recursos licenciados, mas mantém o Copilot Chat; conta, e-mail e OneDrive não são afetados.

Atribuição de licenças do Copilot

Feita no centro de administração do Microsoft 365 (ou no Entra), para usuários ou grupos; para 200 usuários de uma vez, atribui-se a um grupo que os contém. Só é possível atribuir licenças compradas e disponíveis, então erro ao atribuir indica falta de licenças na assinatura. Licenças paradas, vistas no relatório de uso, devem ser realocadas para quem vai usar.

Cobrança conforme o uso (pay-as-you-go)

Cobra o consumo de agentes de usuários sem licença, medido em mensagens processadas, na assinatura do Azure vinculada. A política de cobrança vincula uma assinatura do Azure aos serviços cobertos (como Copilot Chat e SharePoint) e aos usuários ou grupos. Sem licença e sem política de cobrança, agentes que usam dados do locatário ficam indisponíveis para esses usuários.

Controle de custos da cobrança por uso

O gasto é acompanhado no Gerenciamento de Custos do Azure da assinatura vinculada, que mostra o consumo por serviço e permite criar orçamentos e alertas. Se o orçamento estourar, o administrador revisa o consumo e ajusta o orçamento, os usuários ou os serviços cobertos. Para quem usa muito agente e quase nada do Copilot nos apps, a cobrança por uso tende a ser mais econômica que a licença por usuário.

Configurações do Copilot no centro de administração

A página do Copilot no centro de administração do Microsoft 365 reúne os controles de recursos, como pesquisa na web e plug-ins, que podem ser habilitados ou desabilitados sem tirar licenças. Ali também se fixa o Copilot Chat nos aplicativos (Teams, Outlook, aplicativo Microsoft 365 Copilot), o que aumenta descoberta e adoção, inclusive para quem não tem licença. A página também mostra a situação das licenças.

Researcher (Pesquisador)

Agente de raciocínio incluído no Microsoft 365 Copilot para pesquisa aprofundada em várias etapas. Combina dados de trabalho (e-mails, reuniões, arquivos) e da web para gerar relatórios fundamentados com citações. Leva mais tempo, por isso vale para perguntas complexas, não para correções rápidas.

Analyst (Analista)

Agente de raciocínio incluído no Microsoft 365 Copilot para análise de dados. Usa raciocínio em cadeia e executa código Python sobre planilhas e arquivos de dados (CSV) para limpar dados, achar tendências, fazer previsões e gerar gráficos, explicando o raciocínio.

Agentes personalizados e Copilot integrado

Agentes personalizados combinam instruções, fontes de conhecimento e ações e fazem sentido quando a tarefa depende de dados, processos ou ações próprios da organização (dúvidas de RH com políticas internas, modelos de contrato do jurídico, API de pedidos). Tarefas gerais, como redigir um documento, reescrever um parágrafo ou resumir um e-mail longo, o Copilot integrado resolve. No Outlook, o Copilot integrado resume conversas, redige respostas e ajuda a preparar reuniões.

Componentes de um agente

Instruções definem objetivo, tom, estilo e limites do que o agente deve ou não fazer. Fontes de conhecimento (sites, arquivos) definem o que ele consulta, sempre respeitando as permissões do usuário. Ações, como conectores e APIs, permitem executar tarefas, como abrir chamados em um sistema de suporte.

Construtor de agentes

Opção mais simples, sem código, dentro do Microsoft 365 Copilot. O usuário define nome, instruções e fontes de conhecimento, pode sugerir prompts iniciais e testar o agente antes de compartilhar. Atende casos simples, como um agente que responde sobre documentos de um site do SharePoint.

Microsoft Copilot Studio

Para cenários complexos, com conectores, ações, fluxos e publicação em vários canais. Os agentes vivem em ambientes do Power Platform: quem cria é controlado por funções de segurança e políticas do ambiente, e o uso consome créditos de capacidade do Copilot Studio (pacotes pré-pagos ou cobrança por uso). Políticas de dados (DLP do Power Platform) classificam conectores como comerciais, não comerciais ou bloqueados.

Agente declarativo x mecanismo personalizado

Agentes declarativos estendem o Copilot com instruções, conhecimento e ações e usam a orquestração do próprio Copilot. Agentes com mecanismo personalizado trazem modelo e orquestração próprios. A diferença não é preço, aplicativo ou exigência de PIM.

Agentes do SharePoint

Cada site pode ter um agente pronto que responde sobre o conteúdo do site, e só quem tem acesso ao conteúdo pode usá-lo, porque as permissões de cada usuário são respeitadas. Usuários sem licença do Copilot podem usar agentes do SharePoint com cobrança por uso, desde que exista uma política de cobrança que cubra o SharePoint.

Compartilhamento, aprovação e publicação

Para poucos colegas, o criador compartilha o agente com pessoas específicas, sem aprovação. Para toda a organização, o agente enviado ao catálogo aparece nas solicitações da página de agentes do centro de administração, onde um administrador revisa fontes de dados, ações e permissões e aprova ou rejeita com comentários ao criador. Aprovado, ele aparece na loja de agentes, na seção da organização.

Gerenciamento de agentes no centro de administração

O inventário de agentes lista os agentes, seus criadores e quem pode usá-los. A disponibilidade pode ser definida para todos, nenhum ou usuários e grupos específicos; o ciclo de vida inclui aprovar, publicar, monitorar, bloquear (suspender para todos) e remover, além de reatribuir dono de agente órfão. Nas configurações de agentes se permitem ou bloqueiam agentes da Microsoft, de parceiros e da organização e se restringem agentes criados por usuários; em aplicativos integrados se controlam apps e agentes de terceiros.

Relatórios de uso e adoção

O relatório de uso do Microsoft 365 Copilot mostra usuários habilitados e ativos e o uso por aplicativo ao longo do tempo, sem conteúdo de prompts nem credenciais; o relatório de uso do Copilot Chat mostra o uso por quem não tem licença. O Copilot Analytics (Painel do Copilot) traz prontidão, adoção, impacto e sentimento, e permite relatórios personalizados com atributos organizacionais, como cargo e área. A Pontuação de Adoção resume experiências de pessoas e de tecnologia com recomendações; relatórios e insights de agentes mostram usuários ativos, sessões, tendências e erros, e o centro de administração do Power Platform mostra capacidade e análises por ambiente.

Galeria de prompts e prompts agendados

Prompts são salvos a partir da conversa e ficam na área pessoal: só o usuário vê até compartilhar com pessoas ou equipes, sem aprovação de administrador. Na galeria o usuário encontra, edita, compartilha e exclui prompts salvos, compartilhados pela equipe ou sugeridos pela Microsoft. Prompts agendados executam automaticamente na frequência escolhida (resumo diário às 8h, toda segunda-feira) e podem ser editados, pausados e excluídos pelo próprio usuário.

Macetes para memorizar

Researcher x Analyst

Pesquisador PESQUISA fontes e cita; Analista ANALISA números com Python.

Ciclo de vida do agente

Cria, Compartilha, Aprova, Disponibiliza, Monitora, Bloqueia, Remove: o admin manda do inventário ao remover.

Cobrança

Licença = fixo por cabeça; Uso = mensagem na conta do Azure, com orçamento e alerta.

Construtor x Studio

Construtor é o 'faça você mesmo' sem código; Studio é a oficina com fluxos, conectores e canais, morando no Power Platform.

Galeria de prompts

SCAE: Salvar, Compartilhar, Agendar, Excluir (e pausar o agendado nas férias).

Onde medir

Quantos e em quais apps = relatório de uso; impacto e prontidão = Copilot Analytics; adoção geral com recomendações = Pontuação de Adoção; por agente = relatórios de agentes.

Tabela de memorização: não confunda

Quando é...	...e quando é
Microsoft 365 Copilot Chat (sem licença) Chat fundamentado na web com proteção empresarial e agentes por consumo para quem não tem licença.	**Microsoft 365 Copilot (licenciado)** Copilot dentro do Word, Outlook, Teams e demais apps, trabalhando com os dados de trabalho.
Researcher (Pesquisador) Relatório aprofundado cruzando web, e-mails, reuniões e arquivos, com citações.	**Analyst (Analista)** Planilha ou CSV: limpar dados, tendências, previsões e gráficos com Python.
Construtor de agentes Agente simples, rápido e sem código, com nome, instruções e conhecimento.	**Copilot Studio** Fluxos, conectores, ações avançadas e publicação em vários canais, gerenciados por ambiente do Power Platform.
Licença mensal por usuário Usuários que usam o Copilot nos aplicativos com dados de trabalho; preço fixo.	**Cobrança conforme o uso** Usuários sem licença usando agentes (inclusive do SharePoint); paga-se pelas mensagens consumidas na assinatura do Azure.
Compartilhar o agente Poucos colegas específicos, sem passar por aprovação.	**Publicar para a organização** Toda a empresa no catálogo, após revisão e aprovação de um administrador.
Copilot integrado Tarefa geral: redigir, revisar, resumir, criar apresentação simples.	**Agente personalizado** Conhecimento interno, regras de um setor, processo próprio ou API interna.
Bloquear o agente Suspender para todos até corrigir respostas inadequadas.	**Remover o agente** Tirar do catálogo de forma definitiva porque não é mais necessário.

Números que caem

Item	Valor
Peso do domínio na prova	**25 a 30%**
Agentes de raciocínio prontos no Microsoft 365 Copilot	**2: Researcher e Analyst**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Copilot Chat exige a licença completa do Microsoft 365 Copilot ou uma assinatura do Azure para entrar.
Como não cair: Copilot Chat está disponível sem licença, com a conta corporativa e base na web; a licença traz os dados de trabalho nos apps.

⚠ **Alerta de prova:** Ao perder a licença do Copilot, o usuário tem a conta bloqueada ou perde e-mail e OneDrive.
Como não cair: Perde só os recursos licenciados e mantém o Copilot Chat; outros serviços não mudam.

⚠ **Alerta de prova:** Usuários sem licença usam agentes com dados da empresa sem custo ou ganham licença automática.
Como não cair: Sem licença e sem política de cobrança por uso, agentes com dados do locatário ficam indisponíveis.

⚠ **Alerta de prova:** Acompanhar o gasto por uso em relatórios do Entra ou do SharePoint.
Como não cair: Gasto, orçamentos e alertas ficam no Gerenciamento de Custos do Azure da assinatura vinculada.

⚠ **Alerta de prova:** Para relatório com muitas fontes, escolher o Analista; para planilha, o Pesquisador.
Como não cair: Pesquisador = pesquisa ampla com citações; Analista = dados brutos, Python e gráficos. Prompt agendado só roda um prompt em horário definido.

⚠ **Alerta de prova:** O construtor de agentes exige código e o Studio só aceita linguagem natural.
Como não cair: É o contrário: construtor é simples e sem código; Studio é o avançado, com fluxos e ações.

⚠ **Alerta de prova:** Agente com acesso indevido a dados: aprovar e corrigir depois, ou publicar só para convidados.
Como não cair: Rejeitar a solicitação e informar o motivo ao criador; aprovar antes de corrigir expõe dados.

⚠ **Alerta de prova:** Para restringir um agente ao time de vendas, remover a licença do Copilot dos outros departamentos.
Como não cair: Defina a disponibilidade do agente para o grupo no centro de administração.

⚠ **Alerta de prova:** Agente com respostas inadequadas: tirar licenças de todos.
Como não cair: Bloquear o agente no centro de administração suspende só ele, sem afetar os serviços.

⚠ **Alerta de prova:** Criador saiu da empresa: reativar a conta dele ou deixar os agentes sem dono.
Como não cair: Atribuir um novo responsável ou remover os agentes, como parte do ciclo de vida.

⚠ **Alerta de prova:** Prompt salvo vai para toda a organização ou precisa de aprovação do administrador.
Como não cair: Só o próprio usuário vê até compartilhar; não há aprovação de prompts.

⚠ **Alerta de prova:** O relatório de uso do Copilot mostra o conteúdo dos prompts de cada usuário.
Como não cair: Mostra usuários ativos e uso por aplicativo; conteúdo de interações se pesquisa na Descoberta Eletrônica.

Como cai na prova

📝 **Como cai:** Cenário de usuário pedindo qual agente ou recurso usar (Researcher, Analyst, agente personalizado, Copilot integrado).
Como resolver: Veja o insumo: muitas fontes e citações = Researcher; dados tabulares e Python = Analyst; conhecimento ou processo próprio da empresa = agente personalizado; tarefa genérica em um app = Copilot integrado.

📝 **Como cai:** Pergunta de 'onde configurar' algo do Copilot ou de agentes, com alternativas em Exchange, Purview, Entra e DNS.
Como resolver: Recursos do Copilot e agentes ficam no centro de administração do Microsoft 365 (configurações do Copilot, página de agentes, aplicativos integrados); agentes do Studio por ambiente, no Power Platform; custos, no Azure. Descarte portais que não controlam o Copilot.

📝 **Como cai:** Situação de licença ou cobrança (usuário sem licença, perda de licença, erro ao atribuir, departamento que só usa agentes).
Como resolver: Sem licença = só Copilot Chat; agentes com dados exigem licença ou política de cobrança por uso; erro ao atribuir = sem licenças disponíveis; uso concentrado em agentes = pague conforme o uso.

📝 **Como cai:** Problema com um agente (dados indevidos, respostas ruins, dono saiu, não é mais necessário).
Como resolver: Escolha a ação proporcional do ciclo de vida: rejeitar com motivo, bloquear, reatribuir dono, remover. Elimine excluir contas, tirar licenças de todos ou publicar para convidados.

📝 **Como cai:** Pergunta de adoção e monitoramento (quem usa, em que app, impacto, licenças paradas).
Como resolver: Relatório de uso para ativos e apps, realocando licenças paradas; Copilot Analytics para prontidão, impacto e atributos de RH; relatórios de agentes para uso por agente e erros.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
desligar a pesquisa na web ou um recurso do Copilot sem tirar licença	**Configurações do Copilot no centro de administração**
Copilot Chat fixado no Teams e no Outlook para todos	**Fixar o Copilot Chat pelo centro de administração**
planilha, CSV, previsão, Python, gráficos	**Analyst (Analista)**
relatório aprofundado com web, e-mails, reuniões e citações	**Researcher (Pesquisador)**
usuários sem licença usando agentes, pagar só pelo consumo	**Política de cobrança conforme o uso ligada ao Azure**
quanto já foi gasto, orçamento e alerta de custo	**Gerenciamento de Custos do Azure**
agente aguardando aprovação	**Solicitações na página de agentes do centro de administração**
lista de agentes, criadores e quem pode usá-los	**Inventário de agentes**
agentes do Copilot Studio por ambiente, capacidade	**Centro de administração do Power Platform**
impedir conectores não aprovados no Copilot Studio	**Políticas de dados do Power Platform**
tempo economizado, impacto, cruzar com cargo e área	**Copilot Analytics (Painel do Copilot, relatórios personalizados)**
resumo recorrente toda segunda ou todo dia	**Prompt agendado**
Copilot responder sobre a reunião depois que ela acabou	**Transcrição da reunião no Teams**
acelerar adoção com pessoas apoiando colegas por área	**Rede de campeões do Copilot**

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

- Sem licença o usuário ainda tem o Copilot Chat; agentes com dados da empresa exigem licença ou cobrança por uso.
- A política de cobrança por uso = assinatura do Azure + serviços + usuários; o custo é medido em mensagens.
- Publicar para toda a organização passa por aprovação do administrador; compartilhar com poucos colegas não.
- Agentes respeitam as permissões do usuário nas fontes de conhecimento.
- Prompt salvo é privado até ser compartilhado; agendado pode ser pausado pelo próprio usuário.

Essenciais para a prova (checklist)

- ☐ Sei explicar a diferença entre Copilot Chat sem licença e Microsoft 365 Copilot licenciado.
- ☐ Sei atribuir licenças do Copilot a usuários e grupos e o pré-requisito de plano qualificado.
- ☐ Sei montar uma política de cobrança conforme o uso e onde acompanhar e limitar custos.
- ☐ Sei quais recursos do Copilot o administrador liga, desliga e fixa no centro de administração.
- ☐ Sei escolher entre Researcher, Analyst, agente personalizado e Copilot integrado.
- ☐ Sei o que se define ao criar um agente e quando usar construtor de agentes ou Copilot Studio.
- ☐ Sei o fluxo de aprovação de agentes e onde o agente aprovado aparece.
- ☐ Sei controlar disponibilidade, bloqueio, remoção e agentes de terceiros no centro de administração.
- ☐ Sei qual relatório usar para uso, adoção, impacto e uso por agente.
- ☐ Sei salvar, compartilhar, agendar, pausar e excluir prompts.

Questões de revisão do capítulo

R2.1 · Executar tarefas administrativas básicas para o Copilot e os agentes

Em qual situação o agente de pesquisa Researcher é mais útil do que o Copilot Chat comum?

A. Na correção de ortografia de um parágrafo curto
B. Em análises de várias etapas que exigem muitas fontes
C. Em respostas rápidas a uma pergunta simples do dia
D. Na tradução de uma frase curta para o inglês

R2.2 · Executar tarefas administrativas básicas para o Copilot e os agentes

Para acelerar a adoção do Copilot, a empresa quer formar pessoas que apoiem os colegas em cada área. Qual prática é recomendada?

A. Desativar o relatório de uso do Copilot
B. Bloquear o Copilot até todos terem curso
C. Remover a licença de quem fizer perguntas
D. Criar uma rede de campeões do Copilot

R2.3 · Executar tarefas administrativas básicas para o Copilot e os agentes

Qual é a diferença entre o Microsoft 365 Copilot Chat sem licença adicional e o Microsoft 365 Copilot licenciado?

A. O licenciado não funciona no Word nem no Outlook
B. O licenciado trabalha com os dados de trabalho dentro dos aplicativos
C. O Copilot Chat exige uma assinatura do Azure para entrar
D. O Copilot Chat não usa nenhum modelo de IA generativa

R2.4 · Executar tarefas administrativas básicas para o Copilot e os agentes

No relatório de uso do Microsoft 365 Copilot, que informação o administrador encontra?

A. Usuários ativos e uso por aplicativo ao longo do tempo
B. O conteúdo dos prompts enviados por cada usuário
C. A lista de arquivos sensíveis em cada site
D. As senhas e os métodos de MFA de cada usuário

Respostas comentadas

R2.1. B) Em análises de várias etapas que exigem muitas fontes

Por quê: O Researcher faz pesquisa aprofundada e leva mais tempo, por isso vale para perguntas complexas.

✗ A) Incorreta. O chat comum resolve.
✗ C) Incorreta. O chat comum resolve.
✗ D) Incorreta. O chat comum resolve.

> **Dica de prova:** Pergunta complexa com muitas fontes: Researcher.

R2.2. D) Criar uma rede de campeões do Copilot

Por quê: Programas de campeões, treinamentos e cenários por área ajudam a aumentar o uso e o impacto.

✗ A) Incorreta. Perde a medição.
✗ B) Incorreta. Atrasa a adoção.
✗ C) Incorreta. Desestimula o uso.

> **Dica de prova:** Acelerar adoção: rede de campeões.

R2.3. B) O licenciado trabalha com os dados de trabalho dentro dos aplicativos

Por quê: O Copilot Chat é fundamentado na web e pode usar agentes por consumo; a licença traz o Copilot nos aplicativos e com dados de trabalho.

✗ A) Incorreta. Funciona nos aplicativos.
✗ C) Incorreta. Usa a conta corporativa.
✗ D) Incorreta. Também usa IA generativa.

> **Dica de prova:** Licença do Copilot: dados de trabalho nos apps.

R2.4. A) Usuários ativos e uso por aplicativo ao longo do tempo

Por quê: O relatório mostra usuários habilitados e ativos e o uso no Teams, Outlook, Word, Excel, PowerPoint e outros.

✗ B) Incorreta. Não exibe conteúdo.
✗ C) Incorreta. Não é o relatório.
✗ D) Incorreta. Não exibe credenciais.

> **Dica de prova:** Relatório de uso: ativos e uso por app.

03

CAPÍTULO 3 · 30-35% DA PROVA

Identificar os principais recursos e objetos dos serviços do Microsoft 365

Aqui preciso reconhecer, pelo cenário, qual objeto ou recurso do Microsoft 365 resolve o problema: licença, domínio, caixa de correio, grupo, site, biblioteca, equipe, canal ou política. A segunda metade é segurança: Confiança Zero, autenticação x autorização, métodos de MFA, acesso condicional, PIM, logs e o Defender XDR. As questões são quase sempre 'o que criar' ou 'onde configurar', e as alternativas erradas misturam objetos de serviços diferentes (caixa de recurso para dar acesso, rótulo de retenção para controlar login). Onde mais erro: grupos parecidos (lista de distribuição, grupo do Microsoft 365, grupo de segurança habilitado para e-mail, distribuição dinâmica), canal privado x compartilhado, acesso externo x convidado e qual log mostra o quê (entrada, auditoria do Entra, auditoria do Purview).

Neste capítulo

18 tópicos-chave · 14 pegadinhas · 7 macetes · 15 gatilhos · 4 questões comentadas

Tópicos-chave

Licenças e planos de serviço

Cada licença reúne planos de serviço, que podem ser desativados individualmente por usuário ou grupo: se o usuário tem E3 e não abre o Teams, o plano do Teams está desmarcado. Sem o plano do Exchange Online, a caixa de correio não é criada, mesmo que o usuário consiga entrar. Para atribuir licença, o local de uso (país) do usuário é obrigatório, porque a disponibilidade dos serviços varia por país.

Licenciamento baseado em grupo

Atribuir licenças a um grupo faz quem entra no grupo receber as licenças e quem sai perder os serviços correspondentes. É a resposta para 'todo novo funcionário de Vendas deve receber as licenças automaticamente'. Atribuir usuário por usuário funciona, mas dá mais trabalho e gera erros.

Domínios e configurações da organização

Um domínio novo é adicionado na página Domínios do centro de administração do Microsoft 365, e a posse é comprovada criando no DNS o registro de verificação indicado. Depois, o domínio pode ser definido como padrão para os novos usuários; o domínio onmicrosoft.com inicial continua existindo e não pode ser removido. Nas configurações da organização ficam a política de expiração de senha, o perfil da organização e as preferências de versão (versão direcionada para toda a organização ou para usuários selecionados).

Caixas de correio do Exchange

Caixa compartilhada: várias pessoas leem e respondem (suporte@), sem licença própria dentro do limite de armazenamento padrão; também é o destino de converter a caixa de um ex-funcionário. Caixa de recurso: sala ou equipamento (projetor), com reserva pelo calendário do Outlook. Caixa de arquivo morto: armazenamento adicional para e-mails antigos que precisam ser mantidos.

Destinatários e grupos do Exchange

Lista de distribuição: só repassa e-mails (vendas@), sem caixa nem arquivos. Grupo de distribuição dinâmico: membros calculados por filtros sobre atributos (todos de São Paulo pelo campo cidade), sem manutenção manual. Grupo de segurança habilitado para e-mail: recebe e-mails e concede permissões. Contato de email: pessoa externa no catálogo de endereços global, sem credenciais no locatário.

Grupo do Microsoft 365

Cria juntos caixa e calendário compartilhados e um site do SharePoint, e pode ser conectado a uma equipe do Teams. É a resposta quando o projeto pede e-mail, calendário e arquivos compartilhados ao mesmo tempo. Grupos abandonados são limpos pela política de expiração de grupos: os ativos são renovados automaticamente e os sem atividade são excluídos se os donos não renovarem.

Grupos de segurança e associação dinâmica

Usar grupos como objetos de segurança simplifica o acesso a aplicativos, sites e licenças (atribuir o app ao grupo de vendas, não a cem pessoas). A associação dinâmica usa regras sobre atributos, como departamento ou cargo, para colocar e tirar pessoas sozinhas; exige licença Entra ID P1. A associação atribuída exige inclusão manual.

Sites, bibliotecas e permissões do SharePoint

Site de equipe serve para colaboração; site de comunicação, para publicar a um público amplo com poucos autores; site hub conecta sites relacionados com navegação, tema e pesquisa comuns. Documentos com versões e metadados ficam em biblioteca de documentos. Grupos padrão: Proprietários (Controle total, inclusive permissões), Membros (Editar) e Visitantes (Leitura); pasta com acesso diferente exige interromper a herança, usando permissões exclusivas com moderação.

Compartilhamento e administração do SharePoint e OneDrive

A página Sites ativos do centro de administração do SharePoint lista todos os sites com armazenamento e atividade. O compartilhamento externo no nível da organização define o máximo permitido; os sites podem ser iguais ou mais restritos (é ali que se bloqueiam links para qualquer pessoa sem entrar). O link 'Pessoas específicas' exige que o destinatário entre com a conta autorizada; rascunhos pessoais de trabalho ficam no OneDrive.

Equipes, canais e políticas do Teams

Equipe pública: qualquer pessoa da empresa entra sem aprovação; privada: exige convite ou aprovação do dono. Canal privado tem membros próprios e site do SharePoint separado; canal compartilhado usa conexão direta B2B para colaborar com outra organização sem contas de convidado. Políticas de reunião (anônimos, gravação, transcrição), de mensagens (apagar mensagens) e de configuração de aplicativos (fixar apps) são atribuídas a usuários ou grupos; quem não tem atribuição recebe a política global (padrão da organização).

Acesso externo, convidados e identidade híbrida

Acesso externo (federação) permite só chat e chamadas com outros domínios; acesso de convidado (B2B) adiciona a pessoa a equipes e recursos usando a identidade da própria empresa dela. Para o AD local, o Microsoft Entra Connect sincroniza e cria identidades híbridas, com opções como sincronização de hash de senha e autenticação de passagem.

Confiança Zero

Três princípios: verificar explicitamente (avaliar identidade, dispositivo, local e risco antes de cada acesso), usar acesso com privilégio mínimo (JIT e JEA, políticas adaptativas) e presumir a violação (agir como se o invasor já estivesse dentro: segmentar, criptografar de ponta a ponta, analisar). Confiar na rede interna é o modelo de perímetro antigo, o oposto da Confiança Zero.

Autenticação, autorização e métodos

Autenticação confirma quem é (senha, digital, código); autorização define o que pode fazer (permissão de editar um site). SMS e voz são os métodos de MFA mais fracos; métodos sem senha incluem Microsoft Authenticator com entrada por telefone, Windows Hello for Business (biometria ou PIN ligado ao dispositivo), chaves FIDO2 e passkey no Authenticator (resistente a phishing). O Passe de Acesso Temporário (TAP) permite o primeiro acesso para registrar métodos sem senha, e o SSPR reduz chamados de senha.

Acesso condicional

Combina atribuições (usuários, apps, condições como local, plataforma e risco da entrada) com controles (bloquear, exigir MFA, exigir dispositivo em conformidade). Locais nomeados definem países ou IPs; o modo somente relatório mostra o impacto nos logs de entrada sem bloquear ninguém; a força da autenticação exige métodos resistentes a phishing; o acesso condicional baseado em risco usa o sinal do Entra ID Protection. Políticas personalizadas exigem Entra ID P1; sem P1, a opção são os padrões de segurança (registro de MFA, bloqueio de autenticação herdada, proteção de ações privilegiadas).

Aplicativos no Entra ID e SSO

O registro de aplicativo define o app (objeto de aplicativo); o aplicativo empresarial é a instância no locatário (entidade de serviço), onde ficam atribuição de usuários, consentimento e SSO. O SSO por SAML ou OpenID Connect permite entrar uma vez e acessar vários apps com a conta corporativa, com a TI controlando tudo em um só lugar. As configurações de consentimento restringem o usuário de liberar dados a apps de terceiros e podem exigir aprovação do administrador.

Funções privilegiadas e PIM

Privilégio mínimo é atribuir a função mais restrita que permite a tarefa, como Administrador do Exchange em vez de Global. A Microsoft recomenda menos de cinco administradores globais, de preferência com acesso sob demanda. O PIM oferece acesso just-in-time com aprovação, justificativa, MFA, notificações e revisões de acesso periódicas; PIM e ID Protection baseado em risco exigem, em geral, Entra ID P2.

Logs e classificações de segurança

Logs de entrada do Entra ID: por que o login falhou (resultado, método, local, dispositivo e políticas de acesso condicional avaliadas). Log de auditoria do Entra ID: alterações como atribuição de funções e mudanças em grupos. Log de auditoria do Purview: atividades de usuários e administradores nos serviços (quem excluiu um arquivo, quem mudou uma política de compartilhamento). A Classificação de Segurança de Identidade foca nas recomendações do Entra ID; a Classificação de Segurança da Microsoft cobre identidades, dispositivos e apps, e a pontuação sobe conforme o peso de cada ação concluída.

Microsoft Defender XDR

Une endpoints, identidades, e-mail e aplicativos e correlaciona alertas em incidentes na fila de incidentes. Análise de ameaças traz relatórios de especialistas e a exposição da organização; busca avançada usa KQL sobre até 30 dias de dados brutos; interrupção automática de ataques desativa contas e isola dispositivos durante um ataque em andamento. Componentes: Defender para Office 365 (Anexos Seguros, Links Seguros, antiphishing com proteção contra representação), Defender para Identidade (AD local, sensores nos controladores de domínio), Defender para Ponto de Extremidade (dispositivos) e Defender for Cloud Apps (TI invisível, risco de apps de nuvem, sancionar ou bloquear).

Macetes para memorizar

💡 Grupos padrão do site

P-M-V = Pode tudo, Mexe, Vê: Proprietários (Controle total), Membros (Editar), Visitantes (Leitura).

💡 Confiança Zero

VMP: Verificar explicitamente, Menor privilégio, Presumir violação.

💡 Autenticação x autorização

Autenticação = QUEM é você (senha, código no Authenticator, biometria); Autorização = O QUE você pode fazer (permissão no recurso).

💡 Entra ID P1 x P2

P1 = regras (acesso condicional, grupos dinâmicos). P2 = risco e privilégio (ID Protection e PIM).

💡 Componentes do Defender

Office 365 = e-mail; Identidade = AD local; Ponto de Extremidade = dispositivo; Cloud Apps = apps de nuvem; XDR = junta tudo em incidentes.

💡 Três logs

Entrada = o login; Auditoria do Entra = a mudança de identidade; Auditoria do Purview = a ação no serviço.

💡 Canais do Teams

Privado = parte de dentro; Compartilhado = gente de fora.

Tabela de memorização: não confunda

Quando é...	...e quando é
Lista de distribuição Só repassar e-mails a várias pessoas, sem caixa própria nem arquivos compartilhados (vendas@).	**Grupo do Microsoft 365** Precisa de caixa e calendário compartilhados, site do SharePoint e possibilidade de equipe do Teams, criados juntos.
Caixa compartilhada Várias pessoas leem e respondem o mesmo endereço, ou preservar a caixa de ex-funcionário sem pagar licença.	**Caixa de recurso** Reservar sala ou equipamento pelo calendário do Outlook.
Canal privado Só parte da própria equipe (diretores) deve ver conversas e arquivos.	**Canal compartilhado** Colaborar no canal com pessoas de outra organização sem criar contas de convidado (conexão direta B2B).
Acesso externo (federação) Parceiro só precisa de chat e chamadas, sem equipes nem arquivos.	**Acesso de convidado (B2B)** Externo precisa entrar em uma equipe e acessar recursos com a própria conta corporativa.
Logs de entrada do Entra ID Descobrir por que um login foi bloqueado e qual política de acesso condicional agiu.	**Log de auditoria do Entra ID** Descobrir quem atribuiu uma função, criou usuário ou mudou grupo.

Enviar como O remetente deve aparecer só como a caixa compartilhada.	**Enviar em nome de** Aparecem os dois nomes: o usuário em nome da caixa.
Padrões de segurança Empresa sem Entra ID P1 que quer MFA básica para todos.	**Acesso condicional** Regras por sinais (local, dispositivo, risco), como MFA só fora da rede; exige P1.

Números que caem

Item	Valor
Administradores globais recomendados	**menos de cinco, de preferência com acesso sob demanda via PIM**
Busca avançada do Defender XDR (KQL)	**até 30 dias de dados brutos**
Licença Entra ID para grupos dinâmicos e acesso condicional personalizado	**P1**
Licença Entra ID para ID Protection baseado em risco e PIM	**P2 (em geral)**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Usuário entra no Microsoft 365 mas não tem caixa no Outlook, então o problema é senha ou Teams.
Como não cair: Sem caixa de correio é licença sem o plano do Exchange Online; a licença é que cria a caixa.

⚠ **Alerta de prova:** Na licença E3 sem Teams, concluir que o E3 não inclui Teams ou que o domínio não foi verificado.
Como não cair: Item desmarcado na licença é plano de serviço desativado; domínio não verificado não bloquearia só o Teams.

⚠ **Alerta de prova:** Para ex-funcionário que recebia e-mails de clientes, manter a conta ativa com licença.
Como não cair: Converter em caixa compartilhada preserva o conteúdo e dá acesso aos colegas sem licença, dentro do limite padrão.

⚠ **Alerta de prova:** Funcionário desligado hoje: excluir a conta e as caixas de uma vez.
Como não cair: Primeiro bloquear a entrada e revogar as sessões; depois decidir sobre licença, caixa e arquivos. Excluir perde dados úteis.

⚠ **Alerta de prova:** Para e-mail por cidade sem manutenção, escolher lista de distribuição estática.
Como não cair: Lista estática exige manutenção manual; grupo de distribuição dinâmico calcula membros por atributo.

⚠ **Alerta de prova:** Para colaborar com parceiro no Teams, escolher canal privado.
Como não cair: Canal privado restringe a membros da própria equipe; parceiro externo sem conta de convidado é canal compartilhado.

⚠ **Alerta de prova:** Para parceiro só conversar no chat, dar acesso de convidado a uma equipe.
Como não cair: Convidado ganha equipes e arquivos; só chat e chamadas é acesso externo (federação).

⚠ **Alerta de prova:** Para colaborador editar páginas e listas, dar Controle total ou a função de Administrador do SharePoint.
Como não cair: Controle total também gerencia permissões e o Administrador do SharePoint manda em todos os sites; editar sem gerenciar acesso é o nível Editar (Membros).

⚠ **Alerta de prova:** Contar 'exigir senha' ou 'código no Authenticator' como autorização.
Como não cair: Tudo que comprova identidade é autenticação; autorização é conceder permissão a um recurso.

⚠ **Alerta de prova:** Achar que verificar explicitamente significa bloquear dispositivos pessoais ou pedir senha só no primeiro login.
Como não cair: É avaliar todos os sinais (identidade, dispositivo, local, risco) antes de cada acesso, de forma contínua.

⚠ **Alerta de prova:** Empresa sem P1 quer MFA para todos: criar políticas de acesso condicional personalizadas.
Como não cair: Acesso condicional personalizado exige Entra ID P1; sem ele, a resposta é padrões de segurança.

⚠ **Alerta de prova:** Para testar uma política de acesso condicional, atribuí-la a nenhum usuário ou desativar os logs.
Como não cair: Atribuir a ninguém não gera resultados; o modo somente relatório mostra nos logs de entrada como a política agiria.

⚠ **Alerta de prova:** Para ataques ao AD local, escolher Defender for Cloud Apps ou Defender para Office 365.
Como não cair: AD local e movimentação lateral é Defender para Identidade; Cloud Apps foca em apps de nuvem e Office 365 em e-mail e colaboração.

⚠ **Alerta de prova:** Usar a política de reunião do grupo de vendas ou a mais restritiva para quem não tem atribuição.
Como não cair: Sem atribuição, vale sempre a política global (padrão da organização).

Como cai na prova

📝 **Como cai:** Cenário de negócio pedindo 'o que criar no Exchange' com alternativas de vários tipos de caixa e grupo.
Como resolver: Pergunte: precisa só repassar e-mail (lista), por atributo (dinâmica), e-mail + permissão (segurança habilitado para e-mail), caixa usada por várias pessoas (compartilhada), reserva (recurso), externo sem conta (contato)?

📝 **Como cai:** Problema de login ou acesso com alternativas de logs e relatórios de vários portais.
Como resolver: Falha de entrada e política aplicada vão para logs de entrada; alteração de função para auditoria do Entra; ação em arquivo ou configuração para auditoria do Purview. Descarte relatórios de uso e galeria de prompts.

📝 **Como cai:** Requisito de segurança de identidade (MFA por local, só dispositivo gerenciado, login arriscado).
Como resolver: Identifique o sinal (local, dispositivo, risco) e o controle (MFA, conformidade, troca de senha); quase sempre é acesso condicional, salvo empresa sem P1 (padrões de segurança).

📝 **Como cai:** Pergunta sobre princípio de segurança (Confiança Zero, privilégio mínimo) com alternativas de perímetro.
Como resolver: Elimine tudo que confia na rede interna, dá funções permanentes ou compartilha contas; fique com a avaliação contínua e o acesso mínimo e temporário.

📝 **Como cai:** Ameaça descrita (anexo, link no clique, representação, AD local, app não autorizado) pedindo o produto do Defender.
Como resolver: Mapeie o vetor ao componente: anexo isolado = Anexos Seguros; clique = Links Seguros; nome parecido = antiphishing com representação; AD local = Defender para Identidade; TI invisível = Defender for Cloud Apps.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
e-mail, calendário e site de arquivos criados juntos	**Grupo do Microsoft 365**
várias pessoas leem e respondem suporte@ sem licença	**Caixa de correio compartilhada**

reservar sala ou projetor pelo Outlook	**Caixa de recurso (sala ou equipamento)**
externo só no catálogo de endereços, sem conta	**Contato de email**
grupo cujos membros entram e saem sozinhos pelo departamento ou cargo	**Associação dinâmica (exige Entra ID P1)**
e-mail para todos de uma cidade, sem manutenção manual	**Grupo de distribuição dinâmico**
navegação e pesquisa comuns entre sites de departamentos	**Site hub**
publicar notícias para toda a empresa com poucos autores	**Site de comunicação**
função de administrador por algumas horas, com aprovação	**PIM (just-in-time)**
por que o login foi bloqueado / qual política agiu	**Logs de entrada do Entra ID**
quem excluiu o arquivo / quem mudou a configuração de compartilhamento	**Log de auditoria do Microsoft Purview**
bloquear entradas de países sem operação	**Locais nomeados no acesso condicional**
exigir FIDO2 ou método resistente a phishing para administradores	**Força da autenticação**
primeiro dia, sem método de MFA, configurar conta sem senha	**Passe de Acesso Temporário (TAP)**
alertas de e-mail, identidade e notebook do mesmo ataque	**Incidente no Microsoft Defender XDR**

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

- Sem plano do Exchange na licença não existe caixa de correio; plano desmarcado tira só aquele serviço.
- O domínio onmicrosoft.com nunca é removido; o novo domínio é verificado no DNS e definido como padrão.
- Primeiro passo no desligamento é bloquear a entrada e revogar sessões, não excluir a conta.
- SMS é o MFA mais fraco; passkey, FIDO2 e Windows Hello for Business resistem a phishing.
- Quem não tem política do Teams atribuída recebe a política global.

Essenciais para a prova (checklist)

☐ Sei escolher entre lista de distribuição, distribuição dinâmica, grupo de segurança habilitado para e-mail e grupo do Microsoft 365.

☐ Sei quando usar caixa compartilhada, caixa de recurso (sala ou equipamento), arquivo morto e contato de email.

- ☐ Sei diferenciar Enviar como, Enviar em nome de e Acesso total.
- ☐ Sei os grupos padrão de um site e quando interromper a herança de permissões.
- ☐ Sei diferenciar equipe pública x privada, canal privado x compartilhado e acesso externo x convidado.
- ☐ Sei explicar os três princípios da Confiança Zero e o que cada um significa na prática.
- ☐ Sei configurar no acesso condicional locais nomeados, somente relatório, dispositivo em conformidade, risco e força da autenticação.
- ☐ Sei o que exige P1, o que exige P2 e o que os padrões de segurança fazem.
- ☐ Sei qual log usar: entrada, auditoria do Entra ou auditoria do Purview.
- ☐ Sei associar cada componente do Defender XDR à ameaça que ele trata.

Questões de revisão do capítulo

R3.1 · Identificar os principais recursos e objetos dos serviços do Microsoft 365

O que o PIM permite fazer para manter apenas as pessoas certas com funções privilegiadas ao longo do tempo?

A. Desativar os logs de auditoria dos administradores
B. Criar caixas compartilhadas para os administradores
C. Fazer revisões de acesso periódicas das funções
D. Atribuir funções permanentes aos técnicos do suporte

R3.2 · Identificar os principais recursos e objetos dos serviços do Microsoft 365

Um ex-funcionário recebia e-mails de clientes e a equipe precisa continuar acessando a caixa dele sem pagar licença. O que fazer?

A. Manter a conta ativa com a mesma licença
B. Converter a caixa em caixa compartilhada
C. Mover a caixa para um site de comunicação
D. Criar uma lista de distribuição com o nome

R3.3 · Identificar os principais recursos e objetos dos serviços do Microsoft 365

Na Confiança Zero, o que significa "verificar explicitamente"?

A. Confiar no acesso vindo da rede interna e das filiais da empresa
B. Avaliar identidade, dispositivo e local antes de cada acesso
C. Pedir a senha só no primeiro login do funcionário
D. Bloquear o acesso de dispositivos pessoais

R3.4 · Identificar os principais recursos e objetos dos serviços do Microsoft 365

Um usuário quer compartilhar um arquivo do OneDrive só com dois colegas, sem que outras pessoas consigam usar o link. Qual tipo de link escolher?

A. Qualquer pessoa com o link
B. Pessoas com acesso existente
C. Pessoas da organização
D. Pessoas específicas

Respostas comentadas

R3.1. C) Fazer revisões de acesso periódicas das funções

Por quê: O PIM oferece ativação sob demanda, aprovação, justificativa, notificações e revisões de acesso.

✗ A) Incorreta. Reduz a visibilidade.
✗ B) Incorreta. Não revisa funções.
✗ D) Incorreta. Aumenta o risco.

> **Dica de prova:** Manter funções certas: revisões de acesso no PIM.

R3.2. B) Converter a caixa em caixa compartilhada

Por quê: Converter em caixa compartilhada preserva o conteúdo e permite dar acesso aos colegas, dentro do limite sem licença.

✗ A) Incorreta. Gera custo desnecessário.
✗ C) Incorreta. Não é possível.
✗ D) Incorreta. Não preserva os e-mails antigos.

> **Dica de prova:** Caixa de ex-funcionário sem licença: converter em compartilhada.

R3.3. B) Avaliar identidade, dispositivo e local antes de cada acesso

Por quê: Verificar explicitamente é autenticar e autorizar com base em todos os sinais disponíveis, como risco e conformidade do dispositivo.

✗ A) Incorreta. É o modelo de perímetro antigo.
✗ C) Incorreta. Não verifica de forma contínua.
✗ D) Incorreta. Não é o significado do princípio.

> **Dica de prova:** Verificar explicitamente: avaliar todos os sinais.

R3.4. D) Pessoas específicas

Por quê: Links para pessoas específicas exigem que o destinatário entre com a conta autorizada.

✗ A) Incorreta. Funciona para quem tiver o link.
✗ B) Incorreta. Não concede acesso novo.
✗ C) Incorreta. Funciona para toda a empresa.

> **Dica de prova:** Compartilhar só com dois colegas: pessoas específicas.

DIA DA PROVA

Estratégia de prova

O AB-900 é um exame de fundamentos com questões curtas de cenário: descreve uma necessidade de negócio e pergunta qual recurso, objeto, portal ou ação resolve. Quase sempre há uma alternativa correta e três que pertencem a outro serviço (Exchange, Teams, Purview, Entra, DNS) ou que são desproporcionais, como excluir contas ou tirar licenças de todos. O peso maior está em proteção e governança de dados, com foco em como o Copilot respeita permissões e rótulos. Também aparecem questões de múltipla resposta (Escolha DUAS) e comparações diretas do tipo 'qual é a diferença entre A e B'.

Como responder

✓ Leia primeiro a última frase do enunciado para saber se pedem objeto, local de configuração, ação ou diferença; depois volte ao cenário.

✓ Destaque a palavra que define a necessidade (temporário, automaticamente, sem licença, só um grupo, sem manutenção manual): ela separa recursos vizinhos.

✓ Elimine primeiro as alternativas de outro serviço: caixa de recurso, regra de fluxo de e-mail, registro DNS e política de reunião raramente resolvem problema de Copilot ou de proteção de dados.

✓ Descarte medidas desproporcionais (excluir conta, apagar dados, tirar todas as licenças, desativar auditoria ou MFA); a prova premia a ação mínima e correta.

✓ Em questões 'Escolha DUAS', avalie cada alternativa isoladamente como verdadeiro ou falso antes de marcar.

✓ Com cerca de 50 questões em 45 minutos, mantenha ritmo de menos de 1 minuto por questão, marque as dúvidas e volte no fim.

✓ Quando a dúvida for sobre o Copilot ver algo, aplique a regra-mestra: ele só usa o que o usuário pode acessar agora e respeita rótulos e criptografia.

✓ Não deixe nenhuma em branco: a pontuação vai de 1 a 1000 e a aprovação exige 700, então cada acerto conta.

Erros que derrubam candidatos

✗ Achar que o Copilot cria acesso ou ignora rótulos, em vez de reconhecer o compartilhamento excessivo já existente.

✗ Confundir Gerenciador de conteúdo (onde) com Gerenciador de atividades (quem fez), e DLP (dado) com Conformidade de Comunicações (conduta).

✗ Tratar restrições temporárias (Descoberta restrita, Pesquisa Restrita) como solução definitiva no lugar de corrigir permissões.

✗ Supor que usuário sem licença não tem nenhum Copilot ou que pode usar agentes com dados da empresa sem cobrança por uso.

✗ Trocar Researcher por Analyst e construtor de agentes por Copilot Studio.

✗ Misturar grupos e caixas do Exchange, canais do Teams e logs do Entra ID e do Purview.

✗ Errar o princípio de IA responsável por confundir transparência (explicar) com responsabilidade (responder e revisar) e confiabilidade (não causar dano) com privacidade (proteger dados).

Na semana da prova

- ☐ Releia as comparações e pegadinhas dos três capítulos, começando por proteção e governança, que tem o maior peso.
- ☐ Refaça as provas práticas sob tempo (45 minutos) e anote cada erro em uma lista de pares confundidos.
- ☐ Revise os macetes de IA responsável, Confiança Zero, retenção e grupos do site até saber de cor.
- ☐ Na véspera, revise só os itens 'lembrar' e o checklist; nada de conteúdo novo.
- ☐ Explore a área restrita do exame para conhecer a interface e, se o exame não estiver no seu idioma preferencial, solicite os 30 minutos adicionais.

REVISÃO FINAL

Folha de cola

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

1. Entender a proteção e a governança de dados para o Microsoft 365 e o Copilot

‣ funcionário em desligamento levando dados → **Risco Interno: roubo de dados por usuários que estão saindo**

‣ quais apps de IA são usados e dados sensíveis em prompts → **DSPM para IA**

‣ esconder um site do Copilot por enquanto → **Descoberta de Conteúdo Restrita**

‣ só um grupo acessa o site, mesmo com link → **Controle de acesso restrito (SAM)**

‣ Copilot só com sites aprovados enquanto revisa permissões → **Pesquisa Restrita do SharePoint**

⚠ Ele age com as permissões do usuário e respeita rótulos; o usuário já tinha permissão, mesmo sem saber.

⚠ A primeira ação é corrigir as permissões e remover acessos amplos; recursos de restrição são temporários.

⚠ Gerenciador de Conformidade avalia controles regulatórios; quem analisa prompts e respostas é a Conformidade de Comunicações.

2. Executar tarefas administrativas básicas para o Copilot e os agentes

‣ desligar a pesquisa na web ou um recurso do Copilot sem tirar licença → **Configurações do Copilot no centro de administração**

‣ Copilot Chat fixado no Teams e no Outlook para todos → **Fixar o Copilot Chat pelo centro de administração**

‣ planilha, CSV, previsão, Python, gráficos → **Analyst (Analista)**

‣ relatório aprofundado com web, e-mails, reuniões e citações → **Researcher (Pesquisador)**

‣ usuários sem licença usando agentes, pagar só pelo consumo → **Política de cobrança conforme o uso ligada ao Azure**

⚠ Copilot Chat está disponível sem licença, com a conta corporativa e base na web; a licença traz os dados de trabalho nos apps.

⚠ Perde só os recursos licenciados e mantém o Copilot Chat; outros serviços não mudam.

⚠ Sem licença e sem política de cobrança por uso, agentes com dados do locatário ficam indisponíveis.

3. Identificar os principais recursos e objetos dos serviços do Microsoft 365

‣ e-mail, calendário e site de arquivos criados juntos → **Grupo do Microsoft 365**

‣ várias pessoas leem e respondem suporte@ sem licença → **Caixa de correio compartilhada**

‣ reservar sala ou projetor pelo Outlook → **Caixa de recurso (sala ou equipamento)**

‣ externo só no catálogo de endereços, sem conta → **Contato de email**

‣ grupo cujos membros entram e saem sozinhos pelo departamento ou cargo → **Associação dinâmica (exige Entra ID P1)**

⚠ Sem caixa de correio é licença sem o plano do Exchange Online; a licença é que cria a caixa.

⚠ Item desmarcado na licença é plano de serviço desativado; domínio não verificado não bloquearia só o Teams.

⚠ Converter em caixa compartilhada preserva o conteúdo e dá acesso aos colegas sem licença, dentro do limite padrão.

GABARITO

Respostas do diagnóstico

D1. B) Avaliações de risco de dados → revise o capítulo 1

Por quê: As avaliações de risco de dados identificam itens sensíveis com acesso amplo e recomendam ações, como restringir ou rotular.

✗ A) Incorreta. Não avaliam sites.
✗ C) Incorreta. Não avaliam sites.
✗ D) Incorreta. Não avaliam sites.

> **Dica de prova:** Sites sensíveis e expostos: avaliação de risco de dados.

D2. C) Uma cópia é mantida na biblioteca de retenção → revise o capítulo 1

Por quê: No SharePoint e no OneDrive, a biblioteca de retenção para preservação guarda cópias de itens excluídos ou alterados.

✗ A) Incorreta. A retenção impede a perda.
✗ B) Incorreta. Não é o efeito.
✗ D) Incorreta. Não é o efeito.

> **Dica de prova:** Excluiu item retido: biblioteca de retenção.

D3. D) Política de controle de acesso restrito do site → revise o capítulo 1

Por quê: O controle de acesso restrito do SharePoint Advanced Management bloqueia quem não está no grupo definido, mesmo que tenha permissão em arquivos.

✗ A) Incorreta. Trata de guarda, não de acesso.
✗ B) Incorreta. Não controla o site.
✗ C) Incorreta. Não controla o site.

> **Dica de prova:** Só um grupo acessa o site: acesso restrito.

D4. A) Na galeria de prompts do Copilot → revise o capítulo 2

Por quê: A galeria de prompts reúne prompts salvos pelo usuário, compartilhados pela equipe e sugeridos pela Microsoft.

✗ B) Incorreta. Registra eventos, não prompts salvos.
✗ C) Incorreta. Tratam de e-mail.
✗ D) Incorreta. Mostra totais de uso.

> **Dica de prova:** Prompt salvo: galeria de prompts.

D5. C) Usuários ativos, sessões e tendências de uso do agente → revise o capítulo 2

Por quê: Relatórios de agentes mostram uso, usuários e tendências para apoiar decisões de ciclo de vida.

✗ A) Incorreta. Não é o objetivo.
✗ B) Incorreta. Não é exibido.
✗ D) Incorreta. Não são exibidos.

> **Dica de prova:** Insights do agente: uso e tendências.

D6. C) Resumir uma conversa longa de e-mails → revise o capítulo 2

Por quê: No Outlook, o Copilot resume conversas, redige respostas e ajuda a preparar reuniões.

✗ A) Incorreta. É tarefa do Purview.
✗ B) Incorreta. É tarefa administrativa.
✗ D) Incorreta. É tarefa do Entra ID.

> **Dica de prova:** Copilot no Outlook: resumir conversas.

D7. A) Uma caixa de correio de recurso para a sala → revise o capítulo 3

Por quê: Caixas de recurso representam salas e equipamentos e podem aceitar reservas automaticamente conforme regras.

✗ B) Incorreta. Não agenda salas.
✗ C) Incorreta. Não é necessário.
✗ D) Incorreta. Não agenda salas.

> **Dica de prova:** Reservar sala: caixa de correio de recurso.

D8. B) A licença dele não inclui o Exchange Online → revise o capítulo 3

Por quê: Cada licença traz um conjunto de serviços; sem o plano do Exchange Online, a caixa de correio não é criada.

✗ A) Incorreta. Não impede a caixa de correio.
✗ C) Incorreta. Não afeta o e-mail.
✗ D) Incorreta. Não afeta o e-mail.

> **Dica de prova:** Sem caixa de correio: licença sem Exchange.

D9. B) Conceder a um usuário a permissão de editar um site → revise o capítulo 3

Por quê: Autenticação comprova quem é a pessoa; autorização define a que recursos ela tem acesso.

✗ A) Incorreta. Comprova a identidade.
✗ C) Incorreta. Comprova a identidade.
✗ D) Incorreta. Comprova a identidade.

> **Dica de prova:** Autorização: o que o usuário pode fazer.

Agora, treine no formato real

Faça as 6 provas completas do curso AB-900: 300 questões inéditas, tempo do exame, explicação de cada alternativa e link da documentação para revisar.

Ver as 6 provas completas e o cupom do mês →

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

Instagram @strecht.simulados

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

Seguir no Instagram →

YouTube Strecht Simulados

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

Inscrever-se no canal →

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