

Guia de preparação SC-401

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 SC-401: 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. Gerenciar riscos, alertas e atividades	30-35%	18 conceitos · 14 pegadinhas
2. Implementar a prevenção contra perda de dados e a retenção	30-35%	18 conceitos · 14 pegadinhas
3. Implementar a proteção de informações	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 · Gerenciar riscos, alertas e atividades

A analista de DLP da Distribuidora Vale Sul já acessa o painel de alertas de DLP no Purview, mas não consegue ver a prévia do conteúdo nem o conteúdo sensível correspondente nos alertas. O que falta?

A. Ser membro do grupo de funções Content Explorer Content Viewer
B. Ter a licença do Audit (Premium) com o app de auditoria avançada
C. Ter a função Manage alerts no portal do Microsoft Defender XDR
D. Ser membro do grupo de funções Insider Risk Management Investigators

D2 · Gerenciar riscos, alertas e atividades

A TI da Agência de Seguros Escudo vai habilitar a evidência forense da gestão de risco interno. Quais requisitos nos dispositivos e quais prazos a documentação informa?

A. Dispositivos com o cliente do Information Protection; a política e os clipes valem na hora
B. Dispositivos integrados com o Purview Client; até 2 horas para a política e 1 hora por clipe
C. Dispositivos com macOS ou Windows; até 24 horas para a política e 7 dias para cada clipe
D. Dispositivos com o Defender for Endpoint apenas; os clipes ficam visíveis em até 30 dias

D3 · Gerenciar riscos, alertas e atividades

Na Rede de Óticas Ver Bem, o auditor quer investigar acessos ao SharePoint ocorridos há dez meses. Os usuários envolvidos têm licença E3, sem complementos. O que ele encontrará no Audit?

A. Os registros completos, porque o Audit (Standard) guarda tudo por dez anos
B. Os registros completos, porque o SharePoint é retido por um ano para todos
C. Só os registros exportados para CSV, que o Audit mantém por um ano
D. Nada desse período, porque registros de usuários sem E5 ficam 180 dias

D4 · Implementar a prevenção contra perda de dados e a retenção

Na Corretora Imobiliária Porta Aberta, uma política de DLP para SharePoint e OneDrive deve impedir que convidados externos acessem documentos com dados bancários, sem afetar os usuários internos. Qual opção da ação Restrict access or encrypt the content in Microsoft 365 locations usar?

A. Block everyone, mantendo o acesso dos membros internos do site
B. Block only people from outside your organization
C. Audit only, que bloqueia os convidados e registra o evento
D. Encrypt email messages, aplicada aos documentos do SharePoint

D5 · Implementar a prevenção contra perda de dados e a retenção

A administradora da Fintech Moeda Verde criou hoje um escopo adaptável de usuários pelo atributo de departamento e quer usá-lo numa política de retenção amanhã. Ela também quer delegar a outro colega a criação de escopos. O que a documentação orienta?

A. Usar o escopo após uma hora e dar ao colega o grupo de funções Information Protection Readers
B. Usar o escopo na hora, pois a consulta é imediata, e dar ao colega a função Organization Configuration
C. Aguardar 30 dias para o escopo ser validado e dar ao colega a função eDiscovery Administrator
D. Aguardar alguns dias, pois a consulta pode levar até cinco dias para popular, e dar a função Scope Manager

D6 · Implementar a prevenção contra perda de dados e a retenção

A Mineradora Serra Dourada precisa reter por dez anos os e-mails e os arquivos do OneDrive dos executivos. Novos executivos entram com frequência, e a TI não quer manter grupos nem URLs do OneDrive. Que tipo de escopo usar na política de retenção?

A. Um escopo estático para toda a organização, com exclusão dos não executivos
B. Um escopo estático com a lista atualizada de URLs do OneDrive de cada executivo
C. Um escopo de unidade administrativa criado no próprio assistente da política
D. Um escopo adaptável de usuários com a consulta pelo atributo de cargo do Entra

D7 · Implementar a proteção de informações

O administrador da Rede de Padarias Pão Quente alterou o rodapé do rótulo Interno, que já está publicado para todos os funcionários. Ele pergunta se precisa criar uma nova política e quando a mudança chega aos aplicativos.

A. Precisa republicar o rótulo numa política nova; a mudança chega na hora aos aplicativos
B. Precisa excluir e recriar o rótulo; a mudança chega em até 7 dias aos aplicativos
C. Não precisa de nova política; a mudança só vale depois de 30 dias para cada usuário
D. Não precisa de nova política, e a mudança leva até 24 horas para chegar aos apps

D8 · Implementar a proteção de informações

A Editora Páginas Abertas recebe currículos em inglês de candidatos de outros países e quer começar ainda hoje a rotulá-los automaticamente, sem tempo para separar amostras e treinar um modelo. Qual opção atende?

A. Um SIT de entidade nomeada criado a partir de um modelo de currículo em branco
B. Um SIT baseado em EDM com o arquivo de currículos como tabela de origem
C. Um classificador personalizado treinado com 10 currículos como amostra positiva
D. O classificador pré-treinado Resume, que já aparece com o status Ready to use

D9 · Implementar a proteção de informações

O Instituto de Pesquisa Terra Fértil quer criar um classificador treinável personalizado para relatórios de campo escritos em português, já que nenhum classificador pré-treinado atende. O que a documentação informa sobre essa ideia?

A. Classificadores personalizados aceitam qualquer idioma com OCR ativo
B. O suporte a classificadores treináveis personalizados é limitado ao inglês
C. Classificadores personalizados detectam o idioma e traduzem as amostras sozinhos
D. Classificadores personalizados exigem amostras em pelo menos três idiomas

01

CAPÍTULO 1 · 30-35% DA PROVA

Gerenciar riscos, alertas e atividades

Aqui eu preciso dominar a gestão de risco interno (funções, conectores, integrações, indicadores, modelos, prazos, evidência forense, Adaptive Protection, alertas, casos e avisos), a auditoria (Standard x Premium, retenção, pesquisa e exportação), os alertas de DLP no Purview e no Defender XDR, o eDiscovery e a proteção de dados usados por IA com DSPM para IA. A prova pergunta muito qual grupo de funções atende ao menor privilégio e quais prazos e limites valem (180 dias, um ano, 50 mil registros, 48 horas, 120 dias). Onde mais erro: confundir os seis grupos de funções do IRM, os conectores exigidos por modelo e os locais de DLP e retenção do Copilot. Também preciso separar o que impede o Copilot de usar conteúdo (DLP, VIEW e EXTRACT, Restricted Content Discovery) do que só guarda ou registra (retenção, auditoria).

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

Tópicos-chave

Grupos de funções da gestão de risco interno

Seis grupos: Insider Risk Management (tudo), Admins (configuram políticas e configurações, mas não abrem alertas e casos), Analysts (triam alertas e casos, sem evidência forense nem Content explorer do IRM), Investigators (investigam, veem capturas forenses e Content explorer), Auditors (veem e exportam o log de auditoria da solução) e Approvers (aprovam pedidos de captura forense). Configurar o Adaptive Protection exige Insider Risk Management ou Admins. Permissões levam até 30 minutos, e investigadores restritos por unidade administrativa só veem usuários incluídos diretamente, não via grupo.

Conectores do IRM

Conector de RH: CSV, app no Entra, conector no Purview e script agendado; importa desligamentos, mudanças de nível, avaliações e planos de melhoria, e vários conectores são somados. Patient data misuse exige conector de Healthcare e de RH; acesso físico exige Physical badging (JSON) com Priority physical assets. Insider Risk Indicators importa só detecções pré-processadas e agregadas em arquivo; sem RH, a alternativa é verificar a exclusão da conta no Microsoft Entra.

Integração com o Defender for Endpoint

Ative o recurso avançado Share endpoint alerts no Defender para enviar alertas ao Purview. Os modelos de violação de política de segurança exigem assinatura ativa do Defender for Endpoint e essa integração. Em Intelligent detections, escolha quais status de alerta do Defender importar.

Indicadores, gatilhos e reforços

Indicadores globais vêm desligados e precisam ser selecionados em Settings > Policy indicators; alguns só existem com cobrança pay-as-you-go. Indicadores de nuvem (Box, Dropbox, Amazon S3, Azure) exigem conectar os apps no Microsoft Defender. Risk score boosters elevam a pontuação por caso anterior confirmado e por desvio do padrão; priority user groups deixam a pontuação mais sensível e podem restringir a revisão a investigadores escolhidos.

Policy timeframes e Intelligent detections

Activation window vai até 30 dias e Past activity detection até 90 dias, contados a partir do evento disparador. Intelligent detections ajusta o volume de alertas para todas as políticas (Fewer: todos altos, menos médios, nenhum baixo; More: todos médios e altos e a maioria dos baixos), o mínimo de eventos diários para reforçar downloads incomuns, domínios e status de alertas do Defender. Analytics avalia riscos antes de criar políticas, com insights em até 48 horas.

Modelos de política e requisitos

Data theft by departing users usa RH ou exclusão da conta no Entra. Data leaks pode usar DLP como gatilho, mas só alertas com Incident reports de severidade High geram alertas no IRM. Security policy violations dependem do Defender for Endpoint. Risky AI usage exige extensão Microsoft Insider risk no Edge ou a do Purview no Chrome e ao menos um indicador de navegação; o conector de RH é opcional.

Privacidade no IRM

A pseudonimização vem ligada por padrão; com ela, o data risk graph não pode ser usado. Na exportação em CSV o pseudônimo é mantido; na exportação para eDiscovery e pela Office 365 Management Activity API, os nomes aparecem. Nomes em metadados de atividades e arquivos não são anonimizados.

Evidência forense

Vem desligada e usa autorização dupla: Insider Risk Management ou Admins criam pedidos, Insider Risk Management ou Approvers aprovam, e Investigators veem as capturas. Dispositivos Windows 10 e 11 Enterprise integrados ao Purview com o Microsoft Purview Client; até duas horas para a política valer e uma hora por clipe. Specific activities ou All activities (que permite excluir apps e sites); a captura contínua prevalece, e as configurações gerais são janela de captura (10 segundos a 5 minutos), limite diário de envio e cache offline.

Adaptive Protection

Níveis Elevated, Moderate e Minor (diferentes da severidade de alertas), atribuídos por padrão por 7 dias (configurável de 5 a 30). Past activity detection (5 a 30 dias) vale para níveis baseados em atividade diária; a expiração automática, ligada por padrão, encerra o nível quando o alerta associado é descartado (para manter o nível, desligue-a). Integra DLP, gestão do ciclo de vida de dados (preserva por 120 dias o que usuários Elevated excluem) e Conditional Access.

Alertas, casos e avisos do IRM

Status de alerta: Needs review, Confirmed, Dismissed e Resolved. Caso de engano sem risco se resolve como Benign; Confirmed policy violation reforça a pontuação futura. Avisos usam modelos com HTML (href só com aspas simples), vão só ao e-mail do usuário do caso e não fecham o caso; Escalate for investigation abre caso no eDiscovery (Premium).

Audit (Standard) x Audit (Premium)

Standard retém por 180 dias. Premium, para usuários com E5 e o app Microsoft 365 Advanced Auditing habilitado, retém por um ano os registros de Exchange, SharePoint, OneDrive e Entra ID (política padrão imutável), oferece insights como SearchQueryInitiatedExchange (habilitado com Set-Mailbox -AuditOwner) e permite até 10 anos com complemento. Registros de entidades não usuárias ficam um ano fixo; auditoria de caixas de correio já vem ligada.

Políticas de retenção de auditoria

Exigem Organization Configuration; até 50 por organização; usuários, tipos de registro e atividades (atividades só com um tipo de registro); conflito resolvido pela prioridade. Personalizada prevalece sobre a padrão, mesmo mais curta. Durações de 7 e 30 dias exigem E5; 3, 5, 7 e 10 anos exigem o complemento de 10 anos.

Pesquisa e acesso ao log de auditoria

Nos serviços principais, registros aparecem em 60 a 90 minutos; a pesquisa continua com o navegador fechado, pode levar até 48 horas e os trabalhos ficam 30 dias. Exportação: 50 mil registros (Standard) ou 1 milhão (Premium), com Power Query para separar AuditData. Por script, Get/Set-AdminAuditLogConfig e Search-UnifiedAuditLog no Exchange Online PowerShell; para SIEM, Office 365 Management Activity API. Audit Reader só pesquisa e exporta; Audit Manager também liga e desliga; Power BI exige habilitar a auditoria no admin do Power BI.

Alertas de DLP no Purview e no Defender XDR

O ciclo tem seis etapas: disparar, notificar, triar, investigar, remediar e ajustar; o painel de DLP guarda alertas por 30 dias e o Defender, incidentes por seis meses. Alertas agregados por limiar exigem E5 ou complemento, e alertas podem levar até 3 horas para começar. No Defender, função personalizada com Manage Alerts e View-Only DLP Compliance Management basta para investigar; unidades administrativas são respeitadas; com a regra interna de alert tuning, os sinais viram comportamentos em BehaviorInfo e BehaviorEntities.

eDiscovery

eDiscovery Manager acessa só os casos que criou; eDiscovery Administrator acessa todos e remove membros (só usuários individuais via Add-eDiscoveryCaseAdmin). Vários gerentes de uma vez: grupo de segurança habilitado para e-mail com Add-RoleGroupMember. Consultas usam UTC, não diferenciam maiúsculas, operadores (AND, OR, NOT, NEAR) em maiúsculas e palavra-chave vazia retorna tudo; no novo eDiscovery, a pesquisa de conteúdo fica dentro de um caso e estatísticas substituem coleções. Search And Purge exclui até 10 itens por caixa; User Data Search foi aposentada.

Copilot, rótulos e criptografia

Com criptografia, o Copilot só usa o conteúdo se o usuário tiver VIEW e EXTRACT (também em criptografia sem rótulo); S/MIME fica de fora e documentos com senha só se já abertos. A resposta exibe o rótulo de maior prioridade das fontes, e conteúdo novo herda esse rótulo com marcações. DLP no local Microsoft 365 Copilot and Copilot Chat bloqueia respostas a prompts com SITs, bloqueia só a pesquisa na Web (Performing Web Searches) ou impede uso de itens rotulados, com SIT e rótulo em regras separadas; a política padrão vem em simulação.

Retenção, auditoria e exclusão de interações de IA

Retenção de prompts e respostas: local Microsoft Copilot experiences; os dados ficam numa pasta oculta da caixa e, ao vencer, vão para SubstrateHolds. O Microsoft 365 Copilot já é auditado no Audit (Standard), com os recursos acessados; apps de IA de terceiros (AIAppInteraction) usam pay-as-you-go com 180 dias. Copilot no Fabric e Security Copilot precisam de política de coleta para guardar o texto.

DSPM para IA e oversharing

Pré-requisitos: auditoria ativa, licenças do Copilot para quem usa, dispositivos integrados ao Purview, extensão do navegador e pay-as-you-go para apps que não sejam o Microsoft 365 Copilot e o Facilitator. Cria políticas de um clique (descoberta: DLP em auditoria para colar dados em sites de IA e risco interno para visitas) e avaliação semanal de risco dos 100 sites mais usados; a solução convergiu num DSPM único (versão anterior como classic). Funções: Purview Data Security AI Viewer só leitura; AI Content Viewer vê interações. No SharePoint: relatórios de Data access governance, site access reviews, Restricted Content Discovery (some da pesquisa e do Copilot sem mudar permissões) e Restricted site access control (só o grupo de controle acessa).

Macetes para memorizar

Grupos do IRM

Admin configura, Analyst tria, Investigator investiga (vê o vídeo), Auditor audita o log, Approver aprova o vídeo.

Retenção do Audit

180 dias para todos, 1 ano com E5, 10 anos com complemento; não usuário fica 1 ano fixo.

Exportação do Audit

Standard 50 mil, Premium 1 milhão; AuditData se abre no Power Query.

Policy timeframes

Olha 90 para trás, acompanha 30 para frente.

Copilot e criptografia

Sem VIEW e EXTRACT, o Copilot não vê; o rótulo da resposta é o mais alto das fontes.

Pseudônimo do IRM

CSV esconde; eDiscovery e API revelam.

Alertas de DLP

6 etapas, 3 horas para começar, 30 dias no painel, 6 meses no Defender.

Tabela de memorização: não confunda

Quando é...	...e quando é
Insider Risk Management Analysts Triar alertas e casos sem ver capturas forenses nem o Content explorer do IRM.	**Insider Risk Management Investigators** Investigar com acesso às capturas de evidência forense e ao Content explorer.
Audit Reader Só pesquisar e exportar o log de auditoria.	**Audit Manager** Também gerenciar configurações, como ligar e desligar o registro.
Restricted Content Discovery Tirar o site da pesquisa e das respostas do Copilot sem mudar permissões; quem tem acesso continua abrindo.	**Restricted site access control** Só membros do grupo de controle acessam o site, mesmo quem já tinha permissão ou link.
Resolver caso como Benign Engano sem intenção maliciosa e de baixo risco.	**Resolver como Confirmed policy violation** Caso arriscado, grave ou com intenção maliciosa; reforça a pontuação futura do usuário.
DLP no local Microsoft 365 Copilot and Copilot Chat Controlar o que o Microsoft 365 Copilot processa (prompts com SITs, pesquisa na Web, itens rotulados).	**Endpoint DLP com Adaptive Protection** Impedir que dados sejam colados em sites de IA de terceiros no navegador, com aviso ou bloqueio conforme o risco do usuário.

Exportação de alertas do IRM em CSV Mantém o pseudônimo dos usuários.	**Exportação para eDiscovery ou Management Activity API** Mostra os nomes reais, para manter a integridade referencial.
Política de retenção de auditoria personalizada Prazos e escopos próprios; prevalece sobre a padrão, mesmo mais curta; exige Organization Configuration.	**Política padrão do Audit (Premium)** Um ano para Exchange, SharePoint, OneDrive e Entra ID de usuários com E5; não pode ser alterada nem desligada.

Números que caem

Item	Valor
Audit (Standard)	**180 dias**
Audit (Premium) política padrão	**1 ano (Exchange, SharePoint, OneDrive, Entra ID; usuários com E5)**
Retenção máxima de auditoria	**10 anos com complemento**
Registros de entidades não usuárias	**1 ano fixo**
Políticas de retenção de auditoria	**até 50; 7 e 30 dias exigem E5**
Disponibilidade de registros (serviços principais)	**60 a 90 minutos**
Pesquisa de auditoria	**até 48 horas; trabalhos ficam 30 dias**
Exportação de auditoria	**50 mil (Standard) / 1 milhão (Premium)**
Management Activity API	**2.000 requisições por minuto iniciais**
Policy timeframes do IRM	**ativação até 30 dias; histórico até 90 dias**
Adaptive Protection	**nível por 7 dias padrão (5 a 30); exclusões de Elevated preservadas 120 dias**
Evidência forense	**até 2 horas para a política; 1 hora por clipe; janela de 10 segundos a 5 minutos; teste até 20 GB**
Analytics do IRM	**até 48 horas**
Permissões do IRM	**até 30 minutos para valer**
Alertas de DLP	**até 3 horas para começar; painel 30 dias; Defender 6 meses**
Search And Purge	**até 10 itens por caixa por vez**
Site access reviews pela interface	**até 100 sites**
Avaliação de risco do DSPM para IA	**semanal, 100 sites mais usados**
Auditoria de apps de IA de terceiros	**pay-as-you-go, 180 dias**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Dar Insider Risk Management Admins para quem precisa abrir alertas e casos.
Como não cair: Admins configuram, mas não acessam alertas e casos; triagem é Analysts e investigação com forense é Investigators.

⚠ **Alerta de prova:** Achar que o data risk graph mostra pseudônimos.
Como não cair: Com a pseudonimização ligada, o data risk graph não está disponível.

⚠ **Alerta de prova:** Usar o conector Insider Risk Indicators para eventos brutos de catraca ou do Salesforce.
Como não cair: Ele aceita só detecções pré-processadas e agregadas em arquivo; crachás usam Physical badging.

⚠ **Alerta de prova:** Achar que enviar um aviso pelo caso já o resolve, ou mandar o aviso ao gestor.
Como não cair: O aviso vai só ao usuário do caso e não fecha nada; para fechar, Resolve case.

⚠ **Alerta de prova:** Inverter Past activity detection e Activation window, ou usar valores acima do limite.
Como não cair: Histórico até 90 dias, ativação até 30 dias; no Adaptive Protection os prazos vão de 5 a 30 dias.

⚠ **Alerta de prova:** Achar que a política de DLP precisa estar em simulação ou bloquear para gerar alerta no IRM.
Como não cair: O requisito é Incident reports com severidade High; Low e Medium não geram alertas no IRM.

⚠ **Alerta de prova:** Esperar registros de dez meses atrás para usuários E3.
Como não cair: Sem E5, a auditoria guarda 180 dias; um ano exige E5 e dez anos, o complemento.

⚠ **Alerta de prova:** Rodar Get-AdminAuditLogConfig no Security & Compliance PowerShell.
Como não cair: Lá UnifiedAuditLogIngestionEnabled aparece sempre como False; use o Exchange Online PowerShell.

⚠ **Alerta de prova:** Achar que o Audit (Standard) não registra o Copilot ou que é preciso pay-as-you-go para isso.
Como não cair: O Microsoft 365 Copilot já é auditado no Standard; pay-as-you-go é para apps de IA de terceiros.

⚠ **Alerta de prova:** Colocar condição de SIT e de rótulo na mesma regra da DLP do Copilot.
Como não cair: Precisam ficar em regras diferentes da mesma política.

⚠ **Alerta de prova:** Usar retenção ou Restricted Content Discovery para impedir que dados sejam colados no ChatGPT.
Como não cair: Colar em sites de IA de terceiros se controla com Endpoint DLP (dispositivos integrados e extensão), opcionalmente com Adaptive Protection.

⚠ **Alerta de prova:** Adicionar grupo do Microsoft 365, lista de distribuição ou grupo via Add-eDiscoveryCaseAdmin para dar eDiscovery Manager em lote.
Como não cair: Use grupo de segurança habilitado para e-mail com Add-RoleGroupMember; Add-eDiscoveryCaseAdmin aceita só usuários.

⚠ **Alerta de prova:** Achar que a política de auditoria de maior duração ou a mais recente vence.
Como não cair: Entre políticas personalizadas vale a prioridade, e a personalizada vence a padrão.

⚠ **Alerta de prova:** Esperar alertas de DLP em minutos depois de mudar a regra, ou alertas agregados na E3.
Como não cair: Podem levar até 3 horas; alertas agregados por limiar exigem E5 ou complemento.

Como cai na prova

📝 **Como cai:** Pessoa precisa fazer X (triar, ver forense, auditar o log, configurar, aprovar) com menor privilégio.
Como resolver: Mapeie a tarefa ao grupo exato e descarte os amplos (Compliance Administrator, Global Administrator, Organization Management) e os que fazem mais do que o pedido.

📝 **Como cai:** Modelo de política do IRM não gera alertas ou não está disponível.
Como resolver: Cheque o requisito do modelo: conector (RH, Healthcare, badging), integração com Defender for Endpoint, extensão do navegador e indicador de navegação, severidade High na DLP gatilho, indicadores globais ligados.

📝 **Como cai:** Auditoria: o registro não aparece ou sumiu.
Como resolver: Verifique atraso (60 a 90 minutos), licença (180 dias sem E5), habilitação específica (Power BI, SearchQueryInitiatedExchange, app Advanced Auditing) e se a política personalizada tem prioridade.

📝 **Como cai:** Proteger dados usados pelo Copilot ou por IA de terceiros.
Como resolver: Separe objetivo: impedir processamento (DLP do local Copilot), impedir colar em site externo (Endpoint DLP), esconder site (Restricted Content Discovery), restringir acesso (Restricted site access control), guardar (retenção Copilot experiences), registrar (Audit/coleta).

📝 **Como cai:** Ciclo de vida de alertas de DLP e onde investigar.
Como resolver: Lembre as seis etapas, os prazos de retenção (30 dias e 6 meses), as funções mínimas no Defender e que unidades administrativas e alert tuning mudam o que aparece na fila.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Avaliar riscos antes de criar qualquer política	**Analytics do IRM (até 48 horas)**
Datas de desligamento vindas do RH	**Conector de RH (ou exclusão da conta no Entra como alternativa)**
Alertas do Defender for Endpoint no IRM	**Share endpoint alerts + Intelligent detections**
Nenhum usuário recebe pontuação	**Indicadores globais desligados em Policy indicators**
Clipes de tela de um usuário sob investigação	**Evidência forense com pedido e aprovação (Approvers)**
Manter o nível de risco mesmo com alerta descartado	**Desligar a expiração automática do Adaptive Protection**
Caso precisa de revisão jurídica com preservação	**Escalate for investigation (eDiscovery Premium)**
Termos pesquisados pela usuária na própria caixa	**SearchQueryInitiatedExchange via Set-Mailbox - AuditOwner (Audit Premium)**
Logs de auditoria no SIEM	**Office 365 Management Activity API**
Ver o conteúdo nos alertas de DLP	**Content Explorer Content Viewer**
Severidade de risco interno dentro do alerta de DLP	**Compartilhamento de dados (Data sharing) do IRM com Defender XDR e DLP**
Excluir um prompt sensível do Copilot	**eDiscovery com Search And Purge (10 itens por caixa)**
Sites com links Anyone e Everyone except external users antes do Copilot	**Relatórios de Data access governance e site access reviews**
Auditora vê relatórios do DSPM para IA sem criar políticas nem ler prompts	**Purview Data Security AI Viewer**

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

- IRM Admins configuram mas não veem alertas; Investigators veem forense; Approvers aprovam captura.
- DLP só vira gatilho do IRM com Incident reports de severidade High.
- Auditoria: 180 dias sem E5; personalizada vence a padrão; Organization Configuration cria as políticas.
- Copilot precisa de VIEW e EXTRACT; condição de SIT e de rótulo em regras separadas na DLP do Copilot.
- Restricted Content Discovery esconde sem mudar permissões; Restricted site access control muda o acesso.

Essenciais para a prova (checklist)

☐ Sei atribuir cada um dos seis grupos de funções do IRM pela tarefa pedida.

☐ Sei os conectores e integrações exigidos por modelo (RH, Healthcare, badging, Insider Risk Indicators, Defender for Endpoint).

☐ Sei configurar indicadores, policy timeframes, Intelligent detections, priority user groups e risk score boosters.

☐ Sei os requisitos e o fluxo de aprovação da evidência forense.

☐ Sei como o Adaptive Protection atribui, mantém e expira níveis e com quais soluções integra.

☐ Sei tratar alertas, casos, avisos e escalonamento no IRM e o efeito da pseudonimização nas exportações.

☐ Sei diferenciar Audit Standard e Premium, criar políticas de retenção de auditoria e pesquisar e exportar o log.

☐ Sei as funções, licenças e prazos dos alertas de DLP no Purview e no Defender XDR.

☐ Sei as funções e regras de consulta do eDiscovery.

☐ Sei proteger interações de IA com DLP, retenção, auditoria, DSPM para IA e recursos de oversharing do SharePoint.

Questões de revisão do capítulo

R1.1 · Gerenciar riscos, alertas e atividades

Os relatórios de Data access governance da Rede de Postos Combustível Bom mostraram 40 sites com links Anyone e conteúdo compartilhado com Everyone except external users. Por regras de conformidade, a TI não pode abrir os arquivos para avaliar cada caso. Como envolver quem conhece o conteúdo?

A. Iniciar site access reviews pelos relatórios, para os proprietários revisarem
B. Aplicar Restricted Content Discovery nos 40 sites até a TI revisar cada arquivo
C. Atribuir à TI o grupo Content Explorer Content viewer para revisar os arquivos
D. Criar uma política de retenção que exclua os links de compartilhamento dos sites

R1.2 · Gerenciar riscos, alertas e atividades

Um investigador da Seguradora Atalaia iniciou várias pesquisas no Audit e quer saber se pode fechar o navegador e por quanto tempo as pesquisas concluídas ficam disponíveis. Qual resposta está correta?

A. Não pode fechar; a pesquisa é pausada e retomada quando ele volta ao portal
B. Não pode fechar; a pesquisa é cancelada e as concluídas ficam por 24 horas
C. Pode fechar; a pesquisa continua, e as concluídas ficam disponíveis por 180 dias
D. Pode fechar; a pesquisa continua, e as concluídas ficam disponíveis por 30 dias

R1.3 · Gerenciar riscos, alertas e atividades

Na Distribuidora Ponto Final, uma política de risco interno deve olhar o histórico de atividades de até 90 dias antes do evento disparador e continuar avaliando o usuário por 30 dias depois dele. Quais valores de Policy timeframes atendem?

A. Past activity detection de 30 dias e Activation window de 90 dias
B. Activation window de 120 dias, que já inclui o histórico anterior
C. Past activity detection de 90 dias e Activation window de 30 dias
D. Past activity detection de 180 dias e Activation window de 60 dias

R1.4 · Gerenciar riscos, alertas e atividades

A Rede de Lojas Tech Plus quer criar uma política de risco interno do modelo Security policy violations, com alertas do Microsoft Defender for Endpoint sobre instalação de software malicioso e desvio de controles de segurança. O que habilitar no Defender?

A. A conexão com o Microsoft Intune para acesso condicional por risco do dispositivo
B. O recurso avançado Share endpoint alerts, que envia os alertas ao portal do Purview
C. O recurso avançado de automatic attack disruption para todos os dispositivos
D. O recurso avançado que permite executar scripts não assinados no live response

Respostas comentadas

R1.1. A) Iniciar site access reviews pelos relatórios, para os proprietários revisarem

Por quê: Site access reviews (SharePoint Advanced Management) podem ser iniciadas para até 100 sites pela interface dos relatórios, ou mais via PowerShell, para relatórios de links de compartilhamento, de Everyone except external users e de permissões (baseline de oversharing). Não suportam OneDrive.

✗ B) Incorreta. Restricted Content Discovery limita a descoberta na pesquisa e no Copilot, mas não resolve o oversharing nem envolve os proprietários.

✗ C) Incorreta. A premissa é que a TI não deve acessar detalhes de arquivos; além disso, o Content explorer não revisa links de compartilhamento.

✗ D) Incorreta. Retenção trata de guardar ou excluir conteúdo, não de revisar permissões e links.

> **Dica de prova:** Delegar a revisão de oversharing aos donos: site access review.

R1.2. D) Pode fechar; a pesquisa continua, e as concluídas ficam disponíveis por 30 dias

Por quê: Pesquisas amplas em locatários grandes podem levar até 48 horas. Para buscas por script, use Search-UnifiedAuditLog no Exchange Online PowerShell; para integração com SIEM, a Office 365 Management Activity API.

✗ A) Incorreta. A pesquisa não é pausada; continua rodando.

✗ B) Incorreta. A pesquisa não depende do navegador aberto.

✗ C) Incorreta. 180 dias é a retenção padrão de registros no Audit (Standard), não a guarda dos trabalhos de pesquisa.

> **Dica de prova:** Pesquisa do Audit: segue sem o navegador; trabalhos ficam 30 dias.

R1.3. C) Past activity detection de 90 dias e Activation window de 30 dias

Por quê: Os períodos começam a contar quando ocorre um evento disparador para um usuário incluído na política, mesmo que a política tenha sido criada meses antes. As configurações de risco interno valem para todas as políticas.

✗ A) Incorreta. Os valores estão trocados: a janela de ativação vai até 30 dias, e o histórico, até 90.

✗ B) Incorreta. A janela de ativação vai até 30 dias e não inclui o histórico anterior.

✗ D) Incorreta. Esses valores excedem os limites documentados (até 90 e até 30 dias).

> **Dica de prova:** Policy timeframes: histórico até 90 dias; ativação até 30 dias.

R1.4. B) O recurso avançado Share endpoint alerts, que envia os alertas ao portal do Purview

Por quê: Depois da integração, configure os indicadores do Defender for Endpoint nas configurações de risco interno e, em Intelligent detections, escolha quais status de alerta importar. Os modelos de violação de política de segurança dependem dessa integração.

✗ A) Incorreta. A conexão com o Intune serve ao acesso condicional por risco do dispositivo.

✗ C) Incorreta. A interrupção automática de ataques contém ativos comprometidos; não envia alertas à gestão de risco interno.

✗ D) Incorreta. Scripts não assinados no live response não têm relação com a gestão de risco interno.

> **Dica de prova:** Alertas do Defender for Endpoint no IRM: recurso avançado Share endpoint alerts.

02

CAPÍTULO 2 · 30-35% DA PROVA

Implementar a prevenção contra perda de dados e a retenção

Aqui eu preciso desenhar e implantar DLP (intenção, locais, condições, ações, simulação e precedência), configurar o Endpoint DLP com suas configurações globais e grupos de autorização, ligar o Adaptive Protection e entender as políticas de arquivo do Defender for Cloud Apps. Na retenção, a prova cobra a diferença entre política e rótulo, escopos adaptáveis, aplicação automática, princípios de retenção, registros, disposição, Preservation Lock e recuperação de conteúdo retido (caixas inativas, Recoverable Items, Preservation Hold library). Os enunciados são longos e com detalhes que eliminam alternativas: local onde a condição existe, se a ação bloqueia ou só audita, qual prazo vale. Onde mais erro: precedência entre políticas de DLP (soma das mais restritivas x prioridade) e a ordem dos princípios de retenção. Também tropeço nas configurações do Endpoint DLP que parecem iguais (service domains, sensitive service domain groups, network share groups, restricted apps).

Neste capítulo

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

Tópicos-chave

Desenho e planejamento de DLP

Comece envolvendo partes interessadas (conformidade, risco, jurídico, segurança, donos de dados, usuários, TI) e descrevendo as categorias de informação sensível: financeira, médica e de saúde, privacidade e personalizada. O primeiro passo do desenho é a declaração de intenção da política, mapeada para o que monitorar (modelo ou SITs), onde (locais), condições (confiança e contagem de instâncias, a tolerância a vazamento) e ações. A implantação é incremental, começando pela simulação.

Modo de simulação de DLP

Substitui os antigos estados de teste: roda como se a política estivesse imposta, sem impor, com painel próprio. No SharePoint e no OneDrive avalia itens existentes e novos; no Exchange, só novos. Roda por até 15 dias, e os dados ficam 30 dias; com dicas ligadas, Block e Block with override viram Block with override, e sem dicas viram Audit. Para ajustar política em produção: copie como v2, simule a v2 e depois troque.

Locais de DLP

Exchange, SharePoint, OneDrive, Teams, aplicativos do Office, dispositivos Windows e macOS, apps de nuvem e conectados de terceiros (Instances), repositórios locais (exigem o scanner do Information Protection), workspaces do Fabric e do Power BI e Microsoft 365 Copilot. Para tráfego web inline há DLP no Edge for Business e Network Data Security. No Power BI, a avaliação ocorre ao publicar, republicar e atualizar, exceto eventos de entidades de serviço.

Ações, condições e notificações

Restrict access or encrypt the content in Microsoft 365 locations: Block everyone (fica só dono, último modificador e admin do site), Block only people from outside your organization e, no Exchange, Encrypt email messages. Content is shared from Microsoft 365 with people outside my organization limita ao compartilhamento externo. If there's a match for this rule, stop processing additional DLP policies and rules interrompe a avaliação; e-mail personalizado de notificação vale para Exchange, SharePoint e OneDrive, e alerta, relatório e notificação saem uma vez por documento.

Precedência de DLP

Ações idênticas em várias políticas: vale a de maior prioridade; imposta vence simulação. Ações diferentes: soma das mais restritivas, atividade por atividade. Na substituição, No override vence Allow override. Entre regras correspondentes, vale a mais restritiva (no Activity explorer, eventos de endpoint mostram só a regra mais restritiva).

Funções e escopo administrativo de DLP

Criar e implantar políticas: grupo Information Protection Admins ou função DLP Compliance Management. Administrador restrito escolhe só entre as unidades administrativas atribuídas a ele; Full directory é para quem não tem restrição. O gerenciamento de dispositivos (integração) usa só funções do Entra, como Security admin e Compliance admin; funções do Purview não são suportadas ali.

Adaptive Protection na DLP

A condição de nível de risco (Elevated, Moderate, Minor, definidos na gestão de risco interno) existe em Exchange Online, Teams e dispositivos, e a regra se ajusta sozinha quando o risco do usuário muda. A configuração rápida cria políticas para Teams e Exchange e para dispositivos, em simulação; a regra de risco elevado bloqueia só pessoas de fora e avisa com dica, a de moderado e menor só notifica e gera relatório. Em dispositivos, exige Advanced classification ou a condição File type is.

Integração e requisitos do Endpoint DLP

Dispositivos já integrados ao Defender for Endpoint aparecem sem nova etapa; outros métodos: Group Policy, Configuration Manager, Intune, script local e VDI. macOS: só as três versões mais recentes, e com Advanced classification suporta fingerprint, EDM, classificadores e entidades nomeadas. Servidores: Windows Server 2019 ou posterior, sem controlador de domínio nem Server Core, e é preciso habilitar o Endpoint DLP para servidores.

Atividades e classificação no Endpoint DLP

Podem ser auditadas e restringidas: upload a domínio restrito, acesso por navegador não permitido, colar em navegadores, área de transferência, USB, compartilhamento de rede, impressão, Bluetooth e RDP; criar e renomear são só auditados. O Endpoint DLP classifica arquivos criados ou modificados no dispositivo, então arquivo nunca salvo localmente não é classificado. Copiar e colar dentro do mesmo arquivo é permitido; entre arquivos, bloqueado. Always audit file activity for devices registra eventos mesmo sem política.

Configurações do Endpoint DLP

Restricted apps (no Windows, só o nome do .exe), Unallowed browsers (usuário é mandado ao Edge; Windows pelo nome do executável, macOS pelo caminho completo), Service domains em Allow ou Block, Sensitive service domain groups (imprimir, copiar, salvar como, colar em sites específicos), grupos de autorização (Removable USB device groups, printer groups, network share groups) e exclusões de caminho. No Chrome, é preciso a extensão do Microsoft Purview.

Proteção just-in-time (JIT)

Atua em atividades de saída (USB, compartilhamento de rede, impressão, RDP, Bluetooth, upload a domínio restrito; área de transferência em auditoria) sobre arquivos nunca classificados ou classificados por versão antiga da política. Exige cliente antimalware 4.18.23080 ou posterior e ao menos uma hora para as mudanças; o fallback recomendado no início é Allow users to complete actions. Eventos aparecem no Activity explorer com JIT triggered igual a true.

DLP com Defender for Cloud Apps

Para apps de terceiros (Box, Dropbox, Google Workspace, Salesforce) conectados ao Defender for Cloud Apps, a política do Purview usa o local Instances (Specific instances para escolher um app), replicada no Defender for Cloud Apps. O local Instances e as file policies serão aposentados em 6 de janeiro de 2027; a migração usa o assistente DLP to Purview migration (inclui apps de terceiros, não vale para nuvens governamentais). Em file policies, Data Classification Service exige o conector Microsoft 365, a primeira file policy exige permissões de entidade de serviço do Entra e só a ação de governança da primeira política acionada é garantida.

Política x rótulo de retenção

Política aplica configurações ao contêiner (local inteiro ou parte), sem rótulo visível; um item pode estar sob várias políticas. Rótulo trata exceções e itens específicos, pode marcar registro e acionar revisão de disposição; um item tem só um rótulo por vez, não há prioridade entre rótulos de retenção e o existente não é trocado automaticamente. Rótulos são publicados para locais; itens de lista do SharePoint só aceitam rótulos, e pastas e bibliotecas como objetos não são retidas.

Escopos adaptáveis

Três tipos: Users (atributos do Entra, cobre caixas, OneDrive e chats do Teams), SharePoint sites (URL, nome, modelo e RefinableString00 a 99) e Microsoft 365 Groups. Não têm limite de itens por política, permitem mirar caixas inativas (IsInactiveMailbox) e são usados em retenção, rotulagem automática e Communication Compliance. A consulta pode levar até cinco dias para popular, criar escopos exige Scope Manager, pastas públicas exigem escopo estático e escopos adaptáveis não suportam Preservation Lock.

Aplicação de rótulos de retenção

Manual (rótulo publicado), aplicação automática (SITs, consulta KQL com propriedades como NOT(DocumentLink:), classificadores treináveis, anexos em nuvem), padrão de biblioteca ou pasta, modelo do Syntex, regras do Outlook e Power Automate. A simulação só existe para SIT e consulta, é opcional e os resultados expiram em sete dias. No Exchange, a condição de SIT vale só para e-mails em trânsito; ao ligar, só itens sem rótulo recebem o rótulo.

Princípios de retenção

Em ordem: retenção vence exclusão; o período de retenção mais longo vence; exclusão de rótulo vence exclusão de política; política com escopo específico vence a de toda a organização; por fim, a exclusão mais curta vence. Períodos nunca se somam. Atenção ao início da contagem (criação, modificação, rotulagem ou evento).

Registros, disposição e Preservation Lock

Registro regulatório aparece no assistente só após Set-RegulatoryComplianceUI -Enabled $true, não pode ser alterado nem por admins e não pode ser aplicado automaticamente. Revisão de disposição exige a função Disposition Management (global admin não tem por padrão). Preservation Lock é aplicado só por PowerShell (Set-RetentionCompliancePolicy -RestrictiveRetention $true): não desliga, não exclui, não remove locais, não reduz período; em política de rótulos, exige só rótulos de registro regulatório.

Onde o conteúdo retido fica e como recuperar

SharePoint e OneDrive: originais vão para a Preservation Hold library (conta na cota do site). Exchange: pasta Recoverable Items, limpa por timer job em até sete dias, em caixas com pelo menos 10 MB; itens purgados voltam com Restore-RecoverableItems ou Recover deleted items no EAC. Caixa inativa exige retenção antes de excluir a conta; recuperar cria caixa nova (a inativa some), restaurar mescla numa caixa existente (a inativa fica), e caixa inativa com arquivo morto de expansão automática não pode ser recuperada nem restaurada: só resta exportar pelo eDiscovery.

Macetes para memorizar

Princípios de retenção

RETÉM > MAIS LONGO > RÓTULO > ESPECÍFICO > MAIS CURTO: reter ganha, depois desempata.

Simulação de DLP

15 roda, 30 guarda; SharePoint e OneDrive olham o passado, Exchange só o futuro.

Precedência de DLP

Iguais? prioridade. Diferentes? soma do pior. Override? No override sempre.

Exclusão de caminho no Windows

Termina em \ só a pasta; termina em * só as subpastas; sem nada, pasta e subpastas.

Caixa inativa

Recuperar = renasce (nova caixa, a inativa some); Restaurar = empresta (mescla, a inativa fica).

Adaptive Protection na DLP

E-T-D: Exchange, Teams, Dispositivos.

Retenção no Exchange

7 e 10: até sete dias para aplicar e caixa com pelo menos 10 MB.

Tabela de memorização: não confunda

Quando é...	...e quando é
Política de retenção Configuração padrão para um local inteiro ou parte dele (por exemplo, excluir tudo do OneDrive após cinco anos).	**Rótulo de retenção** Exceção por item, decidida pelo usuário ou por condição, marcação de registro, revisão de disposição, itens de lista do SharePoint e retenção baseada em evento.
Escopo adaptável Público que muda por atributo (cargo, departamento), caixas inativas, sem manter listas nem URLs.	**Escopo estático** Local inteiro ou poucos itens fixos, pastas públicas do Exchange e quando é preciso Preservation Lock.
Recuperar caixa inativa Funcionário recontratado precisa de uma caixa ativa nova com todo o conteúdo; a inativa deixa de existir.	**Restaurar caixa inativa** Outra pessoa precisa acessar o conteúdo, que é mesclado numa caixa existente; a inativa continua preservada.
Service domains (Allow/Block) Controlar o upload de arquivos sensíveis para domínios; Allow com os aprovados evita listar milhares de serviços.	**Sensitive service domain groups** Controlar imprimir, copiar dados, salvar como e colar dados sensíveis em sites específicos, como um portal de parceiro.
Removable USB device groups / printer groups Liberar só discos USB ou impressoras específicas numa regra que bloqueia o resto.	**Network share groups** Liberar só um servidor de arquivos (caminho de rede) numa regra que bloqueia cópia para compartilhamentos.

Simulação de DLP Até 15 dias de execução e 30 dias de dados; SharePoint e OneDrive veem o existente, Exchange só o novo.	**Simulação de aplicação automática de rótulo de retenção** Opcional, resultados expiram em sete dias, só para SIT e consulta (não para classificador), e a política pode ser ligada durante a simulação.
Block everyone Bloquear todos, exceto dono, último modificador e administrador do site.	**Block only people from outside your organization** Bloquear só convidados e externos, sem afetar os usuários internos (no Power BI, Guest conta como externo).

Números que caem

Item	Valor
Execução da simulação de DLP / disponibilidade dos dados	**até 15 dias / 30 dias**
População da consulta de escopo adaptável	**até 5 dias**
Aplicação das configurações de retenção e de rótulos publicados	**até 7 dias**
Caixa do Exchange para retenção e rótulos	**pelo menos 10 MB**
Resultados da simulação de rótulo de retenção	**expiram em 7 dias**
Limites da simulação de rótulos de retenção	**30 trabalhos ativos em 12 horas; 100 amostras por caixa; 20.000 locais com escopo adaptável**
Propriedades personalizadas de escopo de sites	**RefinableString00 a 99**
Cliente antimalware para JIT / propagação	**4.18.23080 ou posterior / ao menos 1 hora**
Aposentadoria do local Instances e das file policies	**6 de janeiro de 2027**
Quarentena de administrador no Defender for Cloud Apps	**até 100 ações por dia**
Conta excluída recuperável sem retenção	**30 dias**
In-Place Holds	**sem novas desde julho de 2020**
Necessidades típicas de DLP	**cerca de 85% regulatórias e 15% propriedade intelectual**
macOS no Endpoint DLP	**três versões mais recentes**
Windows Server no Endpoint DLP	**2019 ou posterior**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Com duas políticas de Endpoint DLP com ações diferentes, aplicar só a de maior prioridade ou a mais recente.
Como não cair: Prioridade só desempata ações idênticas; com ações diferentes, cada atividade recebe a ação mais restritiva entre as políticas.

⚠ **Alerta de prova:** Achar que na retenção vale sempre o período mais longo, inclusive para excluir.
Como não cair: Mais longo vale para reter. Só com exclusões, vence o rótulo; entre políticas, a de escopo específico; por fim, a mais curta.

⚠ **Alerta de prova:** Somar períodos de retenção (5 + 10 = 15 anos).
Como não cair: Períodos nunca se somam; aplicam-se os princípios de retenção.

⚠ **Alerta de prova:** Dar Global Administrator ou Organization Configuration para revisar disposição.
Como não cair: Disposição exige Disposition Management; para ver o conteúdo no mini-preview, Content Explorer Content Viewer.

⚠ **Alerta de prova:** Procurar a opção Preservation Lock no assistente do portal ou usar escopo adaptável para travar a política.
Como não cair: Preservation Lock só por PowerShell (-RestrictiveRetention), não existe na interface e escopos adaptáveis não o suportam.

⚠ **Alerta de prova:** Usar o escopo adaptável no dia seguinte e delegar a criação com Organization Configuration.
Como não cair: A consulta leva até cinco dias para popular, e quem cria escopos precisa de Scope Manager.

⚠ **Alerta de prova:** Informar o caminho completo do .exe em Restricted apps no Windows.
Como não cair: No Windows, só o nome do executável (syncapp.exe); caminho completo é para Unallowed browsers no macOS.

⚠ **Alerta de prova:** Colocar o Edge em Unallowed browsers ou usar Network share groups para controlar um site.
Como não cair: O Edge é quem aplica os controles; site específico é Sensitive service domain groups, e network share é caminho de rede.

⚠ **Alerta de prova:** Integrar servidores de arquivos como dispositivos do Endpoint DLP ou conectá-los ao Defender for Cloud Apps para proteger compartilhamentos locais.
Como não cair: Repositórios locais usam o local On-premises repositories com o scanner do Information Protection implantado.

⚠ **Alerta de prova:** Criar retenção depois de excluir a conta, ou criar In-Place Hold, para gerar caixa inativa.
Como não cair: A retenção precisa estar na caixa antes da exclusão; In-Place Holds foram aposentadas e não podem ser criadas desde julho de 2020.

⚠ **Alerta de prova:** Achar que a DLP aplica rótulo de retenção ou bloqueia exclusão de registros.
Como não cair: Rótulos de retenção são aplicados por políticas de aplicação automática ou publicação; DLP não controla retenção.

⚠ **Alerta de prova:** Usar a condição de nível de risco do Adaptive Protection em SharePoint, Power BI ou Copilot.
Como não cair: A condição existe em Exchange Online, Teams e dispositivos.

⚠ **Alerta de prova:** Esperar que a política de retenção do Exchange limpe Recoverable Items em dois dias em qualquer caixa.
Como não cair: O timer job pode levar até sete dias, e a caixa precisa ter ao menos 10 MB.

⚠ **Alerta de prova:** Colocar a v1 em simulação por 90 dias ou editar a política em produção.
Como não cair: Simulação roda até 15 dias; o caminho documentado é copiar como v2, simular e depois trocar.

Como cai na prova

📝 **Como cai:** Várias políticas ou regras de DLP correspondem ao mesmo item com ações diferentes e o enunciado pede o resultado de cada atividade.
Como resolver: Liste a ação de cada política por atividade, aplique a mais restritiva em cada uma (nenhuma bloqueia = fica auditada) e só use prioridade se as ações forem idênticas.

📝 **Como cai:** Item sob duas políticas e/ou um rótulo com períodos e ações diferentes: quando é excluído?
Como resolver: Percorra os princípios em ordem: existe retenção? qual é a mais longa? há rótulo com exclusão? há política específica x da organização? só então a exclusão mais curta.

📝 **Como cai:** Cenário de Endpoint DLP com exceção (alguns USBs, uma impressora, um servidor, um site, um navegador).
Como resolver: Identifique o objeto da exceção e escolha o grupo de autorização correspondente; descarte exclusão de caminho e exceção por usuário, que não resolvem dispositivo específico.

📝 **Como cai:** Requisito de retenção com público dinâmico, caixas inativas ou exceção por documento.
Como resolver: Público dinâmico = escopo adaptável; padrão para todos + exceção do usuário = política + rótulo publicado; fato de negócio = rótulo baseado em evento.

📝 **Como cai:** Prazo ou pré-requisito: por que a política ainda não faz efeito?
Como resolver: Lembre os prazos: escopo adaptável até 5 dias; retenção até 7 dias; JIT 1 hora; simulação de rótulo expira em 7 dias; e verifique requisitos como extensão do Chrome, Advanced classification ou scanner.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Antes de abrir o assistente, ligar a política a uma necessidade de negócio	**Declaração de intenção da política**
Quantas ocorrências e com que certeza	**Nível de confiança e contagem de instâncias (tolerância a vazamento)**
Testar ajustes sem afetar usuários	**Modo de simulação (cópia v2)**
Período conta a partir da saída do funcionário ou fim de contrato	**Rótulo de retenção baseado em evento**
Ninguém, nem o admin global, pode reduzir ou desligar	**Preservation Lock por PowerShell**
Quais políticas de retenção se aplicam a um usuário ou site	**Policy lookup com e-mail ou URL exatos**
Política de retenção com erro de distribuição	**Set-RetentionCompliancePolicy -RetryDistribution**
Todo arquivo de uma biblioteca com o mesmo rótulo de retenção, sem inspecionar conteúdo	**Rótulo de retenção padrão da biblioteca**
Excluir uma biblioteca da aplicação automática por palavra-chave	**Consulta KQL com NOT(DocumentLink:)**
Upload só para domínios aprovados, sem listar milhares de serviços	**Service domains em Allow + upload em Block (e extensão do Purview no Chrome)**
Cópia completa do arquivo que correspondeu à DLP no notebook	**Coleta de evidências de dispositivos em armazenamento do Azure**

Arquivos de dispositivo criados e renomeados no Activity explorer sem política	**Always audit file activity for devices**
DLP só para um app de terceiros conectado	**Local Instances > Specific instances**
E-mail purgado pelo usuário precisa voltar à caixa	**Restore-RecoverableItems ou Recover deleted items no EAC**

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

- DLP com ações diferentes: soma das mais restritivas; ações iguais: prioridade; imposta vence simulação; No override vence.
- Retenção vence exclusão e os períodos nunca se somam.
- Um rótulo de retenção por item, sem prioridade; o existente não é trocado automaticamente.
- Condição do Adaptive Protection: Exchange Online, Teams e dispositivos.
- Preservation Lock só por PowerShell e irreversível; escopo adaptável não aceita.

Essenciais para a prova (checklist)

☐ Sei a sequência de planejamento e desenho de DLP (partes interessadas, categorias, intenção, mapeamento).

☐ Sei como a simulação de DLP se comporta por local, por quanto tempo roda e o que acontece com Block com e sem dicas.

☐ Sei aplicar a precedência de DLP entre regras, políticas, modos e opções de substituição.

☐ Sei os requisitos de integração do Endpoint DLP em Windows, macOS e servidores e as atividades bloqueáveis x só auditáveis.

☐ Sei escolher entre restricted apps, unallowed browsers, service domains, sensitive service domain groups, grupos de autorização e exclusões de caminho.

☐ Sei configurar JIT (candidatos, atividades, fallback, requisitos).

☐ Sei usar Instances, file policies e a migração para o Purview antes de 6 de janeiro de 2027.

☐ Sei quando usar política x rótulo de retenção, escopo adaptável x estático e como aplicar rótulos automaticamente.

☐ Sei resolver conflitos pelos princípios de retenção e explicar registros, disposição e Preservation Lock.

☐ Sei recuperar conteúdo retido: Preservation Hold library, Recoverable Items, caixas inativas e Policy lookup.

Questões de revisão do capítulo

R2.1 · Implementar a prevenção contra perda de dados e a retenção

A gestora de registros da Empresa de Auditoria Sigma precisa marcar documentos como registros regulatórios, mas a opção não aparece no assistente de rótulos de retenção do portal. O que fazer e qual consequência considerar?

A. Aplicar Preservation Lock à política de rótulos, o que exibe a opção no assistente
B. Atribuir a função Disposition Management; só o global admin vê essa opção no assistente
C. Executar Set-RegulatoryComplianceUI -Enabled $true; nem admins mudam o rótulo depois
D. Criar um rótulo de confidencialidade com criptografia, que equivale a registro regulatório

R2.2 · Implementar a prevenção contra perda de dados e a retenção

Na Agência de Viagens Mundo Livre, uma nova política de retenção para o Exchange foi aplicada há dois dias, mas itens expirados ainda não saíram da pasta Recoverable Items de algumas caixas pequenas. O que a documentação explica?

A. Itens em Recoverable Items só são excluídos após revisão de disposição manual
B. O timer job pode levar até sete dias, e a caixa precisa ter ao menos 10 MB
C. A pasta Recoverable Items é limpa ao reiniciar o Outlook do usuário
D. O timer job roda uma vez por mês e só em caixas com licença Audit (Premium)

R2.3 · Implementar a prevenção contra perda de dados e a retenção

Na Agência de Design Traço Livre, o administrador quer que o Endpoint DLP bloqueie o acesso de um aplicativo de sincronização não aprovado a arquivos protegidos. Ao configurar Restricted apps, ele digitou C:\Program Files\SyncApp\syncapp.exe. O que a documentação orienta?

A. Informar só o nome do executável, como syncapp.exe, sem o caminho no Windows
B. Informar o nome do processo pai que inicia o aplicativo de sincronização
C. Informar o hash SHA-256 do executável em vez do nome ou do caminho do aplicativo
D. Informar o caminho completo, porque o Windows exige a pasta de instalação

R2.4 · Implementar a prevenção contra perda de dados e a retenção

A gestora de registros da Companhia de Seguros Âmbar precisa revisar documentos com rótulos de retenção configurados para revisão de disposição. Ela é administradora global, mas não vê a página Disposition. Qual é o motivo e a solução recomendada?

A. A página só aparece depois que o rótulo vira registro regulatório, ativado por PowerShell
B. A revisão exige o grupo de funções Audit Manager e o app de auditoria habilitado
C. Global admin não tem Disposition Management por padrão; criar um grupo com essa função
D. A disposição só aparece para quem tem a função Organization Configuration ativa

Respostas comentadas

R2.1. C) Executar Set-RegulatoryComplianceUI -Enabled $true; nem admins mudam o rótulo depois

Por quê: Rótulos que marcam registros podem ser alterados ou removidos por administradores do contêiner; os de registro regulatório, não. Registros regulatórios não podem ser aplicados por políticas automáticas, só por publicação.

✗ A) Incorreta. O Preservation Lock é aplicado depois e exige rótulos de registro regulatório; não exibe a opção.

✗ B) Incorreta. A opção depende do cmdlet, não da função Disposition Management.

✗ D) Incorreta. Rótulos de confidencialidade não declaram registros.

> **Dica de prova:** Registro regulatório: Set-RegulatoryComplianceUI e restrições máximas.

R2.2. B) O timer job pode levar até sete dias, e a caixa precisa ter ao menos 10 MB

Por quê: Itens editados geram cópia do original em Recoverable Items antes da alteração. Itens sob revisão de disposição não são excluídos definitivamente até a confirmação, e outra retenção ou retenção de eDiscovery suspende a exclusão.

✗ A) Incorreta. Só itens configurados para revisão de disposição esperam a confirmação; os demais são excluídos pelo timer job.

✗ C) Incorreta. A limpeza é feita pelo serviço, não pelo cliente Outlook.

✗ D) Incorreta. O prazo documentado é de até sete dias, sem dependência de licença de auditoria.

> **Dica de prova:** Retenção no Exchange: timer job em até 7 dias; caixa com 10 MB ou mais.

R2.3. A) Informar só o nome do executável, como syncapp.exe, sem o caminho no Windows

Por quê: Restricted apps e restricted app groups definem ações (auditar, bloquear com substituição ou bloquear) quando um aplicativo da lista tenta acessar um arquivo protegido por DLP; a ação vale para a atividade Access by restricted apps na política.

✗ B) Incorreta. A configuração identifica o aplicativo pelo próprio executável.

✗ C) Incorreta. A lista de restricted apps usa o nome do executável.

✗ D) Incorreta. Incluir o caminho contraria a orientação para dispositivos Windows.

> **Dica de prova:** Restricted apps no Windows: só o nome do .exe.

R2.4. C) Global admin não tem Disposition Management por padrão; criar um grupo com essa função

Por quê: Para ver o conteúdo dos itens no mini-preview durante a disposição, adicione os revisores ao grupo Content Explorer Content Viewer. Por padrão, cada revisor vê só os itens atribuídos a ele.

✗ A) Incorreta. A revisão de disposição não depende de registros regulatórios.

✗ B) Incorreta. Audit Manager trata da auditoria; a disposição exige Disposition Management (e a auditoria habilitada).

✗ D) Incorreta. Organization Configuration não é a função de disposição.

> **Dica de prova:** Revisão de disposição: função Disposition Management (global admin não tem).

03

CAPÍTULO 3 · 30-35% DA PROVA

Implementar a proteção de informações

Aqui eu preciso dominar a escolha do classificador certo (SIT interno, SIT personalizado, EDM, fingerprint, entidade nomeada ou classificador treinável), a configuração de rótulos de confidencialidade (escopos, prioridade, políticas, criptografia, marcações, contêineres) e as ferramentas que estendem a proteção: cliente e scanner do Information Protection, Power BI, Defender for Cloud Apps e Message Encryption. A prova cobra muito cenário com cmdlet e parâmetro exato (Set-IRMConfiguration x Set-OMEConfiguration, Install-Scanner, Add-AipServiceSuperUser, Set-Label -LocaleSettings) e com limites numéricos (500 rótulos com criptografia do admin, 256 caracteres no fingerprint, 50 e 150 sementes). Onde mais erro: a ordem de prioridade dos rótulos (o último da lista é o mais forte), rotulagem automática no cliente x no serviço, rótulo padrão da política x da biblioteca e o que cada explorer mostra. Também confundo quem lê o conteúdo (Content viewer) com quem só vê a lista (List viewer).

Neste capítulo

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

Tópicos-chave

SIT interno e cópia (Copy)

Os tipos de informações confidenciais internos (como Brazil CPF Number e Brazil legal entity number para CNPJ) aparecem por padrão e não podem ser editados. Para adaptar um deles, use Copy e edite a cópia, que vira um SIT personalizado; os personalizados ficam no rule package Microsoft.SCCManaged.CustomRulePack. Identificador próprio da empresa com formato definido pede SIT personalizado.

Padrão de SIT personalizado

Cada padrão tem elemento primário (regex, keyword list ou keyword dictionary), elementos de suporte opcionais, nível de confiança (alto, médio, baixo) e proximidade de caracteres. Quanto mais evidência de suporte perto do primário, maior a confiança. A regex usa o motor Boost.RegEx 5.1.3, sem âncoras ^ e $, com exatamente um grupo de captura (alternância dentro dele) e até 1.024 caracteres.

Validador de checksum

Para identificadores com dígito verificador, combine a regex com o validador de checksum (Weights, Mod, CheckDigit e, se preciso, ModCoefficient). Se o dígito verificador não entra no cálculo, use peso 0 para ele. Validadores se aplicam a regex, não a keyword lists, e são o jeito de descartar números com formato certo mas inválidos.

Nível de confiança e contagem de instâncias

Na regra, confiança baixa retorna correspondências de confiança baixa, média e alta; confiança alta retorna só as altas. Alta confiança gera menos falsos positivos e mais falsos negativos. Instance count conta instâncias únicas: mínimo de 1 a 500 e máximo de 1 a 500 ou Any; para pelo menos N sem teto, mínimo N e máximo Any.

Keyword list x keyword dictionary

Keyword list aceita até 2.048 termos de até 50 caracteres cada. Keyword dictionary serve para milhares de termos, em qualquer idioma, até cerca de 1 milhão de caracteres (1 MB comprimido) somando os dicionários do locatário, e pode ser importado de arquivo. Lista enorme de termos em vários idiomas pede dicionário.

Document fingerprinting

Transforma o padrão de palavras de um formulário em hash usado como SIT; o original não é armazenado. O modelo precisa ter de 256 a 204.800 caracteres de texto extraído, e cada nível de confiança aceita correspondência parcial de 30% a 90% ou Exact (texto idêntico, no nível alto). Não detecta arquivos protegidos por senha, só com imagens, acima de 4 MB ou sem todo o texto do modelo; por script, use New-DlpSensitiveInformationType -FileData no Security & Compliance PowerShell.

SIT baseado em EDM (Exact Data Match)

Detecta valores exatos de uma base estruturada (clientes, pacientes, funcionários) com poucos falsos positivos. O esquema define DataStore, campos, quais são pesquisáveis e configurable match; a tabela de origem é convertida em hash com salt e enviada pelo EDM Upload Agent por conta do grupo EDM_DataUploaders, aceita até 100 milhões de linhas e pode ser atualizada diariamente. O campo primário precisa ser detectável por um SIT existente (por exemplo, CPF).

Nova experiência de EDM

Esquema e SIT são criados num só fluxo a partir de um arquivo de exemplo com os mesmos cabeçalhos da base e 10 a 20 linhas de dados fictícios no formato real. Esse arquivo não passa por hash, por isso nunca leva dados reais. O sistema recomenda SITs para os campos primários e gera regras de confiança alta e média.

SITs de entidade nomeada

Detectam nomes de pessoas, endereços físicos e termos médicos. Os agrupados (bundled, como All full names) são amplos; os não agrupados (unbundled) têm foco restrito, como um país. Não podem ser editados nem copiados, e o uso em Endpoint DLP exige Advanced classification scanning and protection.

Classificadores treináveis

Pré-treinados (Resume, Invoice, Agreements, Source code) já vêm Ready to use. Personalizados exigem de 50 a 500 positivos e de 150 a 1.500 negativos, em arquivos de texto, em pastas separadas e dedicadas de um site do SharePoint (não OneDrive nem pasta de Teams); site novo precisa de pelo menos uma hora de indexação. Têm suporte limitado ao inglês, não leem itens criptografados e, depois de publicados, não podem ser retreinados (exclua e recrie).

Data explorer, Content explorer e Activity explorer

Data explorer e Content explorer mostram um retrato dos itens com rótulos ou classificados; as contagens levam até 7 dias (14 no SharePoint), itens criptografados ficam sem prévia e sem download e a lista exporta em .csv. Ver a lista exige Content Explorer List viewer; ler o conteúdo, Content Explorer Content viewer (grupos independentes). O Activity explorer mostra atividades, lê o log de auditoria com atraso, cobre até 30 dias e tem filter sets prontos (como Endpoint DLP activities e Egress activities) ou salvos.

OCR no Purview

Recurso opcional: primeiro um administrador liga a assinatura Azure pay-as-you-go pela cobrança do Microsoft Syntex, depois o admin de conformidade escolhe locais em Settings > Optical character recognition (OCR). Cada imagem é uma transação e cada página de PDF conta à parte; a mesma imagem serve a várias políticas sem custo extra. Matriz: Exchange (DLP, rotulagem automática, retenção automática), SharePoint (DLP, risco interno, retenção automática), OneDrive (DLP, retenção automática), Teams (DLP, risco interno), dispositivos (DLP, risco interno).

Escopos e prioridade dos rótulos

Files & other data assets vem marcado por padrão; Meetings exige Files & other data assets e Emails juntos; Groups & sites só aparece depois de habilitar rótulos para grupos no Microsoft Entra ID e executar Execute-AzureAdLabelSync. Na lista, o primeiro rótulo é o de menor prioridade e o último, o de maior; essa ordem vale para justificativa de rebaixamento, rotulagem automática e Copilot. No esquema moderno, grupos de rótulos organizam (nome, descrição, cor, prioridade) mas não são publicados.

Políticas de rótulos

Definem usuários e grupos (ou unidades administrativas), rótulo padrão, rotulagem obrigatória, justificativa ao rebaixar (Require a justification) e link de ajuda. Entre políticas, vence a de maior número de ordem. Editar um rótulo publicado não exige republicar e leva até 24 horas para chegar aos apps; excluir um rótulo não retira rótulo nem proteção do conteúdo já rotulado.

Criptografia no rótulo

Assign permissions now: o admin define usuários (inclusive Any authenticated users), permissões, expiração e Allow offline access (Never, Always ou dias); há suporte a no máximo 500 rótulos assim por locatário. Let users assign permissions: Do Not Forward ou Encrypt-Only no Outlook e prompt nos apps do Office. Remove access control settings tira a criptografia existente; trocar criptografia exige Export ou Full Control.

Marcações e marca d'água dinâmica

Cabeçalho, rodapé e marca d'água aceitam variáveis; marca d'água vale para documentos, não para e-mails (até 255 caracteres; cabeçalho e rodapé até 1.024). A marca d'água dinâmica mostra quem está vendo e exige rótulo com criptografia. Rótulos de idiomas diferentes: Set-Label -LocaleSettings.

Rótulos para contêineres

No escopo Groups & sites, o rótulo controla privacidade, acesso de convidados, compartilhamento externo do site, acesso de dispositivos não gerenciados, contexto de autenticação do Conditional Access (por exemplo, MFA) e controles de equipes privadas e canais compartilhados (Internal only, Same label only, Private team only). Os arquivos dentro do contêiner não herdam o rótulo. O tipo de link padrão por rótulo é definido via PowerShell.

Message Encryption e Advanced Message Encryption

O Message Encryption usa o Azure Rights Management (não é compatível com AD RMS); valide com Get-IRMConfiguration (AzureRMSLicensingEnabled) e Test-IRMConfiguration -Sender -Recipient. O Advanced Message Encryption acrescenta vários modelos de marca (New-OMEConfiguration aplicados por mail flow rules), expiração externa (ExternalMailExpiryInDays de 1 a 730) e revogação (Get-OMEMessageStatus e Set-OMEMessageRevocation). Anexo do Office sem proteção herda a criptografia do e-mail, não o rótulo, e isso não pode ser desligado.

Macetes para memorizar

Prioridade de rótulos

Quem chega por último manda: o fim da lista é o rótulo mais forte, e a política de maior número de ordem vence.

Sementes do classificador

50 que são, 150 que não são, texto puro, pastas separadas no SharePoint e uma hora de espera.

Escolha do classificador

Formato = SIT; base exata = EDM; formulário = fingerprint; categoria de documento = classificador treinável; nome, endereço, termo médico = entidade nomeada.

Allow offline access

Never para o muito sensível, 7 dias para o sensível, Always para o resto.

Extensões do cliente

P na frente para texto e imagem (.ptxt, .ppng, .pjpg); .pfile para o resto (autentica, mas não impõe direitos); Office mantém a extensão.

IRM x OME

IRM cuida do remetente e do locatário (botão Encrypt, anexos, log do portal); OME cuida do destinatário no portal (login, OTP, marca).

Escopo Meetings

Reunião não anda sozinha: Meetings só com arquivos e e-mails marcados junto.

Tabela de memorização: não confunda

Quando é...	...e quando é
Rotulagem automática no rótulo (cliente) Quando a dica ou a recomendação deve aparecer enquanto o usuário edita no Word ou no Outlook; depende da versão do app, não tem simulação e não substitui rótulo manual.	**Política de rotulagem automática (serviço)** Quando é preciso rotular o que já está parado no SharePoint e no OneDrive ou e-mails em trânsito no Exchange, com simulação antes, sem recomendação ao usuário e podendo substituir rótulo manual de menor prioridade.
Rótulo padrão da política Para que todo documento novo ou editado sem rótulo saia com um rótulo em qualquer local; nunca substitui um rótulo existente.	**Rótulo padrão da biblioteca do SharePoint** Para rotular por local, só no SharePoint, sem inspecionar conteúdo; substitui rótulo de menor prioridade aplicado pela política ou automaticamente, mas nunca um rótulo manual.
SIT baseado em EDM Quando é preciso achar valores exatos de uma base estruturada (CPF de clientes reais, apólices) sem enviar os dados em texto claro.	**Document fingerprinting** Quando é preciso reconhecer um formulário ou modelo padronizado (procuração, bula, relatório) pelo padrão de palavras.

Content Explorer List viewer Quem precisa ver cada item e onde ele está, sem ler o conteúdo.	**Content Explorer Content viewer** Quem precisa abrir a prévia do conteúdo (inclusive no conteúdo dos alertas de DLP e no mini-preview da disposição).
Set-IRMConfiguration Botão Encrypt no Outlook na Web (SimplifiedClientAccessEnabled), anexos descriptografados no download em Encrypt-Only (DecryptAttachmentForEncryptOnly) e log de acesso ao portal (EnablePortalTrackingLogs).	**Set-OMEConfiguration** Experiência do portal e marca: SocialIdSignIn (contas Google, Yahoo, Microsoft), OTPEnabled (senha de uso único), logotipo, textos e expiração.
Encrypt-Only Destinatário pode encaminhar e imprimir, só não pode remover a criptografia.	**Do Not Forward** Impede encaminhar, imprimir e copiar.
Double Key Encryption Quando nem a Microsoft nem o serviço podem ler o conteúdo e uma chave fica só com o cliente; aceita perder coautoria, pesquisa e DLP nesses arquivos.	**Customer Key ou Assign permissions now** Quando os serviços precisam continuar processando o conteúdo (pesquisa, DLP, coautoria, Copilot).

Números que caem

Item	Valor
Rótulos com criptografia definida pelo administrador por locatário	**até 500**
Replicação de alteração de rótulo para os apps	**até 24 horas**
Sementes de classificador personalizado	**50 a 500 positivos e 150 a 1.500 negativos**
Espera de indexação de site novo de sementes	**pelo menos 1 hora**
Modelo de document fingerprinting	**256 a 204.800 caracteres de texto; arquivos acima de 4 MB não detectados**
Correspondência parcial do fingerprint	**30% a 90% (ou Exact)**
Rule pack de fingerprints	**até 300 KB (cerca de 100 fingerprints)**
Tabela de origem do EDM	**até 100 milhões de linhas, atualização diária**
Arquivo de exemplo do EDM	**10 a 20 linhas fictícias**
Keyword list	**até 2.048 termos de até 50 caracteres**
Keyword dictionaries	**cerca de 1 milhão de caracteres (1 MB comprimido) no locatário**
Regex de SIT	**até 1.024 caracteres**

Instance count	**mínimo 1 a 500; máximo 1 a 500 ou Any**
Marca d'água / cabeçalho e rodapé	**255 / 1.024 caracteres**
Activity explorer	**até 30 dias de dados**
Contagens do Data/Content explorer	**até 7 dias (14 no SharePoint)**
ExternalMailExpiryInDays (AME)	**1 a 730 dias**
Allow offline access Always	**abre por até 30 dias após perder o acesso**
Boa prática de quantidade de rótulos	**até 5 rótulos principais e até 5 sub-rótulos por principal**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Achar que o rótulo mais restritivo deve ficar no topo da lista de rótulos.
Como não cair: O primeiro da lista é o de menor prioridade; o mais restritivo vai para o fim. Na lista de políticas, também vence o maior número de ordem.

⚠ **Alerta de prova:** Achar que o anexo de um e-mail criptografado herda o rótulo do e-mail.
Como não cair: O anexo do Office sem proteção herda a criptografia, não o rótulo, e essa herança não pode ser desligada.

⚠ **Alerta de prova:** Treinar classificador personalizado com 10 exemplos, imagens digitalizadas ou pasta do OneDrive.
Como não cair: Mínimo de 50 positivos e 150 negativos, só arquivos de texto, em pastas separadas de um site do SharePoint.

⚠ **Alerta de prova:** Retreinar um classificador já publicado para melhorar a precisão.
Como não cair: Publicado não retreina: exclua e crie outro com mais amostras. Retreino só antes de publicar.

⚠ **Alerta de prova:** Colocar a analista no grupo definido por Set-AipServiceSuperUserGroup para abrir arquivos hoje.
Como não cair: A associação ao grupo fica em cache; para acesso imediato, Enable-AipServiceSuperUserFeature e Add-AipServiceSuperUser.

⚠ **Alerta de prova:** Usar marca d'água estática ou marca dinâmica sem criptografia para identificar quem vê.
Como não cair: Só a marca d'água dinâmica mostra quem está vendo, e ela exige rótulo com criptografia; para cópias baixadas pararem de abrir, offline Never.

⚠ **Alerta de prova:** Escolher Customer Key ou Assign permissions now quando nem a Microsoft pode acessar o conteúdo.
Como não cair: Chave exclusiva do cliente com serviço sem acesso é Double Key Encryption, com perda de coautoria, pesquisa e DLP.

⚠ **Alerta de prova:** Esperar que o rótulo de contêiner criptografe ou marque os arquivos do site.
Como não cair: Rótulo de Groups & sites controla o acesso ao espaço; os itens não herdam o rótulo.

⚠ **Alerta de prova:** Pedir uma política de rotulagem automática do Exchange que recomende o rótulo ao usuário.
Como não cair: Recomendação existe só na rotulagem automática do próprio rótulo (cliente); a política no serviço aplica sem interação.

⚠ **Alerta de prova:** Achar que o rótulo com criptografia no Power BI impede o acesso no serviço.
Como não cair: No serviço vale a permissão do workspace; a criptografia protege o que é exportado. No Power BI Desktop, a criptografia do .pbix controla quem abre.

⚠ **Alerta de prova:** Montar a regex do SIT com ^ e $ ou com vários grupos de captura separados por barra vertical.
Como não cair: Sem âncoras, com um único grupo de captura e a alternância dentro dele.

⚠ **Alerta de prova:** Instalar o scanner nas estações ou usá-lo para o SharePoint Online.
Como não cair: O scanner roda como serviço no Windows Server, com SQL Server, e varre compartilhamentos de rede e SharePoint Server.

⚠ **Alerta de prova:** Achar que o Message Encryption depende do Advanced Message Encryption ou do AD RMS.
Como não cair: O pré-requisito é o Azure Rights Management ativo; o AME só acrescenta marcas múltiplas, expiração e revogação.

⚠ **Alerta de prova:** Achar que excluir um rótulo remove a criptografia dos documentos.
Como não cair: O rótulo não é removido automaticamente e a proteção continua; editar o rótulo também não muda a versão já aplicada.

Como cai na prova

📝 **Como cai:** Cenário com requisito de detecção (base de clientes, formulário, identificador próprio) e quatro métodos de classificação.
Como resolver: Pergunte: é formato com padrão, valor exato de base, formulário ou categoria de documento? Depois verifique o detalhe que elimina (dados em texto claro, idioma, limite de 2.048 termos, 256 caracteres).

📝 **Como cai:** Rótulo não aparece ou não se comporta como esperado (contêiner, Meetings, prioridade, rebaixamento sem justificativa).
Como resolver: Cheque o pré-requisito de habilitação (Entra ID + Execute-AzureAdLabelSync, escopos combinados), depois a posição na lista e se a configuração é do rótulo ou da política.

📝 **Como cai:** Escolha do cmdlet ou parâmetro certo entre quatro parecidos (Message Encryption, scanner, superusuário).
Como resolver: Associe cada parâmetro ao seu efeito: SimplifiedClientAccessEnabled = botão Encrypt; SocialIdSignIn/OTPEnabled = login no portal; Install-Scanner = serviço e cluster; Set-Authentication = token; Add-AipServiceSuperUser = acesso imediato.

📝 **Como cai:** Conflito entre dois rótulos ou proteções (padrão da biblioteca x manual, rótulo automático x IRM de mail flow rule, Copilot com vários arquivos).
Como resolver: Aplique as regras fixas: manual não é sobrescrito pela biblioteca; rótulo com criptografia substitui o IRM da regra; conteúdo novo herda o rótulo de maior prioridade.

📝 **Como cai:** Ferramenta de visibilidade: explorer vazio, contagens atrasadas, item sem prévia.
Como resolver: Activity explorer = atividades, até 30 dias, com atraso do log; Data/Content explorer = retrato, até 7 dias (14 no SharePoint); criptografado fica sem prévia e sem download.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Valores exatos de uma base, sem enviar em texto claro, conta de serviço para upload diário	**SIT baseado em EDM com EDM Upload Agent, hash com salt e grupo EDM_DataUploaders**
Formulário ou modelo padronizado da empresa (procuração, bula, relatório)	**Document fingerprinting**
Começar hoje, sem tempo de treinar, categoria comum como currículos ou faturas	**Classificador pré-treinado Ready to use**
Número com dígito verificador e falsos positivos com CEP e telefone	**Regex com validador de checksum e palavra-chave como suporte**
Ver o item e o local, sem ler o conteúdo	**Content Explorer List viewer**

Números de cartão em imagens digitalizadas	**OCR com cobrança pay-as-you-go do Microsoft Syntex**
Rótulo para Teams desabilitado ou escopo Groups & sites ausente	**Habilitar rótulos para grupos no Entra ID e Execute-AzureAdLabelSync**
MFA ao abrir documentos de sites com determinado rótulo	**Contexto de autenticação do Conditional Access no rótulo de contêiner**
Pesquisa, DLP e coautoria não funcionam em criptografados no SharePoint	**Habilitar rótulos de confidencialidade para arquivos do Office no SharePoint e no OneDrive**
Rotular PDF e imagens pelo File Explorer	**File labeler do cliente do Microsoft Purview Information Protection**
Scanner com Enforce em On não aplica rótulo recomendado	**Treat recommended labeling as automatic no content scan job**
Logotipos diferentes por departamento em e-mail criptografado ou expiração para externos	**Advanced Message Encryption com modelos de marca e mail flow rules**
Quem leu, baixou ou encaminhou no portal de mensagens criptografadas	**EnablePortalTrackingLogs e pesquisa no Audit**
Rótulos no idioma de cada usuário	**Set-Label -LocaleSettings**

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

- Último da lista de rótulos = maior prioridade; política de rótulos com maior número de ordem vence.
- SIT interno não se edita: Copy; entidade nomeada não se edita nem se copia.
- Classificador personalizado: inglês, texto, SharePoint, não lê criptografado e não retreina depois de publicado.
- Rótulo com criptografia substitui o IRM de mail flow rule; anexo herda a criptografia, não o rótulo.
- Rótulo padrão da biblioteca nunca passa por cima de rótulo manual.

Essenciais para a prova (checklist)

☐ Sei escolher entre SIT interno, SIT personalizado, EDM, fingerprint, entidade nomeada e classificador treinável a partir do requisito.

☐ Sei as regras de regex de SIT (sem ^ e $, um grupo de captura, 1.024 caracteres) e quando usar o validador de checksum.

☐ Sei os requisitos de sementes, idioma, indexação e retreino de classificadores personalizados.

☐ Sei a diferença entre Data/Content explorer e Activity explorer, prazos e os grupos List viewer e Content viewer.

☐ Sei habilitar o OCR e a matriz de locais e soluções suportados.

☐ Sei configurar escopos, prioridade, políticas, criptografia (Assign x Let users) e acesso offline de rótulos.

☐ Sei o que um rótulo de contêiner controla e como habilitá-lo (Entra ID + Execute-AzureAdLabelSync).

☐ Sei diferenciar rotulagem automática no cliente e no serviço, rótulo padrão da política e da biblioteca.

☐ Sei instalar e operar o scanner (Install-Scanner, Set-Authentication, Enforce, Rescan all files) e o cliente (file labeler, extensões, PowerShellOnly).

☐ Sei os cmdlets e parâmetros do Message Encryption e do Advanced Message Encryption, inclusive revogação e expiração.

Questões de revisão do capítulo

R3.1 · Implementar a proteção de informações

A equipe de mensagens da Distribuidora Norte Frio quer usar o Microsoft Purview Message Encryption, mas o teste com Test-IRMConfiguration falha ao obter os modelos. Qual pré-requisito do serviço deve ser verificado primeiro?

A. Se o Active Directory RMS local está publicado para o Exchange
B. Se o serviço Azure Rights Management está ativo no locatário
C. Se existe um modelo de marca criado com New-OMEConfiguration
D. Se o Advanced Message Encryption foi licenciado para os usuários

R3.2 · Implementar a proteção de informações

A Transportadora Rota Sul quer que as políticas de DLP do Exchange e do SharePoint também encontrem números de cartão de crédito em imagens digitalizadas. O administrador abre o Microsoft Purview e não consegue habilitar o recurso. O que precisa existir antes de configurar o OCR?

A. Um classificador treinável publicado para cada tipo de imagem digitalizada
B. Uma assinatura Azure pay-as-you-go ligada à cobrança do Microsoft Syntex
C. Uma política de rotulagem automática em modo de simulação para imagens
D. Um scanner do Information Protection instalado em um servidor Windows

R3.3 · Implementar a proteção de informações

A Rede de Escolas Aprender Mais quer que o rótulo Interno aplique uma marca d'água com o nome do rótulo em documentos e e-mails, e um rodapé com o nome do arquivo. Qual afirmação está correta?

A. O rodapé com variável exige o cliente do Information Protection instalado no Windows
B. A marca d'água e o rodapé exigem que o rótulo também aplique criptografia ao documento rotulado
C. A marca d'água vale para documentos, não para e-mails, e as marcações aceitam variáveis
D. A marca d'água vale para documentos e e-mails, mas as marcações não aceitam variáveis

R3.4 · Implementar a proteção de informações

Na Fábrica de Móveis Madeira Nobre, uma regra de DLP usa um SIT personalizado com nível de confiança baixo, e outra regra usa o mesmo SIT com nível alto. A analista quer entender a diferença nas correspondências. Qual afirmação está correta?

A. O nível alto exige menos evidência de suporte perto do elemento primário e, por isso, gera mais falsos positivos
B. O nível baixo retorna só correspondências de confiança baixa; o alto retorna as de confiança média e alta
C. O nível baixo retorna correspondências de confiança baixa, média e alta; o alto retorna só as de confiança alta
D. O nível baixo exige que o elemento de suporte esteja a menos de 100 caracteres do elemento primário

Respostas comentadas

R3.1. B) Se o serviço Azure Rights Management está ativo no locatário

Por quê: O Microsoft Purview Message Encryption usa a proteção do Azure Rights Management. Se o serviço estiver ativo, a criptografia de mensagens é habilitada automaticamente; Get-IRMConfiguration (AzureRMSLicensingEnabled) e Test-IRMConfiguration validam a configuração.

✗ A) Incorreta. O Message Encryption não é compatível com o AD RMS; quem usa AD RMS com o Exchange Online precisa migrar para o Azure Rights Management.

✗ C) Incorreta. Modelos de marca personalizam a experiência, mas não são exigidos para criptografar; a marca padrão já existe.

✗ D) Incorreta. O Advanced Message Encryption acrescenta recursos como expiração e revogação; o Message Encryption básico não depende dele.

> **Dica de prova:** Message Encryption: Azure Rights Management ativo é o pré-requisito.

R3.2. B) Uma assinatura Azure pay-as-you-go ligada à cobrança do Microsoft Syntex

Por quê: O OCR permite que DLP, rotulagem automática, retenção automática e gestão de risco interno analisem imagens. É um recurso opcional: um administrador configura a assinatura Azure pay-as-you-go pela cobrança do Microsoft Syntex, e o administrador de conformidade escolhe locais e grupos em Settings > Optical character recognition (OCR).

✗ A) Incorreta. Com o OCR habilitado, os SITs e classificadores existentes passam a detectar caracteres em imagens; não é preciso um classificador por tipo de imagem.

✗ C) Incorreta. Simular rotulagem automática não habilita a leitura de imagens; o requisito é a cobrança pay-as-you-go.

✗ D) Incorreta. O scanner atua em compartilhamentos de rede e no SharePoint Server; o OCR do Purview para Exchange e SharePoint Online é configurado no portal.

> **Dica de prova:** OCR no Purview: primeiro a cobrança pay-as-you-go (Syntex), depois Settings > OCR.

R3.3. C) A marca d'água vale para documentos, não para e-mails, e as marcações aceitam variáveis

Por quê: Marcações de conteúdo: cabeçalho, rodapé e marca d'água, com variáveis. Limites: marca d'água até 255 caracteres; cabeçalho e rodapé até 1.024 (no Excel, 255 no total, incluindo códigos de formatação).

✗ A) Incorreta. Marcações com variáveis são configuradas no próprio rótulo e aplicadas pelos aplicativos do Office que suportam rótulos.

✗ B) Incorreta. Marcação de conteúdo e criptografia são configurações independentes do rótulo.

✗ D) Incorreta. E-mails não recebem marca d'água, e as marcações de conteúdo aceitam variáveis.

> **Dica de prova:** Marca d'água: documentos sim, e-mails não.

R3.4. C) O nível baixo retorna correspondências de confiança baixa, média e alta; o alto retorna só as de confiança alta

Por quê: O nível de confiança reflete quanta evidência de suporte foi encontrada junto ao elemento primário. Alta confiança: menos falsos positivos e mais falsos negativos; baixa: o contrário. A documentação sugere padrões de confiança alta com contagens baixas (5 a 10) e de confiança baixa com contagens maiores (20 ou mais).

✗ A) Incorreta. O nível alto exige mais evidência de suporte e gera menos falsos positivos, com mais falsos negativos.

✗ B) Incorreta. O nível baixo é o mais abrangente: inclui também as correspondências de confiança média e alta.

✗ D) Incorreta. A proximidade é definida no padrão do SIT, não pelo nível de confiança escolhido na regra.

> **Dica de prova:** Confiança baixa inclui média e alta; alta inclui só alta.

DIA DA PROVA

Estratégia de prova

O SC-401 é uma prova de administração do Microsoft Purview baseada em cenários: cada enunciado descreve uma empresa, um requisito de negócio e restrições (menor privilégio, sem afetar usuários, sem manter listas, ainda hoje), e a resposta é o recurso, a função ou o cmdlet exato que atende a todas elas. As alternativas erradas costumam ser recursos reais de outra área do Purview (Activity explorer no lugar de Content explorer, DLP no lugar de retenção, Set-OMEConfiguration no lugar de Set-IRMConfiguration) ou o comportamento invertido (Exchange x SharePoint na simulação, topo x fim da lista de rótulos). Os três domínios têm o mesmo peso (30-35% cada), então não há área para deixar de lado. Há itens de múltipla escolha e de múltipla resposta (Escolha DUAS ou TRÊS), e muitos cenários longos escondem um detalhe decisivo no fim do enunciado.

Como responder

✓ Planeje cerca de 50 itens em 100 minutos (a Microsoft não divulga o número exato), com pontuação de 1 a 1000 e mínimo de 700: isso dá perto de dois minutos por item, folga suficiente para ler cenários longos com calma.

✓ Leia primeiro a pergunta final e depois o cenário, sublinhando mentalmente cada restrição (menor privilégio, sem editar a política, sem criar política separada, em simulação, até amanhã); a alternativa certa atende a todas.

✓ Classifique o requisito antes de olhar as alternativas: detectar, rotular, bloquear, reter, investigar ou auditar; isso elimina de cara as soluções de outra área.

✓ Em itens de funções, procure o grupo mais específico para a tarefa e descarte Global Administrator, Compliance Administrator e Organization Management quando o enunciado fala em menor privilégio.

✓ Em itens de conflito (DLP, retenção, rótulos, auditoria), aplique a regra fixa de precedência passo a passo em vez de confiar na intuição de que o maior período ou a política mais nova vence.

✓ Em Escolha DUAS ou TRÊS, julgue cada alternativa como verdadeira ou falsa isoladamente; os distratores costumam trocar o local (Exchange x SharePoint), o valor (15 x 30 dias) ou a direção (topo x fim).

✓ Desconfie de alternativas com números redondos fora do padrão (90 dias de simulação, 24 horas para retenção, 5.000 no instance count): confira contra os limites que você memorizou.

✓ Marque para revisão os itens de cenário muito longo e volte a eles no fim; os itens curtos de cmdlet e de função costumam ser rápidos. Se for fazer pausa, revise antes: depois dela não dá para voltar aos itens já vistos, nem aos marcados para revisão.

Erros que derrubam candidatos

✗ Inverter a prioridade dos rótulos, achando que o mais restritivo fica no topo da lista.

✗ Somar ações por prioridade em DLP quando as ações são diferentes, em vez de aplicar o mais restritivo por atividade.

✗ Aplicar o período mais longo também para exclusão na retenção e esquecer que rótulo e escopo específico desempatam antes da exclusão mais curta.

✗ Confundir os explorers: Activity explorer (atividades, 30 dias), Content/Data explorer (retrato dos itens) e Audit (eventos do log).

✗ Escolher o grupo de funções amplo ou parecido (IRM Admins para ver alertas, Audit Manager para quem só lê, Content viewer para quem só precisa da lista).

✗ Trocar os cmdlets do Message Encryption (Set-IRMConfiguration x Set-OMEConfiguration) e os parâmetros de cada um.

✗ Ignorar o pré-requisito escondido no cenário: extensão do Purview no Chrome, Advanced classification, scanner para repositórios locais, E5 para auditoria longa.

Na semana da prova

- ☐ Revise as tabelas de números de cada capítulo até saber de cor os prazos (5 dias, 7 dias, 15 e 30 dias, 180 dias, 1 ano) e os limites (500 rótulos, 2.048 termos, 256 caracteres, 50 e 150 sementes).
- ☐ Refaça as provas práticas focando nos itens errados e escreva, para cada erro, a regra que desfaz a confusão.
- ☐ Treine as regras de precedência (DLP, retenção, rótulos, auditoria) resolvendo cenários em voz alta, passo a passo.
- ☐ Monte uma folha de uma página com os grupos de funções (IRM, Content explorer, Audit, eDiscovery, DLP, DSPM para IA) e a tarefa de cada um.
- ☐ Na véspera, revise só a seção lembrar de cada capítulo e durma bem; no dia, chegue cedo e use o tempo de dois minutos por item com tranquilidade.

REVISÃO FINAL

Folha de cola

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

1. Gerenciar riscos, alertas e atividades

‣ Avaliar riscos antes de criar qualquer política → **Analytics do IRM (até 48 horas)**

‣ Datas de desligamento vindas do RH → **Conector de RH (ou exclusão da conta no Entra como alternativa)**

‣ Alertas do Defender for Endpoint no IRM → **Share endpoint alerts + Intelligent detections**

‣ Nenhum usuário recebe pontuação → **Indicadores globais desligados em Policy indicators**

‣ Clipes de tela de um usuário sob investigação → **Evidência forense com pedido e aprovação (Approvers)**

⚠ Admins configuram, mas não acessam alertas e casos; triagem é Analysts e investigação com forense é Investigators.

⚠ Com a pseudonimização ligada, o data risk graph não está disponível.

⚠ Ele aceita só detecções pré-processadas e agregadas em arquivo; crachás usam Physical badging.

2. Implementar a prevenção contra perda de dados e a retenção

‣ Antes de abrir o assistente, ligar a política a uma necessidade de negócio → **Declaração de intenção da política**

‣ Quantas ocorrências e com que certeza → **Nível de confiança e contagem de instâncias (tolerância a vazamento)**

‣ Testar ajustes sem afetar usuários → **Modo de simulação (cópia v2)**

‣ Período conta a partir da saída do funcionário ou fim de contrato → **Rótulo de retenção baseado em evento**

‣ Ninguém, nem o admin global, pode reduzir ou desligar → **Preservation Lock por PowerShell**

⚠ Prioridade só desempata ações idênticas; com ações diferentes, cada atividade recebe a ação mais restritiva entre as políticas.

⚠ Mais longo vale para reter. Só com exclusões, vence o rótulo; entre políticas, a de escopo específico; por fim, a mais curta.

⚠ Períodos nunca se somam; aplicam-se os princípios de retenção.

3. Implementar a proteção de informações

‣ Valores exatos de uma base, sem enviar em texto claro, conta de serviço para upload diário → **SIT baseado em EDM com EDM Upload Agent, hash com salt e grupo EDM_DataUploaders**

‣ Formulário ou modelo padronizado da empresa (procuração, bula, relatório) → **Document fingerprinting**

‣ Começar hoje, sem tempo de treinar, categoria comum como currículos ou faturas → **Classificador pré-treinado Ready to use**

‣ Número com dígito verificador e falsos positivos com CEP e telefone → **Regex com validador de checksum e palavra-chave como suporte**

‣ Ver o item e o local, sem ler o conteúdo → **Content Explorer List viewer**

⚠ O primeiro da lista é o de menor prioridade; o mais restritivo vai para o fim. Na lista de políticas, também vence o maior número de ordem.

⚠ O anexo do Office sem proteção herda a criptografia, não o rótulo, e essa herança não pode ser desligada.

⚠ Mínimo de 50 positivos e 150 negativos, só arquivos de texto, em pastas separadas de um site do SharePoint.

GABARITO

Respostas do diagnóstico

D1. A) Ser membro do grupo de funções Content Explorer Content Viewer → revise o capítulo 1

Por quê: Para o painel de alertas de DLP: função Manage alerts e DLP Compliance Management ou View-Only DLP Compliance Management. Se o administrador precisa ver alertas sem conteúdo sensível, crie uma função personalizada sem Data classification content viewer.

✗ B) Incorreta. Licenças de auditoria não liberam a prévia de conteúdo dos alertas.

✗ C) Incorreta. Ela já acessa o painel; a prévia de conteúdo depende do Content Explorer Content Viewer.

✗ D) Incorreta. Esse grupo é da gestão de risco interno, não da prévia de conteúdo de DLP.

> **Dica de prova:** Ver o conteúdo nos alertas de DLP: Content Explorer Content Viewer.

D2. B) Dispositivos integrados com o Purview Client; até 2 horas para a política e 1 hora por clipe → revise o capítulo 1

Por quê: Também é preciso liberar domínios de armazenamento das capturas no firewall e no proxy. As capturas ficam numa única região, a mesma do Exchange Online da organização, e há capacidade de teste de até 20 GB.

✗ A) Incorreta. A captura usa o Microsoft Purview Client, e os prazos não são imediatos.

✗ C) Incorreta. As plataformas suportadas são Windows 10 e 11 Enterprise, e os prazos documentados são de até duas horas e uma hora.

✗ D) Incorreta. É preciso integrar ao Purview e instalar o Purview Client; os prazos documentados são de horas.

> **Dica de prova:** Evidência forense: Purview Client nos dispositivos; até 2 h para valer e 1 h por clipe.

D3. D) Nada desse período, porque registros de usuários sem E5 ficam 180 dias → revise o capítulo 1

Por quê: O Audit (Standard) retém registros por 180 dias (padrão desde outubro de 2023). Para guardar mais, use o Audit (Premium) e políticas de retenção de auditoria ou exporte para um SIEM pela Office 365 Management Activity API.

✗ A) Incorreta. Retenção de dez anos exige E5 e o complemento de 10 anos.

✗ B) Incorreta. A retenção padrão de um ano depende de licenciamento E5 dos usuários.

✗ C) Incorreta. Exportar para CSV gera um arquivo local; não muda a retenção no Audit.

> **Dica de prova:** Sem E5: auditoria por 180 dias.

D4. B) Block only people from outside your organization → revise o capítulo 2

Por quê: A ação de restrição no Microsoft 365 oferece bloquear todos (exceto dono, último modificador e administrador do site), bloquear só externos e, no Exchange, criptografar e-mails. As ações disponíveis dependem dos locais selecionados.

✗ A) Incorreta. Block everyone deixa com acesso só o dono do conteúdo, o último modificador e o administrador do site.

✗ C) Incorreta. Audit only registra, mas não bloqueia.

✗ D) Incorreta. Encrypt email messages vale só para conteúdo no Exchange.

> **Dica de prova:** Bloquear só convidados: Block only people from outside your organization.

D5. D) Aguardar alguns dias, pois a consulta pode levar até cinco dias para popular, e dar a função Scope Manager → revise o capítulo 2

Por quê: Escopos adaptáveis são usados em políticas de retenção, rotulagem automática e Communication Compliance. Há três tipos (Users, SharePoint sites e Microsoft 365 Groups), e consultas avançadas podem ser validadas com PowerShell ou com a pesquisa do SharePoint.

✗ A) Incorreta. Uma hora não basta, e Information Protection Readers não cria escopos adaptáveis.

✗ B) Incorreta. As consultas não são imediatas, e Organization Configuration não é a função de escopos adaptáveis.

✗ C) Incorreta. O prazo de população é de até cinco dias, e eDiscovery Administrator não cria escopos.

> **Dica de prova:** Escopo adaptável novo: espere até 5 dias; quem cria precisa de Scope Manager.

D6. D) Um escopo adaptável de usuários com a consulta pelo atributo de cargo do Entra → revise o capítulo 2

Por quê: Escopos adaptáveis não têm limite de itens por política e permitem aplicar configurações específicas a caixas inativas. Escopos estáticos são mais simples quando se quer o local inteiro ou poucos itens fixos.

✗ A) Incorreta. Excluir um por um os não executivos seria inviável e frágil.

✗ B) Incorreta. Com escopo estático, é preciso atualizar a política a cada novo executivo e quando a URL do OneDrive muda (por exemplo, com troca de UPN).

✗ C) Incorreta. Unidades administrativas vêm do Microsoft Entra ID; o escopo de retenção que se atualiza por atributos é o adaptável.

> **Dica de prova:** Público que muda por atributo: escopo adaptável.

D7. D) Não precisa de nova política, e a mudança leva até 24 horas para chegar aos apps → revise o capítulo 3

Por quê: Para editar uma política, basta salvar as mudanças: não há ação específica de publicar ou republicar. Crie várias políticas só quando usuários precisam de rótulos ou configurações diferentes.

✗ A) Incorreta. Não há ação de republicar: a política existente já distribui a versão editada, e a replicação não é imediata.

✗ B) Incorreta. Excluir o rótulo é desnecessário e arriscado; basta editá-lo.

✗ C) Incorreta. O prazo documentado para replicar alterações é de até 24 horas.

> **Dica de prova:** Rótulo editado: sem republicar; até 24 horas para replicar.

D8. D) O classificador pré-treinado Resume, que já aparece com o status Ready to use → revise o capítulo 3

Por quê: Classificadores pré-treinados da Microsoft (como Resume, Invoice, Agreements e Source code) ficam prontos para uso em rotulagem automática, retenção automática e DLP. Confira os idiomas suportados de cada um na página de definições.

✗ A) Incorreta. SITs de entidade nomeada não são criados pelo administrador; um modelo em branco é a entrada do document fingerprinting.

✗ B) Incorreta. O EDM procura valores exatos de uma base estruturada, não categorias de documentos como currículos.

✗ C) Incorreta. Um classificador personalizado exige ao menos 50 amostras positivas e 150 negativas, além do tempo de processamento.

> **Dica de prova:** Sem tempo para treinar: classificador pré-treinado (Ready to use).

D9. B) O suporte a classificadores treináveis personalizados é limitado ao inglês → revise o capítulo 3

Por quê: Classificadores pré-treinados avaliam os idiomas listados em suas definições; classificadores personalizados têm suporte limitado ao inglês. Para conteúdo em português, avalie SITs, keyword dictionaries (qualquer idioma) ou fingerprints.

✗ A) Incorreta. O OCR lê texto em imagens; não amplia os idiomas suportados por classificadores personalizados.

✗ C) Incorreta. O Purview não traduz amostras; o suporte a classificadores personalizados é limitado ao inglês.

✗ D) Incorreta. Não há exigência de vários idiomas; a limitação documentada é o suporte ao inglês.

> **Dica de prova:** Classificador personalizado: suporte limitado ao inglês.

Agora, treine no formato real

Faça as 6 provas completas do curso SC-401: 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.