

Microsoft Certified: Information Security Administrator Associate

Principales conceptos, temas oficiales y habilidades clave del temario de SC-401, para repasar antes del examen.

Nivel: Intermediate (Associate) Duración: 100 min Nota de corte: 700/1000 Fuente: guía de estudio oficial de Microsoft Learn

1. Implement information protection

30–35%

Implement and manage data classification

- Microsoft Purview identifica elementos confidenciales de tres formas: manualmente por los usuarios, con tipos de información confidencial basados en patrones y con clasificadores entrenables de aprendizaje automático. Cada requisito se traduce en un clasificador: SIT integrados o de entidad con nombre, coincidencia exacta de datos, huella digital de documento, credenciales o OCR para imágenes.
- Un requisito se traduce en un patrón de SIT: elemento principal (expresión regular, lista o diccionario de palabras clave o función), elementos de apoyo, proximidad de caracteres y nivel de confianza. Los SIT integrados no se editan, pero se pueden copiar como plantilla; los de entidad con nombre no se copian y se aprovechan en las plantillas mejoradas. Los valores de fecha o suma de comprobación reducen falsos positivos.
- Un SIT personalizado se crea en el portal (nombre, patrones con elemento principal, proximidad, elementos de apoyo y nivel de confianza) o con PowerShell mediante paquetes de reglas XML. Las expresiones regulares no usan anclas y emplean un solo grupo de captura con alternancia. Los diccionarios de palabras clave escalan mejor que las listas, y el contenido existente de SharePoint debe volver a rastrearse.
- La huella digital de documento convierte un formulario estándar, idealmente en blanco, en un tipo de información confidencial que solo guarda un hash. Se usa en DLP (Exchange, SharePoint, OneDrive, Teams y dispositivos) y en el etiquetado automático, con coincidencia parcial por porcentaje o exacta. No detecta archivos protegidos con contraseña ni solo con imágenes, y en dispositivos exige Advanced Classification Searching and Protection.
- Un SIT de coincidencia exacta de datos detecta valores reales de tu propia tabla de origen, que se somete a hash con sal y se carga con EDM Upload Agent desde una cuenta del grupo EDM_DataUploaders; lo recomendable es aplicar hash y cargar desde dos equipos distintos. El esquema define los campos buscables y opciones como caseInsensitive e ignoredDelimiters, y la nueva experiencia crea esquema y SIT en un único flujo.

Implement and manage sensitivity labels in Microsoft Purview

- Para crear y configurar etiquetas se usan los grupos de roles Information Protection e Information Protection Admins, o un grupo personalizado con el rol Sensitivity Label Administrator (Sensitivity Label Reader para solo lectura). Los permisos no hacen falta para aplicar etiquetas, y las unidades administrativas de Microsoft Entra limitan a un administrador a los usuarios de sus ámbitos.
- El ámbito de una etiqueta decide dónde se configura y dónde se ve: archivos, correos, reuniones (requiere archivos y correos) o grupos y sitios, que protege contenedores sin etiquetar sus elementos. El orden de la lista fija la prioridad (la más restrictiva al final), los grupos de etiquetas sustituyen a las primarias y quitar una etiqueta de sus directivas es como eliminarla.
- El control de acceso de una etiqueta usa Azure Rights Management: el administrador asigna permisos ahora (usuarios, grupos o dominios, caducidad y acceso sin conexión) o deja que los usuarios los asignen con Do Not Forward, Encrypt-Only o permisos personalizados en Word, PowerPoint y Excel. El marcado de contenido añade encabezados, pies y marcas de agua con variables; la marca de agua dinámica exige cifrado.
- Las etiquetas se publican a usuarios y grupos, no directivas de etiquetas que definen la etiqueta predeterminada (documentos, correos, reuniones, contenedores y Power BI), el etiquetado obligatorio, la justificación al rebajar y un vínculo de ayuda. Si un usuario recibe varias directivas y hay conflicto, gana la de número de orden más alto;
- Las directivas de etiquetado automático funcionan en el servicio para archivos en tránsito de SharePoint y OneDrive y correo en tránsito de Exchange, sin intervención del usuario, y deben pasar antes por simulación. Requieren la auditoría activada y las etiquetas habilitadas para archivos de Office; por defecto no sustituyen etiquetas aplicadas a mano, aunque pueden configurarse para sustituir las de menor prioridad.

Implement information protection for Windows, file shares, and Exchange

- El cliente de Microsoft Purview Information Protection solo funciona en Windows, sustituye al cliente de etiquetado unificado de AIP y aporta el etiquetador de archivos del Explorador, el visor, el escáner y el módulo de PowerShell; no incluye complemento de Office. Las actualizaciones no interactivas desde AIP necesitan la clave AllowMajorVersionUpgrade. Los equipos sin conexión solo admiten etiquetas sin cifrado.
- El cliente de Microsoft Purview Information Protection etiqueta y cifra archivos desde el Explorador o con PowerShell. Los archivos de Office y PDF reciben cifrado nativo; .jpg o .txt pasan a una extensión con p y el resto recibe cifrado genérico .pfile, sin aplicar derechos de uso. Excluye tipos de sistema como .exe o .pst, y la configuración avanzada de la directiva de Microsoft Purview Information Protection es un azar.
- El escáner de Microsoft Purview Information Protection es un servicio de Windows Server que recorre por ciclos recursos compartidos de red y bibliotecas de SharePoint Server para detectar, etiquetar y cifrar archivos. Necesita el cliente completo, SQL Server y una cuenta de servicio sincronizada con Microsoft Entra ID. Se configura con un cluster y un trabajo de examen del contenido, y por defecto solo cifra archivos de Office y PDF.
- Microsoft Purview Message Encryption se basa en el servicio Azure Rights Management, su único requisito previo, y no es compatible con AD RMS. Los usuarios cifran desde Outlook y los administradores automatizan el cifrado con reglas de flujo de correo o directivas de DLP, con las opciones Encrypt-Only, Do Not Forward o plantillas. Los destinatarios de Microsoft 365 leen el mensaje en Outlook y en el portal de mensajes cifrados.
- Microsoft Purview Advanced Message Encryption amplía Message Encryption con varias plantillas de personalización de marca, caducidad y revocación de mensajes y registros de actividad del portal de mensajes cifrados. Solo funciona con destinatarios externos que leen el correo en el portal, algo que se garantiza aplicando una plantilla personalizada mediante una regla de flujo de correo que se procesa después de la regla de cifrado.

2. Implement data loss prevention and retention

30–35%

Create and configure data loss prevention policies

- Diseñar una directiva de prevención de pérdida de datos empieza con las partes interesadas y una declaración de intención que responde qué supervisar, el ámbito, dónde, con qué condiciones y qué acciones aplicar. Las ubicaciones elegidas limitan cómo se define el contenido: al combinarlas, prevalece la que no admite un método. Se recomienda desplegar en modo de simulación, primero sin y luego con sugerencias de directiva, antes de aplicarla.
- Para crear e implementar directivas DLP hace falta pertenecer a grupos como Compliance Administrator, Compliance Data Administrator, Information Protection o Information Protection Admins; Analysts e Investigators gestionan alertas y solo leen las directivas, y Readers solo ve informes. Un administrador con unidad administrativa solo gestiona directivas y alertas de su unidad, y un rol de Entra prevalece sobre una asignación con ámbito.
- Una directiva DLP se despliega confirmando estado, acciones y ámbito. Se crea en Keep it off, pasa a modo de simulación, luego a simulación con sugerencias para un grupo piloto y por último se activa. Allow solo existe para Devices, Block with override deja omitir el bloqueo con un motivo y, en Devices, la directiva solo se aplica si usuario y dispositivo están en el ámbito.
- Adaptive Protection añade a DLP la condición Insider risk level for Adaptive Protection is (Elevated, Moderate, Minor) en Exchange Online, Devices y Teams. La configuración rápida crea dos directivas DLP en modo de simulación y, en dispositivos, hace falta clasificación avanzada o la condición File type is. Crear estas directivas requiere roles como Compliance Data Administrator o DLP Compliance Management.
- En Exchange, SharePoint y OneDrive las reglas tienen prioridades por orden de creación y se aplica la regla más restrictiva, aunque se registran todas las coincidencias. En los dispositivos se suman las acciones más restrictivas de todas las directivas coincidentes; ante acciones idénticas mandan la directiva activada y la de mayor prioridad, y sin invalidación gana a permitir invalidación.

Implement and monitor Microsoft Purview Endpoint DLP

- Endpoint DLP necesita dispositivos Windows unidos a Microsoft Entra (o híbridos o registrados), con protección en tiempo real y monitor de comportamiento activos y MpDlpService.exe permitido; los ya incorporados a Defender for Endpoint no requieren más pasos. Las extensiones de Purview para Chrome y Firefox solo se usan en Windows, y los servidores necesitan activar Endpoint DLP tras incorporarse.
- Las reglas DLP para dispositivos admiten condiciones con AND, OR y NOT en grupos anidados, y acciones por actividad que se pueden matizar con grupos de autorización (impresoras, USB, recursos compartidos de red) y excepciones de red, donde la VPN debe tener la máxima prioridad. La configuración de un grupo de aplicaciones restringidas prevalece sobre la lista de aplicaciones restringidas dentro de la misma regla.
- La configuración de Endpoint DLP es global y se aplica a todas las directivas de DLP para dispositivos: clasificación avanzada en la nube (coincidencia exacta de datos, clasificadores entrenables), exclusiones de rutas, aplicaciones restringidas y grupos (el grupo prevalece sobre la lista en la misma regla), Auto-quarantine, dominios de servicio, y grupos de impresoras, USB y recursos compartidos de red.
- La protección Just-in-time retiene actividades de salida (Imprimir, copiar a USB o red, RDP, Bluetooth, carga a dominios restringidos) sobre archivos nunca evaluados o con clasificación obsoleta mientras termina la evaluación, solo si una regla bloquea esa actividad. La acción de reserva decide qué ocurre si falla la clasificación; sus exclusiones de ruta solo afectan a JIT.
- Tras incorporar un dispositivo, su actividad auditada llega al explorador de actividades incluso sin directivas; Always audit file activity for devices audita Office, PDF y CSV sin coincidencia de directiva. Los servidores Windows requieren activar Endpoint DLP. Las alertas se revisan en el panel de alertas de DLP o en Defender XDR, y la recopilación de pruebas guarda copias completas en Azure.

Implement and manage retention

- Las etiquetas de retención actúan por elemento y aportan lo que las directivas no tienen: inicio al etiquetar o por evento, declaración de registros y revisión para eliminación. La revisión requiere el rol Disposition Management y el contenido no se mueve mientras espera. File plan permite importar etiquetas en bloque y los eventos inician la retención basada en eventos.
- Un ámbito adaptable es una consulta diaria sobre atributos de usuarios, grupos de Microsoft 365 o propiedades de sitios de SharePoint, así que la pertenencia se actualiza sola. Los crean los grupos de roles con Scope Manager; el generador avanzado usa OPATH o KeyQL y es necesario para excluir buzones inactivos. Las consultas se validan con PowerShell o la búsqueda de SharePoint.
- Las etiquetas de retención aplican excepciones por elemento a las directivas de retención: solo retener, solo eliminar o retener y después eliminar, con inicio en la creación, la última modificación o el etiquetado. Al final pueden cambiar a otra etiqueta o desactivar la retención. Tras guardarlas no se cambian el nombre ni la opción de registro, y solo se eliminan si no están en ninguna directiva.
- Publicar etiquetas de retención requiere una directiva de etiquetas que las ponga a disposición de usuarios y administradores en Exchange, SharePoint, OneDrive y grupos de Microsoft 365. Si es adaptable, los ámbitos deben existir antes y determinan las ubicaciones elegibles. Teams, Viva Engage y carpetas públicas no admiten etiquetas; los errores de distribución se reintentan con -RetryDistribution.
- Una directiva de aplicación automática asigna una única etiqueta de retención al contenido sin etiquetar que contiene tipos de información confidencial, palabras clave o propiedades consultables, o coincide con clasificadores entrenables; también etiqueta adjuntos en la nube. Admite simulación con tipos de información confidencial y consultas, nunca reemplaza una etiqueta aplicada y los clasificadores requieren ámbito estático.

3. Manage risks, alerts, and activities

30–35%

Implement and manage Microsoft Purview Insider Risk Management

- Insider Risk Management usa seis grupos de roles: Insider Risk Management (acceso completo), Admins (directivas, configuración y Adaptive Protection), Analysts (alertas y casos), Investigators (además pruebas forenses y explorador de contenido), Auditors (registros de auditoría) y Approvers (aprobar capturas forenses). Las unidades administrativas restringen a los miembros a los usuarios de una región o departamento.
- Insider Risk Management importa señales externas con conectores de datos: el conector de RR. HH. (archivos CSV con dimisiones, cambios de nivel, evaluaciones y planes de mejora), el de Healthcare (auditoría del sistema de historias clínicas) y el de Physical badging (accesos físicos en JSON). Se crean con el rol Data Connector Admin, una aplicación registrada en Microsoft Entra y un script que sube los datos con el identificador del trabajo.
- Las plantillas de infracciones de directivas de seguridad usan alertas de Microsoft Defender for Endpoint sobre evasión de controles de seguridad y software no deseado. Requieren una suscripción activa de Defender for Endpoint, activar en sus características avanzadas el uso compartido de alertas con Microsoft Purview y seleccionar sus indicadores; las alertas se importan a diario según los estados de evaluación elegidos.
- La configuración de Insider Risk Management se aplica a todas las directivas, sea cual sea la plantilla. Privacy anonimiza los nombres de usuario; Policy timeframes fija la ventana de activación y la detección de actividad pasada; Intelligent detections ajusta el volumen de alertas e importa alertas de Defender for Endpoint; Global exclusions excluye dominios, rutas, tipos de archivo o palabras clave de la puntuación.
- Todos los indicadores globales están deshabilitados de forma predeterminada: se habilitan en Policy indicators y solo entonces se eligen en cada directiva, donde se ajustan sus umbrales. Hay indicadores de Office, dispositivo, DLP, Communication Compliance, Microsoft Entra ID y nube, potenciadores de puntuación, variantes con grupos de detección e indicadores personalizados mediante un conector.

Manage information security alerts and activities

- Audit (Premium) incluye todo Audit (Standard) y añade directivas de retención, retención más larga e información inteligente. Para registrar sus eventos, cada usuario necesita una licencia válida y el plan Microsoft 365 Advanced Auditing habilitado; la búsqueda en Exchange (SearchQueryInitiated) se activa por buzón. La retención de 10 años exige una licencia complementaria por usuario y no es retroactiva.
- Para buscar en el registro de auditoría hacen falta los roles Audit Logs o View-Only Audit Logs (grupos Audit Manager o Audit Reader). La búsqueda admite fechas, usuarios, actividades, nombres de operación exactos, tipos de registro y cargas de trabajo; la palabra clave solo busca en contenido indexado. Los administradores restringidos por unidades administrativas no ven algunos eventos, y MailItemsAccessed ayuda a acotar un buzón comprometido.
- Las directivas de retención del registro de auditoría son de Audit (Premium) y requieren el rol Organization Configuration. Se definen por usuarios, tipos de registro y actividades, con una duración y una prioridad: el valor más bajo gana y cualquier directiva personalizada prevalece sobre la predeterminada, que no se puede editar. Los cambios no afectan a los registros ya confirmados.
- Activity explorer ofrece una vista histórica de las actividades sobre contenido etiquetado y de las coincidencias de DLP; procede del registro de auditoría unificado y no es en tiempo real. Se analiza con filtros y conjuntos de filtros, como las actividades de Endpoint DLP o las etiquetas cambiadas. Algunos orígenes, como Power BI, solo constan en el registro de auditoría y las reglas que permiten sin auditar no generan eventos de coincidencia.
- Las alertas de DLP se configuran en las reglas de la directiva y se revisan en el panel de alertas de DLP, que requiere el rol Manage alerts más DLP Compliance Management o su versión de solo lectura. Se filtran, se revisan los eventos, se asigna la propiedad con comentarios y se marcan como resueltas. La vista previa del contenido exige Content Explorer Content Viewer, y la retención de auditoría marca cuánto siguen visibles.

Protect data used by AI services

- Purview protege el uso de IA con controles existentes: las etiquetas con cifrado exigen los derechos VIEW y EXTRACT, la ubicación de DLP para Microsoft 365 Copilot impide procesar elementos etiquetados o enviar a la búsqueda web mensajes con datos confidenciales, Endpoint DLP actúa en sitios de IA de terceros y auditoría, eDiscovery, retención y Communication Compliance gestionan los mensajes y respuestas.
- SharePoint Advanced Management ayuda a preparar Copilot: los informes de gobierno de acceso a datos detectan sitios sobrecompartidos, Restricted Content Discovery oculta temporalmente un sitio en la búsqueda y en Copilot sin cambiar permisos, y el control de acceso restringido limita un sitio u OneDrive a miembros de grupos concretos, algo que Copilot también respeta.
- DSPM for AI necesita la auditoría de Purview activada y licencias de Microsoft 365 Copilot para ver las interacciones de Copilot; para sitios de IA de terceros hay que incorporar los dispositivos a Purview e implementar la extensión de explorador. Otros Copilot y aplicaciones de IA requieren directivas de recopilación, integración con el SDK de Purview o una directiva de configuración de Edge y Fabric exige una aplicación registrada en Entra.
- El Data Security Posture Management pueden crear y editar el rol Compliance Administrator de Purview; Global Administrator y el grupo de roles Compliance Administrator de Purview; Security Reader, Data Security AI Viewer y AI Administrator son de solo lectura. Ver mensajes y respuestas de IA exige Data Security AI Content Viewer o Content Explorer Content Viewer, y Data Security AI Admin edita directivas de DLP de Copilot sin leerlos.
- DSPM for AI ofrece directivas de un clic que se crean en otras soluciones de Purview (DLP, gestión de riesgos internos, Communication Compliance y directivas de recopilación) y se editan allí. Las que usan Adaptive Protection lo activan con niveles de riesgo predeterminados, la directiva de red exige una integración SASE o SSE, y con unidades administrativas solo un administrador sin restricciones puede crearlas.