



# SC-401T00

## Protect sensitive information with Microsoft Purview in the AI era



### Información general.

El curso te dota de las habilidades necesarias para planificar e implementar la seguridad de la información para datos sensibles utilizando Microsoft Purview y servicios relacionados. El curso aborda temas esenciales como la protección de la información, la prevención de pérdida de datos (DLP), la retención y la gestión de riesgos internos. Aprendes a proteger los datos dentro de entornos de colaboración de Microsoft 365 frente a amenazas internas y externas. Además, aprendes a gestionar alertas de seguridad y responder a incidentes investigando actividades, atendiendo alertas DLP y gestionando casos de riesgo interno. También aprendes a proteger los datos utilizados por los servicios de IA dentro de entornos Microsoft e implementar controles para salvaguardar el contenido en estos entornos.

### Duración.

4 Días.

### Perfil del público.

Como Administrador de Seguridad de la Información, planificas e implementas la seguridad de la información para datos sensibles utilizando Microsoft Purview y servicios relacionados. Eres responsable de mitigar riesgos protegiendo los datos dentro de los entornos de colaboración de Microsoft 365 frente a amenazas internas y externas, así como de proteger los datos utilizados por los servicios de IA. Tu función implica implementar la protección de la información, la prevención de pérdida de datos (DLP), la retención y la gestión de riesgos internos. También gestionáis

alertas de seguridad y respondéis a incidentes investigando actividades, respondiendo a alertas DLP y gestionando casos de riesgo interno. En este puesto, colaboras con otros responsables de gobernanza, datos y seguridad para desarrollar políticas que aborden los objetivos de seguridad de la información y reducción de riesgos de tu organización. Trabajas con administradores de cargas de trabajo, propietarios de aplicaciones empresariales y partes interesadas en gobernanza para implementar soluciones tecnológicas que apoyen estas políticas y controles.

### Examen.

SC-401: Administering Information Security in Microsoft 365.

### Temario.

#### **Ruta de aprendizaje: Implementar la Protección de la Información de Microsoft Purview.**

Las organizaciones necesitan una protección eficaz de la información para prevenir la exposición de datos, garantizar el cumplimiento normativo y mantener la seguridad en entornos cloud y locales. Microsoft Purview permite la clasificación, el etiquetado y el cifrado para proteger datos sensibles en los servicios de Microsoft 365, Exchange y almacenamiento local.

#### **Módulo 1: Proteger los datos sensibles en un mundo digital.**

Descubre cómo Microsoft Purview ayuda a las organizaciones a clasificar, proteger y monitorizar datos sensibles en entornos



de nube, endpoint e IA. Este módulo explora estrategias para asegurar los datos mediante la clasificación, el etiquetado, el cifrado y la gestión proactiva de riesgos.

- Introducción.
- La creciente necesidad de protección de datos.
- Los retos de gestionar datos sensibles.
- Proteger los datos en un mundo de Confianza Cero.
- Comprender la clasificación y protección de datos.
- Prevenir filtraciones de datos y amenazas internas.
- Gestionar alertas de seguridad y responder a amenazas.
- Proteger los datos generados y procesados por IA.

## **Módulo 2: Clasificar datos para protección y gobernanza.**

Conoce la información disponible para ayudarte a entender tu panorama de datos y conocer tus datos.

- Resumen de la clasificación de datos.
- Clasificar datos utilizando tipos de información sensibles.
- Clasificar datos usando clasificadores entrenables.
- Crea un clasificador entrenado personalizado.

## **Módulo 3: Revisar y analizar la clasificación y protección de datos.**

Descubre cómo Microsoft Purview ayuda a las organizaciones a monitorizar y analizar la clasificación y protección de datos. Este módulo explora cómo los equipos de seguridad pueden seguir tendencias de clasificación, investigar contenido etiquetado y evaluar la efectividad de las políticas utilizando Informes de Protección de Información, explorador de datos, explorador de contenidos y explorador de actividades.

- Revisa información sobre clasificación y protección.
- Analizar datos clasificados con explorador de datos y contenido.
- Monitorizar y revisar las acciones sobre los datos etiquetados.

## **Módulo 4: Crear y gestionar tipos de información sensible.**

Aprende a utilizar tipos de información sensible para apoyar tu estrategia de protección de la información.

- Resumen de tipos de información sensible.
- Compara tipos de información sensible incorporados frente a personalizados.
- Crear y gestionar tipos de información sensible personalizados.
- Crea y gestiona los tipos exactos de datos sensibles a la coincidencia.
- Implementar la huella digital de documentos.
- Describe entidades nombradas.
- Crear un diccionario de palabras clave.

## **Módulo 5: Crear y configurar etiquetas de sensibilidad con Microsoft Purview.**

Las etiquetas de sensibilidad Microsoft Purview te permiten clasificar y proteger datos sensibles en toda tu organización, tanto en la nube como en dispositivos. Este módulo cubre cómo clasificar y proteger información sensible para garantizar su seguridad y cumplimiento.

- Resumen de etiquetas de sensibilidad.
- Crear y configurar etiquetas de sensibilidad y políticas de etiquetas.
- Configurar el cifrado con etiquetas de sensibilidad.
- Implementar políticas de autoetiquetado.
- Rastrear y evaluar el uso de etiquetas de sensibilidad en Microsoft Purview.

## **Módulo 6: Aplicar etiquetas de sensibilidad para la protección de datos.**

Aprende cómo se utilizan las etiquetas de sensibilidad para clasificar y proteger los datos empresariales, asegurando al tiempo que la productividad de los usuarios y su capacidad de colaboración no se vean obstaculizadas.

- Fundamentos de la integración de etiquetas de sensibilidad en Microsoft 365.
- Gestionar etiquetas de sensibilidad en aplicaciones de Office.
- Aplica etiquetas de sensibilidad con Microsoft 365 Copilot para una colaboración segura.
- Proteger las reuniones con etiquetas de sensibilidad.
- Aplica etiquetas de sensibilidad a Microsoft Teams, grupos de Microsoft 365 y sitios de SharePoint.





## Módulo 7: Clasificar y proteger los datos locales con Microsoft Purview.

Aprende a clasificar y proteger los datos sensibles almacenados en las instalaciones usando Microsoft Purview. Este módulo te guía en el despliegue del escáner de Protección de Información, la aplicación de etiquetas de sensibilidad y la aplicación de políticas DLP para reducir los riesgos de exposición de datos.

- Proteger los archivos locales con Microsoft Purview.
- Prepara tu entorno para el escáner de Protección de Información Microsoft Purview.
- Configura e instala el escáner de Protección de Información Microsoft Purview.
- Ejecuta y gestiona el escáner.
- Hacer cumplir las políticas de prevención de pérdida de datos en archivos locales.

## Módulo 8: Entiende el cifrado de Microsoft 365.

Descubre cómo Microsoft 365 cifra los datos en reposo y en tránsito, gestiona de forma segura las claves de cifrado y ofrece opciones de gestión de claves a los clientes para satisfacer sus necesidades empresariales y obligaciones de cumplimiento.

- Introducción al cifrado de Microsoft 365.
- Aprende cómo los datos de Microsoft 365 están cifrados en reposo.
- Entiende el cifrado de servicios en Microsoft Purview.
- Explora la gestión de claves de cliente usando la clave de cliente.
- Aprende cómo se cifran los datos durante el tránsito.

## Módulo 9: Protege el correo electrónico con el cifrado de mensajes Microsoft Purview.

Aprende a configurar el cifrado de mensajes Microsoft Purview para proteger el correo sensible, aplicar cifrado con reglas de flujo de correo y personalizar la experiencia del destinatario con plantillas de marca.

- Entender el cifrado de mensajes.
- Plan para el cifrado de mensajes de Microsoft Purview.
- Configurar el cifrado de mensajes de Microsoft Purview.
- Personaliza la marca cifrada del correo electrónico con Microsoft Purview.

- Controla el acceso al correo electrónico cifrado con Encriptación Avanzada de Mensajes.
- Utiliza las plantillas de cifrado de mensajes de Microsoft Purview en las reglas de flujo de correo.

## Ruta de aprendizaje: Implementar y gestionar la Prevención de Pérdidas de Datos de Microsoft Purview.

Las organizaciones deben prevenir la pérdida de datos y proteger la información sensible en entornos cloud y endpoint. Microsoft Purview ofrece políticas de prevención de pérdida de datos (DLP) para detectar, restringir y responder a actividades riesgosas que involucren datos sensibles. Aprende a planificar y configurar las políticas DLP, hacer seguimiento de la eficacia de las políticas y analizar riesgos de seguridad de datos para mejorar la estrategia de protección de tu organización.

## Módulo 10: Comprender y planificar la prevención de pérdidas de datos.

La prevención eficaz de la pérdida de datos (DLP) comienza con entender cómo se evalúa el riesgo y cómo se aplican las decisiones de protección. Este módulo se centra en los conceptos y consideraciones de planificación que ayudan a las organizaciones a diseñar políticas DLP que protejan datos sensibles sin interrumpir el trabajo cotidiano.

- Comprender el papel de la prevención de pérdida de datos.
- Entiende cómo el DLP aplica la protección.
- Planificar y diseñar políticas DLP.
- Comprender el despliegue y el modo de simulación de DLP.
- Evalúa controles avanzados de DLP para tu entorno.

## Módulo 11: Crear y gestionar políticas de prevención de pérdidas de datos.

Las políticas efectivas de prevención de pérdida de datos (DLP) se moldean a partir de una serie de decisiones deliberadas en lugar de en entornos individuales. La intención clara, la detección bien definida, el alcance adecuado y las acciones medidas determinan cómo se comportan las políticas en los flujos de trabajo reales. La validación y el ajuste continuo ayudan a garantizar que la protección siga siendo efectiva a medida que cambian los riesgos y el uso.

- Entender cómo encajan entre sí las decisiones de política DLP.
- Elige una plantilla o crea una política personalizada.
- Define qué detecta la póliza.
- Alinear el alcance de la póliza con el riesgo.
- Define cómo responde la póliza.
- Validar el comportamiento de la política usando el modo de simulación.
- Gestionar políticas DLP.
- Ajustar la aplicación de la ley dinámicamente en función del riesgo.
- Guía guía: Crear una política DLP.

## Módulo 12: Implementar la prevención de pérdida de datos en endpoints (DLP) con Microsoft Purview.

El DLP de endpoint en Microsoft Purview ayuda a las organizaciones a proteger datos sensibles en los dispositivos endpoint monitorizando, restringiendo o permitiendo acciones como transferencias de archivos, copias y compartición. Aprende a incorporar dispositivos, configurar configuraciones y crear políticas personalizadas para garantizar la seguridad de los datos en toda tu organización.

- Visión general de la prevención de pérdida de datos en endpoints (DLP).
- Entiende el flujo de trabajo de implementación de DLP en endpoints.
- Dispositivos a bordo para DLP en endpoints.
- Configurar la configuración para el DLP de endpoint.
- Crear y gestionar políticas DLP de endpoint.
- Despliega la extensión de navegador Microsoft Purview.
- Configurar la protección justo a tiempo (JIT).

## Módulo 13: Configurar políticas DLP para Microsoft Defender para aplicaciones en la nube y Power Platform.

Aprende a configurar e implementar políticas de prevención de pérdida de datos e integrarlas con Microsoft Defender para aplicaciones en la nube.

- Configurar políticas de prevención de pérdida de datos para Power Platform.
- Integrar la prevención de pérdida de datos en Microsoft Defender para aplicaciones en la nube.

- Configurar políticas en Microsoft Defender para aplicaciones en la nube.
- Gestionar violaciones de prevención de pérdida de datos en Microsoft Defender for Cloud Apps.

## Módulo 14: Investigar y responder a las alertas de Prevención de Pérdidas de Datos de Microsoft Purview.

Microsoft Purview y Microsoft Defender XDR ayudan a las organizaciones a detectar posibles riesgos de pérdida de datos y a responder rápidamente para proteger la información sensible. Las actividades de investigación y respuesta incluyen revisar alertas DLP, aplicar acciones de remediación adecuadas y documentar los hallazgos de manera estructurada y consistente.

- Comprender las alertas de prevención de pérdida de datos (DLP).
- Entiende el ciclo de vida de las alertas DLP.
- Configurar las políticas DLP para generar alertas.
- Investigar alertas DLP en el ámbito de Microsoft.
- Investigar alertas DLP en Microsoft Defender XDR.
- Investiga alertas DLP con Security Copilot y agentes de IA.
- Responder a alertas DLP.

**Ejercicio: Investigar una alerta DLP y un incidente relacionado.**

## Ruta de aprendizaje: Implementar y gestionar la retención y recuperación de Microsoft 365.

Aprende a gestionar el ciclo de vida de los datos en Microsoft 365 utilizando políticas de retención y etiquetas. Entiende cómo configurar y aplicar configuraciones de retención que cumplan con los requisitos organizativos para preservar o eliminar contenido en los servicios de Microsoft 365.

## Módulo 15: Entiende la retención en Microsoft Champview.

La retención de Microsoft Purview ayuda a las organizaciones a gestionar cuánto tiempo se conservan los datos y cuándo pueden eliminarse. Aprende a aplicar la retención de forma estratégica para cumplir con los requisitos de cumplimiento, reducir riesgos y proteger información importante a lo largo de su ciclo de vida.





- Visión general de la retención y el ciclo de vida de los datos.
- Comprende las etiquetas y políticas de retención.
- Decide cuándo solicitar la retención.

### **Módulo 16: Implementar y gestionar la retención y recuperación de Microsoft 365.**

Microsoft Purview ofrece herramientas para gestionar cuánto tiempo se conserva el contenido y cuándo se elimina en los servicios de Microsoft 365. Estos ajustes de retención aplican reglas del ciclo de vida usando etiquetas, políticas y ámbitos adaptativos. Cuando se elimina contenido, las opciones de recuperación se gestionan dentro de los servicios individuales, como SharePoint y Exchange. En conjunto, estas herramientas apoyan el cumplimiento normativo y la seguridad de la información reduciendo el riesgo de retener datos innecesarios o desactualizados.

- Planifica la retención y disposición con etiquetas de retención.
- Crear y publicar etiquetas de retención.
- Crea y gestiona etiquetas de retención de auto-aplicación.
- Crear y configurar ámbitos adaptativos.
- Crear y configurar políticas de retención.
- Comprender la precedencia de políticas y etiquetas en el ámbito de Microsoft.
- Recuperar contenido en cargas de trabajo de Microsoft 365.

### **Ruta de aprendizaje: Implementar y gestionar la gestión de riesgos internos de Microsoft Purview.**

Implementar Microsoft Purview Insider Risk Management para detectar, investigar y responder a riesgos internos, protegiendo los datos, asegurando el cumplimiento y manteniendo la confianza de los empleados.

### **Módulo 17: Entiende la gestión interna de riesgos de Microsoft Purview.**

Comprende los riesgos internos y descubre cómo Microsoft Purview Insider Risk Management identifica actividades riesgosas, analiza el contexto y ayuda a las organizaciones a proteger los datos respetando la privacidad.

- ¿Qué es un riesgo interno?
- Resumen de Microsoft Purview Insider Risk Management.

- Funciones de Gestión de Riesgos Insider de Microsoft Purview.
- Caso de Estudio: Proteger datos sensibles con Gestión de Riesgos Internos.

### **Módulo 18: Prepárate para Microsoft Purview Insider Risk Management.**

Descubre estrategias para planificar y configurar Microsoft Purview Insider Risk Management para satisfacer las necesidades organizativas y proteger la privacidad.

- Plan para la Gestión de Riesgos Internos.
- Prepara a tu organización para la Gestión de Riesgos Internos.
- Configurar la configuración para la Gestión de Riesgos Internos.
- Integra la Gestión de Riesgos Internos con fuentes de datos y herramientas.

### **Módulo 19: Crear y gestionar políticas de Gestión de Riesgos Internos.**

Crear y gestionar políticas de Gestión de Riesgos Internos de Microsoft Purview para detectar y abordar posibles riesgos internos, al tiempo que apoyan la seguridad y privacidad de la organización.

- Comprender las plantillas de políticas de Gestión de Riesgos Internos.
- Compara pólizas de riesgo interno rápidas y personalizadas.
- Crea una política personalizada de Gestión de Riesgos Internos.
- Gestionar políticas en la Gestión de Riesgos Internos.

### **Módulo 20: Investigar alertas de riesgos internos y actividades relacionadas.**

Investigar alertas de riesgo internos y gestionar casos relacionados en el ámbito de Microsoft para evaluar el comportamiento de los usuarios, tomar las medidas adecuadas y coordinar revisiones más profundas entre equipos.

- Entiende las alertas de riesgos internos e investigaciones.
- Gestionar el volumen de alertas en la gestión de riesgos internos.

- Investigar y triaje alertas de riesgo interno en el ámbito de Microsoft.
- Investiga alertas de riesgo interno con Security Copilot y agentes de IA.
- Analizar el contexto de la alerta con la pestaña de Todos los factores de riesgo.
- Investiga los detalles de la actividad con la pestaña Explorador de actividades.
- Revisa patrones a lo largo del tiempo con la pestaña de actividad del usuario.
- Investiga alertas de riesgo interno en Microsoft Defender XDR.
- Gestionar y actuar en casos de riesgo interno.

**Ejercicio: Investigar posibles robos de datos utilizando Gestión de Riesgos Internos.**

### **Módulo 21: Implementar la protección adaptativa en la gestión de riesgos internos.**

Entiende cómo la Protección Adaptativa aplica el aprendizaje automático para evaluar el riesgo del usuario y aplicar automáticamente el nivel adecuado de controles de seguridad. Al asignar dinámicamente políticas de prevención de pérdida de datos, gestión del ciclo de vida de datos y acceso condicional, se refuerza la seguridad de los datos mientras se reducen alertas innecesarias e intervenciones manuales.

- Visión general de la Protección Adaptativa.
- Comprender y configurar los niveles de riesgo en la Protección Adaptativa.
- Configurar la protección adaptativa.
- Gestionar la protección adaptativa.

### **Ruta de aprendizaje: Auditoría y actividad de búsqueda en el ámbito de Microsoft.**

Entiende cómo usar Microsoft Purview para registrar la actividad y buscar contenido en los servicios de Microsoft 365. Descubre cómo el registro de auditorías apoya las investigaciones y los requisitos de cumplimiento, y cómo la búsqueda de contenido puede ayudar a localizar correos electrónicos, documentos y otros elementos específicos cuando sea necesario.

### **Módulo 22: Busca e investiga con Microsoft Purview Audit.**

Mejora la seguridad y el cumplimiento de los datos con Microsoft Purview Audit configurando auditorías detalladas, gestionando registros y analizando patrones de acceso.

- Resumen de la auditoría Microsoft Purview.
- Configurar y gestionar Microsoft Purview Audit.
- Realizar búsquedas con Auditoría (Estándar).
- Auditar Microsoft Copilot para interacciones con Microsoft 365.
- Investiga actividades con Auditoría (Premium).
- Exportar datos de registro de auditoría.
- Configurar la retención de auditoría con Auditoría (Premium).

### **Módulo 23: Buscar contenido con Microsoft Purview eDiscovery.**

Utiliza Microsoft Purview eDiscovery para buscar contenido en Microsoft 365. Este módulo explica cómo configurar casos, definir criterios de búsqueda y localizar mensajes, archivos y otros datos organizativos.

- Comprender las capacidades de eDiscovery y búsqueda de contenido.
- Requisitos previos para usar eDiscovery en Microsoft Purview.
- Crear una búsqueda de eDiscovery.
- Realiza una búsqueda de eDiscovery.
- Exportar resultados de búsqueda de eDiscovery.

### **Ruta de aprendizaje: Interacciones y entornos seguros de IA con Microsoft Purview.**

Herramientas de IA como Microsoft Copilot y aplicaciones de IA personalizadas pueden acceder y generar contenido sensible en toda tu organización. Aprendes cómo:

- Aplicar etiquetas de sensibilidad y políticas de prevención de pérdida de datos para que la IA respete las protecciones existentes.
- Utiliza la Gestión de Postura de Seguridad de Datos para IA y herramientas de auditoría para descubrir e investigar riesgos relacionados con la IA.
- Aplica el eDiscovery y el Cumplimiento de la Comunicación para gestionar el contenido generado por IA.





- Utiliza la Gestión de Riesgos Internos y la Protección Adaptativa para responder a conductas de riesgo y reducir el exceso de información.

## Módulo 24: Entiende cómo proteger los datos de IA con el ámbito de Microsoft.

Microsoft Purview ayuda a las organizaciones a evaluar cómo interactúan Microsoft 365 Copilot y otras herramientas de IA con datos sensibles. Utilizando la Gestión de Postura de Seguridad de Datos (DSPM) para la IA, las organizaciones pueden evaluar los riesgos de exposición, entender qué herramientas de IA se utilizan e identificar cómo se accede a los datos sensibles durante las interacciones con IA. La auditoría proporciona transparencia sobre prompts y respuestas específicas de Copilot para escenarios de cumplimiento e investigación.

- Comprende los riesgos de seguridad de los datos de la IA.
- Entiende cómo Microsoft Purview protege los datos de IA.
- Evaluar los riesgos de cumplimiento normativo por el uso de IA.
- Identificar los riesgos de exposición a datos relacionados con la IA.
- Entiende cómo Microsoft Purview controla el acceso a los datos de la IA.
- Detectar y responder a actividades de IA de riesgo.
- Conservar y buscar prompts y respuestas de Copilot.

## Módulo 25: Interacciones seguras de Microsoft 365 Copilot con Microsoft Purview.

Herramientas de IA como Microsoft 365 Copilot crean nuevas formas de interactuar con datos sensibles, pero también introducen nuevos riesgos. Descubre cómo Microsoft Purview te ayuda a aplicar controles de seguridad y cumplimiento que protegen los datos, gestionan la actividad de la IA y apoyan un uso responsable a gran escala.

- Entiende cómo Microsoft 365 Copilot cambia las necesidades de protección de datos.
- Evalúa el cumplimiento normativo de Copilot con el Responsable de Cumplimiento.
- Interacciones de Audit Copilot con Microsoft Purview.
- Analizar las interacciones de Copilot con el cumplimiento de comunicaciones.

- Clasifica y protege el contenido de Copilot con etiquetas de sensibilidad.
- Aplicar políticas DLP a Microsoft 365 Copilot.
- Aplica políticas de retención a los prompts y respuestas de Copilot.
- Investigar y eliminar la actividad de Copilot con eDiscovery.

## Módulo 26: Aplicaciones de IA empresariales y de navegador seguras con Microsoft Purview.

Las herramientas de IA en entornos empresariales y públicos crean nuevas oportunidades, pero también introducen riesgos de seguridad y cumplimiento de los datos. Microsoft Purview ayuda a reducir estos riesgos descubriendo el uso de la IA, evaluando las necesidades de cumplimiento normativo y aplicando controles integrados para su protección, retención y uso responsable.

- Comprende los riesgos de las herramientas de IA empresariales y no de Microsoft.
- Evaluar el uso de la IA para garantizar la seguridad y el cumplimiento normativo.
- Identificar infracciones de políticas con Cumplimiento de Comunicación.
- Detecta el uso riesgoso de IA con Gestión de Riesgos Internos.
- Proteger datos sensibles en aplicaciones de IA con Microsoft Purview DLP.
- Caso de Estudio: Utilizar la Protección Adaptativa para responder al riesgo relacionado con la IA.
- Aplica políticas de retención a las preguntas y respuestas de las aplicaciones de IA.

## Módulo 27: Entornos de IA seguros para desarrolladores con Microsoft Purview.

Microsoft Purview proporciona herramientas para proteger los entornos de IA de los desarrolladores mediante la detección de aplicaciones, la evaluación del acceso a datos y la aplicación de las protecciones adecuadas. Esto incluye detectar el uso de IA generativa, asignar niveles de riesgo para el usuario y aplicar una aplicación dinámica basada en el comportamiento del usuario y la sensibilidad de los datos.

- Comprender los riesgos y responsabilidades en los entornos de desarrollo de IA.
- Descubre y evalúa aplicaciones de IA con DSPM para IA.



## SC-401T00

Protect sensitive information with Microsoft Purview in the AI era

C

- Clasificar, restringir y conservar datos de prompts de IA.
- Hacer cumplir las protecciones en Microsoft Foundry y Foundry Tools.
- Aplicar controles para aplicaciones de IA personalizadas registradas en Microsoft Entra.
- Agentes de IA seguros integrados en Copilot Studio.
- Gestionar los riesgos de datos en Copilot en Fabric.
- Investigar y responder a actividades de IA de riesgo.

[clientes@ked.com.mx](mailto:clientes@ked.com.mx)

