The DevSecOps Company

Microsoft Partner

SC-401T00
Information Security Administrator

Información general.

Este curso proporciona las habilidades necesarias para planificar e implementar la seguridad de la información para datos confidenciales utilizando Microsoft Purview y servicios relacionados. El curso cubre temas esenciales como la protección de la información, la prevención de la pérdida de datos (DLP), la retención y la gestión de riesgos internos. Aprende a proteger los datos dentro de los entornos de colaboración de Microsoft 365 de amenazas internas y externas. Además, aprenderá a administrar alertas de seguridad y responder a incidentes investigando actividades, respondiendo a alertas de DLP y administrando casos de riesgo interno. También aprenderá a proteger los datos utilizados por los servicios de IA dentro de los entornos de Microsoft e implementar controles para salvaguardar el contenido en estos entornos.

Duración.

4 Días.

Perfil del público.

Como administrador de seguridad de la información, usted planifica e implementa la seguridad de la información para datos confidenciales utilizando Microsoft Purview y servicios relacionados. Usted es responsable de mitigar los riesgos al proteger los datos dentro de los entornos de colaboración de Microsoft 365 de amenazas internas y externas, así como de salvaguardar los datos utilizados por los servicios de IA. Su función incluye la implementación de la protección de la información, la prevención de la pérdida de datos (DLP), la retención y la gestión de riesgos internos. También gestiona las alertas de seguridad y responde a los incidentes investigando actividades, respondiendo a las alertas de DLP y gestionando casos de riesgo interno. En este rol, colaboras con otros roles responsables de la gobernanza, los datos y la seguridad para desarrollar políticas que aborden los objetivos de seguridad de la información y reducción de riesgos de tu organización. Trabaja con administradores de carga de trabajo, propietarios de aplicaciones empresariales y partes interesadas de gobernanza para implementar soluciones tecnológicas que respalden estas políticas y controles.

Examen.

Este curso no tiene un examen asociado.

Temario.

Ruta de aprendizaje: Implementación de Microsoft Purview Information Protection.

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

Módulo 1: Protección de datos confidenciales en un mundo digital.

Descubra cómo Microsoft Purview ayuda a las organizaciones a clasificar, proteger y supervisar datos confidenciales en entornos

KeD es una empresa sustentable, Por favor no imprimas este documento si no es necesario.

de nube, punto de conexión e inteligencia artificial. En este módulo se exploran las estrategias para proteger los datos mediante la clasificación, el etiquetado, el cifrado y la administración proactiva de riesgos.

- Introducción.
- La creciente necesidad de protección de datos.
- Los desafíos de la administración de datos confidenciales.
- Protección de datos en un mundo de confianza cero.
- Descripción de la clasificación y protección de datos.
- Prevención de pérdidas de datos y amenazas internas.
- Administración de alertas de seguridad y respuesta a amenazas.
- Protección de los datos generados por la inteligencia artificial y procesados por ia.

Módulo 2: Clasificación de datos para protección y gobernanza.

Obtenga información sobre la información disponible para ayudarle a comprender el panorama de los datos y conocer sus datos.

- Información general sobre la clasificación de datos.
- Clasificar los datos mediante tipos de información confidencial.
- Clasificar los datos con clasificadores que se pueden entrenar.
- Creación de un clasificador personalizado que se puede entrenar.

Módulo 3: Revisión y análisis de la clasificación y protección de datos.

Descubra cómo Microsoft Purview ayuda a las organizaciones a monitorear y analizar la clasificación y protección de datos. Este módulo explora cómo los equipos de seguridad pueden realizar un seguimiento de las tendencias de clasificación, investigar el contenido etiquetado y evaluar la eficacia de las políticas mediante los informes de protección de la información, el explorador de datos, el explorador de contenido y el explorador de actividades.

- Revisar la clasificación y los conocimientos de protección. Analizar datos clasificados con el explorador de datos y contenido.
- Supervisar y revisar las acciones sobre los datos etiquetados.

Módulo 4: Creación y administración de tipos de información confidencial.

Obtenga información sobre cómo usar tipos de información confidencial para respaldar su estrategia de protección de la información.

- Información general sobre tipos de información confidencial.
- Comparación de tipos de información confidencial integrados y personalizados.
- Creación y administración de tipos de información confidencial personalizados.
- Crear y administrar datos exactos que coincidan con tipos de información confidencial.
- Implementación de huellas digitales de documentos.
- Describir las entidades con nombre.
- Creación de un diccionario de palabras clave.

Módulo 5: Creación y configuración de etiquetas de confidencialidad con Microsoft Purview.

Las etiquetas de confidencialidad de Microsoft Purview le permiten clasificar y proteger datos confidenciales en toda la organización, incluidos en la nube y en los dispositivos. En este módulo se explica cómo clasificar y proteger la información confidencial para garantizar su seguridad y cumplimiento.

- Introducción a la etiqueta de confidencialidad.
- Creación y configuración de etiquetas de confidencialidad y directivas de etiquetas.
- Configuración del cifrado con etiquetas de confidencialidad.
- Implementación de directivas de etiquetado automático.
- Seguimiento y evaluación del uso de etiquetas de confidencialidad en Microsoft Purview.

Módulo 6: Aplicación de etiquetas de confidencialidad para la protección de datos.

Obtenga información sobre cómo se usan las etiquetas de confidencialidad para clasificar y proteger los datos empresariales, a la vez que se asegura de que la productividad del usuario y su capacidad de colaborar no se ven afectadas.

- Fundamentos de la integración de etiquetas de confidencialidad en Microsoft 365.
- Administración de etiquetas de confidencialidad para aplicaciones de Office.

KeD es una empresa sustentable, Por favor no imprimas este documento si no es necesario.

- Aplicación de etiquetas de confidencialidad con Microsoft 365 Copilot para la colaboración segura.
- Protección de reuniones con etiquetas de confidencialidad.
- Aplicar etiquetas de confidencialidad a Microsoft Teams, grupos de Microsoft 365 y sitios de SharePoint.

Módulo 7: Clasificación y protección de datos locales con Microsoft Purview.

Obtenga información sobre cómo clasificar y proteger los datos confidenciales almacenados en el entorno local mediante Microsoft Purview. Este módulo le guía a través de la implementación del analizador de Information Protection, la aplicación de etiquetas de confidencialidad y la aplicación de directivas DLP para reducir los riesgos de exposición de datos.

- Protección de archivos locales con Microsoft Purview.
- Prepárese el entorno para el analizador de Protección de la Información de Microsoft Purview.
- Configuración e instalación del analizador de Microsoft Purview Information Protection.
- Ejecución y administración del analizador.
- Aplicación de directivas de prevención de pérdida de datos en archivos locales.

Módulo 8: Descripción del cifrado de Microsoft 365.

Obtenga información sobre cómo Microsoft 365 cifra los datos en reposo y en tránsito, administra de forma segura las claves de cifrado y proporciona opciones de administración de claves a los clientes para satisfacer sus necesidades empresariales y obligaciones de cumplimiento.

- Introducción al cifrado de Microsoft 365.
- Obtenga información sobre cómo se cifran los datos de Microsoft 365 en reposo.
- Descripción del cifrado de servicio en Microsoft Purview.
- Explorar la administración de claves de cliente mediante la clave de cliente.
- Obtenga información sobre cómo se cifran los datos en tránsito.

Módulo 9: Protección del correo electrónico con el cifrado de mensajes de Microsoft Purview.

Obtenga información sobre cómo configurar el cifrado de mensajes de Microsoft Purview para proteger el correo electrónico confidencial, aplicar cifrado con reglas de flujo de correo y personalizar la experiencia del destinatario con plantillas de marca.

- Descripción del cifrado de mensajes.
- Planear el cifrado de mensajes de Microsoft Purview.
- Configuración del cifrado de mensajes de Microsoft Purview.
- Personalización de la marca de correo electrónico cifrada con Microsoft Purview.
- Control del acceso cifrado al correo electrónico con cifrado de mensajes avanzado.
- Uso de plantillas de cifrado de mensajes de Microsoft Purview en reglas de flujo de correo.

Ruta de aprendizaje: Implementación y administración de la prevención de pérdida de datos de Microsoft Purview.

Las organizaciones deben evitar la pérdida de datos y proteger la información confidencial en entornos de nube y punto de conexión. Microsoft Purview proporciona directivas de prevención de pérdida de datos (DLP) para detectar, restringir y responder a actividades de riesgo que implican datos confidenciales. Aprenda a planear y configurar directivas DLP, realizar un seguimiento de la eficacia de las directivas y analizar los riesgos de seguridad de datos para mejorar la estrategia de protección de su organización.

Módulo 10: Evitar la pérdida de datos en Microsoft Purview.

La prevención de pérdida de datos (DLP) de Microsoft Purview ayuda a proteger la información confidencial mediante la supervisión y la prevención de pérdidas accidentales de datos en las plataformas digitales de su organización. En este módulo, aprenderá a planear, implementar y ajustar directivas DLP para proteger los datos confidenciales de su organización, lo que garantiza la seguridad sin interrumpir el trabajo diario.

- Descripción general de la prevención de la pérdida de datos.
- Planificar y diseñar políticas de DLP.
- Comprender el modo de implementación y simulación de la política de DLP.
- Crear y gestionar políticas de DLP.
- Integrar la protección adaptativa con DLP.

KeD® es una marca registrada ante el Instituto Mexicano de la Propiedad Intelectual

- Utilice el análisis de DLP (vista previa) para identificar los riesgos de los datos.
- Comprender las alertas de DLP y el seguimiento de la actividad.

Módulo 11: Implementación de la prevención de pérdida de datos (DLP) en punto de conexión con Microsoft Purview.

Endpoint DLP en Microsoft Purview ayuda a las organizaciones a proteger los datos confidenciales en los dispositivos de punto final al monitorear, restringir o permitir acciones como transferencias de archivos, copiar y compartir. Aprenda a incorporar dispositivos, configurar ajustes y crear políticas personalizadas para garantizar la seguridad de los datos en toda su organización.

- Descripción general de la prevención de la pérdida de datos de punto final (DLP).
- Comprender el flujo de trabajo de implementación de DLP. Dispositivos integrados para DLP de punto final.
- Configurar los ajustes para el DLP del punto final.
- Crear y administrar políticas de DLP de punto final.
- Implemente la extensión del navegador Microsoft Purview.
- Configurar la protección justo a tiempo (JIT).

Módulo 12: Configuración de directivas DLP para Microsoft Defender for Cloud Apps y Power Platform.

Aprenda a configurar e implementar directivas de prevención de pérdida de datos e integrarlas con Microsoft Defender for Cloud Apps.

- Configuración de directivas de prevención de pérdida de datos para Power Platform.
- Integración de la prevención de pérdida de datos en Microsoft Defender for Cloud Apps.
- Configuración de directivas en Microsoft Defender for Cloud Apps.
- Administración de infracciones de prevención de pérdida de datos en Microsoft Defender for Cloud Apps.

Módulo 13: Investigar y responder a alertas de prevención de pérdida de datos de Microsoft Purview.

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

- Descripción de las alertas de prevención de pérdida de datos.
- Descripción del ciclo de vida de las alertas DLP.
- Configuración de directivas DLP para generar alertas.
- Investigar las alertas de DLP en Microsoft Purview.
- Investiga las alertas DLP en Microsoft Defender XDR.
- Responder a alertas DLP.

Ruta de aprendizaje: Implementación y administración de riesgos internos de Microsoft Purview.

Implemente Administración de riesgos internos de Microsoft Purview para detectar, investigar y responder a riesgos internos al tiempo que protege los datos, garantiza el cumplimiento y mantiene la confianza de los empleados.

Módulo 14: Comprender la Administración de riesgos internos de Microsoft Purview.

Comprenda los riesgos internos y descubra cómo Administración de riesgos internos de Microsoft Purview identifica las actividades de riesgo, analiza el contexto y ayuda a las organizaciones a proteger los datos al tiempo que respeta la privacidad.

- ¿Qué es un riesgo interno?
- Introducción a la Administración de riesgos internos de Microsoft Purview.
- Características de la Administración de riesgos internos de Microsoft Purview.

Caso práctico: Protección de datos confidenciales con la administración de riesgos internos.

Módulo 15: Preparación para la administración de riesgos internos de Microsoft Purview.

Descubra estrategias para planear y configurar Microsoft Purview Insider Risk Management para satisfacer las necesidades de la organización y proteger la privacidad.

KeD es una empresa sustentable, Por favor no imprimas este documento si no es necesario.

- Planeamiento de la administración de riesgos internos.
- Preparación de la organización para la administración de riesgos internos.
- Configuración de las opciones de administración de riesgos internos.
- Integrar la administración de riesgos internos con fuentes de datos y herramientas.

Módulo 16: Creación y administración de directivas de administración de riesgos internos.

Cree y administre las directivas de administración de riesgos internos de Microsoft Purview para detectar y abordar posibles riesgos internos al tiempo que respalda la seguridad y la privacidad de la organización.

- Descripción de las plantillas de directiva de administración de riesgos internos.
- Comparación de directivas de riesgo interno rápidas y personalizadas.
- Creación y administración de directivas en la administración de riesgos internos.

Módulo 17: Investigación de alertas de riesgo interno y actividad relacionada.

Investigue las alertas de riesgo interno y administre casos relacionados en Microsoft Purview para evaluar el comportamiento del usuario, tomar las medidas adecuadas y coordinar las revisiones más profundas en todos los equipos.

- Comprender las alertas e investigaciones de riesgos internos.
- Gestionar el volumen de alertas en la gestión de riesgos internos.
- Investigar y clasificar las alertas de riesgos internos en Microsoft Purview.
- Analizar el contexto de la alerta con la pestaña Todos los factores de riesgo.
- Investiga los detalles de la actividad con la pestaña Explorador de actividades.
- Revise los patrones a lo largo del tiempo con la pestaña de actividad del usuario.
- Investigue las alertas de riesgo interno en Microsoft Defender XDR.
- Gestionar y tomar medidas en casos de riesgo interno.

Módulo 18: Implementación de la protección adaptable en Insider Risk Management.

Comprenda cómo Adaptive Protection aplica el aprendizaje automático para evaluar el riesgo del usuario y aplicar automáticamente el nivel adecuado de controles de seguridad. Al asignar dinámicamente la prevención de pérdida de datos, la administración del ciclo de vida de los datos y las directivas de acceso condicional, se refuerza la seguridad de los datos, a la vez que se reducen las alertas innecesarias y la intervención manual.

- Introducción a Adaptive Protection.
- Descripción y configuración de los niveles de riesgo en Adaptive Protection.
- Configurar la Protección adaptativa.
- Administrar la Protección adaptativa.

Ruta de aprendizaje: Proteja los datos en entornos de IA con Microsoft Purview.

Las herramientas de IA como Microsoft Copilot están cambiando la forma en que las personas trabajan, pero también aumentan el riesgo de compartir en exceso y exposición accidental de datos. Microsoft Purview ayuda a las organizaciones a aplicar los controles correctos para mantener protegidos los datos confidenciales en entornos habilitados para IA.

Módulo 19: Descubra las interacciones de IA con Microsoft Purview.

Microsoft Purview ayuda a las organizaciones a descubrir cómo interactúan Microsoft 365 Copilot y otras herramientas de IA con los datos. Usando la gestión de la postura de seguridad de datos (DSPM) para la IA y la auditoría, los equipos de seguridad pueden detectar la actividad de la IA, evaluar los riesgos potenciales y recopilar información para apoyar las estrategias de protección de datos y cumplimiento.

- Comprender los riesgos de seguridad de la IA.
- Descripción general de Microsoft Purview Data Security Posture Management (DSPM) para IA.
- Configurar DSPM para IA.
- Revisar los informes de seguridad de la IA.
- Auditar las actividades de Microsoft 365 Copilot e interacciones de IA con Microsoft Purview.

KeD® es una marca registrada ante el Instituto Mexicano de la Propiedad Intelectual

Módulo 20: Proteja los datos confidenciales de los riesgos relacionados con la IA.

Microsoft Purview ayuda a las organizaciones a proteger los datos confidenciales en entornos que utilizan herramientas de IA. Aprenda a reducir los riesgos de seguridad de los datos aplicando etiquetas de sensibilidad, utilizando controles de prevención de pérdida de datos e implementando protecciones recomendadas a través de DSPM para IA.

- Aplicar recomendaciones de seguridad de IA con DSPM para IA.
- Utilice etiquetas de confidencialidad para proteger el contenido de Microsoft 365 Copilot.
- Utilice Endpoint DLP para evitar la exposición de datos generativos de IA.

Módulo 21: Gobierna el uso de la IA con Microsoft Purview.

Aprenda a aplicar políticas y administrar el ciclo de vida del contenido generado por IA utilizando Microsoft Purview. Este módulo muestra cómo conservar, eliminar, investigar y revisar el contenido creado en Microsoft 365 Copilot y otras aplicaciones de IA.

- Aplicar políticas de retención a los mensajes y respuestas de Microsoft 365 Copilot.
- Investigar y eliminar las interacciones de Copilot con Microsoft Purview eDiscovery.
- Detecta y gestiona las comunicaciones de Copiloto e IA con Microsoft Purview.

Módulo 22: Evalúe y mitigue los riesgos de IA con Microsoft Purview.

Microsoft Purview incluye herramientas que ayudan a detectar actividades de riesgo y aplicar protecciones basadas en políticas en entornos de IA. Esto incluye detectar el uso generativo de la IA, asignar niveles de riesgo al usuario y ajustar las acciones de aplicación en función de esos niveles.

- Utilice evaluaciones de datos para detectar riesgos de sobrecompartir.
- Detecta el uso de IA de riesgo con Insider Risk Management.
- Estudio de caso: Utilice la protección adaptativa para responder al riesgo relacionado con la IA.

Ruta de aprendizaje: Implementación y administración de la retención y recuperación de Microsoft 365.

Obtenga información sobre cómo administrar el ciclo de vida de los datos en Microsoft 365 mediante directivas y etiquetas de retención. Comprenda cómo configurar y aplicar opciones de retención que cumplan los requisitos de la organización para conservar o eliminar contenido en los servicios de Microsoft 365.

Módulo 23: Comprender la retención en Microsoft Purview.

La retención de Microsoft Purview ayuda a las organizaciones a administrar cuánto tiempo se conservan los datos y cuándo se pueden eliminar. Obtenga información sobre cómo aplicar la retención estratégicamente para cumplir los requisitos de cumplimiento, reducir el riesgo y proteger información importante a lo largo de su ciclo de vida.

- Descripción de la retención y el ciclo de vida de los datos.
- Comprender las etiquetas de retención y las políticas de retención.
- Decidir cuándo aplicar la retención.

Módulo 24: Implementación y administración de la retención y recuperación de Microsoft 365.

Microsoft Purview proporciona herramientas para administrar cuánto tiempo se conserva el contenido y cuándo se elimina en los servicios de Microsoft 365. Esta configuración de retención aplica reglas de ciclo de vida mediante etiquetas, directivas y ámbitos adaptables. Cuando se elimina el contenido, las opciones de recuperación se administran dentro de los servicios individuales, como SharePoint y Exchange. Conjuntamente, estas herramientas admiten el cumplimiento y la seguridad de la información al reducir el riesgo de conservar datos innecesarios o obsoletos.

- Plan de retención y disposición con etiquetas de retención.
- Crear y publicar etiquetas de retención.
- Crear y gestionar etiquetas de retención de aplicación automática.
- Crear y configurar ámbitos adaptativos y políticas de retención.
- Comprender la precedencia de políticas y etiquetas en Microsoft Purview.
- Recuperar contenido en las cargas de trabajo de Microsoft 365.

KeD es una empresa sustentable, Por favor no imprimas este documento si no es necesario.

Ruta de aprendizaje: Actividad de auditoría y búsqueda en Microsoft Purview.

Comprenda cómo usar Microsoft Purview para registrar la actividad y buscar contenido en los servicios de Microsoft 365. Obtenga información sobre cómo el registro de auditoría admite investigaciones y requisitos de cumplimiento, y cómo la búsqueda de contenido puede ayudar a localizar correos electrónicos, documentos y otros elementos específicos cuando sea necesario.

Módulo 25: Búsqueda e investigación con Microsoft Purview Audit.

Mejore la seguridad de los datos y el cumplimiento con Microsoft Purview Audit mediante la configuración de auditorías detalladas, la administración de registros y el análisis de patrones de acceso.

- Introducción a Auditoría de Microsoft Purview.
- Configuración y administración de Auditoría de Microsoft Purview.
- Realización de búsquedas con Auditoría (Estándar).
- Auditar interacciones de Microsoft Copilot para Microsoft 365.
- Investigar actividades con Auditoría (Premium).
- Exportar datos de registro de auditoría.
- Configuración de la retención de auditoría con Auditoría (Prémium).

Módulo 26: Buscar contenido con eDiscovery de Microsoft Purview.

Use eDiscovery de Microsoft Purview para buscar contenido en Microsoft 365. En este módulo se explica cómo configurar casos, definir criterios de búsqueda y buscar mensajes, archivos y otros datos de la organización.

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