ExecuTrain

Impulsamos tu talento tecnológico

MICROSOFT	RED HAT	VIRTUALIZACIÓN
CIBERSEGURIDAD	DESARROLLO	OFFICE
BIG DATA	BLOCK CHAIN	BASES DE DATOS
GESTIÓN DE SERVICIOS IT	CLOUD COMPUTING	METODOLOGÍAS EN PROYECTOS
SISTEMAS OPERATIVOS	Y MÁS...	

www.executrain.com.mx

¿Por qué ExecuTrain?

ExecuTrain es un proveedor de entrenamiento corporativo a nivel internacional y líder mundial en la capacitación empresarial. Contamos con más de 30 años de Experiencia y con más de 75 mil personas capacitadas a nivel Nacional.

Te guiamos en la definición de tus requerimientos de capacitación, en las diferentes etapas:

- ✓ Detección de necesidades, evaluación de conocimientos, plan de capacitación y seguimiento posterior para elegir el plan de capacitación como tú lo necesitas.
- ✓ El **más amplio catálogo de cursos**, desde un nivel básico hasta los niveles de conocimientos más especializados.
- ✓ En ExecuTrain el material y la **metodología están diseñados por expertos en aprendizaje humano**. Lo que te garantiza un mejor conocimiento en menor tiempo.
- ✓ Tú puedes confiar y estar seguro del aprendizaje porque nuestro **staff de instructores es de primer nivel**, algunos de los cuales son consultores en reconocidas empresas.
- ✓ No pierdas tu tiempo, los cursos están diseñados para un aprendizaje práctico.

Nuestro compromiso es que tú aprendas, si no quedas satisfecho con los resultados del programa, podrás volver a tomar los cursos hasta tu entera satisfacción o la devolución de tu dinero.

Modalidad de Servicio

Cursos en Fecha Calendario

Súmate a nuestros grupos en fechas públicas.

Cursos Privados

On site, en nuestras instalaciones o en línea con instructor en vivo.

Autoestudio con soporte de instructor

Cursos en modalidad autoestudio, con acceso 24/7 a la plataforma de estudio, con soporte de instructor y foros de ayuda

ExecuTrain
Impulsamos tu talento tecnológico

Duración: 28 horas

SC-401 / Protect sensitive information with Microsoft Purview in the AI era

El curso de Administrador de Seguridad de la Información le proporciona las habilidades necesarias para planificar e implementar la seguridad de la información para datos confidenciales mediante Microsoft Purview y servicios relacionados. El curso abarca temas esenciales como la protección de la información, la prevención de pérdida de datos (DLP), la retención y la gestión de riesgos internos. Aprenderá a proteger los datos en entornos de colaboración de Microsoft 365 contra amenazas internas y externas. Además, aprenderá a administrar alertas de seguridad y a responder a incidentes mediante la investigación de actividades, la respuesta a alertas de DLP y la gestión de casos de riesgo interno. También aprenderá a proteger los datos utilizados por los servicios de IA en entornos Microsoft e implementar controles para salvaguardar el contenido en estos entornos.

Perfil del Público

Como Administrador de Seguridad de la Información, planificará e implementará la seguridad de la información para datos confidenciales mediante Microsoft Purview y servicios relacionados. Será responsable de mitigar riesgos protegiendo los datos en los entornos de colaboración de Microsoft 365 contra amenazas internas y externas, así como de salvaguardar los datos utilizados por los servicios de IA. Su función implica implementar la protección de la información, la prevención de pérdida de datos (DLP), la retención y la gestión de riesgos internos. También gestionará alertas de seguridad y responderá a incidentes investigando actividades, respondiendo a alertas de DLP y gestionando casos de riesgo interno. En esta función, colaborará 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 su organización. Trabajará con administradores de cargas de trabajo, propietarios de aplicaciones empresariales y partes interesadas en la gobernanza para implementar soluciones tecnológicas que respalden estas políticas y controles.

Rol de trabajo: Administrador de Protección de la Información y Cumplimiento Administrador de Riesgos
Preparación para el examen: SC-401

Requisitos Previos

Antes de participar en este curso, los alumnos deben tener:

- ✓ Familiaridad con las soluciones de cumplimiento de Microsoft Purview
- ✓ Conocimientos básicos sobre la protección de datos y los conceptos de seguridad

Módulos

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 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
- Evaluación de módulos
- Resumen

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.

- Introducción
- Descripción general de la clasificación de datos
- Clasificar datos utilizando tipos de información confidencial
- Clasifique datos utilizando clasificadores entrenables
- Crear un clasificador entrenable personalizado
- Evaluación del módulo
- Resumen

Revisión y análisis de la clasificación y protección de datos

Descubra cómo Microsoft Purview ayuda a las organizaciones a supervisar y analizar la clasificación y protección de datos. En este módulo se 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 directivas mediante informes de Information Protection, Explorador de datos, Explorador de contenido y Explorador de actividades.

- Introducción
- Revisar los conocimientos sobre clasificación y protección
- Analice datos clasificados con el explorador de datos y contenido
- Supervisar y revisar acciones sobre datos etiquetados
- Evaluación del módulo
- Resumen

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.

- Introducción
- 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
- Evaluación de módulos
- Resumen y recursos

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
- Descripción general de la etiqueta de sensibilidad
- Crear y configurar etiquetas de confidencialidad y políticas de etiquetas
- Configurar el cifrado con etiquetas de confidencialidad
- Implementar políticas de etiquetado automático
- Realizar un seguimiento y evaluar el uso de etiquetas de confidencialidad en Microsoft Purview
- Evaluación del módulo
- Resumen

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

- Introducción
- Fundamentos de la integración de etiquetas de confidencialidad en Microsoft 365
- Administración de etiquetas de confidencialidad para aplicaciones de Office
- 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
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- Proteja los archivos locales con Microsoft Purview
- Prepare su entorno para el escáner de Microsoft Purview Information Protection
- Configurar e instalar el escáner Microsoft Purview Information Protection
- Ejecutar y administrar el escáner
- Aplicar políticas de prevención de pérdida de datos en los archivos locales
- Evaluación del módulo
- Resumen

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
- Resumen y prueba de conocimientos

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.

- Introducción
- Implementación de cifrado de mensajes de Microsoft Purview
- Implementar Cifrado de mensajes avanzado de Microsoft Purview
- Uso de plantillas de cifrado de mensajes de Microsoft Purview en reglas de flujo de correo
- Evaluación de módulos
- Resumen y recursos

Comprender y planear la prevención de pérdida de datos

La prevención efectiva de pérdida de datos (DLP) comienza con la comprensión de 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 directivas DLP que protegen datos confidenciales sin interrumpir el trabajo diario.

- Introducción
- Descripción del rol de prevención de pérdida de datos (DLP)
- Comprender cómo aplica DLP protección
- Planeamiento y diseño de directivas DLP
- Descripción de la implementación y el modo de simulación de DLP
- Evaluación de controles DLP avanzados para su entorno
- Evaluación del módulo
- Resumen

Creación y administración de directivas de prevención de pérdida de datos

Las directivas eficaces de prevención de pérdida de datos (DLP) están configuradas por una serie de decisiones deliberadas en lugar de configuraciones individuales. La intención clara, la detección bien definida, el ámbito adecuado y las acciones medidaes determinan cómo se comportan las directivas en flujos de trabajo reales. La validación y el ajuste continuo ayudan a garantizar que la protección siga siendo eficaz a medida que cambien el riesgo y el uso.

- Introducción
- Comprender cómo encajan las decisiones de directiva DLP
- Elección de una plantilla o creación de una directiva personalizada
- Definición de lo que detecta la directiva
- Alineación del ámbito de directiva con el riesgo
- Definir cómo responde la directiva
- Validación del comportamiento de la directiva mediante el modo de simulación
- Gestionar políticas DLP
- Ajustar el cumplimiento dinámicamente en función del riesgo
- Tutorial guiado: Creación de una directiva DLP
- Evaluación del módulo
- Resumen

Implementación de la prevención de pérdida de datos (DLP) en punto de conexión con Microsoft Purview

DLP en punto de conexión en Microsoft Purview ayuda a las organizaciones a proteger los datos confidenciales en los dispositivos de punto de conexión mediante la supervisión, restricción o

autorización de acciones como la transferencia, copia y uso compartido de archivos. Aprenda a incorporar dispositivos, establecer la configuración y crear directivas personalizadas para garantizar la seguridad de los datos en toda su organización.

- Introducción
- Introducción a la prevención de pérdida de datos de punto de conexión (DLP)
- Descripción del flujo de trabajo de implementación de DLP del punto de conexión
- Incorporación de dispositivos para DLP de punto de conexión
- Configuración de la DLP del punto de conexión
- Creación y administración de directivas DLP de punto de conexión
- Implementación de la extensión del explorador Microsoft Purview
- Configuración de la protección Just-In-Time (JIT)
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- 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
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- Descripción de las alertas de prevención de pérdida de datos (DLP)
- 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
- Evaluación del módulo
- Resumen

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.

- Introducción
- Información general sobre la retención y el ciclo de vida de los datos
- Descripción de las etiquetas de retención y las directivas de retención
- Decidir cuándo aplicar la retención
- Evaluación del módulo
- Resumen

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.

- Introducción
- Planear la retención y eliminación con etiquetas de retención
- Creación y publicación de etiquetas de retención
- Creación y administración de etiquetas de retención de aplicación automática
- Creación y configuración de ámbitos adaptables
- Crear y configurar directivas de retención
- Comprender la precedencia de directivas y etiquetas en Microsoft Purview
- Recuperación de contenido en cargas de trabajo de Microsoft 365
- Evaluación del módulo
- Resumen

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.

- Introducción
- ¿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
- Evaluación de módulos
- Resumen

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.

- Introducción
- 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 gestión de riesgos internos con fuentes de datos y herramientas
- Evaluación de módulos
- Resumen

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.

- Introducción
- Descripción de las plantillas de directiva de administración de riesgos internos
- Comparar directivas de riesgo interno rápidas y personalizadas
- Creación de una directiva personalizada de administración de riesgos internos
- Administración de directivas en la administración de riesgos internos
- Evaluación de módulos
- Resumen

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.

- Introducción
- Comprender las alertas de riesgo corporativo interno y las investigaciones
- Administración del volumen de alertas en la administración de riesgos internos
- Investigación y evaluación de alertas de riesgo interno en Microsoft Purview
- Investigación de alertas de riesgo interno con Security Copilot y agentes de Inteligencia Artificial
- Análisis del contexto de alerta con la pestaña Todos los factores de riesgo
- Investigar los detalles de la actividad con la pestaña Explorador de actividades
- Revisión de patrones a lo largo del tiempo con la pestaña Actividad de usuario
- Investigar alertas de riesgo interno en Microsoft Defender XDR
- Administración y toma de medidas en casos de riesgo interno
- Ejercicio: Investigación del posible robo de datos mediante la administración de riesgos internos
- Evaluación del módulo
- Resumen

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

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
- 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)
- Evaluación de módulos
- Resumen

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.

- Introducción
- Descripción de las funcionalidades de búsqueda de contenido y eDiscovery

- Requisitos previos para usar eDiscovery en Microsoft Purview
- Creación de una búsqueda de eDiscovery
- Realización de una búsqueda de eDiscovery
- Exportación de resultados de búsqueda de eDiscovery
- Evaluación del módulo
- Resumen y recursos

Información sobre cómo proteger datos de IA con Microsoft Purview

Microsoft Purview ayuda a las organizaciones a evaluar cómo interactúan Microsoft 365 Copilot y otras herramientas de inteligencia artificial con datos confidenciales. Con Data Security Posture Management (DSPM) para la inteligencia artificial, las organizaciones pueden evaluar los riesgos de exposición, comprender qué herramientas de inteligencia artificial están en uso e identificar cómo se accede a los datos confidenciales durante las interacciones de ia. La auditoría proporciona visibilidad de las solicitudes y respuestas específicas de Copilot para escenarios de cumplimiento e investigación.

- Introducción
- Descripción de los riesgos de seguridad de datos de inteligencia artificial
- Comprender cómo Microsoft Purview protege los datos de inteligencia artificial
- Evaluación de los riesgos de cumplimiento para el uso de inteligencia artificial
- Identificación de los riesgos de exposición de datos relacionados con la inteligencia artificial
- Comprender cómo Microsoft Purview controla el acceso a datos de IA
- Detección y respuesta a la actividad de inteligencia artificial de riesgo
- Conservar y buscar solicitudes y respuestas de Copilot
- Evaluación del módulo
- Resumen

Protección de las interacciones de Copilot de Microsoft 365 con Microsoft Purview

Las herramientas de inteligencia artificial como Microsoft 365 Copilot crean nuevas formas de interactuar con datos confidenciales, pero también presentan nuevos riesgos. Obtenga información sobre cómo Microsoft Purview le ayuda a aplicar controles de seguridad y cumplimiento que protegen los datos, administran la actividad de inteligencia artificial y admiten el uso responsable a escala.

- Introducción
- Comprender cómo Microsoft 365 Copilot cambia las necesidades de protección de datos
- Evaluación del cumplimiento normativo de Copilot con el Administrador de cumplimiento
- Auditar las interacciones de Copilot con Microsoft Purview
- Análisis de interacciones de Copilot con el cumplimiento de comunicaciones
- Clasificación y protección del contenido de Copilot con etiquetas de confidencialidad
- Aplicación de directivas DLP a Microsoft 365 Copilot
- Aplicación de directivas de retención a solicitudes y respuestas de Copilot
- Investigación y eliminación de la actividad de Copilot con eDiscovery
- Evaluación del módulo
- Resumen

Protección de aplicaciones de inteligencia artificial empresariales y basadas en explorador con Microsoft Purview

Las herramientas de inteligencia artificial en entornos empresariales y públicos crean nuevas oportunidades, pero también presentan riesgos de seguridad y cumplimiento de datos. Microsoft Purview ayuda a reducir estos riesgos mediante la detección del uso de inteligencia artificial, la evaluación de las necesidades de cumplimiento y la aplicación de controles integrados para la protección, retención y uso responsable.

- Introducción
- Comprender los riesgos de las herramientas de inteligencia artificial empresarial y que no son de Microsoft
- Evaluación del uso de inteligencia artificial para la seguridad y el cumplimiento
- Identificación de infracciones de directiva con el cumplimiento de comunicaciones
- Detección del uso de inteligencia artificial de riesgo con la administración de riesgos internos
- Protección de datos confidenciales en aplicaciones de inteligencia artificial con DLP de Microsoft Purview
- Caso práctico: Uso de la protección adaptable para responder al riesgo relacionado con la inteligencia artificial
- Aplicación de directivas de retención a las solicitudes y respuestas de la aplicación de IA
- Evaluación del módulo
- Resumen

Protección de entornos de inteligencia artificial para desarrolladores con Microsoft Purview

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

- Introducción
- Descripción de los riesgos y responsabilidades en los entornos de desarrollo de inteligencia artificial
- Detección y evaluación de aplicaciones de inteligencia artificial con DSPM para IA
- Clasificación, restricción y retención de datos de solicitud de IA
- Aplicar protecciones en Microsoft Foundry y Foundry Tools
- Aplicación de controles para aplicaciones de IA personalizadas registradas por Microsoft Entra
- Protección de agentes de IA integrados en Copilot Studio
- Administración de riesgos de datos en Copilot en Fabric
- Investigación y respuesta a la actividad de inteligencia artificial de riesgo
- Evaluación del módulo
- Resumen