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: 35 horas

MS-102 / MICROSOFT 365 ADMINISTRATOR ESSENTIALS

Este curso cubre los siguientes elementos clave de la administración de Microsoft 365: administración de inquilinos de Microsoft 365, sincronización de identidades de Microsoft 365 y seguridad y cumplimiento de Microsoft 365. En la administración de inquilinos de Microsoft 365, aprenderá cómo configurar su inquilino de Microsoft 365, incluido su perfil organizacional, opciones de suscripción de inquilinos, servicios de componentes, licencias y cuentas de usuario, grupos de seguridad y roles administrativos. Luego pasará a configurar Microsoft 365, centrándose principalmente en configurar la conectividad del cliente de Office. Finalmente, explorará cómo administrar instalaciones de clientes controladas por el usuario de Aplicaciones Microsoft 365 para implementaciones empresariales. Luego, el curso pasa a un examen en profundidad de la sincronización de identidades de Microsoft 365, con un enfoque en Azure Active Directory Connect y Connect Cloud Sync. Aprenderá cómo planificar e implementar cada una de estas opciones de sincronización de directorios, cómo administrar identidades sincronizadas y cómo implementar la administración de contraseñas en Microsoft 365 mediante autenticación multifactor y administración de contraseñas de autoservicio. En la gestión de seguridad de Microsoft 365, comenzará a examinar los tipos comunes de vectores de amenazas y violaciones de datos que enfrentan las organizaciones hoy en día. Luego aprenderá cómo las soluciones de seguridad de Microsoft 365 abordan cada una de estas amenazas. Se le presenta Microsoft Secure Score, así como Azure Active Directory Identity Protection. Luego aprenderá a administrar los servicios de seguridad de Microsoft 365, incluida la protección de Exchange Online, los archivos adjuntos seguros y los vínculos seguros. Finalmente, se le presentan los diversos informes que monitorean el estado de seguridad de una organización. Luego pasa de los servicios de seguridad a la inteligencia sobre amenazas; específicamente, usando Microsoft 365 Defender, Microsoft Defender para aplicaciones en la nube y Microsoft Defender para endpoint. Una vez que comprenda el paquete de seguridad de Microsoft 365, examinará los componentes clave de la administración de cumplimiento de Microsoft 365. Esto comienza con una descripción general de todos los aspectos clave del gobierno de datos, incluido el archivado y la retención de datos, el cifrado de mensajes de Microsoft Purview y la prevención de pérdida de datos (DLP). Luego profundizará en el archivado y la retención, prestando especial atención a la gestión de riesgos internos, las barreras de información y las políticas de DLP de Microsoft Purview. Luego examinará cómo implementar estas funciones de cumplimiento mediante el uso de etiquetas de confidencialidad y clasificación de datos.

Perfil del Público

Este curso está diseñado para personas que aspiran a la función de administrador de Microsoft 365 Enterprise y han completado, como mínimo, una de las rutas de certificación de administrador basadas en roles de Microsoft 365.

Rol de trabajo: Administrador
Preparación para el examen: MS-102

Requisitos Previos

Antes de asistir a este curso, los estudiantes deben tener:

- ✓ Un curso de administrador basado en roles, como Mensajería, Trabajo en equipo, Seguridad y cumplimiento, o Colaboración.
- ✓ Conocimiento competente de DNS y experiencia funcional básica con los servicios de Microsoft 365.
- ✓ Un conocimiento competente de las prácticas generales de TI.
- ✓ Conocimientos prácticos de PowerShell

Módulos

MS-102 Configure su inquilino de Microsoft 365

Esta ruta de aprendizaje proporciona instrucciones sobre cómo configurar su inquilino de Microsoft 365, incluido su perfil organizacional, suscripciones de inquilino, cuentas y licencias de usuario, grupos, dominios personalizados y conectividad de cliente.

- **Configure su experiencia de Microsoft 365**

Este módulo examina cada una de las tareas que una organización debe completar para configurar correctamente su experiencia de Microsoft 365.

- Introducción
- Explore su entorno de nube de Microsoft 365
- Configure su perfil organizacional de Microsoft 365
- Administre sus suscripciones de inquilinos en Microsoft 365
- Integrar Microsoft 365 con aplicaciones de participación del cliente
- Configurar ajustes de uso compartido a nivel de inquilino para SharePoint y OneDrive
- Configurar ajustes a nivel de inquilino para Microsoft Teams
- Habilite el registro de auditoría unificado en Microsoft 365
- Complete la configuración de su inquilino en Microsoft 365
- Verificación de conocimientos
- Resumen

- **Administrar usuarios, licencias, invitados y contactos en Microsoft 365**

Este módulo proporciona instrucciones sobre cómo crear y administrar cuentas de usuario, asignar licencias de Microsoft 365 a los usuarios, recuperar cuentas de usuarios eliminadas y crear y administrar invitados y contactos.

- Introducción
- Determinar el modelo de identidad de usuario para su organización.
- Crear cuentas de usuario en Microsoft 365
- Administrar la configuración de la cuenta de usuario en Microsoft 365
- Administrar licencias de usuario en Microsoft 365
- Recuperar cuentas de usuario eliminadas en Microsoft 365
- Realizar mantenimiento masivo de usuarios en Microsoft Entra ID
- Crear y administrar usuarios invitados mediante la colaboración B2B
- Colaborar con invitados en un sitio de SharePoint

o Crear y gestionar contactos.

- Verificación de conocimientos
- Resumen

- **Administrar grupos en Microsoft 365**

Este módulo proporciona instrucciones sobre cómo crear grupos para distribuir correo electrónico a múltiples usuarios dentro de Exchange Online. También explica cómo crear grupos para respaldar la colaboración en SharePoint Online.

- Introducción
- Examinar grupos en Microsoft 365
- Crear y administrar grupos en Microsoft 365
- Crear grupos dinámicos usando el generador de reglas de Microsoft Entra
- Crear una política de nomenclatura de grupos de Microsoft 365
- Crear grupos en Exchange Online y SharePoint Online
- Verificación de conocimientos
- Resumen

- **Agregar un dominio personalizado en Microsoft 365**

Este módulo proporciona instrucciones sobre cómo agregar un dominio personalizado a su implementación de Microsoft 365. También examina los requisitos de DNS necesarios para admitir un nuevo dominio.

- Introducción
- Planifique un dominio personalizado para su implementación de Microsoft 365
- Planificar las zonas DNS para un dominio personalizado
- Planificar los requisitos de registro DNS para un dominio personalizado
- Crear un dominio personalizado en Microsoft 365
- Verificación de conocimientos
- Resumen

- **Configurar la conectividad del cliente a Microsoft 365**

Este módulo examina cómo los clientes se conectan a Microsoft 365. También proporciona instrucciones sobre cómo configurar la resolución de nombres y los clientes de Outlook, y cómo solucionar problemas de conectividad del cliente.

- Introducción
- Examinar cómo funciona la configuración automática del cliente.
- Explorar los registros DNS necesarios para la configuración del cliente
- Configurar clientes de Outlook
- Solucionar problemas de conectividad del cliente.
- Verificación de conocimientos
- Resumen

MS-102 Administre su inquilino de Microsoft 365

Esta ruta de aprendizaje proporciona instrucciones sobre cómo administrar su inquilino de Microsoft 365, incluidos los roles administrativos, el estado y los servicios del inquilino, las aplicaciones de Microsoft 365 para empresas y el análisis del lugar de trabajo mediante Microsoft Viva Insights.

- **Configurar roles administrativos en Microsoft 365**

Este módulo examina la funcionalidad clave que está disponible en los roles de administrador de Microsoft 365 más utilizados. También proporciona instrucciones sobre cómo configurar estos roles.

- Introducción
- Explore el modelo de permisos de Microsoft 365
- Explorar los roles de administrador de Microsoft 365

- Asignar roles de administrador a usuarios en Microsoft 365
- Delegar funciones administrativas a los socios
- Administrar permisos usando unidades administrativas en Microsoft Entra ID
- Aumente los privilegios mediante Microsoft Entra Privileged Identity Management
- Examinar las mejores prácticas al configurar roles administrativos.
- Verificación de conocimientos
- Resumen

- **Administrar el estado y los servicios de los inquilinos en Microsoft 365**

Este módulo examina cómo monitorear la transición de su organización a Microsoft 365 usando las herramientas de Microsoft 365. También examina cómo desarrollar un plan de respuesta a incidentes y solicitar asistencia de Microsoft.

- Introducción
- Supervisar el estado de sus servicios de Microsoft 365
- Supervisar el estado de los inquilinos mediante Microsoft 365 Adoption Score
- Supervisar el estado de los inquilinos mediante análisis de uso de Microsoft 365
- Implementar evaluaciones e información de conectividad de red de Microsoft 365
- Implementar copia de seguridad de Microsoft 365 (versión preliminar)
- Desarrollar un plan de respuesta a incidentes.
- Solicitar asistencia de Microsoft
- Verificación de conocimientos
- Resumen

- **Implementar aplicaciones de Microsoft 365 para empresas**

Este módulo examina cómo implementar el paquete de aplicaciones Microsoft 365 para productividad empresarial en implementaciones centralizadas y dirigidas por el usuario.

- Introducción
- Explorar las aplicaciones Microsoft 365 para la funcionalidad empresarial
- Completar una instalación de autoservicio de Aplicaciones Microsoft 365 para empresas
- Implementar aplicaciones Microsoft 365 para empresas con Microsoft Configuration Manager
- Implementar aplicaciones Microsoft 365 para empresas desde la nube
- Implementar aplicaciones Microsoft 365 para empresas desde una fuente local
- Administrar actualizaciones de Aplicaciones Microsoft 365 para empresas
- Explore los canales de actualización para Aplicaciones Microsoft 365 para empresas
- Administre sus aplicaciones en la nube utilizando el centro de administración de aplicaciones de Microsoft 365
- Verificación de conocimientos
- Resumen

- **Analice los datos de su lugar de trabajo de Microsoft 365 usando Microsoft Viva Insights**

Este módulo examina las características analíticas del lugar de trabajo de Microsoft Viva Insights, incluido cómo funciona y cómo genera conocimientos y mejora la colaboración dentro de una organización.

- Introducción
- Examinar las características analíticas de Microsoft Viva Insights
- Explorar conocimientos personales

- Explorar las ideas del equipo
- Explorar conocimientos de la organización
- Explorar conocimientos avanzados
- Verificación de conocimientos
- Resumen

MS-102 Implementar sincronización de identidad

Esta ruta de aprendizaje examina cómo las organizaciones deben planificar e implementar la sincronización de identidades en una implementación híbrida de Microsoft 365. Aprenderá cómo implementar Microsoft Entra Connect Sync y Microsoft Entra Cloud Sync, y cómo administrar identidades sincronizadas.

- **Explorar la sincronización de identidades**

Este módulo examina la sincronización de identidades y explora las opciones de autenticación y aprovisionamiento que se pueden utilizar, y el funcionamiento interno de la sincronización de directorios.

- Introducción
- Examinar modelos de identidad para Microsoft 365.
- Examinar las opciones de autenticación para el modelo de identidad híbrida.
- Explorar la sincronización de directorios
- Verificación de conocimientos
- Resumen

- **Prepárese para la sincronización de identidades con Microsoft 365**

Este módulo examina todos los aspectos de planificación que se deben considerar al implementar la sincronización de directorios entre Active Directory local y Microsoft Entra ID.

- Introducción
- Planifique la implementación de Microsoft Entra ID
- Prepárese para la sincronización del directorio
- Elija su herramienta de sincronización de directorios
- Planifique la sincronización de directorios mediante Microsoft Entra Connect Sync
- Planifique la sincronización de directorios mediante Microsoft Entra Cloud Sync
- Verificación de conocimientos
- Resumen

- **Implementar herramientas de sincronización de directorios.**

Este módulo examina los requisitos de instalación de Microsoft Entra Connect Sync y Microsoft Entra Cloud Sync, las opciones para instalar y configurar las herramientas y cómo monitorear los servicios de sincronización usando Microsoft Entra Connect Health.

- Introducción
- Configurar los requisitos previos de Microsoft Entra Connect Sync
- Configurar la sincronización de Microsoft Entra Connect
- Monitorear los servicios de sincronización usando Microsoft Entra Connect Health
- Configurar los requisitos previos de Microsoft Entra Cloud Sync
- Configurar Microsoft Entra Cloud Sync
- Verificación de conocimientos
- Adoptar un enfoque de Confianza Cero
- Verificación de conocimientos
- Resumen

- **• Administrar el acceso seguro de los usuarios en Microsoft 365**

Este módulo examina las diversas características proporcionadas en el ecosistema de Microsoft 365 para proteger el acceso de los usuarios, como políticas de acceso condicional, autenticación multifactor, administración de contraseñas de autoservicio, políticas de

bloqueo inteligente y valores predeterminados de seguridad.

- Introducción
- Examinar las herramientas de identidad y acceso utilizadas en Microsoft 365.
- Administrar contraseñas de usuario
- Implementar políticas de acceso condicional
- Habilitar la autenticación PassThrough
- Implementar autenticación multifactor
- Explorar opciones de autenticación sin contraseña
- Explore la gestión de contraseñas de autoservicio
- Implementar el bloqueo inteligente de Microsoft Entra
- Explorar los valores predeterminados de seguridad en Microsoft Entra ID
- Investigar problemas de autenticación mediante registros de inicio de sesión
- Verificación de conocimientos
- Resumen

- **Explorar soluciones de seguridad en Microsoft Defender XDR**

Este módulo le presenta varias características de Microsoft 365 que pueden ayudar a proteger su organización contra amenazas cibernéticas, detectar cuándo un usuario o una computadora está comprometida y monitorear su organización en busca de actividades sospechosas.

- Introducción
- Mejore la protección de Exchange Online con Microsoft Defender para Office 365
- Proteja las identidades de su organización utilizando Microsoft Defender for Identity
- Proteja su red empresarial contra amenazas avanzadas utilizando Microsoft Defender para Endpoint
- Protéjase contra ataques cibernéticos utilizando Microsoft 365 Threat Intelligence
- Proporcionar información sobre actividades sospechosas utilizando Microsoft Defender para Cloud App Security
- Revisar los informes de seguridad en Microsoft Defender XDR
- Verificación de conocimientos
- Resumen

- **Examinar la puntuación segura de Microsoft**

Este módulo examina cómo Microsoft Secure Score ayuda a las organizaciones a comprender lo que han hecho para reducir el riesgo de sus datos y mostrarles qué pueden hacer para reducir aún más ese riesgo.

- Introducción
- Explore la puntuación segura de Microsoft
- Evalúe su postura de seguridad con Microsoft Secure Score
- Mejore su puntuación segura
- Realice un seguimiento de su historial de Microsoft Secure Score y cumpla sus objetivos
- Verificación de conocimientos
- Resumen

- **Examinar la gestión de identidades privilegiadas en Microsoft Entra ID**

Este módulo examina cómo Microsoft Entra Privileged Identity Management (PIM) garantiza que los usuarios de su organización tengan los privilegios adecuados para realizar las tareas que necesitan realizar.

- Introducción
- Explore la administración de identidades privilegiadas en Microsoft Entra ID
- Configurar la gestión de identidades privilegiadas

- Auditoría de gestión de identidades privilegiadas
- Verificación de conocimientos
- Resumen

- **Examinar la protección de identificación de Microsoft Entra**

Este módulo examina cómo Azure Identity Protection proporciona a las organizaciones los mismos sistemas de protección que utiliza Microsoft para proteger las identidades.

- Introducción
- Explore la protección de identificación de Microsoft Entra
- Habilite las políticas de protección predeterminadas en Microsoft Entra ID Protection
- Explorar las vulnerabilidades y eventos de riesgo detectados por Microsoft Entra ID Protection
- Planifique su investigación de identidad
- Verificación de conocimientos
- Resumen

MS-102 Administre sus servicios de seguridad en Microsoft Defender XDR

Esta ruta de aprendizaje examina cómo administrar los servicios de seguridad de Microsoft 365, con un enfoque especial en los informes de seguridad y la administración de las características de archivos adjuntos seguros y vínculos seguros en Microsoft Defender para Office 365.

- **Examinar la protección del correo electrónico en Microsoft 365**

Este módulo examina cómo Exchange Online Protection (EOP) protege a las organizaciones contra el phishing y la suplantación de identidad. También explora cómo EOP bloquea el spam, el correo electrónico masivo y el malware antes de que lleguen a los buzones de correo de los usuarios.

- Introducción
- Implementar políticas antimalware.
- Implementar políticas antispam.
- Detectar mensajes con spam o malware mediante la purga automática de hora cero
- Explore la protección contra suplantación de identidad proporcionada por Exchange Online Protection
- Explore otras protecciones contra la suplantación de identidad
- Examinar el filtrado de spam saliente
- Verificación de conocimientos
- Resumen

- **Mejore su protección de correo electrónico con Microsoft Defender para Office 365**

Este módulo examina cómo Microsoft Defender para Office 365 extiende la protección EOP a través de varias herramientas, incluidos archivos adjuntos seguros, vínculos seguros, inteligencia falsificada, políticas de filtrado de spam y la lista de inquilinos permitidos/bloqueados.

- Introducción
- Suba la escalera de seguridad desde EOP a Microsoft Defender para Office 365
- Ampliar las protecciones de EOP mediante el uso de archivos adjuntos seguros y enlaces seguros
- Gestionar inteligencia falsificada
- Configurar políticas de filtrado de spam saliente
- Administrar el acceso al correo electrónico en Microsoft 365
- Enviar mensajes, URL, archivos y archivos adjuntos a Microsoft para su análisis.
- Verificación de conocimientos
- Resumen

- **Administrar archivos adjuntos seguros**

Este módulo examina cómo administrar archivos adjuntos seguros en su inquilino de Microsoft 365 mediante la creación y configuración de políticas y el uso de reglas de transporte para deshabilitar que una política entre en vigor en ciertos escenarios.

  - Introducción
  - Proteger a los usuarios de archivos adjuntos maliciosos mediante el uso de archivos adjuntos seguros
  - Crear políticas de archivos adjuntos seguros usando Microsoft Defender para Office 365
  - Crear políticas de archivos adjuntos seguros usando PowerShell
  - Modificar una política de archivos adjuntos seguros existente
  - Crear una regla de transporte para eludir una política de archivos adjuntos seguros
  - Examinar la experiencia del usuario final con Safe Attachments
  - Verificación de conocimientos
  - Resumen

- **Administrar enlaces seguros**

Este módulo examina cómo administrar vínculos seguros en su inquilino mediante la creación y configuración de políticas y el uso de reglas de transporte para deshabilitar que una política entre en vigencia en ciertos escenarios.

  - Introducción
  - Proteger a los usuarios de URL maliciosas mediante enlaces seguros
  - Crear políticas de enlaces seguros usando Microsoft Defender XDR
  - Crear políticas de Enlaces Seguros usando PowerShell
  - Modificar una política de Enlaces Seguros existente
  - Crear una regla de transporte para evitar una política de Enlaces Seguros
  - Examinar la experiencia del usuario final con Safe Links
  - Verificación de conocimientos
  - Resumen

MS-102 Implementar protección contra amenazas mediante Microsoft Defender XDR

Esta ruta de aprendizaje examina cómo administrar las características de inteligencia de amenazas de Microsoft 365 que brindan a las organizaciones información y protección contra los ciberataques internos y externos que amenazan a sus inquilinos.

- **Explorar la inteligencia sobre amenazas en Microsoft Defender XDR**

Este módulo examina cómo Microsoft 365 Threat Intelligence proporciona a los administradores conocimiento basado en evidencia y consejos prácticos que pueden usarse para tomar decisiones informadas sobre la protección y la respuesta a los ciberataques contra sus inquilinos.

  - Introducción
  - Explore el gráfico de seguridad inteligente de Microsoft
  - Explorar políticas de alerta en Microsoft 365
  - Ejecutar investigaciones y respuestas automatizadas.
  - Explore la búsqueda de amenazas con Microsoft Threat Protection
  - Explore la búsqueda avanzada de amenazas en Microsoft Defender XDR
  - Explore el análisis de amenazas en Microsoft 365

- Identificar problemas de amenazas mediante informes de Microsoft Defender
- Verificación de conocimientos
- Resumen

- **Implementar protección de aplicaciones mediante Microsoft Defender para aplicaciones en la nube**

Este módulo examina cómo implementar Microsoft Defender para aplicaciones en la nube, que identifica y combate las ciberamenazas en todos sus servicios en la nube de Microsoft y de terceros.

- Introducción
- Explore las aplicaciones en la nube de Microsoft Defender
- Implementar Microsoft Defender para aplicaciones en la nube
- Configurar políticas de archivos en Microsoft Defender para aplicaciones en la nube
- Administrar y responder a alertas en Microsoft Defender para aplicaciones en la nube
- Configurar Cloud Discovery en Microsoft Defender para aplicaciones en la nube
- Solucionar problemas de Cloud Discovery en Microsoft Defender para aplicaciones en la nube
- Verificación de conocimientos
- Resumen

- **Implementar protección de puntos finales mediante Microsoft Defender para puntos finales**

Este módulo examina cómo Microsoft Defender para Endpoint ayuda a las redes empresariales a prevenir, detectar, investigar y responder a amenazas avanzadas mediante el uso de sensores de comportamiento de endpoints, análisis de seguridad en la nube e inteligencia sobre amenazas.

- Introducción
- Explore Microsoft Defender para endpoints
- Configurar Microsoft Defender para endpoint en Microsoft Intune
- Dispositivos integrados en Microsoft Defender para Endpoint
- Administre las vulnerabilidades de los terminales con Microsoft Defender Vulnerability Management
- Gestionar el descubrimiento de dispositivos y la evaluación de vulnerabilidades.
- Reducir su exposición a amenazas y vulnerabilidades
- Verificación de conocimientos
- Resumen

- **Implementar protección contra amenazas mediante Microsoft Defender para Office 365**

Este módulo examina la pila de protección de Microsoft Defender para Office 365 y sus características de inteligencia de amenazas correspondientes, incluido el Explorador de amenazas, los Rastreadores de amenazas y la capacitación en simulación de ataques.

- Introducción
- Explore la pila de protección de Microsoft Defender para Office 365
- Examinar las políticas y reglas de seguridad utilizadas en Microsoft Defender para Office 365
- Investigar ataques de seguridad mediante el uso de Threat Explorer
- Identificar problemas de ciberseguridad mediante el uso de Threat Trackers
- Prepárese para los ataques con entrenamiento de simulación de ataques

- Verificación de conocimientos
- Resumen

MS-102 Explorar el gobierno de datos en Microsoft 365

Esta ruta de aprendizaje le presenta las características de gobierno de datos de Microsoft 365, que sirven para el cumplimiento normativo, pueden facilitar el descubrimiento electrónico y son parte de una estrategia empresarial para proteger la integridad del patrimonio de datos.

- **Examinar las soluciones de gobierno de datos en Microsoft Purview**

Este módulo presenta Microsoft Purview, que está diseñado para enfrentar los desafíos del lugar de trabajo descentralizado y rico en datos de hoy al proporcionar un conjunto integral de soluciones que ayudan a las organizaciones a gobernar, proteger y administrar todo su patrimonio de datos.

- Introducción
- Explorar el gobierno de datos y el cumplimiento en Microsoft Purview
- Proteja los datos confidenciales con Microsoft Purview Information Protection
- Gobernar los datos organizacionales utilizando Microsoft Purview Data Lifecycle Management
- Minimizar los riesgos internos con Microsoft Purview Insider Risk Management
- Explorar las soluciones de eDiscovery de Microsoft Purview
- Verificación de conocimientos
- Resumen

- **Explorar el archivado y la administración de registros en Microsoft 365**

Este módulo examina cómo Microsoft 365 admite la gobernanza de datos al permitir a las organizaciones archivar contenido mediante buzones de correo de archivo y administrar su contenido de alto valor para obligaciones legales, comerciales o regulatorias mediante la implementación de administración de registros.

- Introducción
- Explorar buzones de archivo en Microsoft 365
- Habilitar buzones de archivo en Microsoft 365
- Explore la administración de registros de Microsoft Purview
- Implementar la gestión de registros de Microsoft Purview
- Restaurar datos eliminados en Exchange Online
- Restaurar datos eliminados en SharePoint Online
- Verificación de conocimientos
- Resumen

- **Explorar la retención en Microsoft 365**

Este módulo examina cómo se pueden conservar y, en última instancia, eliminar los datos en Microsoft 365 mediante el uso de políticas de retención de datos y etiquetas de retención de datos en las políticas de retención.

- Introducción
- Explore la retención mediante el uso de políticas de retención y etiquetas de retención.
- Comparar capacidades en políticas de retención y etiquetas de retención
- Definir el alcance de una política de retención.
- Examinar los principios de retención.
- Implementar la retención mediante políticas de retención, etiquetas de retención y retenciones de exhibición de documentos electrónicos.
- Restringir los cambios de retención mediante el uso de Bloqueo de preservación
- Verificación de conocimientos
- Resumen

- **Explorar el cifrado de mensajes de Microsoft Purview**

Este módulo presenta Microsoft Purview Message Encryption, un servicio en línea basado en Microsoft Azure Rights Management e incluye políticas de cifrado, identidad y autorización para ayudar a las organizaciones a proteger su correo electrónico.

  - Introducción
  - Examinar el cifrado de mensajes de Microsoft Purview
  - Configurar el cifrado de mensajes de Microsoft Purview
  - Definir reglas de flujo de correo para cifrar mensajes de correo electrónico.
  - Agregar marca organizacional a mensajes de correo electrónico cifrados
  - Explore el cifrado de mensajes avanzado de Microsoft Purview
  - Verificación de conocimientos
  - Resumen

MS-102 Implementar el cumplimiento en Microsoft 365

Esta ruta de aprendizaje proporciona instrucciones sobre cómo implementar las características de gobierno de datos de Microsoft 365, incluido cómo calcular su preparación para el cumplimiento, implementar soluciones de cumplimiento y crear barreras de información, políticas de DLP y sugerencias de políticas.

- **Explorar el cumplimiento en Microsoft 365**

Este módulo explora las herramientas que proporciona Microsoft 365 para ayudar a garantizar el cumplimiento normativo de una organización, incluido el portal de cumplimiento de Microsoft Purview, el Administrador de cumplimiento y la puntuación de cumplimiento de Microsoft.

  - Introducción
  - Plan de seguridad y cumplimiento en Microsoft 365
  - Planifique sus tareas iniciales de cumplimiento en Microsoft Purview
  - Administre sus requisitos de cumplimiento con Compliance Manager
  - Examinar el panel del Administrador de Cumplimiento
  - Analizar la puntuación de cumplimiento de Microsoft.
  - Verificación de conocimientos
  - Resumen

- **Implementar la gestión de riesgos internos de Microsoft Purview**

Este módulo examina cómo Microsoft Purview Insider Risk Management ayuda a las organizaciones a minimizar los riesgos internos al permitirles detectar, investigar y actuar sobre actividades maliciosas e inadvertidas.

  - Introducción
  - Explorar la gestión de riesgos internos
  - Plan de gestión de riesgos internos.
  - Explorar políticas de gestión de riesgos internos.
  - Crear políticas de gestión de riesgos internos.
  - Investigar las actividades y alertas de gestión de riesgos internos.
  - Explorar casos de gestión de riesgos internos
  - Verificación de conocimientos
  - Resumen

- **Implementar barreras de información de ámbito de Microsoft**

Este módulo examina cómo Microsoft Purview utiliza barreras de información para restringir la comunicación y la colaboración en Microsoft Teams, SharePoint Online y OneDrive for Business.

- Introducción
- Explore las barreras de información del ámbito de Microsoft
- Configurar barreras de información en Microsoft Purview
- Examinar las barreras de información en Microsoft Teams
- Examinar las barreras de información en OneDrive
- Examinar las barreras de información en SharePoint
- Verificación de conocimientos
- Resumen

- **Explore la prevención de pérdida de datos de Microsoft Purview**

Este módulo examina las características de prevención de pérdida de datos en Microsoft 365 que ayudan a las organizaciones a identificar, monitorear, informar y proteger datos confidenciales a través de un análisis de contenido profundo mientras ayudan a los usuarios a comprender y administrar los riesgos de los datos.

- Introducción
- Examinar la prevención de pérdida de datos para cargas de trabajo.
- Examinar las políticas de DLP
- Explore la prevención de pérdida de datos de endpoints
- Explorar la protección adaptativa en Microsoft Purview
- Ver los resultados de la política DLP
- Verificación de conocimientos
- Resumen

- **Implementar la prevención de pérdida de datos de Microsoft Purview**

Este módulo examina cómo las organizaciones pueden usar Microsoft Purview Data Loss Prevention para ayudar a proteger datos confidenciales y definir las acciones de protección que las organizaciones pueden tomar cuando se infringe una regla DLP.

- Introducción
- Plan para implementar la protección contra pérdida de datos de Microsoft Purview
- Implementar las políticas DLP predeterminadas de Microsoft Purview.
- Diseñar una política DLP personalizada
- Crear una política DLP personalizada a partir de una plantilla
- Configurar notificaciones por correo electrónico para políticas DLP
- Configurar sugerencias de políticas para políticas DLP
- Verificación de conocimientos
- Resumen

MS-102 Administrar el cumplimiento en Microsoft 365

Esta ruta de aprendizaje proporciona instrucciones sobre cómo administrar las características de gobierno de datos de Microsoft 365, incluido cómo implementar la retención en el correo electrónico, etiquetas de confidencialidad y Windows Information Protection, y cómo solucionar problemas de prevención de pérdida de datos.

- **Implementar clasificación de datos de información sensible.**

Este módulo le presenta la clasificación de datos en Microsoft 365, incluido cómo crear y entrenar clasificadores, ver datos confidenciales mediante el Explorador de contenido y el Explorador de actividades, e implementar la huella digital de documentos.

- Introducción
- Explorar la clasificación de datos.
- Implementar clasificación de datos en Microsoft 365

- Explora clasificadores entrenables
- Crear y volver a entrenar un clasificador entrenable
- Ver datos confidenciales utilizando el explorador de contenido y el explorador de actividades
- Detectar documentos con información confidencial mediante la huella digital de documentos.
- Verificación de conocimientos
- Resumen

- **Explorar etiquetas de confidencialidad**

Este módulo examina cómo las etiquetas de confidencialidad de la solución Microsoft Information Protection le permiten clasificar y proteger los datos de su organización, al tiempo que garantiza que la productividad y la colaboración del usuario no se vean obstaculizadas.

- Introducción
- Gestionar la protección de datos mediante etiquetas de confidencialidad.
- Explore lo que pueden hacer las etiquetas de confidencialidad
- Determinar el alcance de una etiqueta de confidencialidad.
- Aplicar etiquetas de confidencialidad automáticamente
- Explorar las políticas de etiquetas de confidencialidad
- Verificación de conocimientos
- Resumen

- **Implementar etiquetas de confidencialidad**

Este módulo examina el proceso para implementar etiquetas de confidencialidad, incluida la aplicación de permisos administrativos adecuados, la determinación de una estrategia de implementación, la creación, configuración y publicación de etiquetas, y la eliminación y eliminación de etiquetas.

- Introducción
- Planifique su estrategia de implementación para etiquetas de confidencialidad
- Habilitar etiquetas de confidencialidad para archivos en SharePoint y OneDrive
- Examinar los requisitos para crear una etiqueta de confidencialidad.
- Crear etiquetas de confidencialidad
- Publicar etiquetas de confidencialidad
- Eliminar y eliminar etiquetas de confidencialidad
- Verificación de conocimientos
- Resumen