The DevSecOps Company

Microsoft Partner

MS-102T00
Microsoft 365 Administrator

Información general.

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 a configurar el inquilino de Microsoft 365, incluido el perfil de la organización, las opciones de suscripción de inquilinos, los servicios de componentes, las cuentas de usuario y las licencias, los grupos de seguridad y los roles administrativos. A continuación, pasa a configurar Microsoft 365, con un enfoque principal en la configuración de la conectividad de cliente de Office.

Por último, explorará cómo administrar las instalaciones de cliente controladas por el usuario de Aplicaciones Microsoft 365 para implementaciones empresariales. A continuación, el curso pasa a un examen en profundidad de la sincronización de identidades de Microsoft 365, centrándose en Azure Active Directory Connect y Connect Cloud Sync. Aprenderá a planear e implementar cada una de estas opciones de sincronización de directorios, a administrar identidades sincronizadas y a implementar la administración de contraseñas en Microsoft 365 mediante la autenticación multifactor y la administración de contraseñas de autoservicio. En la administración de seguridad de Microsoft 365, comienza a examinar los tipos comunes de vectores de amenazas y filtraciones de datos a los que se enfrentan las organizaciones hoy en día. A continuación, aprenderá cómo las soluciones de seguridad de Microsoft 365 abordan cada una de estas amenazas. Se le presenta la puntuación de seguridad de Microsoft, así como Azure Active Directory Identity Protection.

A continuación, aprenderá a administrar los servicios de seguridad de Microsoft 365, incluidos Exchange Online Protection, datos adjuntos seguros y vínculos seguros. Por último, se le presentan los distintos informes que supervisan el estado de la seguridad de una organización. A continuación, se pasa de los servicios de seguridad a la inteligencia de amenazas; en concreto, mediante Microsoft 365 Defender, Microsoft Defender for Cloud Apps y Microsoft Defender for Endpoint. Una vez que tenga esta comprensión del conjunto de aplicaciones de seguridad de Microsoft 365, examine los componentes clave de la administración de cumplimiento de Microsoft 365. Esto comienza con una descripción general de todos los aspectos clave de la gobernanza 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). A continuación, profundizará en el archivado y la retención, prestando especial atención a la administración de riesgos internos de Microsoft Purview, las barreras de información y las directivas de DLP. A continuación, examinará cómo implementar estas características de cumplimiento mediante la clasificación de datos y las etiquetas de confidencialidad.

Duración.

5 Días.

Perfil del público.

Este curso está diseñado para personas que aspiran al rol de administrador de Microsoft 365 y han completado al menos una de las rutas de certificación de administrador basadas en roles de Microsoft 365.

Examen.

MS-102: Microsoft 365 Administrator.

Temario.

Ruta de aprendizaje: Configuración del inquilino de Microsoft 365.

Esta ruta de aprendizaje proporciona instrucciones sobre cómo configurar el inquilino de Microsoft 365, incluido el perfil de la organización, las suscripciones de inquilino, las cuentas de usuario y las licencias, los grupos, los dominios personalizados y la conectividad del cliente.

Módulo 1: Configurar la 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.

- Explore su entorno en la nube de Microsoft 365.
- Configurar el perfil de organización de Microsoft 365.
- Administración de las suscripciones de inquilino en Microsoft 365.
- Integración de Microsoft 365 con aplicaciones de involucración del cliente.
- Configuración de las opciones de uso compartido de nivel de inquilino para SharePoint y OneDrive.
- Configuración de opciones de nivel de inquilino para Microsoft Teams.
- Habilitación del registro de auditoría unificado en Microsoft 365.
- Complete la configuración del inquilino en Microsoft 365.

Módulo 2: 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 usuario eliminadas y crear y administrar invitados y contactos.

- Determine 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 el identificador de Microsoft Entra.
- Creación y administración de usuarios invitados mediante la colaboración B2B.
- Colaborar con invitados en un sitio de SharePoint.
- Crear y administrar contactos.

Módulo 3: Administrar grupos en Microsoft 365.

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

- Examinar grupos en Microsoft 365.
- Crear y administrar grupos en Microsoft 365.
- Creación de grupos dinámicos con el generador de reglas de Microsoft Entra.
- Creación de una directiva de nomenclatura de grupo de Microsoft 365.
- Creación de grupos en Exchange Online y SharePoint Online.

Módulo 4: Agregar un dominio personalizado en Microsoft 365.

En este módulo se proporcionan instrucciones sobre cómo agregar un dominio personalizado a la implementación de Microsoft 365. También examina los requisitos de DNS que son necesarios para admitir un nuevo dominio.

- Planeación de un dominio personalizado para la implementación de Microsoft 365.
- Planeación de las zonas DNS para un dominio personalizado.
- Planeación de los requisitos de registro DNS para un dominio personalizado.
- Creación de un dominio personalizado en Microsoft 365.

Módulo 5: Configuración de la conectividad de cliente con Microsoft 365.

En este módulo se examina cómo se conectan los clientes 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.

- Examinar cómo funciona la configuración automática de clientes.
- Explore los registros DNS necesarios para la configuración del cliente.
- Configurar clientes de Outlook.
- Solución de problemas de conectividad del cliente.

Ruta de aprendizaje: Administrar el inquilino de Microsoft 365.

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

Módulo 6: Administrar permisos, roles y grupos de roles en Microsoft 365.

En este módulo se examina el uso de roles y grupos de roles en el modelo de permisos de Microsoft 365, incluida la administración de roles, los procedimientos recomendados al configurar roles de administrador, delegar roles y elevar privilegios.

- Examinar el uso de roles en el modelo de permisos de Microsoft 365.
- Administración de roles en el ecosistema de Microsoft 365.
- Explorar los roles de administrador en Microsoft 365.
- Examine las prácticas recomendadas al configurar roles administrativos.
- Asignar roles de administrador a usuarios en Microsoft 365.
- Delegar roles de administrador a los socios.
- Implementación de grupos de roles en Microsoft 365.
- Administración de permisos mediante unidades administrativas en el identificador de Microsoft Entra.
- Administrar los permisos de SharePoint para evitar el uso compartido excesivo de datos.
- Eleve los privilegios con Microsoft Entra Privileged Identity Management.

Módulo 7: Administrar el estado y los servicios del inquilino en Microsoft 365.

En este módulo se examina cómo supervisar la transición de su organización a Microsoft 365 mediante las herramientas de Microsoft 365. También se examina cómo desarrollar un plan de respuesta a incidentes y solicitar asistencia a Microsoft.

- Supervisión del estado de los servicios de Microsoft 365.
- Supervisión del estado del inquilino mediante la puntuación de adopción de Microsoft 365.
- Supervisión del estado del inquilino mediante el análisis de uso de Microsoft 365.
- Implementación de evaluaciones e información de conectividad de red de Microsoft 365.
- Implementación de Copia de seguridad de Microsoft 365 (versión preliminar).
- Desarrollar un plan de respuesta a incidentes.
- Solicitar asistencia de Microsoft.

Módulo 8: Implementación de Aplicaciones de Microsoft 365 para empresas.

En este módulo se examina cómo implementar el conjunto de aplicaciones de productividad de Microsoft 365 para empresas en implementaciones centralizadas y controladas por el usuario.

- Explorar la funcionalidad de Aplicaciones de Microsoft 365 para empresas.
- Completar una instalación de autoservicio de Aplicaciones Microsoft 365 para empresas.
- Implementación de Aplicaciones de Microsoft 365 para empresas con Microsoft Configuration Manager.
- Implementación de Aplicaciones de Microsoft 365 para empresas desde la nube y desde un origen local.
- Administrar actualizaciones de Aplicaciones de Microsoft 365 para empresas.
- Explorar los canales de actualización de Aplicaciones Microsoft 365 para empresas.
- Administrar las aplicaciones en la nube mediante el Centro de administración de Aplicaciones Microsoft 365.
- Agregar Aplicaciones de Microsoft 365 para empresas a Microsoft Intune.
- Implementación de la línea base de seguridad de Aplicaciones Microsoft 365 para empresas.

Módulo 9: Analice los datos del área de trabajo de Microsoft 365 con Microsoft Viva Insights.

En este módulo se examinan las características analíticas del lugar de trabajo de Microsoft Viva Insights, incluido su funcionamiento, cómo genera información y mejora la colaboración dentro de una organización.

- Examinar las características analíticas de Microsoft Viva Insights.
- Explora Perspectivas personales.
- Explora las perspectivas del equipo.
- Explore la información de la organización.
- Explora Perspectivas avanzadas.

Ruta de aprendizaje: Implementación de la sincronización de identidades.

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

Módulo 10: Explora la sincronización de identidades.

En este módulo se examina la sincronización de identidades y se exploran las opciones de autenticación y aprovisionamiento que se pueden utilizar, así como el funcionamiento interno de la sincronización de directorios.

- Examen de los modelos de identidad para Microsoft 365.
- Examen de las opciones de autenticación para el modelo de identidad híbrida.
- Explorar la sincronización de directorios.

Módulo 11: Preparación para la sincronización de identidades con Microsoft 365.

En este módulo se examinan todos los aspectos de planeación que se deben tener en cuenta al implementar la sincronización de directorios entre el Directorio activo local y el identificador de Microsoft Entra.

- Planeación de la implementación de Microsoft Entra ID.
- Preparación para la sincronización de directorios.
- Elija su herramienta de sincronización de directorios.
- Planeación de la sincronización de directorios mediante Microsoft Entra Connect Sync.
- Planeación de la sincronización de directorios mediante Microsoft Entra Cloud Sync.

Módulo 12: Implementación de herramientas de sincronización de directorios.

En este módulo se examinan los requisitos de instalación de Microsoft Entra Connect Sync y Microsoft Entra Cloud Sync, las opciones para instalar y configurar las herramientas y cómo supervisar los servicios de sincronización mediante Microsoft Entra Connect Health.

- Configuración de los requisitos previos de Microsoft Entra Connect Sync.
- Configurar Microsoft Entra Connect Sync.
- Supervisión de los servicios de sincronización mediante Microsoft Entra Connect Health.
- Configuración de los requisitos previos de Microsoft Entra Cloud Sync.
- Configurar Microsoft Entra Cloud Sync.

Módulo 13: Administración de identidades sincronizadas.

En este módulo se examina cómo administrar las identidades de usuario al configurar Microsoft Entra Connect Sync, cómo administrar usuarios y grupos en Microsoft 365 con Microsoft Entra Connect Sync y cómo mantener la sincronización de directorios.

- Administrar usuarios con sincronización de directorios.
- Administrar grupos con sincronización de directorios.
- Mantener la sincronización de directorios mediante grupos de seguridad de sincronización de Microsoft Entra Connect.
- Configurar filtros de objetos para la sincronización de directorios.
- Explorar Microsoft Identity Manager.
- Solución de problemas de sincronización de directorios.

Ruta de aprendizaje: Administrar la identidad y el acceso en Microsoft 365.

Esta ruta de aprendizaje examina los vectores de amenazas y las filtraciones de datos a los que se enfrentan las organizaciones hoy en día en su panorama de ciberseguridad, y la amplia gama de soluciones de seguridad que Microsoft 365 proporciona para combatir esas amenazas.

Módulo 14: Examinar los vectores de amenazas y las filtraciones de datos.

Este módulo examina los tipos de vectores de amenazas y sus posibles resultados con los que las organizaciones deben lidiar a diario y cómo los usuarios pueden permitir que los piratas informáticos accedan a los objetivos mediante la ejecución involuntaria de contenido malicioso.

- Explore el panorama actual de trabajo y amenazas.
- Examinar cómo el phishing recupera información confidencial.
- Examine cómo la suplantación de identidad engaña a los usuarios y compromete la seguridad de los datos.
- Compara el spam y el malware.
- Examinar las infracciones de la cuenta.
- Examinar la elevación de los ataques de privilegios.
- Examine cómo la exfiltración de datos saca los datos del inquilino.
- Examine cómo los atacantes eliminan datos del inquilino.
- Examine cómo el derrame de datos expone los datos fuera del inquilino.
- Examinar otros tipos de ataques.

Módulo 15: Explora el modelo de seguridad Zero Trust.

En este módulo se examinan los conceptos y principios del modelo de seguridad Confianza cero, así como la forma en que Microsoft 365 lo admite y cómo su organización puede implementarlo.

- Examinar los principios y componentes del modelo Zero Trust.
- Planifique un modelo de seguridad de Confianza cero en su organización.
- Examinar la estrategia de Microsoft para las redes Zero Trust.
- Adopte un enfoque de Confianza cero.

Módulo 16: Administrar el acceso seguro de usuarios en Microsoft 365.

En este módulo se examinan las distintas características proporcionadas en el ecosistema de Microsoft 365 para proteger el acceso de los usuarios, como las directivas de acceso condicional, la autenticación multifactor, la administración de contraseñas de autoservicio, las directivas de bloqueo inteligente y los valores predeterminados de seguridad.

- Examinar las herramientas de identidad y acceso usadas en Microsoft 365.
- Administrar contraseñas de usuario.
- Implementación de directivas de acceso condicional.
- Habilitación de la autenticación de paso a través.
- Implementación de la autenticación multifactor.
- Explora las opciones de autenticación sin contraseña.
- Explore la administración de contraseñas de autoservicio.
- Implementación de Microsoft Entra Smart Lockout.
- Explorar los valores predeterminados de seguridad en el identificador de Microsoft Entra.
- Investigación de problemas de autenticación mediante registros de inicio de sesión.

Módulo 17: Explore las soluciones de seguridad en Microsoft Defender XDR.

En este módulo se presentan varias características de Microsoft 365 que pueden ayudar a proteger su organización contra las ciberamenazas, detectar cuándo un usuario o un equipo está en peligro y supervisar su organización en busca de actividades sospechosas.

- Mejora de Exchange Online Protection con Microsoft Defender para Office 365.
- Proteja las identidades de su organización con Microsoft Defender for Identity.
- Proteja la red empresarial frente a amenazas avanzadas con Microsoft Defender para punto de conexión.
- Protéjase contra ataques cibernéticos con Microsoft 365 Threat Intelligence.
- Proporcionar información sobre la actividad sospechosa mediante Microsoft Defender for Cloud App Security.
- Revisión de los informes de seguridad en Microsoft Defender XDR.

Módulo 18: Examinar la puntuación de seguridad de Microsoft.

En este módulo se examina cómo la puntuación de seguridad de Microsoft ayuda a las organizaciones a comprender lo que han hecho para reducir el riesgo para sus datos y les muestra lo que pueden hacer para reducir aún más ese riesgo.

- Explorar la puntuación de seguridad de Microsoft.
- Evalúe su posición de seguridad con la puntuación de seguridad de Microsoft.
- Mejore su puntuación de seguridad.
- Realice un seguimiento de su historial de puntuación de seguridad de Microsoft y cumpla sus objetivos.

Módulo 19: Examen de Privileged Identity Management en Microsoft Entra ID.

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

- Explore Privileged Identity Management en Microsoft Entra ID.
- Configurar Privileged Identity Management.
- Auditoría de la gestión de identidades privilegiadas.

Módulo 20: Examinar la protección de ID de Microsoft Entra.

En este módulo se examina cómo Azure Identity Protection proporciona a las organizaciones los mismos sistemas de protección que Microsoft usa para proteger las identidades.

- Explorar la protección de ID de Microsoft Entra.
- Habilitación de las directivas de protección predeterminadas en Microsoft Entra ID Protection.
- Explore las vulnerabilidades y los eventos de riesgo detectados por Microsoft Entra ID Protection.
- Planeación de la investigación de identidad.

Ruta de aprendizaje: Administrar los servicios de seguridad en Microsoft Defender XDR.

En esta ruta de aprendizaje se examina cómo administrar los servicios de seguridad de Microsoft 365, con especial atención a los informes de seguridad y a la administración de las características de datos adjuntos seguros y vínculos seguros en Microsoft Defender para Office 365.

Módulo 21: Examinar la protección de correo electrónico en Microsoft 365.

En este módulo se examina cómo Exchange Online Protection (EOP) protege a las organizaciones frente a la suplantación de identidad (phishing) y la suplantación de identidad. También explora cómo EOP bloquea el correo no deseado, el correo electrónico masivo y el malware antes de que lleguen a los buzones de los usuarios.

- Implementación de políticas antimalware.
- Implementación de políticas contra correo no deseado.
- Detecte mensajes con spam o malware mediante la purga automática de horas cero.
- Explore la protección contra la suplantación de identidad proporcionada por la protección de Exchange Online.
- Explora otras protecciones contra la suplantación de identidad.
- Examinar el filtrado de spam saliente.

Módulo 22: Mejore la protección del correo electrónico con Microsoft Defender para Office 365.

En este módulo se examina cómo Microsoft Defender para Office 365 amplía la protección de EOP a través de varias herramientas, como datos adjuntos seguros, vínculos seguros, inteligencia suplantada, directivas de filtrado de correo no deseado y la lista de permitidos o bloqueados inquilinos.

- Sube la escalera de seguridad de EOP a Microsoft Defender para Office 365.
- Amplíe las protecciones de EOP mediante datos adjuntos seguros y vínculos seguros.
- Administrar inteligencia suplantada.
- Configurar directivas de filtrado de correo no deseado saliente.
- Administrar el acceso al correo electrónico en Microsoft 365.
- Enviar mensajes, direcciones URL, archivos y datos adjuntos a Microsoft para su análisis.

Módulo 23: Administrar archivos adjuntos seguros.

En este módulo se examina cómo administrar datos adjuntos seguros en el inquilino de Microsoft 365 mediante la creación y configuración de directivas y el uso de reglas de transporte para deshabilitar una directiva para que no surta efecto en determinados escenarios.

- Proteger a los usuarios de datos adjuntos malintencionados mediante datos adjuntos seguros.
- Creación de directivas de datos adjuntos seguros mediante Microsoft Defender para Office 365.
- Creación de directivas de datos adjuntos seguros mediante PowerShell.
- Modificar una directiva de datos adjuntos seguros existente.
- Creación de una regla de transporte para omitir una directiva de datos adjuntos seguros.
- Examinar la experiencia del usuario final con los datos adjuntos seguros.

Módulo 24: Administrar vínculos seguros.

En este módulo se examina cómo administrar vínculos seguros en el inquilino mediante la creación y configuración de directivas y el uso de reglas de transporte para deshabilitar una directiva para que no surta efecto en determinados escenarios.

- Proteger a los usuarios de direcciones URL malintencionadas mediante vínculos seguros.
- Creación de directivas de vínculos seguros mediante Microsoft 365 Defender.
- Creación de directivas de vínculos seguros mediante PowerShell.
- Modificación de una directiva de vínculos seguros existente.
- Creación de una regla de transporte para omitir una directiva de vínculos seguros.
- Examinar la experiencia del usuario final con vínculos seguros.

Ruta de aprendizaje: Implementación de la protección contra amenazas mediante Microsoft Defender XDR.

En esta ruta de aprendizaje se examina cómo administrar las características de inteligencia sobre amenazas de Microsoft 365 que proporcionan a las organizaciones información y protección frente a los ciberataques internos y externos que amenazan a sus inquilinos.

Módulo 25: Exploración de la inteligencia sobre amenazas en Microsoft Defender XDR.

En este módulo se examina cómo Microsoft 365 Threat Intelligence proporciona a los administradores conocimientos basados en pruebas y consejos prácticos que se pueden usar para tomar decisiones informadas sobre cómo proteger y responder a los ciberataques contra sus inquilinos.

- Explore Microsoft Intelligent Security Graph.
- Explorar las directivas 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.
- Explorar el análisis de amenazas en Microsoft 365.
- Identificación de problemas de amenazas mediante informes de Microsoft Defender.

Módulo 26: Implementación de la protección de aplicaciones mediante Microsoft Defender for Cloud Apps.

En este módulo se examina cómo implementar Microsoft Defender for Cloud Apps, que identifica y combate las ciberamenazas en todos los servicios en la nube de Microsoft y de terceros.

- Explorar las aplicaciones en la nube de Microsoft Defender.
- Implementación de Microsoft Defender for Cloud Apps.
- Configuración de directivas de archivo en Microsoft Defender for Cloud Apps.
- Administración y respuesta a alertas en Microsoft Defender for Cloud Apps.
- Configuración de Cloud Discovery en Microsoft Defender for Cloud Apps.
- Solución de problemas de detección de nubes en Microsoft Defender for Cloud Apps.

Módulo 27: Implementación de la protección de puntos de conexión mediante Microsoft Defender para punto de conexión.

En este módulo se examina cómo Microsoft Defender para punto de conexión ayuda a las redes empresariales a prevenir, detectar, investigar y responder a amenazas avanzadas mediante sensores de comportamiento de punto de conexión, análisis de seguridad en la nube e inteligencia sobre amenazas.

- Exploración de Microsoft Defender para punto de conexión.
- Configuración de Microsoft Defender para punto de conexión en Microsoft Intune.
- Incorporación de dispositivos en Microsoft Defender para punto de conexión.
- Administración de vulnerabilidades de puntos de conexión con la administración de vulnerabilidades de Microsoft Defender.
- Gestione la detección de dispositivos y la evaluación de vulnerabilidades.
- Reduzca su exposición a amenazas y vulnerabilidades.

Módulo 28: Implementación de la protección contra amenazas mediante Microsoft Defender para Office 365.

En este módulo se examina la pila de protección de Microsoft Defender para Office 365 y sus características de inteligencia sobre amenazas correspondientes, incluido el Explorador de amenazas, los rastreadores de amenazas y el entrenamiento de simulación de ataques.

- Exploración de la pila de protección de Microsoft Defender para Office 365.
- Examine las directivas y reglas de seguridad usadas en Microsoft Defender para Office 365.
- Investigación de ataques de seguridad mediante el Explorador de amenazas.
- Identifique los problemas de ciberseguridad mediante el uso de rastreadores de amenazas.
- Prepárese para los ataques con el entrenamiento de simulación de ataques.

Ruta de aprendizaje: Explorar la gobernanza de datos en Microsoft 365.

En esta ruta de aprendizaje se presentan las características de gobernanza de datos de Microsoft 365, que sirven para el cumplimiento normativo, pueden facilitar la exhibición de documentos electrónicos y forman parte de una estrategia empresarial para proteger la integridad del patrimonio de datos.

Módulo 29: Examen de las soluciones de gobernanza de datos en Microsoft Purview.

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

- Explore la gobernanza de datos y el cumplimiento en Microsoft Purview.
- Proteja los datos confidenciales con Microsoft Purview Information Protection.
- Gobernar los datos de la organización mediante la administración del ciclo de vida de los datos de Microsoft Purview.
- Minimice los riesgos internos con Microsoft Purview Insider Risk Management.
- Explore las soluciones de exhibición de documentos electrónicos de Microsoft Purview.

Módulo 30: Explorar las prácticas de administración de datos en Microsoft 365.

En este módulo se examina cómo Microsoft 365 admite la gobernanza de datos al permitir que las organizaciones archiven contenido mediante buzones de archivo y restauren datos eliminados en Exchange Online y SharePoint Online.

- Explorar buzones de archivo en Microsoft 365.
- Habilitación de buzones de archivo en Microsoft 365.
- Restaurar datos eliminados en Exchange Online.
- Restaurar datos eliminados en SharePoint Online.

Módulo 31: Explorar la retención en Microsoft 365.

En este módulo se examina cómo se pueden conservar los datos y, en última instancia, eliminarlos en Microsoft 365 mediante directivas de retención de datos y etiquetas de retención de datos en directivas de retención.

- Explore la retención mediante directivas de retención y etiquetas de retención.
- Comparación de las capacidades de las directivas de retención y las etiquetas de retención.
- Definir el ámbito de una política de retención.
- Examinar los principios de retención.
- Implementación de la retención mediante directivas

de retención, etiquetas de retención y suspensiones de exhibición de documentos electrónicos.
- Restricción de cambios de retención mediante el bloqueo de conservación.

Ruta de aprendizaje: Implementación de cumplimiento en Microsoft 365.

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

Módulo 32: Explorar el cumplimiento en Microsoft 365.

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

- Planeación de la seguridad y el cumplimiento en Microsoft 365.
- Planeación de las tareas de cumplimiento iniciales en Microsoft Purview.
- Administración de los requisitos de cumplimiento con el Administrador de cumplimiento.
- Examine el panel del Administrador de cumplimiento.
- Análisis de la puntuación de cumplimiento de Microsoft.

Módulo 33: Implementación de la administración de riesgos internos de Microsoft Purview.

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

- Explora la gestión de riesgos internos.
- Planeación de la administración de riesgos internos.
- Explore las directivas de administración de riesgos internos.
- Creación de directivas de administración de riesgos internos.
- Investigue las actividades y alertas de administración de riesgos internos.
- Explore los casos de administración de riesgos internos.

Módulo 34: Implementación de barreras de información de Microsoft Purview.

En este módulo se examina cómo Microsoft Purview usa las barreras de información para restringir la comunicación y la colaboración en Microsoft Teams, SharePoint Online y OneDrive para la Empresa.

- Explorar las barreras de información de Microsoft Purview.
- Configuración de 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.

Módulo 35: Explore la prevención de pérdida de datos de Microsoft Purview.

En este módulo se examinan las características de prevención de pérdida de datos de Microsoft 365 que ayudan a las organizaciones a identificar, supervisar, informar y proteger los datos confidenciales a través de un análisis profundo del contenido, al tiempo que ayudan a los usuarios a comprender y administrar los riesgos de los datos.

- Examinar la prevención de pérdida de datos para cargas de trabajo.
- Examen de las directivas DLP.
- Explore la prevención de pérdida de datos de endpoints.
- Exploración de la protección adaptable en Microsoft Purview.
- Visualización de los resultados de la directiva DLP.

Módulo 36: Implementación de la prevención de pérdida de datos de Microsoft Purview.

En este módulo se examina cómo las organizaciones pueden usar la prevención de pérdida de datos de Microsoft Purview para ayudar a proteger los datos confidenciales y definir las acciones de protección que las organizaciones pueden realizar cuando se infringe una regla DLP.

- Planear la implementación de la protección contra pérdida de datos de Microsoft Purview.
- Implementación de las directivas DLP predeterminadas de Microsoft Purview.
- Diseño de una directiva DLP personalizada.
- Creación de una directiva DLP personalizada a partir de una plantilla.
- Configuración de notificaciones por correo electrónico para directivas DLP.
- Configuración de sugerencias de directiva para directivas DLP.

Ruta de aprendizaje: Administrar el cumplimiento en Microsoft 365.

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

Módulo 37: Implementar la clasificación de datos de información confidencial.

En este módulo se 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.

- Explorar la clasificación de datos.
- Implementación de la clasificación de datos en Microsoft 365.
- Explora los clasificadores entrenables.
- Creación y reentrenamiento de un clasificador entrenable.
- Visualización de datos confidenciales mediante el Explorador de contenido y el Explorador de actividades.
- Detección de documentos de información confidencial mediante la huella digital de documentos.

Módulo 38: Explora las etiquetas de confidencialidad.

En este módulo se 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 se asegura de que la productividad y la colaboración de los usuarios no se vean obstaculizadas.

- Administración de la protección de datos mediante etiquetas de confidencialidad.
- Explore lo que pueden hacer las etiquetas de confidencialidad.
- Determinación del ámbito de una etiqueta de confidencialidad.
- Aplicación automática de etiquetas de confidencialidad.
- Exploración de las directivas de etiquetas de confidencialidad.

Módulo 39: Implementación de etiquetas de confidencialidad.

En este módulo se examina el proceso de implementación de 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.

- Planeación de la estrategia de implementación de etiquetas de confidencialidad.
- Habilitar etiquetas de confidencialidad para archivos en SharePoint y OneDrive.
- Examine los requisitos para crear una etiqueta de confidencialidad.
- Creación de etiquetas de confidencialidad.
- Publicación de etiquetas de confidencialidad.
- Quitar y eliminar etiquetas de confidencialidad.