The DevOps Company

Microsoft Partner

MS-101T00
Microsoft 365 Mobility and Security

Sobre este curso.

Este curso cubre tres elementos centrales de la administración empresarial de Microsoft 365: administración de seguridad de Microsoft 365, administración de cumplimiento de Microsoft 365 y administración de dispositivos de Microsoft 365. En Microsoft 365 security management, examinará todos los tipos comunes de vectores de amenazas y violaciones de datos que enfrentan las organizaciones hoy en día, y aprenderá cómo las soluciones de seguridad de Microsoft 365 abordan estas amenazas de seguridad. Se le presentará Microsoft Secure Score y Azure Active Directory Identity Protection. Luego aprenderá a administrar los servicios de seguridad de Microsoft 365, incluidos Exchange Online Protection, Safe Attachments, y Safe Links. Finalmente, se le presentarán los diversos informes que supervisan su estado de seguridad. Después, pasará de los servicios de seguridad a la inteligencia sobre amenazas; específicamente, mediante Microsoft 365 Defender, las aplicaciones de Microsoft Defender for Cloud y Microsoft Defender para punto de conexión. Con sus componentes de seguridad de Microsoft 365 ahora firmemente en su lugar, examinará los componentes clave de la administración de cumplimiento de Microsoft 365. Comienza con una introducción a todos los aspectos clave de la gobernanza de datos, incluidos el archivado y la retención de datos, el cifrado de mensajes de Microsoft Purview y la prevención de pérdida de datos (DLP). Después, 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 DLP. Luego, examinará cómo implementar estas características de cumplimiento mediante el uso de etiquetas de confidencialidad y clasificación de datos. Concluirá esta sección aprendiendo a administrar la búsqueda y la investigación en el portal de cumplimiento de Microsoft Purview. Cubrirá Auditoría de Microsoft Purview (Estándar y Premium) y Microsoft Purview eDiscovery (Estándar y Premium). El curso concluye con un examen en profundidad de la administración de dispositivos de Microsoft 365. Comenzará planeando diversos aspectos de la administración de dispositivos, incluida la preparación de los dispositivos Windows para la administración conjunta, la planificación de la administración de aplicaciones móviles, el examen de escenarios de implementación de cliente de Windows, los modelos de implementación de Windows Autopilot y la planificación de la estrategia de suscripción de cliente de Windows. Por último, pasará de planear a implementar la administración de dispositivos; en concreto, la estrategia de implementación de cliente de Windows, Windows Autopilot, Administración de dispositivos móviles (MDM), la inscripción de dispositivos en MDM y la seguridad de los puntos de conexión en Microsoft Intune.

Duración.

5 Días.

Perfil del público.

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

Requisitos previos.

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

- Completó 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.

Examen.

MS-101: Microsoft 365 Mobility and Security.

Temario.

Módulo 1: 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 ejecutando sin darse cuenta contenido malicioso.

- Explora el panorama actual del trabajo y las 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 spam y malware.
- Examinar cómo una violación de la cuenta compromete una cuenta de usuario.
- Examinar la elevación de los ataques de privilegios.
- Examine cómo la filtración de datos aleja los datos de su inquilino.
- Examine cómo los atacantes eliminan los datos de su inquilino.
- Examine cómo el derrame de datos expone los datos fuera de su inquilino.
- Examina otros tipos de ataques.

Al final de este módulo, podrás:

- Describir las técnicas que utilizan los piratas informáticos para comprometer las cuentas de usuario a través del correo electrónico.
- Describir las técnicas que los hackers utilizan para obtener control sobre los recursos.
- Describir las técnicas que utilizan los hackers para comprometer los datos.
- Mitigar una violación de la cuenta.
- Evitar un ataque de elevación de privilegios.
- Evitar la exfiltración de datos, la eliminación de datos y el derrame de datos.

Módulo 2: Explora el modelo de seguridad Zero Trust.

Este módulo examina los conceptos y principios del modelo de seguridad Zero Trust, así como cómo 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.
- Adoptar un enfoque de confianza cero.

Al final de este módulo, podrás:

- Describir el enfoque de confianza cero para la seguridad en Microsoft 365.
- Describir los principios y componentes del modelo de seguridad Zero Trust.
- Describa los cinco pasos para implementar un modelo de seguridad Zero Trust en su organización.
- Explicar la historia y la estrategia de Microsoft en torno a las redes de Zero Trust.

Módulo 3: Explora las soluciones de seguridad en Microsoft 365 Defender.

Este módulo le presenta varias características de Microsoft 365 que pueden ayudar a proteger a su organización contra las ciberamenazas, detectar cuando un usuario o un ordenador se ha visto comprometido y supervisar a su organización en busca de actividades sospechosas.

- Mejore la seguridad de su correo electrónico con Microsoft Defender para Office 365.
- Proteja las identidades de su organización con Microsoft Defender for Identity.

- Proteja su red empresarial contra amenazas avanzadas utilizando Microsoft Defender for Endpoint.
- Protéjase contra los ciberataques utilizando Microsoft 365 Threat Intelligence.
- Proporcione información sobre la actividad sospechosa utilizando Microsoft Defender para aplicaciones en la nube.
- Revisa los informes de seguridad en Microsoft 365 Defender.
-
- Al final de este módulo, podrás:
- Identificar las características de Microsoft Defender para Office 365 que mejoran la seguridad del correo electrónico en una implementación de Microsoft 365.
- Explique cómo Microsoft Defender for Identity identifica, detecta e investiga amenazas avanzadas, identidades comprometidas y acciones internas maliciosas dirigidas a su organización.
- Explicar cómo Microsoft Defender for Endpoint ayuda a las redes empresariales a prevenir, detectar, investigar y responder a amenazas avanzadas.
- Describa cómo Microsoft 365 Threat Intelligence puede ser beneficioso para los oficiales y administradores de seguridad de su organización.
- Describa cómo Microsoft Defender for Cloud Apps mejora la visibilidad y el control sobre su inquilino de Microsoft 365 a través de tres áreas principales.

Módulo 4: Examine la puntuación de Microsoft Secure.

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 lo que pueden hacer para reducir aún más ese riesgo.

- Explora Microsoft Secure Score.
- Examine el panel de puntuación segura.
- Recopilar datos de Secure Score utilizando la API de Secure Score.
- Mejora tu postura de seguridad.

Al final de este módulo, podrás:

- Describir los beneficios de Secure Score y qué tipo de servicios se pueden analizar.
- Describir cómo recopilar datos utilizando la API de Secure Score.
- Describa cómo usar la herramienta para identificar las brechas entre su estado actual y dónde le gustaría estar con respecto a la seguridad.
- Identifique las acciones que aumentarán su seguridad al mitigar los riesgos.
- Explique dónde buscar para determinar las amenazas que cada acción mitigará y el impacto que tiene en los usuarios.

Módulo 5: Examinar la gestión de identidades privilegiadas.

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

- Explora la gestión de identidades privilegiadas en Azure AD.
- Configurar la gestión de identidades con privilegios.
- Auditoría de gestión de identidades privilegiadas.
- Explora el Administrador de identidades de Microsoft.
- Controle las tareas de administración privilegiadas utilizando la gestión de acceso privilegiado.

Al final de este módulo, podrás:

- Describa cómo la gestión de identidades privilegiadas le permite gestionar, controlar y supervisar el acceso a recursos importantes de su organización.
- Configure la gestión de identidades privilegiadas para su uso en su organización.
- Describa cómo el historial de auditoría de Privileged Identity Management le permite ver todas las asignaciones y activaciones de usuarios dentro de un período de tiempo determinado para todos los roles privilegiados.
- Explicar cómo Microsoft Identity Manager ayuda a las organizaciones a gestionar los usuarios, las credenciales, las políticas y el acceso dentro de sus organizaciones y entornos híbridos.
- Explicar cómo Privileged Access Management proporciona un control de acceso granular sobre las tareas de administración privilegiadas en Microsoft 365.

Módulo 6: Examine Azure Identity Protection.

Este módulo examina cómo Azure Identity Protection proporciona a las organizaciones los mismos sistemas de protección utilizados por Microsoft para asegurar las identidades.

- Explora Azure Identity Protection.
- Habilitar las políticas de protección predeterminadas en AIP.
- Explore las vulnerabilidades y los eventos de riesgo detectados por AIP.
- Planifica tu investigación de identidad.

Al final de este módulo, podrás:

- Describa Azure Identity Protection (AIP) y qué tipo de identidades se pueden proteger.
- Habilitar las políticas de protección predeterminadas en AIP.
- Identificar las vulnerabilidades y los eventos de riesgo detectados por AIP.
- Planifique su investigación para proteger las identidades basadas en la nube.
- Planifique cómo proteger su entorno de Azure Active Directory de las brechas de seguridad.

Módulo 7: Examine la protección de Exchange Online.

Este módulo examina cómo Exchange Online Protection (EOP) protege a las organizaciones del 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 los usuarios.

- Examine la canalización antimalware.
- Detecta mensajes con spam o malware usando la purga automática de cero horas.
- Explore la protección antisuplantación proporcionada por Exchange Online Protection.
- Explora otras protecciones anti-spoofing.
- Examine el filtrado de spam saliente.

Al final de este módulo, podrás:

- Describa cómo Exchange Online Protection analiza el correo electrónico para proporcionar protección contra la canalización antimalware.
- Enumere varios mecanismos utilizados por Exchange Online Protection para filtrar el spam y el malware.
- Describir otras soluciones que los administradores pueden implementar para proporcionar una protección adicional contra el phishing y la suplantación de identidad.
- Comprenda cómo EOP proporciona protección contra el spam saliente.

Módulo 8: Examinar Microsoft Defender para Office 365.

Este módulo examina cómo Microsoft Defender para Office 365 extiende la protección EOP filtrando ataques dirigidos como ataques de día cero en archivos adjuntos de correo electrónico y documentos de Office, y la protección de tiempo de clic contra URL maliciosas.

- Sube la escalera de seguridad de EOP a Microsoft Defender para Office 365.
- Amplíe las protecciones EOP mediante el uso de archivos adjuntos seguros y enlaces seguros.
- Proteja a los usuarios de archivos adjuntos maliciosos mediante el uso de archivos adjuntos seguros.
- Proteja a los usuarios de URL maliciosas mediante el uso de enlaces seguros.
- Gestionar la inteligencia de la parodia.
- Configurar políticas de filtrado de spam saliente.
- Desbloquear a los usuarios del envío de correo electrónico.

Al final de este módulo, podrás:

- Describa cómo la función de archivos adjuntos seguros de Microsoft Defender para Office 365 bloquea el malware de día cero en los archivos adjuntos y documentos de correo electrónico.
- Describa cómo la función de enlaces seguros de Microsoft Defender para Office 365 protege a los usuarios de las URL maliciosas incrustadas en el correo electrónico y los documentos que apuntan a sitios web maliciosos.
- Crea políticas de filtrado de spam saliente.
- Desbloquear a los usuarios que hayan violado las políticas de filtrado de spam para que puedan reanudar el envío de correos electrónicos.

Módulo 9: Administrar archivos adjuntos seguros.

Este módulo examina cómo administrar los archivos adjuntos seguros en su inquilino de Microsoft 365 creando y configurando políticas y utilizando reglas de transporte para desactivar que una política entre en vigor en ciertos escenarios.

- 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 archivos adjuntos seguros.

Al final de este módulo, podrás:

- Crear y modificar una política de archivos adjuntos seguros usando Microsoft 365 Defender.
- Crear una política de archivos adjuntos seguros usando PowerShell.
- Configurar una política de archivos adjuntos seguros.
- Describir cómo una regla de transporte puede deshabilitar una política de archivos adjuntos seguros.
- Describa la experiencia del usuario final cuando se escanea un archivo adjunto de correo electrónico y se descubre que es malicioso.

Módulo 10: Administrar enlaces seguros.

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

- Crear políticas de enlaces seguros usando Microsoft Defender para Office 365.
- 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.

Al final de este módulo, podrás:

- Crear y modificar una política de enlaces seguros utilizando Microsoft 365 Defender.
- Crear una política de enlaces seguros usando PowerShell.
- Configurar una política de enlaces seguros.
- Describa cómo una regla de transporte puede desactivar una política de enlaces seguros.
- Describir la experiencia del usuario final cuando Safe Links identifica un enlace a un sitio web malicioso incrustado en el correo electrónico, y un enlace a un archivo malicioso alojado en un sitio web.

Módulo 11: Explora la inteligencia de amenazas en Microsoft 365 Defender.

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

- Explora Microsoft Intelligent Security Graph.
- Explora las políticas de alerta en Microsoft 365.
- Ejecutar investigaciones y respuestas automatizadas.
- Explora la caza de amenazas con Microsoft Threat Protection.
- Explora la caza avanzada de amenazas en Microsoft 365 Defender.
- Explora el análisis de amenazas en Microsoft 365.

Al final de este módulo, podrás:

- Describa cómo la inteligencia de amenazas en Microsoft 365 está impulsada por el gráfico de seguridad inteligente de Microsoft.
- Crea alertas que puedan identificar eventos maliciosos o sospechosos.
- Comprenda cómo funciona el proceso automatizado de investigación y respuesta de Microsoft 365 Defender.
- Describa cómo la búsqueda de amenazas permite a los operadores de seguridad identificar las amenazas de ciberseguridad.
- Describa cómo la caza avanzada en Microsoft 365 Defender inspecciona de forma proactiva los eventos en su red para localizar indicadores y entidades de amenazas.

Módulo 12: Implementar la protección de aplicaciones mediante el uso de Microsoft Defender para aplicaciones en la nube.

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

- Explora Microsoft Defender para aplicaciones en la nube.
- Implementar Microsoft Defender para aplicaciones en la nube.
- Configurar políticas de archivos en Microsoft Defender para aplicaciones en la nube.
- Administrar y responder a las alertas en Microsoft Defender para aplicaciones en la nube.

- Configurar Cloud Discovery en Microsoft Defender para aplicaciones en la nube.
- Solucionar problemas de descubrimiento de la nube en Microsoft Defender para aplicaciones en la nube.

Al final de este módulo, podrás:

- Describa cómo Microsoft Defender for Cloud Apps proporciona una mejor visibilidad de la actividad de la nube de la red y aumenta la protección de los datos críticos en las aplicaciones en la nube.
- Explicar cómo implementar Microsoft Defender para aplicaciones en la nube.
- Controla tus aplicaciones en la nube con políticas de archivos.
- Administre y responda a las alertas generadas por esas políticas.
- Configurar y solucionar problemas de Cloud Discovery.

Módulo 13: Implementar la protección de punto final utilizando Microsoft Defender para Endpoint.

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

- Explora Microsoft Defender para Endpoint.
- Configurar Microsoft Defender para Endpoint en Microsoft Intune.
- Dispositivos integrados en Microsoft Defender para Endpoint.
- Gestionar las amenazas y vulnerabilidades de los puntos finales.
- Gestionar el descubrimiento de dispositivos y la evaluación de la vulnerabilidad.
- Reduzca su exposición a amenazas y vulnerabilidades.

Después de completar este módulo, podrás:

- Describa cómo Microsoft Defender for Endpoint ayuda a las redes empresariales a prevenir, detectar, investigar y responder a amenazas avanzadas.
- Dispositivos compatibles integrados con Microsoft Defender for Endpoint.
- Implementar el módulo de gestión de amenazas y vulnerabilidades para identificar, evaluar y corregir eficazmente las debilidades de los puntos finales.
- Configure el descubrimiento de dispositivos para ayudar a encontrar dispositivos no gestionados conectados a su red corporativa.
- Reduzca la exposición a amenazas y vulnerabilidades de su organización remediando los problemas basados en recomendaciones de seguridad priorizadas.

Módulo 14: Implementar la protección contra amenazas mediante el uso de Microsoft Defender para Office 365.

Este módulo examina la pila de protección de Microsoft Defender para Office 365 y sus correspondientes características de inteligencia de amenazas, incluyendo Threat Explorer, Threat Trackers y entrenamiento de simulación de ataques.

- Explora la pila de protección de Microsoft Defender para Office 365.
- Investigar los ataques de seguridad mediante el uso de Threat Explorer.
- Identificar problemas de ciberseguridad mediante el uso de rastreadores de amenazas.
- Prepárate para los ataques con el entrenamiento de simulación de ataque.

Después de completar este módulo, podrás:

- Describa la pila de protección proporcionada por Microsoft Defender para Office 365.
- Comprenda cómo se puede utilizar Threat Explorer para investigar amenazas y ayudar a proteger a su inquilino.
- Describa los widgets y vistas de Threat Tracker que le proporcionan información sobre diferentes problemas de ciberseguridad que podrían afectar a su empresa.
- Ejecute escenarios de ataque realistas utilizando Attack Simulator para ayudar a identificar a los usuarios vulnerables antes de que un ataque real afecte a su organización.

Módulo 15: Examinar las soluciones de gobernanza y cumplimiento 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 al proporcionar un conjunto completo de soluciones que ayudan a las organizaciones a gobernar, proteger y administrar todo su estado de datos.

- Explore la gobernanza y el cumplimiento de los datos en Microsoft Purview.
- Proteja los datos confidenciales con Microsoft Purview Information Protection.
- Gestionar los datos de la organización utilizando Microsoft Purview Data Lifecycle Management.
- Minimice los riesgos internos con Microsoft Purview Insider Risk Management.
- Explore las soluciones de Microsoft Purview eDiscovery.

Al final de este módulo, podrás:

- Proteja los datos confidenciales con Microsoft Purview Information Protection.
- Gobierna los datos de la organización utilizando Microsoft Purview Data Lifecycle Management.
- Minimice los riesgos internos con Microsoft Purview Insider Risk Management.
- Explique las soluciones de Microsoft Purview eDiscovery.

Módulo 16: Explora el archivo y la gestión de registros en Microsoft 365.

Este módulo examina cómo Microsoft 365 apoya la gobernanza de datos al permitir a las organizaciones archivar contenido mediante el uso de buzones de archivo y gestionar su contenido de alto valor para obligaciones legales, comerciales o reglamentarias mediante la implementación de la gestión de registros.

- Explora los buzones de archivo en Microsoft 365.
- Habilitar buzones de archivo en Microsoft 365.
- Explora la gestión de registros en Microsoft 365.
- Implementar la gestión de registros en Microsoft 365.
- Restaurar datos eliminados en Exchange Online.
- Restaurar datos eliminados en SharePoint Online.

Al final de este módulo, podrás:

- Habilite y deshabilite un buzón de archivo en el portal de cumplimiento de Microsoft Purview y a través de Windows PowerShell.
- Ejecute pruebas de diagnóstico en un buzón de archivo.
- Aprenda cómo se pueden usar las etiquetas de retención para permitir o bloquear acciones cuando los documentos y correos electrónicos se declaran registros.
- Cree su plan de archivos para la configuración y las acciones de retención y eliminación.
- Determine cuándo se deben marcar los elementos como registros importando un plan existente (si ya tiene uno) o cree nuevas etiquetas de retención.
- Restaurar los datos eliminados en Exchange Online y SharePoint Online.

Módulo 17: Explora la retención en Microsoft 365.

Este módulo examina cómo se pueden retener 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.

- Explore la retención utilizando 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 utilizando políticas de retención, etiquetas de retención y retenciones de eDiscovery.
- Restringir los cambios de retención mediante el bloqueo de preservación.

Al final de este módulo, podrás:

- Explique cómo funcionan las políticas de retención y las etiquetas de retención.
- Identifique las capacidades tanto de las políticas de retención como de las etiquetas de retención.
- Seleccione el alcance apropiado para una política en función de los requisitos del negocio.
- Explicar los principios de retención.
- Identifique las diferencias entre la configuración de retención y las retenciones de eDiscovery.
- Restrinja los cambios de retención mediante el bloqueo de preservación.

Módulo 18: Explora el cifrado de mensajes de Microsoft Purview.

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

- Examine el cifrado de mensajes de Microsoft.
- Configurar el cifrado de mensajes de Microsoft Purview.
- Definir reglas de flujo de correo para cifrar los mensajes de correo electrónico.
- Añadir la marca de la organización a los mensajes de correo electrónico cifrados.
- Explora el cifrado de mensajes avanzado de Microsoft Purview.

Al final de este módulo, podrás:

- Describa las características del cifrado de mensajes de Microsoft Purview.
- Explique cómo funciona el cifrado de mensajes de Microsoft Purview y cómo configurarlo.
- Defina reglas de flujo de correo que apliquen plantillas de marca y cifrado para cifrar los mensajes de correo electrónico.
- Añade una marca organizativa a los mensajes de correo electrónico cifrados.
- Explique las capacidades adicionales proporcionadas por Microsoft Purview Advanced Message Encryption.

Módulo 19: Explora el cumplimiento en Microsoft 365.

Este módulo explora las herramientas que Microsoft 365 proporciona 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.

- Planificar la seguridad y el cumplimiento en Microsoft 365.
- Planifique sus tareas iniciales de cumplimiento en Microsoft Purview.
- Gestione sus requisitos de cumplimiento con el Gerente de Cumplimiento.
- Examine el panel de control del Administrador de Cumplimiento.
- Analizar la puntuación de cumplimiento de Microsoft.

Al final de este módulo, podrás:

- Describa cómo Microsoft 365 ayuda a las organizaciones a gestionar los riesgos, proteger los datos y seguir cumpliendo con las regulaciones y estándares.
- Planifique sus tareas iniciales de cumplimiento en Microsoft Purview.
- Gestione sus requisitos de cumplimiento con Compliance Manager.
- Gestione la postura de cumplimiento y las acciones de mejora utilizando el panel de control de Compliance Manager.
- Explicar cómo se determina la puntuación de cumplimiento de una organización.

Módulo 20: Implementar la gestión de riesgos de Microsoft Purview Insider.

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.

- Explora la gestión de riesgos con información privilegiada.
- Plan para la gestión de riesgos internos.
- Explore las políticas de gestión de riesgos de información privilegiada.
- Crear políticas de gestión de riesgos con información privilegiada.
- Investigar las actividades y alertas de gestión de riesgos internos.
- Explora casos de gestión de riesgos internos.

Al final de este módulo, podrás:

- Describir la funcionalidad de gestión de riesgos internos en Microsoft 365.
- Desarrolle un plan para implementar la solución de gestión de riesgos de Microsoft Purview Insider.
- Crear políticas de gestión de riesgos con información privilegiada.
- Gestione las alertas y casos de gestión de riesgos internos.

Módulo 21: Crear barreras de información en Microsoft 365.

Este módulo examina cómo Microsoft 365 utiliza las barreras de información para restringir la comunicación y la colaboración en Microsoft Teams, SharePoint Online y OneDrive for Business.

- Explora las barreras de la información en Microsoft 365.
- Configurar barreras de información.
- Examinar las barreras de información en Microsoft Teams.

- Examinar las barreras de información en OneDrive.
- Examinar las barreras de información en SharePoint.

Al final de este módulo, podrás:

- Describa cómo las barreras de la información pueden restringir o permitir la comunicación y la colaboración entre grupos específicos de usuarios.
- Describa los componentes de una barrera de la información y cómo habilitar las barreras de la información.
- Comprenda cómo los modos de barrera de la información ayudan a fortalecer quién puede ser agregado o eliminado de un equipo de Microsoft, una cuenta de OneDrive y un sitio de SharePoint.
- Describa cómo las barreras de información impiden que los usuarios o grupos se comuniquen y colaboren en Microsoft Teams, OneDrive y SharePoint.

Módulo 22: Explora la prevención de pérdida de datos en Microsoft 365.

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 los datos confidenciales a través de un análisis de contenido profundo, al tiempo que ayuda a los usuarios a comprender y gestionar los riesgos de los datos.

- Examinar la prevención de la pérdida de datos.
- Explora la prevención de pérdida de datos de puntos finales.
- Examinar las políticas de DLP.
- Ver los resultados de la política de DLP.
- Explora los informes de DLP.

Al final de este módulo, podrás:

- Describa cómo se gestiona la prevención de pérdida de datos (DLP) en Microsoft 365
- Comprender cómo DLP en Microsoft 365 utiliza tipos de información confidencial y patrones de búsqueda
- Describa cómo Microsoft Endpoint DLP amplía las capacidades de monitoreo y protección de la actividad de DLP.
- Describa qué es una política de DLP y qué contiene
- Ver los resultados de la política de DLP utilizando tanto consultas como informes

Módulo 23: Implementar políticas de prevención de pérdida de datos.

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

- Plan para la prevención de la pérdida de datos.
- Implementar la política DLP predeterminada.
- Diseñar una política DLP personalizada.
- Crear una política DLP personalizada a partir de una plantilla.
- Configurar notificaciones por correo electrónico para las políticas de DLP.
- Configurar consejos de política para las políticas de DLP.

Al final de este módulo, podrás:

- Crear un plan de implementación de prevención de pérdida de datos. Implementar la política DLP predeterminada de Microsoft 365.
- Crea una política DLP personalizada a partir de una plantilla DLP y desde cero.
- Crea notificaciones por correo electrónico y consejos de política para los usuarios cuando se aplique una regla DLP.
- Crear consejos de política para los usuarios cuando se aplique una regla DLP.
- Configurar notificaciones por correo electrónico para las políticas de DLP.

Módulo 24: Implementar la clasificación de datos de información confidencial.

Este módulo le presenta la clasificación de datos en Microsoft 365, incluyendo cómo crear y entrenar clasificadores, ver datos confidenciales utilizando el Explorador de contenido y el explorador de actividad, e implementar la huella digital del documento.

- Explorar la clasificación de datos de información confidencial.
- Implementar la clasificación de datos en Microsoft 365.
- Explora los clasificadores entrenables.
- Crear y volver a entrenar un clasificador entrenable.
- Ver datos confidenciales usando el Explorador de contenido y el explorador de actividad.
- Detectar documentos de información confidencial usando las huellas dactilares del documento.

Al final de este módulo, podrás:

- Explicar los beneficios y puntos débiles de crear un marco de clasificación de datos.
- Identifique cómo se maneja la clasificación de datos de elementos confidenciales en Microsoft 365.
- Comprenda cómo Microsoft 365 utiliza clasificadores entrenables para proteger los datos confidenciales.
- Analice los resultados de sus esfuerzos de clasificación de datos en el Explorador de contenido y el explorador de actividad.
- Implementar la huella digital del documento para proteger la información confidencial que se envía a través de Exchange Online.

Módulo 25: Explora las etiquetas de sensibilidad.

Este módulo examina cómo las etiquetas de sensibilidad de la solución de protección de la información de Microsoft Purview le permiten clasificar y proteger los datos de su organización, al tiempo que se asegura de que la productividad y la colaboración del usuario no se vean obstaculizadas.

- Gestionar la protección de datos utilizando etiquetas de sensibilidad.
- Explora lo que pueden hacer las etiquetas de sensibilidad.
- Determinar el alcance de una etiqueta de sensibilidad.
- Explorar las políticas de etiquetas de sensibilidad.

Al final de este módulo, podrás:

- Describa cómo las etiquetas de sensibilidad le permiten clasificar y proteger los datos de su organización.
- Identificar las razones comunes por las que las organizaciones utilizan etiquetas de sensibilidad.
- Explicar qué es una etiqueta de sensibilidad y qué pueden hacer por una organización.
- Configurar el alcance de una etiqueta de sensibilidad.
- Explique por qué es importante el orden de las etiquetas de sensibilidad en su centro de administración.
- Describir lo que pueden hacer las políticas de etiquetas.

Módulo 26: Implementar etiquetas de sensibilidad.

Este módulo examina el proceso para implementar etiquetas de sensibilidad, 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.

- Examine los requisitos para crear una etiqueta de sensibilidad.
- Planifique su estrategia de implementación para las etiquetas de sensibilidad.
- Crear etiquetas de sensibilidad.
- Publicar etiquetas de sensibilidad.
- Eliminar y eliminar las etiquetas de sensibilidad.

Al final de este módulo, podrás:

- Describir el proceso general para crear, configurar y publicar etiquetas de sensibilidad.
- Identificar los permisos administrativos que deben asignarse a los miembros del equipo de cumplimiento para implementar etiquetas de sensibilidad.
- Desarrolle un marco de clasificación de datos que proporcione la base para sus etiquetas de sensibilidad.
- Crear y configurar etiquetas de sensibilidad.
- Publicar etiquetas de sensibilidad creando una política de etiquetas.
- Identificar las diferencias entre eliminar y eliminar las etiquetas de sensibilidad.

Módulo 27: Buscar contenido en el portal de cumplimiento de Microsoft Purview.

Este módulo examina cómo buscar contenido en el portal de cumplimiento de Microsoft Purview utilizando la funcionalidad de búsqueda de contenido, incluyendo cómo ver y exportar los resultados de búsqueda y configurar el filtrado de permisos de búsqueda.

- Explore las soluciones de Microsoft Purview eDiscovery.
- Crear una búsqueda de contenido.
- Ver los resultados de búsqueda y las estadísticas.
- Exportar los resultados de la búsqueda y el informe de búsqueda.
- Configurar el filtrado de permisos de búsqueda.
- Buscar y eliminar mensajes de correo electrónico.

Al final de este módulo, podrás:

- Describa cómo utilizar la búsqueda de contenido en el portal de cumplimiento de Microsoft Purview.
- Diseña y crea una búsqueda de contenido.

- Obtenga una vista previa de los resultados de la búsqueda.
- Vea las estadísticas de búsqueda.
- Exporta los resultados de la búsqueda y el informe de búsqueda.
- Configure el filtrado de permisos de búsqueda.

Módulo 28: Administrar la auditoría de gestión de Microsoft (estándar).

Este módulo examina cómo buscar actividades auditadas utilizando la solución Microsoft Purview Audit (Standard), incluyendo cómo exportar, configurar y ver los registros de registro de auditoría que se recuperaron de una búsqueda de registro de auditoría.

- Explore las soluciones de auditoría de Microsoft Purview.
- Implementar la auditoría de competencia de Microsoft (estándar).
- Buscar en el registro de auditoría.
- Exportar, configurar y ver los registros de auditoría.
- Utilice la búsqueda de registros de auditoría para investigar problemas comunes de soporte.

Al final de este módulo, podrás:

- Describa las diferencias entre Auditoría (Estándar) y Auditoría (Premium).
- Identifique las características principales de la solución de auditoría (estándar).
- Configure e implemente la búsqueda de registros de auditoría utilizando la solución de auditoría (estándar).
- Exportar, configurar y ver los registros de registro de auditoría.
- Utilice la búsqueda del registro de auditoría para solucionar problemas comunes de soporte.

Módulo 29: Gestionar la auditoría de competencia de Microsoft (Premium).

Este módulo explora las diferencias entre Microsoft Purview Audit (Standard) y Audit (Premium), además de la funcionalidad clave de Audit (Premium), incluidos los requisitos de configuración, la habilitación del registro de auditoría, la creación de políticas de retención de registros de auditoría y la realización de investigaciones forenses.

- Explore la auditoría de alcance de Microsoft (Premium).
- Implementar Microsoft Purview Audit (Premium).
- Gestionar las políticas de retención de registros de auditoría.
- Investigar cuentas de correo electrónico comprometidas.

Al final de este módulo, podrás:

- Describa las diferencias entre Auditoría (Estándar) y Auditoría (Premium).
- Configurar e implementar Microsoft Purview Audit (Premium).
- Crear políticas de retención de registros de auditoría.
- Realizar investigaciones forenses de cuentas de usuario comprometidas.

Módulo 30: Administrar Microsoft Purview eDiscovery (estándar).

Este módulo explora cómo usar Microsoft Purview eDiscovery (Standard) para crear un caso de eDiscovery y una retención para un caso, cómo administrar el contenido del caso y cómo cerrar, reabrir y eliminar un caso.

- Explore las soluciones de Microsoft Purview eDiscovery.
- Implementar Microsoft Purview eDiscovery (estándar).
- Crear retenciones de eDiscovery.
- Buscar contenido en un caso.
- Exportar contenido de un caso.
- Cerrar, volver a abrir y eliminar un caso.

Al final de este módulo, podrás:

- Describa cómo Microsoft Purview eDiscovery (Standard) se basa en la funcionalidad básica de búsqueda y exportación de la búsqueda de contenido.
- Describa el flujo de trabajo básico de eDiscovery (Estándar).
- Crea un caso de eDiscovery.
- Crea una retención de eDiscovery para un caso de eDiscovery.
- Busca contenido en un caso y luego exporta ese contenido.
- Cierra, vuelve a abrir y elimina un caso.

Módulo 31: Administrar Microsoft Purview eDiscovery (Premium).

Este módulo explora cómo usar Microsoft Purview eDiscovery (Premium) para preservar, recopilar, analizar, revisar y exportar

contenido que responda a las investigaciones internas y externas de una organización, y comunicarse con los custodios involucrados en un caso.

- Explora Microsoft Purview eDiscovery (Premium).
- Implementar Microsoft Purview eDiscovery (Premium).
- Crear y gestionar un caso de eDiscovery (Premium).
- Gestionar los custodios y las fuentes de datos no privativas de la custodia.
- Analizar el contenido del caso.

Al final de este módulo, podrás:

- Describe cómo Microsoft Purview eDiscovery (Premium) se basa en eDiscovery (Estándar).
- Describir el flujo de trabajo básico de eDiscovery (Premium).
- Crear y gestionar casos en eDiscovery (Premium).
- Administrar custodios y fuentes de datos sin custodia.
- Analice el contenido del caso y utilice herramientas analíticas para reducir el tamaño de los conjuntos de resultados de búsqueda.

Módulo 32: Explora la gestión de dispositivos usando Microsoft Endpoint Manager.

Este módulo explora las características de gestión de dispositivos de Microsoft Endpoint Manager, incluyendo Microsoft Intune, Configuration Manager, la cogestión de dispositivos y los perfiles de configuración para los dispositivos que usan Intune.

- Explora la gestión de dispositivos en Microsoft Endpoint Manager.s
- Explora la cogestión de dispositivos Windows.
- Administrar dispositivos usando Configuration Manager.
- Administrar dispositivos usando Microsoft Intune.
- Crear perfiles de dispositivos en Microsoft Intune.

Al final de este módulo, podrás:

- Describa las capacidades de gestión de dispositivos que se encuentran en Microsoft Endpoint Manager.
- Describa cómo los dispositivos Windows se pueden cogestionr en Endpoint Manager utilizando Configuration Manager e Intune.
- Administrar dispositivos usando Configuration Manager.
- Administre dispositivos usando Microsoft Intune.
- Crea perfiles de dispositivo en Microsoft Intune.

Módulo 33: Prepare sus dispositivos Windows para la gestión conjunta.

Este módulo examina los pasos involucrados en la preparación de su entorno existente para la cogestión, desde la revisión de los requisitos previos de la cogestión hasta la configuración de Configuration Manager para la cogestión y la inscripción de dispositivos Windows 10 en Intune.

- Planifica tu estrategia de cogestión.
- Explore los requisitos previos para el uso de la cogestión.
- Configurar el Administrador de configuración para la cogestión.
- Inscribir dispositivos Windows 10 en Intune.
- Modifique su configuración de cogestión.
- Transferir la gestión de la carga de trabajo de Configuration Manager a Intune.

Al final de este módulo, podrás:

- Describir los requisitos previos para usar la cogestión.
- Configurar Microsoft Endpoint Configuration Manager para la cogestión.
- Inscribir dispositivos Windows 10 en Intune.

Módulo 34: Plan para la gestión de aplicaciones móviles en Microsoft Intune.

Este módulo examina cómo planificar la gestión de aplicaciones móviles utilizando Microsoft Intune, con un enfoque en la adición de aplicaciones a Intune, utilizando políticas de protección de aplicaciones y políticas de configuración de aplicaciones, y la solución de problemas de la implementación de políticas de protección de aplicaciones.

- Explora la gestión de aplicaciones móviles en Microsoft Intune.
- Añadir aplicaciones a Microsoft Intune.
- Proteja los datos de la empresa mediante el uso de políticas de protección de aplicaciones.
- Explorar las políticas de configuración de aplicaciones para Intune.
- Solucionar problemas de implementación de políticas de protección de aplicaciones en Intune.

Al final de este módulo, podrás:

- Describir la funcionalidad básica de la gestión de aplicaciones móviles en Microsoft Intune.
- Evalúe los requisitos de su aplicación y agregue aplicaciones a Intune.

- Proteja los datos de la empresa mediante el uso de políticas de protección de aplicaciones.
- Implemente políticas de configuración de aplicaciones para eliminar los problemas de configuración de aplicaciones.
- Solucionar problemas de implementación de políticas de protección de aplicaciones en Intune.

Módulo 35: Examinar los escenarios de implementación del cliente de Windows.

Este módulo examina el modelo de servicio para Windows como servicio, cómo planificarlo en su organización y los modelos de implementación de Windows 10/11, incluidos los métodos de implementación modernos, dinámicos y tradicionales.

- Explora Windows como servicio.
- Explora los modelos de implementación de clientes de Windows.
- Examinar los métodos de implementación modernos.
- Examinar los métodos de despliegue dinámicos y tradicionales.

Al final de este módulo, podrás:

- Explique cómo el modelo de Windows como servicio proporciona continuamente nuevas capacidades y actualizaciones al tiempo que mantiene un alto nivel de compatibilidad de hardware y software.
- Explique cómo el moderno modelo de implementación de Windows 10/11 combina los servicios tradicionales en las instalaciones y en la nube para ofrecer una experiencia de implementación optimizada y rentable.
- Explique cómo el modelo de implementación dinámico de Windows 10/11 puede transformar la versión existente de Windows 10/11 que se incluye en un dispositivo en una versión personalizada que se utiliza en su empresa sin necesidad de reinstalar Windows.
- Explique cómo el modelo de implementación tradicional de Windows 10/11 está basado en imágenes y utiliza la infraestructura local de una organización.

Módulo 36: Explora los modelos de implementación del piloto automático de Windows.

Este módulo examina los modelos de implementación del piloto automático de Windows y cómo le permiten implementar nuevos dispositivos sin la necesidad de crear, mantener y aplicar imágenes personalizadas del sistema operativo a los dispositivos.

- Explora el piloto automático de Windows.
- Examinar los requisitos previos del piloto automático de Windows.
- Planifica la configuración de los perfiles del piloto automático de Windows.
- Examine el modelo de autoimplementación del piloto automático de Windows.
- Examine el modelo de implementación preaprovisionada del piloto automático de Windows.
- Examine el modelo de implementación impulsado por el usuario de Windows Autopilot.
- Implementar el cifrado BitLocker para dispositivos con piloto automático.

Al final de este módulo, podrás:

- Describa los requisitos de implementación del piloto automático de Windows.
- Crea y asigna un perfil de piloto automático de Windows.
- Explique cómo el modelo de autoimplementación del piloto automático implementa Windows 10 y 11 con poca o ninguna interacción del usuario.
- Explique cómo el modelo de implementación preaprovisionada del piloto automático permite a los usuarios finales aprovisionar nuevos dispositivos mediante el uso de la imagen y los controladores OEM preinstalados.
- Explique cómo el modelo de implementación impulsado por el usuario del piloto automático permite que los nuevos dispositivos Windows 10 y 11 se transformen desde su estado inicial de fábrica sin necesidad de que el personal de TI toque el dispositivo.
- Implemente el cifrado BitLocker para dispositivos con piloto automático.

Módulo 37: Planifique su estrategia de activación de la suscripción al cliente de Windows.

Este módulo examina cómo la activación de la suscripción de Windows 10/11 permite una actualización en línea sin problemas de Windows 10/11 Pro a Windows 10/11 Enterprise, cómo proporciona la activación automática de la suscripción y cómo se pueden implementar las licencias empresariales.

- Explore la disponibilidad de Windows 10/11 Enterprise E3 a través del canal de proveedores de servicios en la nube.

- Configurar el acceso al escritorio virtual para la activación automática de la suscripción en máquinas virtuales.
- Implementar licencias de Windows 10/11 Enterprise.

Al final de este módulo, podrás:

- Describa cómo se pueden comprar las suscripciones a Windows 10/11 Enterprise E3 a través del canal del proveedor de servicios en la nube.
- Configure el acceso al escritorio virtual para la activación automática de la suscripción en máquinas virtuales.
- Explique cómo las licencias de Windows 10/11 Enterprise se pueden implementar de forma automática y sin reiniciar el dispositivo.

Módulo 38: Explora la gestión de dispositivos móviles.

Este módulo examina las capacidades integradas de la gestión de dispositivos móviles en Microsoft 365, incluida una comparación de las dos soluciones MDM de Microsoft, la configuración de políticas para dispositivos móviles y el control del acceso al correo electrónico y a los documentos.

- Explora la gestión de dispositivos móviles en Microsoft 365.
- Explora los servicios de gestión de dispositivos móviles en Microsoft 365.
- Examine la configuración de la política de gestión de dispositivos móviles en Microsoft 365.
- Examine cómo se controla el acceso al correo electrónico y a los documentos en los dispositivos gestionados por dispositivos móviles.

Al final de este módulo, podrás:

- Describa las dos soluciones de autoridad de MDM incluidas en Microsoft 365: Microsoft Intune y Basic Mobility and Security.
- Compara las características básicas de Microsoft Intune y Movilidad y seguridad básicas.
- Describir la configuración de la política para dispositivos móviles en Microsoft Intune y Basic Mobility and Security.
- Explicar cómo se controla el acceso al correo electrónico y a los documentos en los dispositivos gestionados por MDM.

Módulo 39: Implementar la gestión de dispositivos móviles.

Este módulo examina cómo implementar la gestión de dispositivos móviles en Microsoft 365, incluida la activación de los servicios de MDM, la configuración de las políticas de MDM, la inscripción de dispositivos, la adición de registros DNS de clientes y la obtención de un certificado APNS para dispositivos iOS.

- Activar los servicios de gestión de dispositivos móviles en Microsoft 365.
- Configurar dominios para la gestión de dispositivos móviles.
- Obtener un certificado del servicio de notificación push de Apple para dispositivos iOS.
- Gestionar las políticas de seguridad para los dispositivos gestionados por dispositivos móviles.
- Definir una política de inscripción de dispositivos corporativos.

Al final de este módulo, podrás:

- Activar e implementar servicios de gestión de dispositivos móviles en Microsoft 365.
- Configure dominios para MDM agregando registros DNS para que los clientes utilicen Autodiscover al inscribir dispositivos.
- Obtener un certificado APNS para inscribir y administrar dispositivos iOS.
- Administrar las políticas de seguridad del dispositivo que pueden controlar la configuración de la contraseña, la configuración de cifrado y la configuración que controla el uso de las características del dispositivo.
- Definir una política de inscripción de dispositivos corporativos que pueda limitar la inscripción y habilitar la autenticación multifactorial.

Módulo 40: Inscribir dispositivos en la gestión de dispositivos móviles.

Este módulo examina la inscripción de dispositivos en MDM, incluidos los métodos de inscripción de dispositivos, los dispositivos unidos de Azure AD, los dispositivos híbridos unidos de Azure AD, los métodos de inscripción de dispositivos en Intune y la inscripción para dispositivos Windows.

- Revisar los métodos de inscripción de dispositivos.
- Examine los dispositivos registrados en Azure AD.
- Explora los dispositivos conectados a Azure AD.

- Explora los dispositivos híbridos conectados a Azure AD.
- Examinar la inscripción de dispositivos en Intune.
- Examinar las capacidades de inscripción de dispositivos.
- Configurar la inscripción para dispositivos Windows.

Al final de este módulo, podrás:

- Inscriba los dispositivos en la gestión de dispositivos móviles en Microsoft Intune.
- Explora el uso de los dispositivos conectados de Azure AD e híbridos de Azure AD.
- Explique cómo los usuarios pueden inscribir sus dispositivos personales.
- Describir las mejores prácticas y capacidades para cada método de inscripción de dispositivos.

Módulo 41: Gestionar el cumplimiento de los dispositivos.

Este módulo examina las políticas de cumplimiento de dispositivos, cómo las organizaciones las utilizan de manera efectiva, cómo crear políticas y configurar usuarios y grupos condicionales, cómo crear políticas de acceso condicional y cómo monitorear los dispositivos inscritos.

- Plan para el cumplimiento de los dispositivos.
- Implementar políticas de cumplimiento para los dispositivos gestionados por Intune.
- Supervise los resultados de las políticas de cumplimiento de su dispositivo Intune.
- Implementar grupos de usuarios y dispositivos para supervisar el cumplimiento de los dispositivos.
- Explorar las políticas de acceso condicional.
- Crear políticas de acceso condicional.
- Supervisar los dispositivos inscritos.

Al final de este módulo, podrás:

- Planifique el cumplimiento del dispositivo definiendo las reglas y configuraciones que deben configurarse en un dispositivo para que se considere que cumple
- Configurar usuarios y grupos condicionales para implementar perfiles, políticas y aplicaciones
- Cree políticas para implementar decisiones de control de acceso automatizado para acceder a sus aplicaciones en la nube
- Supervisar los dispositivos inscritos para controlar sus actividades de Intune y su estado de cumplimiento

Módulo 42: Implementar la seguridad de los puntos finales en Microsoft Intune.

Este módulo explora cómo las organizaciones utilizan Microsoft Intune para implementar la seguridad de los puntos finales, incluido el uso de la configuración de dispositivos y las políticas de cumplimiento de los dispositivos, la gestión de dispositivos, las líneas de base de seguridad y las reglas de reducción de la superficie de ataque.

- Protege datos y dispositivos con Microsoft Intune.
- Explora la seguridad de los puntos finales en Microsoft Intune.
- Administrar dispositivos con seguridad de punto final en Intune.
- Utilice las líneas de base de seguridad para configurar dispositivos Windows en Intune.
- Administrar perfiles de línea de base de seguridad en Microsoft Intune.
- Implementar reglas de reducción de la superficie de ataque.

Al final de este módulo, podrás:

- Describir cómo Microsoft Intune permite a las organizaciones proteger sus datos y dispositivos.
- Comprenda cómo la seguridad de los puntos finales en Microsoft Intune se centra en la seguridad de los dispositivos y la mitigación de riesgos.
- Gestiona dispositivos con seguridad de punto final en Intune.
- Utilice las líneas de base de seguridad para configurar dispositivos Windows en Intune.
- Implementar reglas de reducción de la superficie de ataque para reducir la superficie de ataque de una organización.