



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

MD-102 / Manage and secure Microsoft 365 endpoints by using Intune

En este curso, los alumnos aprenden a planear y ejecutar una estrategia de implementación, configuración y administración de puntos de conexión mediante Microsoft Intune como plataforma unificada de administración de puntos de conexión. En el curso se describe la preparación de la infraestructura de identidades y dispositivos con Microsoft Entra ID, la inscripción y configuración de dispositivos, la administración de aplicaciones y la protección de puntos de conexión y datos. Los alumnos también exploran la automatización con PowerShell y Microsoft Graph, la administración asistida por IA con Microsoft Security Copilot, las funcionalidades extendidas de Microsoft Intune Suite y la entrega de escritorios hospedados en la nube con Windows 365 y Azure Virtual Desktop. Entre las tecnologías exploradas se incluyen Microsoft Intune, Microsoft Entra ID, Windows Autopilot, Microsoft Defender para punto de conexión, Microsoft Tunnel, Microsoft Cloud PKI, Windows 365, Microsoft Intune Suite y Azure Virtual Desktop.

Perfil del Público

Como candidato para este curso y el examen asociado, tiene experiencia en la materia para administrar dispositivos y aplicaciones cliente en un inquilino de Microsoft 365 mediante Microsoft Intune. Los administradores de puntos de conexión colaboran con arquitectos, administradores de Microsoft 365, administradores de seguridad y otros administradores de cargas de trabajo para planear e implementar una estrategia de área de trabajo moderna que satisfaga las necesidades empresariales de una organización. Usted es responsable de:

Implementar soluciones para una implementación y administración eficientes de puntos de conexión en varios sistemas operativos, plataformas y tipos de dispositivo.

Implementación y administración de puntos de conexión a escala mediante Microsoft Intune, Microsoft Intune Suite, Windows Autopilot, Microsoft Security Copilot, Microsoft Defender para punto de conexión, Id. de Microsoft Entra, Azure Virtual Desktop y Windows 365.

Implementación de identidades, seguridad, acceso, directivas, actualizaciones y aplicaciones para puntos de conexión.

Rol de trabajo: Administrador

Preparación para el examen: MD-102

Requisitos Previos

- Conocimientos básicos de los conceptos de administración de Microsoft 365
- Familiaridad con Microsoft Entra ID y administración de usuarios o grupos
- Acceso a un inquilino de prueba de Microsoft 365 (recomendado para la práctica)



Módulos

Descripción de las estrategias de administración de puntos de conexión y Microsoft Intune

En este módulo se presentan Microsoft Intune y estrategias modernas de administración de puntos de conexión. Explorará los modelos de administración, el rol de Microsoft Entra ID y las funcionalidades de MDM que permiten la administración de dispositivos basada en la nube.

- Introducción
- ¿Qué es Microsoft Intune y cómo funciona?
- Comparar Administrador de configuración, Intune y administración conjunta
- Comprender el rol de Microsoft Entra ID en Intune
- Evaluación de modelos de administración de dispositivos
- Explorar las funcionalidades de MDM en Intune
- Comprobación de conocimientos
- Resumen

Configuración de Microsoft Entra ID para la administración de dispositivos y directivas

Configure Microsoft Entra ID para admitir la administración de puntos de conexión basada en Intune mediante la administración de usuarios, grupos, roles y configuración de registro de dispositivos para lograr una aplicación eficaz de la seguridad y el destino de las directivas.

- Introducción
- Descripción del rol de Microsoft Entra ID en la administración de puntos de conexión
- Creación y administración de usuarios y grupos en Microsoft Entra ID
- Asignación de roles de Microsoft Entra ID para la administración de dispositivos
- Configuración de Microsoft Entra ID configuración de registro de dispositivos
- Uso de filtros y pertenencia a grupos dinámicos en Microsoft Entra ID
- Comprobación de conocimientos

- Resumen

Administración de la identidad y la autenticación del dispositivo mediante Microsoft Entra ID

En este módulo se explica cómo Microsoft Entra ID representa los dispositivos, las diferencias entre el registro, la unión Entra y la unión híbrida, y cómo la autenticación basada en dispositivos y la confianza admiten la administración Intune y el acceso condicional.

- Introducción
- Descripción de las identidades de dispositivo en Microsoft Entra ID
- Comparación del registro de dispositivos, la unión Microsoft Entra y la unión híbrida
- Descripción de los métodos de autenticación: confianza de claves, confianza de certificados y TPM
- Configuración de la confianza del dispositivo y la unión
- Validación y solución de problemas de identidad y confianza del dispositivo
- Comprobación de conocimientos
- Resumen

Planear e implementar la inscripción de dispositivos mediante Microsoft Intune

En este módulo se explica cómo planear e implementar la inscripción de dispositivos en Microsoft Intune en las plataformas Windows, iOS/iPadOS, macOS y Android. Configuraré las restricciones de inscripción y solucionará errores comunes de inscripción.

- Introducción
- Elección de una estrategia de inscripción
- Inscripción de dispositivos Windows mediante Microsoft Intune
- Inscripción de dispositivos iOS y iPadOS
- Inscripción de dispositivos macOS
- Inscripción de dispositivos Android

- Configuración de restricciones de inscripción
- Solución de problemas de inscripción de dispositivos
- Comprobación de conocimientos
- Resumen

Implementación de dispositivos Windows mediante Windows Autopilot

En este módulo se explica cómo usar Windows Autopilot para implementar dispositivos Windows sin la creación de imágenes tradicional. Puede registrar dispositivos, configurar perfiles de implementación, aprovisionar previamente dispositivos, asignar perfiles, supervisar implementaciones y solucionar problemas comunes.

- Introducción
- Descripción de los escenarios y las ventajas de Windows Autopilot
- Registro e importación de dispositivos en Autopilot
- Configuración de perfiles y modos de implementación de Autopilot
- Aprovisionamiento previo de dispositivos mediante Autopilot
- Asignación de perfiles y supervisión de implementaciones de Autopilot
- Solución de problemas de implementación de Autopilot
- Comprobación de conocimientos
- Resumen

Configuración de perfiles de dispositivo y administración de directivas mediante Microsoft Intune

En este módulo se explica cómo crear y asignar perfiles de configuración y directivas de cumplimiento en Intune, usar grupos y filtros para la implementación de destino y analizar directiva de grupo migración con análisis de directiva de grupo.

- Introducción
- Descripción de los perfiles de configuración del dispositivo y su rol en la aplicación de directivas

- Creación de perfiles de configuración
- Asignación de perfiles de configuración mediante grupos y filtros
- Creación de directivas de cumplimiento
- Asignación de directivas de cumplimiento mediante grupos y filtros
- Análisis y migración de directiva de grupo mediante análisis de directiva de grupo
- Solución de problemas de aplicación de directivas y configuración de dispositivos
- Comprobación de conocimientos
- Resumen

Supervisión y mantenimiento de dispositivos mediante Microsoft Intune

En este módulo se trata la supervisión del estado y el rendimiento de los dispositivos con Endpoint Analytics, el uso de correcciones proactivas, la generación de informes de cumplimiento y de dispositivos y la automatización de tareas rutinarias con PowerShell.

- Introducción
- Comprender el rol de la supervisión en la administración de puntos de conexión
- Uso de Endpoint Analytics para supervisar el estado y el rendimiento del dispositivo
- Uso de correcciones para corregir problemas comunes del dispositivo
- Supervisión de anillos de Windows Update e implementaciones de actualizaciones de características
- Visualización del estado del dispositivo y la directiva en el centro de administración de Intune
- Generación e interpretación de informes de cumplimiento y dispositivos
- Automatización de tareas de administración mediante PowerShell
- Comprobación de conocimientos
- Resumen

Administrar las actualizaciones y el ciclo de vida de Windows mediante Microsoft Intune

En este módulo se explican los modelos de mantenimiento de Windows y cómo

implementar anillos de actualización, actualizaciones de características, Hotpatch y Autopatch para mantener el cumplimiento y el ciclo de vida de las actualizaciones de dispositivos.

- Introducción
- Descripción del modelo de mantenimiento de Windows y los tipos de actualización
- Implementar anillos de actualización y directivas de actualización de características en Intune
- Configuración y administración de Hotpatch con Microsoft Intune
- Administración de canales de mantenimiento de Windows para dispositivos empresariales
- Implementación de Windows Autopatch para la administración automatizada de actualizaciones
- Solución de problemas de cumplimiento e implementación de actualizaciones
- Retirar y restablecer dispositivos mediante Microsoft Intune
- Comprobación de conocimientos
- Resumen

Solución de problemas de dispositivos y directivas mediante Microsoft Intune

En este módulo se tratan los Intune el flujo de trabajo de solución de problemas, los errores comunes de inscripción y cumplimiento, los diagnósticos con registros y la hoja Solución de problemas, y la automatización de las correcciones.

- Introducción
- Descripción del flujo de trabajo de solución de problemas en Microsoft Intune
- Solución de problemas de inscripción de dispositivos y errores de cumplimiento
- Solución de problemas de conflictos de directivas y perfiles de configuración
- Uso de registros y diagnósticos para investigar problemas del dispositivo

- Use la hoja solución de problemas de Intune para diagnósticos basados en el usuario.
- Automatización de la resolución de problemas mediante scripts de corrección
- Comprobación de conocimientos
- Resumen

Implementación y administración de aplicaciones mediante Microsoft Intune

Planee y ejecute implementaciones de aplicaciones en toda la organización mediante Microsoft Intune. Elija el método de implementación adecuado para Microsoft Store, Microsoft 365, Win32 y las aplicaciones de línea de negocio, configure el comportamiento de destino y actualización y solucione los errores de instalación.

- Escenario de ejemplo
- Descripción de las opciones de implementación de aplicaciones en Microsoft Intune
- Planeamiento de la implementación de aplicaciones para su organización
- Implementación de aplicaciones de Microsoft Store con Microsoft Intune
- Implementación de aplicaciones de Microsoft 365 mediante Microsoft Intune
- Implementación de aplicaciones Win32 con Microsoft Intune
- Implementación de aplicaciones de línea de negocio (LOB) mediante Microsoft Intune
- Configuración de la disponibilidad, la segmentación y el comportamiento de instalación de la aplicación
- Configuración de la actualización y asignación de aplicaciones
- Supervisión de la implementación de aplicaciones y solución de problemas de errores
- Administración de errores de implementación de aplicaciones mediante registros y herramientas de solución de problemas
- Comprobación de conocimientos
- Puntos clave

Implementación de la protección y la seguridad de aplicaciones mediante Microsoft Intune

En este módulo se explica cómo usar Microsoft Intune Mobile Application Management (MAM) y las directivas de protección de aplicaciones (APP) para proteger los datos corporativos en el nivel de aplicación. Aprenderá a planear estrategias de protección, a configurar directivas para dispositivos corporativos inscritos y BYOD no inscritos, a definir la protección de datos y a la configuración de inicio condicional, a aplicar el acceso con Microsoft Entra acceso condicional y a asignar, supervisar y solucionar problemas de directivas en la base de usuarios.

- Introducción
- Descripción de la administración de aplicaciones móviles (MAM) y las directivas de Protección de aplicaciones
- Planear estrategias de protección de aplicaciones para BYOD y dispositivos corporativos
- Configuración de directivas de Protección de aplicaciones para dispositivos BYOD no inscritos
- Configuración de directivas de Protección de aplicaciones para dispositivos corporativos inscritos
- Definición de la configuración de protección de datos, cifrado y restricción de aplicaciones
- Definición de requisitos de acceso y comportamientos de inicio condicional
- Configuración de directivas de acceso condicional para el control de acceso de aplicaciones
- Asignación y supervisión de directivas de App Protection
- Solución de problemas de directivas de protección de aplicaciones
- Comprobación de conocimientos
- Resumen

Administración del ciclo de vida de la aplicación y la experiencia del usuario mediante Microsoft Intune

Administre el ciclo de vida completo de la aplicación en Microsoft Intune, desde la adición

e implementación de aplicaciones hasta la configuración de la experiencia del usuario, la aplicación del cumplimiento, la supervisión del uso y la retirada de aplicaciones.

- Introducción
- Descripción de la administración del ciclo de vida de las aplicaciones en Microsoft Intune
- Actualización y retirada de aplicaciones en Microsoft Intune
- Asignación de aplicaciones mediante grupos, filtros y destino
- Administración de grupos de usuarios y dispositivos para la entrega de aplicaciones
- Configuración de la configuración predeterminada de la aplicación y la experiencia del usuario
- Aplicación de los requisitos de cumplimiento para las aplicaciones
- Supervisión del ciclo de vida de la aplicación y el análisis de uso
- Comprobación de conocimientos
- Resumen

Supervisión y optimización del rendimiento de las aplicaciones mediante Microsoft Intune

Supervise el estado y el rendimiento de las aplicaciones en los dispositivos administrados mediante Microsoft Intune. Realice un seguimiento del éxito de la implementación y las tasas de errores, use Análisis de puntos de conexión para medir la confiabilidad de las aplicaciones y aplique información basada en datos para optimizar la experiencia del usuario.

- Introducción
- Descripción del estado y el rendimiento de las aplicaciones en entornos modernos
- Supervisión de la implementación y el cumplimiento de aplicaciones mediante Intune
- Seguimiento del éxito de la instalación y los informes de errores
- Uso de Endpoint Analytics para medir el rendimiento de la aplicación y los tiempos de inicio

- Uso de Intune herramientas de informes para identificar y resolver problemas de rendimiento
- Optimización de la experiencia del usuario con información útil
- Comprobación de conocimientos
- Resumen

Administración de aplicaciones del Catálogo de aplicaciones empresariales

En este módulo se explica cómo usar Microsoft Intune Catálogo de aplicaciones empresariales para implementar aplicaciones Win32 preempaquetados en dispositivos Windows administrados, configurar las opciones predeterminadas de instalación y detección, supervisar las actualizaciones y usar la sustitución para ofrecer versiones más recientes y usar el informe Aplicaciones administradas para comprobar el estado de implementación en dispositivos individuales.

- Introducción
- Detección e implementación de aplicaciones desde el catálogo
- Configuración de la instalación y detección predeterminadas
- Supervisión de actualizaciones y sustitución
- Uso del informe aplicaciones administradas para obtener información
- Comprobación de conocimientos
- Resumen

Implementación de la seguridad del punto de conexión con Microsoft Defender y Microsoft Intune

En este módulo se muestra cómo implementar la seguridad de los puntos de conexión con Microsoft Defender a través de Microsoft Intune. Incorporará dispositivos Windows, macOS y móviles, configurará líneas base de seguridad y directivas de seguridad de puntos de conexión, implementará directivas de detección y respuesta de puntos de conexión (EDR) e investigará y evaluará los incidentes en el portal de Microsoft Defender.

- Introducción

- Comprender cómo Microsoft Defender protege los puntos de conexión
- Incorporación de dispositivos para Microsoft Defender mediante Intune
- Configuración de las líneas base y los valores de seguridad del punto de conexión de Microsoft Defender
- Configuración de directivas de detección y respuesta de puntos de conexión
- Investigar y responder a amenazas de punto de conexión mediante Microsoft Defender
- Supervisión y evaluación de los incidentes en el portal de Microsoft Defender
- Comprobación de conocimientos
- Resumen

Implementar directivas de seguridad y cifrado de dispositivos mediante Microsoft Intune

Implemente y administre el cifrado de dispositivos en los puntos de conexión de Windows mediante Microsoft Intune. Configure directivas de BitLocker, administre claves de recuperación, supervise el cumplimiento y audite el estado de cifrado con Microsoft Defender.

- Introducción
- Comprender la importancia del cifrado de dispositivos para el cumplimiento y la seguridad
- Configuración de directivas de BitLocker mediante Microsoft Intune
- Administración de claves de recuperación de BitLocker y opciones de autoservicio de usuario
- Supervisión del estado de cifrado y cumplimiento de BitLocker en Microsoft Intune
- Auditar el cifrado de dispositivos con Microsoft Defender
- Comprobación de conocimientos
- Resumen

Implementación de la protección contra amenazas avanzada mediante Microsoft Intune y Microsoft Defender

En este módulo se muestra cómo implementar la protección contra amenazas avanzada en puntos de conexión administrados. Combinará Microsoft Intune aplicación de directivas con Microsoft Defender para detectar shadow IT, reducir la superficie expuesta a ataques, aplicar Confianza cero acceso y automatizar la corrección.

- Introducción
- Descripción de las estrategias avanzadas de protección contra amenazas para entornos de punto de conexión
- Detección y supervisión de aplicaciones en la nube con Microsoft Defender
- Configurar reglas de reducción de superficie expuesta a ataques mediante Microsoft Intune
- Aplicación de principios de Confianza cero para Endpoint Protection
- Comprobación de conocimientos
- Resumen

Aplicar el cumplimiento y corregir problemas de seguridad mediante Microsoft Intune

En este módulo se muestra cómo operacionalizar las directivas de cumplimiento de Microsoft Intune como base de una arquitectura de Confianza cero. Creará directivas específicas de la plataforma, las limitará con grupos de Microsoft Entra y filtros de asignación, configurará acciones graduadas para no cumplimiento, automatizará la corrección y supervisará el estado de cumplimiento en todo el inquilino.

- Introducción
- Descripción de las directivas de cumplimiento y el cumplimiento basado en riesgos
- Creación de directivas de cumplimiento para plataformas admitidas
- Asignación y ámbito de directivas de cumplimiento mediante grupos y filtros

- Configuración de acciones para dispositivos no compatibles
- Corrección de problemas de dispositivo mediante directivas de cumplimiento y configuración
- Supervisión e informe de los resultados de cumplimiento
- Comprobación de conocimientos
- Resumen

Aplicar el cumplimiento y corregir problemas de seguridad mediante Microsoft Intune

En este módulo se muestra cómo operacionalizar las directivas de cumplimiento de Microsoft Intune como base de una arquitectura de Confianza cero. Creará directivas específicas de la plataforma, las limitará con grupos de Microsoft Entra y filtros de asignación, configurará acciones graduadas para no cumplimiento, automatizará la corrección y supervisará el estado de cumplimiento en todo el inquilino.

- Introducción
- Descripción de las directivas de cumplimiento y el cumplimiento basado en riesgos
- Creación de directivas de cumplimiento para plataformas admitidas
- Asignación y ámbito de directivas de cumplimiento mediante grupos y filtros
- Configuración de acciones para dispositivos no compatibles
- Corrección de problemas de dispositivo mediante directivas de cumplimiento y configuración
- Supervisión e informe de los resultados de cumplimiento
- Comprobación de conocimientos
- Resumen

Implementación de la PKI en la nube de Microsoft

En este módulo se muestra cómo implementar y operar la PKI de Microsoft Cloud en Microsoft Intune. Creará una jerarquía de CA de dos niveles, automatizará la emisión y renovación de certificados basados en SCEP y supervisará el estado de los certificados en toda la

organización, sin NDES local ni infraestructura de conectores.

- Introducción
- Configuración de PKI basada en la nube
- Automatización de la emisión y renovación de certificados
- Supervisión del estado y el cumplimiento de certificados
- Comprobación de conocimientos
- Resumen

Automatización de la administración de puntos de conexión mediante PowerShell y Microsoft Graph

Automatice y optimice la administración de puntos de conexión mediante Microsoft Intune junto con Microsoft Graph y PowerShell. Cree scripts comunes Intune tareas, administre dispositivos a escala, integre señales de seguridad y cree flujos de trabajo repetibles y fáciles de auditar.

- Introducción
- Descripción de las opciones de automatización para administrar Microsoft Intune
- Registro y protección del acceso de Microsoft Graph API para Intune
- Autenticación y uso del Graph API de Microsoft para Intune
- Uso de PowerShell para ejecutar scripts en Microsoft Intune
- Automatización de tareas de dispositivos y directivas mediante Microsoft Graph
- Comprobación de conocimientos
- Resumen

Optimización de la administración de dispositivos mediante herramientas de IA y Copilot

En este módulo se muestra cómo los administradores de puntos de conexión usan herramientas con tecnología de inteligencia artificial en Microsoft Intune y Microsoft Defender para exponer patrones en la telemetría de puntos de conexión, investigar incidentes de seguridad más rápido, solucionar problemas de dispositivos con lenguaje natural,

analizar tendencias de rendimiento y convertir la información de Defender en acciones prácticas Intune.

- Introducción
- Descripción del rol de la inteligencia artificial en la administración moderna de puntos de conexión
- Uso de Microsoft Security Copilot para investigar amenazas
- Uso de recomendaciones con tecnología de inteligencia artificial en Microsoft Intune
- Uso de Microsoft Defender información para admitir las decisiones de punto de conexión
- Comprobación de conocimientos
- Resumen

Supervisión y optimización del rendimiento del punto de conexión mediante Microsoft Intune

Supervise el rendimiento de los puntos de conexión e implemente la corrección proactiva mediante Microsoft Intune y análisis de puntos de conexión. Mida la confiabilidad, implemente scripts de corrección y optimice la experiencia del usuario para dispositivos Windows administrados en la nube.

- Introducción
- Descripción de la optimización del rendimiento en entornos administrados en la nube
- Uso de Endpoint Analytics para optimizar el rendimiento del dispositivo
- Configuración de scripts de corrección mediante Microsoft Intune
- Supervisión de la confiabilidad del punto de conexión y la experiencia del usuario con Endpoint Analytics
- Comprobación de conocimientos
- Resumen

Implementación de informes y visibilidad de datos mediante Microsoft Intune

En este módulo se explica cómo acceder e interpretar los informes integrados de Microsoft Intune, personalizar filtros de informe y vistas

guardadas, compilar Azure supervisar libros y paneles del Centro de administración y automatizar la exportación segura de datos de informes a las partes interesadas.

- Introducción
- Descripción de las opciones de informes integradas en Microsoft Intune
- Personalización de Intune informes y filtros para obtener información útil
- Uso de Microsoft Intune libros y paneles
- Exportación, programación y uso compartido de datos de informes de forma segura
- Comprobación de conocimientos
- Resumen

Aplicación de RBAC y delegación de administración en Microsoft Intune

En este módulo se explica cómo delegar Microsoft Intune administración de forma segura mediante Role-Based Access Control (RBAC), etiquetas de ámbito y asignaciones de roles basadas en grupos. Aprenderá a crear particiones de visibilidad, configurar la administración con ámbito para administradores regionales o departamentales y auditar las acciones administrativas para detectar el desfase de configuración.

- Introducción
- Descripción de las etiquetas de ámbito y RBAC en Microsoft Intune
- Asignación de roles y permisos para entornos multiadministrador
- Configuración de la administración con ámbito para la separación de unidades de negocio o regionales
- Auditar acciones de administrador y supervisar los cambios de configuración
- Comprobación de conocimientos
- Resumen

Mantenimiento del estado del inquilino y preparación de soporte técnico

En este módulo se explica cómo supervisar Microsoft Intune estado del servicio y las comunicaciones, configurar alertas y

notificaciones proactivas en las capas de cumplimiento y servicio, usar herramientas de diagnóstico y soporte técnico integradas y documentar los cambios de inquilino para establecer y mantener líneas base operativas.

- Introducción
- Supervisión del estado del inquilino y las comunicaciones del servicio Intune
- Configuración de alertas y notificaciones en Microsoft Intune
- Uso de herramientas de soporte técnico y solución de problemas relacionados con el servicio
- Documentar los cambios de inquilino y establecer líneas base operativas
- Comprobación de conocimientos
- Resumen

Exploración de las funcionalidades de Microsoft Intune Suite

En este módulo se presenta la Microsoft Intune Suite, una colección de funcionalidades de complemento premium que amplían la funcionalidad básica Intune para escenarios avanzados de administración, seguridad y soporte técnico de puntos de conexión. Aprenderá lo que hace cada componente, cómo se comparan las características de Suite con los Intune principales y cómo planear las licencias y la implementación.

- Introducción
- Comprender el propósito y el valor de la Microsoft Intune Suite
- Identificar los componentes clave del Microsoft Intune Suite
- Comparación de características de Microsoft Intune Suite con funcionalidades básicas de Intune
- Planear estrategias de licencia e implementación para el Microsoft Intune Suite
- Comprobación de conocimientos
- Resumen

Implementar escenarios de Ayuda remota mediante Microsoft Intune

Ayuda remota es una funcionalidad Microsoft Intune Suite que permite a los equipos ayudar de forma segura a los usuarios en tiempo real, con sesiones vinculadas a la identidad, los permisos y el cumplimiento de la organización. En este módulo se muestra cómo configurar, implementar y operar Ayuda remota, incluidos los roles auxiliares y de sharer, la supervisión de sesiones y las consideraciones de privacidad.

- Introducción
- Descripción de Ayuda remota y su rol en la compatibilidad con el usuario final
- Configuración e implementación de Ayuda remota con Microsoft Intune
- Compatibilidad y supervisión de sesiones de Ayuda remota
- Evaluación de consideraciones de privacidad, permisos y cumplimiento
- Comprobación de conocimientos
- Resumen

Análisis de señales avanzadas de dispositivos con Microsoft Intune Suite

Microsoft Intune Suite Análisis avanzado enriquece los informes de Intune estándar con el estado del dispositivo en tiempo real, la detección de anomalías y la telemetría de seguridad, y se integra con Microsoft Defender para puentear las operaciones de TI y seguridad. En este módulo se muestra cómo usar esas señales avanzadas para pasar de los informes de cumplimiento estáticos a la administración proactiva y basada en riesgos de puntos de conexión.

- Introducción
- Exploración de informes avanzados con análisis de Intune Suite
- Identificación y respuesta a la información de detección de anomalías
- Integración de Intune con Microsoft Defender para señales de amenazas proactivas

- Uso de información avanzada para admitir decisiones de directivas basadas en riesgos
- Comprobación de conocimientos
- Resumen

Evaluación de Administración con privilegios para puntos de conexión con Microsoft Intune

Administración con privilegios para puntos de conexión (EPM) es una funcionalidad de Microsoft Intune Suite que permite a las organizaciones quitar derechos de administrador local permanente y, en su lugar, conceder elevación Just-In-Time a aplicaciones, instaladores o scripts aprobados. En este módulo se muestra cómo diseñar, configurar, supervisar y refinar las implementaciones de EPM para admitir Confianza cero sin interrumpir la productividad.

- Introducción
- Descripción de la elevación Just-In-Time en Administración con privilegios para puntos de conexión
- Configuración de directivas y reglas de elevación
- Supervisión de acciones con privilegios elevados y revisión de informes
- Solución de problemas y refinamiento de una implementación de EPM
- Comprobación de conocimientos
- Resumen

Exploración de Windows 365 para la implementación de equipos en la nube

Windows 365 transmite un escritorio de Windows seguro y personalizado desde la nube de Microsoft, lo que permite a los usuarios acceder a un equipo en la nube desde prácticamente cualquier dispositivo. Este módulo presenta Windows 365: su rol en las estrategias modernas de puntos de conexión, cómo se compara con la VDI tradicional, las licencias y los requisitos previos, los casos de uso y las opciones de experiencia de punto de conexión disponibles para administradores y usuarios.

- Introducción
- Comprender el rol de Windows 365
- Comparación de Windows 365 con VDI tradicional
- Identificar Windows 365 licencias, planes de servicio y requisitos previos
- Identificar casos de uso Windows 365
- Explorar la experiencia del punto de conexión Windows 365
- Comprobación de conocimientos
- Resumen

Configuración y administración de Windows 365 con Microsoft Intune

Windows 365 ofrece equipos en la nube desde la nube de Microsoft y Microsoft Intune es la capa de administración que controla cómo se aprovisionan, configuran, protegen y supervisan esos equipos en la nube. En este módulo se muestra cómo configurar directivas de aprovisionamiento, asignar y administrar equipos en la nube, aplicar perfiles de configuración y supervisar el uso, el rendimiento y el estado desde el centro de administración de Intune.

- Introducción
- Configuración de directivas de aprovisionamiento de Windows 365
- Asignación y administración de equipos en la nube
- Aplicación de directivas y perfiles de configuración a equipos en la nube
- Supervisión del uso, el rendimiento y el estado del equipo en la nube
- Comprobación de conocimientos
- Resumen

Exploración de Azure Virtual Desktop

Azure Virtual Desktop ofrece aplicaciones y escritorios de Windows virtualizados desde Azure. En este módulo se explora Azure arquitectura de Virtual Desktop, se compara con Windows 365 y se explica cómo los grupos de hosts, los hosts de sesión, los grupos de aplicaciones y los planes de escalado

automático ofrecen capacidad de escritorio flexible a los usuarios.

- Introducción
- Descripción de Azure arquitectura de Virtual Desktop
- Comparar Azure Virtual Desktop con Windows 365
- Examen de grupos de hosts, hosts de sesión y escalado
- Comprobación de conocimientos
- Resumen

Integración de Azure Virtual Desktop con Microsoft Intune

La integración de Azure Virtual Desktop con Microsoft Intune incluye hosts de sesión en el mismo plano de administración de puntos de conexión modernos que se usa para dispositivos físicos y pc en la nube. En este módulo se muestra cómo inscribir hosts de sesión, aplicar directivas de cumplimiento y configuración, supervisar y solucionar problemas del entorno y abordar la gobernanza, las licencias y las consideraciones híbridas.

- Introducción
- Inscribir Azure hosts de sesión de Virtual Desktop en Microsoft Intune
- Aplicación de directivas de cumplimiento y configuración a hosts de sesión
- Supervisión y solución de problemas de Azure Virtual Desktop con Microsoft Intune
- Abordar escenarios de gobernanza, licencias e híbridos
- Comprobación de conocimientos
- Resumen