The DevOps Company

Microsoft Partner

MS-102T00
Microsoft 365 Administrator Essentials

Sobre este curso.

En este curso se tratan los siguientes elementos clave de la administración de Microsoft 365: Administración de inquilinos, sincronización de identidades y seguridad y cumplimiento. En la administración de inquilinos de Microsoft 365, aprenderá cómo configurar su inquilino de Microsoft 365, incluido su perfil de organización, opciones de suscripción de inquilino, servicios de componentes, cuentas y licencias de usuario, grupos de seguridad y roles administrativos. A continuación, realizará la transición a la configuración de Microsoft 365, con un enfoque principal en la configuración de la conectividad de cliente de Office. Por último, verá cómo administrar las instalaciones de cliente controladas por el usuario de implementaciones de Aplicaciones de Microsoft 365 para empresas.

A continuación, se pasa a un examen detallado de la sincronización de identidades de Microsoft 365, con un enfoque en Azure Active Directory Connect y Connect Cloud Sync. Aprenderá a planificar e implementar cada una de estas opciones de sincronización de directorios, cómo administrar identidades sincronizadas y cómo implementar la administración de contraseñas en Microsoft 365 mediante la autenticación multifactor y la administración de contraseñas de autoservicio.

En la parte de administración de seguridad de Microsoft 365, comenzamos por examinar los tipos habituales de vectores de amenazas y filtraciones de datos a los que se enfrentan hoy en día las organizaciones. A continuación, verá cómo las soluciones de seguridad de Microsoft 365 abordan cada una de estas amenazas. 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 el estado de seguridad de una organización. 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.

Una vez hayamos visto el conjunto de seguridad de Microsoft 365, examinaremos 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.

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, como mínimo, 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:

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

Examen.

MS-102: Microsoft 365 Administrator.

Temario.

Módulo 1: Configura tu experiencia con Microsoft 365.

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

- Configura tu experiencia con Microsoft 365.
- Administre sus suscripciones de inquilinos en Microsoft 365.
- Integrar Microsoft 365 con aplicaciones de compromiso con el cliente.
- Complete la configuración de su inquilino en Microsoft 365.

Al final de este módulo, deberías ser capaz de:

- Configure el perfil de organización de su empresa, que es esencial para configurar el inquilino de su empresa.
- Mantenga los requisitos mínimos de suscripción para su empresa.
- Administre sus servicios y complementos asignando más licencias, comprando más almacenamiento, etc.
- Cree una lista de verificación que le permita confirmar que su inquilino de Microsoft 365 satisface las necesidades de su negocio.

Módulo 2: Administrar usuarios, licencias y contactos de correo 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 contactos de correo.

- 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 el mantenimiento masivo de usuarios en Azure Active Directory.
- Crear y gestionar usuarios invitados.
- Crear y gestionar contactos de correo.

Al final de este módulo, deberías ser capaz de:

- Identifique qué modelo de identidad de usuario es el más adecuado para su organización.
- Crea cuentas de usuario tanto desde el centro de administración de Microsoft 365 como desde Windows PowerShell.
- Administrar cuentas de usuario y licencias en Microsoft 365.
- Recuperar cuentas de usuario eliminadas en Microsoft 365.
- Realice el mantenimiento masivo de los usuarios en Azure Active Directory.
- Crea y gestiona contactos de correo desde el nuevo centro de administración de Exchange y Exchange Online PowerShell.

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 explica cómo crear grupos para apoyar la colaboración en SharePoint Online.

- Examinar grupos en Microsoft 365.
- Crear y gestionar grupos en Microsoft 365.
- Crear grupos dinámicos usando el generador de reglas de Azure.
- Crear una política de nomenclatura de grupo de Microsoft 365.
- Crear grupos en Exchange Online y SharePoint Online.

Al final de este módulo, deberías ser capaz de:

- Describe los diversos tipos de grupos disponibles en Microsoft 365.
- Crea y administra grupos utilizando el centro de administración de Microsoft 365 y Windows PowerShell.
- Crea y gestiona grupos en Exchange Online y SharePoint Online.

Módulo 4: Añadir un dominio personalizado en Microsoft 365.

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

- Planifique un dominio personalizado para su implementación de Microsoft 365.
- Planifica las zonas DNS para un dominio personalizado.
- Planificar los requisitos de registro DNS para un dominio personalizado.
- Crear un dominio personalizado en Microsoft 365.

Al final de este módulo, deberías ser capaz de:

- Identifique los factores que deben tenerse en cuenta al añadir un dominio personalizado a Microsoft 365.
- Planifique las zonas DNS utilizadas en un dominio personalizado.
- Planifique los requisitos de registro DNS para un dominio personalizado.
- Añade un dominio personalizado a tu implementación de Microsoft 365.

Módulo 5: Configurar la conectividad del cliente con Microsoft 365.

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

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

Al final de este módulo, deberías ser capaz de:

- Describe cómo Outlook utiliza Autodiscover para conectar un cliente de Outlook a Exchange Online.
- Identifique los registros DNS necesarios para que Outlook y otros clientes relacionados con Office localicen automáticamente los servicios en Microsoft 365 utilizando el proceso de descubrimiento automático.
- Describa los protocolos de conectividad que permiten que Outlook se conecte a Microsoft 365.
- Identifique las herramientas que pueden ayudarle a solucionar problemas de conectividad en las implementaciones de Microsoft 365.

Módulo 6: Configurar funciones administrativas en Microsoft 365.

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

- Explora el modelo de permisos de Microsoft 365.
- Explora los roles de administrador de Microsoft 365.
- Asignar funciones de administrador a los usuarios en Microsoft 365.
- Delegar funciones administrativas a los socios.
- Administrar permisos utilizando unidades administrativas en Azure Active Directory.
- Elevar privilegios utilizando la gestión de identidades con privilegios de Azure AD.

Al final de este módulo, deberías ser capaz de:

- Describir el modelo de permisos Azure RBAC utilizado en Microsoft 365.
- Describe las funciones de administrador más comunes de Microsoft 365.
- Identificar las tareas clave asignadas a los roles comunes de administrador de Microsoft 365.
- Delegar funciones de administrador a los socios.
- Administre los permisos utilizando unidades administrativas en Azure Active Directory.
- Elevar los privilegios para acceder a los centros de administración mediante el uso de Azure AD Privileged Identity Management.

Módulo 7: Administrar la salud y los servicios de los inquilinos en Microsoft 365.

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

- Supervise el estado de sus servicios de Microsoft 365.
- Supervisar el estado de los inquilinos utilizando la puntuación de adopción de Microsoft 365.
- Supervisar la salud de los inquilinos utilizando el análisis de uso de Microsoft 365.
- Desarrollar un plan de respuesta a incidentes.
- Solicitar asistencia a Microsoft.

Al final de este módulo, deberías ser capaz de:

- Supervise el estado del servicio Microsoft 365 de su organización en el centro de administración de Microsoft 365.
- Desarrolle un plan de respuesta a incidentes para hacer frente a los incidentes que puedan ocurrir con su servicio de Microsoft 365.
- Solicite asistencia a Microsoft para abordar los problemas técnicos, de preventa, de facturación y de soporte de suscripción.

Módulo 8: Implementar aplicaciones de Microsoft 365 para empresas.

Este módulo examina cómo implementar el paquete de productividad de Microsoft 365 Apps for Enterprise tanto en implementaciones impulsadas por el usuario como centralizadas.

- Explora las aplicaciones de Microsoft 365 para la funcionalidad empresarial.
- Explore la compatibilidad de su aplicación utilizando el kit de herramientas de preparación.
- Completar una instalación de autoservicio de las aplicaciones de Microsoft 365 para empresas.
- Implementar aplicaciones de Microsoft 365 para empresas con Microsoft Configuration Manager.
- Implementar aplicaciones de Microsoft 365 para empresas desde la nube.
- Despliegue las aplicaciones de Microsoft 365 para empresas desde una fuente local.
- Gestionar las actualizaciones de las aplicaciones de Microsoft 365 para empresas.
- Explore los canales de actualización de las aplicaciones de Microsoft 365 para empresas.
- Administre sus aplicaciones en la nube utilizando el centro de administración de aplicaciones de Microsoft 365.

Al final de este módulo, deberías ser capaz de:

- Describa las aplicaciones de Microsoft 365 para la funcionalidad empresarial.
- Configurar el kit de herramientas de preparación.
- Planifique una estrategia de implementación para las aplicaciones de Microsoft 365 para empresas.
- Completa una instalación basada en el usuario de Microsoft 365 Apps para empresas.
- Implemente aplicaciones de Microsoft 365 para empresas con Microsoft Endpoint Configuration Manager.
- Identifique los mecanismos para gestionar las implementaciones centralizadas de las aplicaciones de Microsoft 365 para empresas.
- Implemente aplicaciones de Microsoft 365 para empresas con el kit de herramientas de implementación de Office.
- Describir cómo administrar las aplicaciones de Microsoft 365 para las actualizaciones empresariales.
- Determine qué canal de actualización y método de aplicación se aplica a su organización.

Módulo 9: Analice los datos de su lugar de trabajo de Microsoft 365 utilizando Microsoft Viva Insights.

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

- Examine las características analíticas de Microsoft Viva Insights.
- Crea análisis personalizados con Microsoft Viva Insights.
- Configurar Microsoft Viva Insights.
- Examine las fuentes de datos de Microsoft 365 utilizadas en Microsoft Viva Insights.
- Preparar datos de la organización en Microsoft Viva Insights.

Después de completar este módulo, deberías ser capaz de:

- Identifique cómo Microsoft Viva Insights puede ayudar a mejorar los comportamientos de colaboración en su organización.
- Descubre las fuentes de datos utilizadas en Microsoft Viva Insights.
- Explica la información de alto nivel disponible a través de Microsoft Viva Insights.

- Crea análisis personalizados con Microsoft Viva Insights.
- Resuma las tareas y consideraciones para configurar Microsoft Viva Insights y gestionar la privacidad.

Módulo 10: Explora la sincronización de identidades.

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

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

Al final de este módulo, deberías ser capaz de:

- Describir las opciones de autenticación y aprovisionamiento de Microsoft 365.
- Explicar los dos modelos de identidad en Microsoft 365: identidad solo en la nube e identidad híbrida.
- Explicar los tres métodos de autenticación en el modelo de identidad híbrida: sincronización de hash de contraseña, autenticación de paso y autenticación federada.
- Describir cómo Microsoft 365 utiliza comúnmente la sincronización de directorios.

Módulo 11: Prepararse para la sincronización de identidad con Microsoft 365.

Este módulo examina todos los aspectos de planificación que deben tenerse en cuenta al implementar la sincronización de directorios entre Active Directory local y Microsoft 365.

- Planifique su implementación de Azure Active Directory.
- Prepárate para la sincronización de directorios.
- Elige tu herramienta de sincronización de directorios.
- Planifique la sincronización de directorios utilizando Azure AD Connect.
- Planifique la sincronización de directorios con Azure AD Connect Cloud Sync.

Al final de este módulo, deberías ser capaz de:

- Identifique las tareas necesarias para configurar su entorno de Azure Active Directory.
- Planifique la sincronización de directorios para sincronizar sus objetos locales de Active Directory con Azure AD.
- Identifique las características de Azure AD Connect sync y Azure AD Connect Cloud Sync.
- Elija qué sincronización de directorios se adapta mejor a su entorno y a las necesidades de su negocio.

Módulo 12: Implementar herramientas de sincronización de directorios.

Este módulo examina los requisitos de instalación de Azure AD Connect y Azure AD Connect Cloud Sync, las opciones para instalar y configurar las herramientas y cómo supervisar los servicios de sincronización utilizando Azure AD Connect Health.

- Configurar los requisitos previos de Azure AD Connect.
- Configurar Azure AD Connect.
- Supervisar los servicios de sincronización utilizando Azure AD Connect Health.
- Configurar los requisitos previos de Azure AD Connect Cloud Sync.
- Configurar Azure AD Connect Cloud Sync.

Al final de este módulo, debería ser capaz de:

- Configurar los requisitos previos de Azure AD Connect y Azure AD Connect Cloud Sync.
- Configurar Azure AD Connect y Azure AD Connect Cloud Sync.
- Supervisar los servicios de sincronización utilizando Azure AD Connect Health.

Módulo 13: Gestionar identidades sincronizadas.

Este módulo examina cómo administrar las identidades de los usuarios cuando se configura Azure AD Connect, cómo administrar usuarios y grupos en Microsoft 365 con Azure AD Connect y cómo mantener la sincronización de directorios.

- Administrar usuarios con sincronización de directorios.
- Administrar grupos con sincronización de directorios.
- Utilice los grupos de seguridad de sincronización de Azure AD Connect para ayudar a mantener la sincronización de directorios.
- Configurar filtros de objetos para la sincronización de directorios.
- Solucionar problemas de sincronización de directorios.

Al final de este módulo, deberías ser capaz de:

- Garantizar que los usuarios se sincronicen de manera eficiente.
- Administrar grupos con sincronización de directorios.
- Utilice los grupos de seguridad de sincronización de Azure AD Connect para ayudar a mantener la sincronización de directorios.
- Configurar filtros de objetos para la sincronización de directorios.
- Solucionar problemas de sincronización de directorios utilizando varias tareas y herramientas de solución de problemas.

Módulo 14: Administrar el acceso seguro de los usuarios en Microsoft 365.

Este módulo examina varias tareas relacionadas con la contraseña para usuarios y administradores, incluyendo la creación y configuración de políticas de contraseñas,la configuración de la gestión de contraseñas de autoservicio, configuración de la autenticación multifactor, la implementación de paquetes de derechos e implementar políticas de acceso condicional.

- Administrar contraseñas de usuario.
- Habilitar la autenticación de paso.
- Habilitar la autenticación multifactor.
- Habilitar el inicio de sesión sin contraseña con Microsoft Authenticator.
- Explora la gestión de contraseñas de autoservicio.
- Explora Windows Hello para empresas.
- Implementar Azure AD Smart Lockout.
- Implementar políticas de acceso condicional.
- Explora los valores predeterminados de seguridad en Azure AD.
- Investigar problemas de autenticación utilizando registros de inicio de sesión.

Al final de este módulo, deberías ser capaz de:

- Administrar contraseñas de usuario.
- Describir la autenticación de paso.
- Habilitar la autenticación multifactor.
- Describir la gestión de contraseñas de autoservicio.
- Implementar Azure AD Smart Lockout.
- Implementar paquetes de derechos en Azure AD Identity Governance.
- Implementar políticas de acceso condicional.
- Crear y realizar una revisión de acceso.

Módulo 15: Examinar los vectores de amenazas y las filtraciones de datos.

Este módulo examina los tipos de vectores de amenaza y sus resultados potenciales 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.

- Explora el trabajo de hoy y el panorama de las amenazas.
- Examine 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 los ataques de elevación de privilegios.
- Examine cómo la exfiltración de datos saca 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.
- Examinar otros tipos de ataques.

Al final de este módulo, deberías ser capaz de:

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

Módulo 16: 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 Zero Trust en su organización.

- Examinar la estrategia de Microsoft para la creación de redes Zero Trust.
- Adoptar un enfoque de confianza cero.

Al final de este módulo, deberías ser capaz de:

- Describir el enfoque de confianza cero 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 la red Zero Trust.

Módulo 17: 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 cuándo un usuario o un ordenador se ha visto comprometido y supervisar su organización en busca de actividades sospechosas.

- Mejore la seguridad de su correo electrónico con Exchange Online Protection y 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 ataques cibernéticos utilizando Microsoft 365 Threat Intelligence.
- Proporcionar información sobre la actividad sospechosa utilizando Microsoft Cloud App Security.
- Revisa los informes de seguridad en Microsoft 365 Defender.

Al final de este módulo, deberías ser capaz de:

- 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 beneficiosa para los oficiales de seguridad y administradores de su organización
- Describa cómo Microsoft Cloud App Security mejora la visibilidad y el control sobre su inquilino de Microsoft 365 a través de tres áreas principales

Módulo 18: Examinar Microsoft Secure Score.

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

- Explora Microsoft Secure Score.
- Evalúe su postura de seguridad con Microsoft Secure Score.
- Mejora tu puntuación segura.
- Haz un seguimiento de tu historial de Microsoft Secure Score y cumple tus objetivos.

Al final de este módulo, deberías ser capaz de:

- Describir los beneficios de Secure Score y qué tipo de servicios se pueden analizar.
- Describir cómo recopilar datos con 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 aumenten su seguridad al mitigar los riesgos.
- Explicar dónde buscar para determinar las amenazas que cada acción mitiga y el impacto que tiene en los usuarios.

Módulo 19: Examinar la gestión de identidades privilegiadas.

Este módulo examina cómo la gestión de identidades privilegiadas garantiza que los usuarios de su organización tengan los privilegios adecuados para realizar las tareas que necesitan realizar.

- Explore la gestión de identidades privilegiadas en Azure AD..
- Configurar la gestión de identidades privilegiadas.
- Auditoría de gestión de identidades privilegiadas.
- Explora el Administrador de identidades de Microsoft.
- Controlar tareas de administración privilegiadas utilizando la gestión de acceso privilegiado.

Al final de este módulo, deberías ser capaz de:

- 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 los 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 la gestión de acceso privilegiado proporciona un control de acceso granular sobre las tareas de administración privilegiadas en Microsoft 365.

Módulo 20: Examinar la protección de identidad de Azure.

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

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

Al final de este módulo, deberías ser capaz de:

- Describir Azure Identity Protection (AIP) y qué tipo de identidades se pueden proteger.
- Habilitar las tres 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 21: Examinar Exchange Online Protection.

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 tubería antimalware.
- Detectar mensajes con spam o malware usando la purga automática de cero horas.
- Explore la protección contra la suplantación de identidad proporcionada por Exchange Online Protection.
- Explora otras medidas contra la suplantación de identidad.
- Examine el filtrado de spam saliente.

Al final de este módulo, deberías ser capaz de:

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

Módulo 22: Examinar Microsoft Defender para Office 365.

Este módulo examina cómo Microsoft Defender para Office 365 amplía la protección EOP filtrando ataques dirigidos, como ataques de día cero en archivos adjuntos de correo electrónico y documentos de Office, y protección contra el 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.
- Gestionar la inteligencia falsificada.
- Configurar las políticas de filtrado de spam saliente.
- Desbloquear a los usuarios del envío de correo electrónico.

Al final de este módulo, debería ser capaz de:

- 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.
- Crear políticas de filtrado de spam saliente.
- Desbloquee a los usuarios que violaron las políticas de filtrado de spam para que puedan reanudar el envío de correos electrónicos.

Módulo 23: Gestionar 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 deshabilitar la entrada en vigor de una política en ciertos escenarios.

- Proteja a los usuarios de archivos adjuntos maliciosos mediante el uso de archivos adjuntos seguros.
- Crear políticas de archivos adjuntos seguros utilizando 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 los archivos adjuntos seguros.

Al final de este módulo, deberías ser capaz de:

- Crear y modificar una política de archivos adjuntos seguros utilizando Microsoft 365 Defender.
- Crear una política de archivos adjuntos seguros utilizando PowerShell.
- Configurar una política de archivos adjuntos seguros.
- Describir cómo una regla de transporte puede desactivar 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 24: 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 la entrada en vigor de una política en ciertos escenarios.

- Proteja a los usuarios de URL maliciosas mediante el uso de enlaces seguros.
- Crear políticas de enlaces seguros usando Microsoft 365 Defender.
- Crear políticas de enlaces seguros usando PowerShell.
- Modificar una política de enlaces seguros existente.
- Crear una regla de transporte para eludir una política de enlaces seguros.
- Examine la experiencia del usuario final con Safe Links.

Al final de este módulo, deberías ser capaz de:

- Crear y modificar una política de enlaces seguros usando Microsoft 365 Defender.
- Crear una política de enlaces seguros usando PowerShell.
- Configurar una política de enlaces seguros.
- Describir 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 25: 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 el gráfico de seguridad inteligente de Microsoft.
- Explorar las políticas de alerta en Microsoft 365.
- Ejecutar investigaciones y respuestas automatizadas.
- Explora la caza de amenazas con Microsoft Threat Protection.
- Explora la búsqueda avanzada de amenazas en Microsoft 365 Defender y Explora el análisis de amenazas en Microsoft 365.
- Identificar problemas de amenaza utilizando los informes de Microsoft Defender.

Al final de este módulo, deberías ser capaz de:

- Describe cómo la inteligencia de amenazas en Microsoft 365 funciona con 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 caza de amenazas permite a los operadores de seguridad identificar las amenazas de ciberseguridad.
- Describa cómo la búsqueda avanzada en Microsoft 365 Defender inspecciona de forma proactiva los eventos de su red para localizar indicadores de amenaza y entidades.

Módulo 26: Implemente la protección de la aplicación mediante el uso de Microsoft Defender para aplicaciones en la nube.

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

- Explora las aplicaciones en la nube de Microsoft Defender.
- Implementar Microsoft Defender para aplicaciones en la nube.
- Configurar políticas de archivos en Microsoft Defender para aplicaciones en la nube.
- Gestionar 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, deberías ser capaz de:

- 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 todas 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.
- Gestionar y responder a las alertas generadas por esas políticas.
- Configurar y solucionar problemas de Cloud Discovery.

Módulo 27: Implementar la protección de puntos finales mediante el uso de 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.
- Gestione las vulnerabilidades de los puntos finales con la gestión de vulnerabilidades de Microsoft Defender.
- Gestionar el descubrimiento de dispositivos y la evaluación de vulnerabilidades.
- Reduzca su exposición a amenazas y vulnerabilidades.

Después de completar este módulo, deberías ser capaz de:

- Describa cómo Microsoft Defender for Endpoint ayuda a las redes empresariales a prevenir, detectar, investigar y responder a amenazas avanzadas.
- Dispositivos compatibles integrados en Microsoft Defender para Endpoint.
- Implementar el módulo de gestión de amenazas y vulnerabilidades para identificar, evaluar y remediar de manera efectiva las debilidades de los puntos finales.
- Configure el descubrimiento de dispositivos para ayudar a encontrar dispositivos no administrados conectados a su red corporativa.
- Reduzca la exposición a amenazas y vulnerabilidades de su organización solucionando los problemas en función de las recomendaciones de seguridad prioritarias.

Módulo 28: Implemente 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, incluido el Explorador de amenazas, los rastreadores de amenazas y el entrenamiento de simulación de ataques.

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

Después de completar este módulo, deberías ser capaz de:

- 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 del rastreador de amenazas 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.