MS-500T00-A
Microsoft 365 Security Administration

Sobre este curso

En este curso aprenderá cómo asegurar el acceso de los usuarios a los recursos de su organización. El curso cubre la protección de contraseña de usuario, la autenticación multifactor, cómo habilitar la Protección de identidad de Azure, cómo configurar y usar Azure AD Connect, y le presenta el acceso condicional en Microsoft 365. Aprenderá sobre las tecnologías de protección contra amenazas que ayudan a proteger su entorno Microsoft 365. Específicamente, aprenderá acerca de los vectores de amenazas y las soluciones de seguridad de Microsoft para mitigar las amenazas. Aprenderá sobre Secure Score, la protección de Exchange Online, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection y la gestión de amenazas. En este curso aprenderá sobre las tecnologías de protección de la información que ayudan a proteger su entorno Microsoft 365. Este curso analiza el contenido administrado por los derechos de información, el cifrado de mensajes, así como las etiquetas, políticas y reglas que admiten la prevención de pérdida de datos y la protección de la información. Finalmente, en este curso aprenderá sobre el archivado y la retención en Microsoft 365, así como sobre el gobierno de datos y cómo realizar búsquedas e investigaciones de contenido. Este curso cubre las políticas y etiquetas de retención de datos, la administración de registros en el lugar para SharePoint, la retención de correo electrónico y cómo realizar búsquedas de contenido que admitan investigaciones de descubrimiento electrónico.

Duración

32hs.

Audience Profile

El Microsoft 365 Security Administrator colabora con el Microsoft 365 Enterprise Administrator, las partes interesadas de negocios y otros administradores de carga de trabajo para planificar e implementar estrategias de seguridad y garantiza que las soluciones cumplan con las directivas y regulaciones de la organización. Este rol asegura proactivamente los entornos empresariales de Microsoft 365. Las responsabilidades incluyen responder a amenazas, implementar, administrar y monitorear soluciones de seguridad y cumplimiento para el entorno de Microsoft 365. Responden a incidentes, investigaciones y aplicación de la gobernanza de datos. El administrador de seguridad de Microsoft 365 está familiarizado con las cargas de trabajo de Microsoft 365 y los entornos híbridos. Este rol tiene fuertes habilidades y experiencia con protección de identidad, protección de información, protección contra amenazas, gestión de seguridad y gobierno de datos.

MS-500T00-A
Microsoft 365 Security Administration

Requisitos Previos

Los estudiantes deben comenzar este curso con las siguientes habilidades:

- Comprensión conceptual básica de Microsoft Azure.
- Experiencia con dispositivos Windows 10.
- Experiencia con Office 365.
- Conocimientos básicos de autorización y autenticación.
- Conocimientos básicos de redes informáticas.
- Conocimiento práctico de la gestión de dispositivos móviles.

Esquema del curso

Módulo 1: Protección de usuarios y grupos

Este módulo explica cómo administrar cuentas de usuario y grupos en Microsoft 365. Le presenta Privileged Identity Management en Azure AD, así como también Identity Protection. El módulo establece las bases para el resto del curso.

Lecciones

- Conceptos de gestión de identidad y acceso
- Seguridad Zero Trust
- Cuentas de usuario en Microsoft 365
- Roles de administrador y grupos de seguridad en Microsoft 365
- Gestión de contraseñas en Microsoft 365
- Protección de identidad de Azure AD

Laboratorio: Inicializar su inquilino de prueba

- Configure su inquilino de Microsoft 365

Laboratorio: Configurar la gestión de identidad privilegiada

- Descubrir y administrar recursos de Azure

MS-500T00-A
Microsoft 365 Security Administration

- Asignar roles de Directory
- Activar y desactivar roles PIM
- Roles de directorio (general)
- Flujos de trabajo de recursos PIM
- Ver el historial de auditoría de los roles de Azure AD en PIM

Después de completar este módulo, los estudiantes podrán:

- Crear y administrar cuentas de usuario.
- Describir y usar roles de administrador de Microsoft 365
- Planificar las políticas de contraseña y autenticación
- Describir los conceptos de seguridad Zero Trust.
- Implemente la autenticación multifactor en Office 365
- Habilitar Azure Identity Protection

Módulo 2: Sincronización de identidad

Este módulo explica conceptos relacionados con la sincronización de identidades para Microsoft 365. Específicamente, se centra en Azure AD Connect y en la administración de la sincronización de directorios para garantizar que las personas adecuadas se conecten a su sistema Microsoft 365.

Lecciones

- Introducción a la sincronización de identidad
- Planificación de Azure AD Connect
- Implementar Azure AD Connect
- Gestionar identidades sincronizadas
- Introducción a las identidades federadas

Laboratorio: Implementación de sincronización de identidad

- Configurar su organización para la sincronización de identidad

Después de completar este módulo, los estudiantes podrán:

- Describir las opciones de autenticación para Microsoft 365.

MS-500T00-A
Microsoft 365 Security Administration

- Explicar la sincronización de directorios
- Planificar sincronización de directorios
- Describir y usar Azure AD Connect.
- Configurar los requisitos previos de Azure AD Connect
- Gestionar usuarios y grupos con sincronización de directorios.
- Describir la federación de Active Directory.

Módulo 3: Gestión de Acceso

Este módulo explica el acceso condicional para Microsoft 365 y cómo se puede usar para controlar el acceso a los recursos en su organización. El módulo también explica el control de acceso basado en roles (RBAC) y las soluciones para acceso externo.

Lecciones

- Acceso condicional
- Administrar el acceso al dispositivo
- Control de acceso basado en roles (RBAC)
- Soluciones para acceso externo

Laboratorio: Usar acceso condicional para habilitar MFA

- Piloto de autenticación MFA (requiere MFA para aplicaciones específicas)
- Acceso condicional de MFA (completar un despliegue de MFA)

Después de completar este módulo, los estudiantes podrán:

- Describir el concepto de acceso condicional.
- Describir y usar políticas de acceso condicional.
- Planificar el cumplimiento de dispositivos.
- Configurar usuarios y grupos condicionales.
- Configurar el control de acceso basado en roles

MS-500T00-A
Microsoft 365 Security Administration

Módulo 4: Seguridad en Microsoft 365

Este módulo explica las diversas amenazas de ciberataque que existen. Luego le presenta las soluciones de Microsoft utilizadas para mitigar esas amenazas. El módulo finaliza con una explicación de Microsoft Secure Score y cómo se puede usar para evaluar e informar la postura de seguridad de su organización.

Lecciones

- Vectores de amenazas y violaciones de datos
- Estrategia y principios de seguridad.
- Security Solutions en Microsoft 365
- Microsoft Secure Score

Laboratorio: Use Microsoft Secure Score

- Mejore su puntuación de seguridad en el Centro de seguridad de Microsoft 365

Después de completar este módulo, los estudiantes podrán:

- Describir varias técnicas que los atacantes utilizan para comprometer las cuentas de los usuarios a través del correo electrónico
- Describir las técnicas que usan los atacantes para obtener control sobre los recursos.
- Enumerar los tipos de amenazas que se pueden evitar mediante el uso de Exchange Online Protection y Office 365 ATP.
- Describir los beneficios de Secure Score y qué tipo de servicios se pueden analizar.
- Describa cómo usar Secure Score para identificar brechas en su actual postura de seguridad de Microsoft 365.

Módulo 5: Advanced Threat Protection

Este módulo explica las diversas tecnologías y servicios de protección contra amenazas disponibles para Microsoft 365. El módulo cubre la protección de mensajes a través de Exchange Online Protection, Azure Advanced Threat Protection y Windows Defender Advanced Threat Protection.

MS-500T00-A
Microsoft 365 Security Administration

Lecciones

- Exchange Online Protection
- Office 365 Advanced Threat Protection
- Administrar archivos adjuntos seguros
- Gestión de enlaces seguros
- Azure Advanced Threat Protection
- Microsoft Defender Advanced Threat Protection

Laboratorio: Administrar los servicios de seguridad de Microsoft 365

- implementar las directrices ATP

Después de completar este módulo, los estudiantes podrán:

- Describir la canalización antimalware a medida que Exchange Online Protection analiza el correo electrónico.
- Describir cómo Safe Attachments se usa para bloquear el malware de día cero en archivos adjuntos de correo electrónico y documentos.
- Describir cómo Safe Links protege a los usuarios de URL maliciosas incrustadas en correos electrónicos y documentos que apuntan
- Configurar Azure Advanced Threat Protection.
- Configurar Windows Defender ATP.

Módulo 6: Administración de amenazas

Este módulo explica Microsoft Threat Management, que le proporciona las herramientas para evaluar y abordar las amenazas cibernéticas y formular respuestas. Aprenderá a usar el panel de seguridad y Azure Sentinel para Microsoft 365. El módulo también explica y configura Microsoft Advanced Threat Analytics.

Lecciones

- Usar el panel de seguridad
- Investigación y respuesta a amenazas de Microsoft 365
- Azure Sentinel para Microsoft 365
- Configurar Advanced Threat Analytics

Laboratorio: Usar el simulador de ataque

- Realizar un ataque simulado de Spear phishing
- Realizar ataques de contraseña simulados

Después de completar este módulo, los estudiantes podrán:

- Describir cómo Threat Explorer puede usarse para investigar amenazas y ayudar a proteger a su inquilino.
- Describir cómo Security Dashboard brinda a los ejecutivos de nivel C información sobre los principales riesgos y tendencias.
- Describir qué es Advanced Thread Analytics (ATA) y qué requisitos se necesitan para implementarlo.
- Configurar Advanced Threat Analytics.
- Usar el simulador de ataque en Microsoft 365.
- Describir cómo se puede usar Azure Sentinel para Microsoft 365.

Módulo 7: Movilidad

Este módulo se enfoca en asegurar dispositivos móviles y aplicaciones. Aprenderá sobre la administración de dispositivos móviles y cómo funciona con Microsoft Intune. También aprenderá sobre cómo Intune y Azure AD se pueden usar para proteger las aplicaciones móviles.

Lecciones

- Plan para la gestión de aplicaciones móviles
- Plan para la gestión de dispositivos móviles
- Implementar la administración de dispositivos móviles
- Registrar dispositivos en la administración de dispositivos móviles

Laboratorio: configurar Azure AD para Intune

- habilitar la administración de dispositivos
- configurar Azure AD para Intune
- Crear políticas de Intune

Después de completar este módulo, los estudiantes podrán:

- Describir las consideraciones de la aplicación móvil.
- Usar Intune para administrar aplicaciones móviles.
- Gestionar dispositivos con MDM.
- Configurar dominios para MDM.
- Administrar políticas de seguridad del dispositivo.
- Inscripción de dispositivos a MDM.
- Configurar un rol de administrador de inscripción de dispositivos.

Módulo 8: Protección de la información

El módulo explica cómo implementar Azure Information Protection y Windows Information Protection.

Lecciones

- Conceptos de protección de la información
- Protección de la información de Azure
- Protección de información avanzada
- Protección de la información de Windows

Laboratorio: Implementar Azure Information Protection y Windows Information Protection

- Implementación de Azure Information Protection
- Implementación de Windows Information Protection

Después de completar este módulo, los estudiantes podrán:

- Configurar etiquetas y políticas para Azure Information Protection.
- Configurar los ajustes avanzados del servicio AIP para las plantillas de Servicios de administración de derechos (RMS).
- Planificar una implementación de las políticas de protección de la información de Windows.

MS-500T00-A
Microsoft 365 Security Administration

Módulo 9: Gestión de derechos y cifrado

Este módulo explica la gestión de derechos de información en Exchange y SharePoint. El módulo también describe las tecnologías de cifrado utilizadas para proteger los mensajes.

Lecciones

- Gestión de derechos de información
- Extensión segura de correo multipropósito de Internet
- Cifrado de mensajes de Office 365

Laboratorio: Configurar el cifrado de mensajes de Office 365 (OME)

- Configurar el cifrado de mensajes de Office 365
- Validar la gestión de derechos de información

Después de completar este módulo, los estudiantes podrán:

- Describir las diferentes opciones de cifrado de Microsoft 365.
- Describir el uso de S/MIME.
- Describir y habilitar el cifrado de mensajes de Office 365.

Módulo 10: Prevención de pérdida de datos

Este módulo se centra en la prevención de pérdida de datos en Microsoft 365. Aprenderá cómo crear políticas, editar reglas y personalizar notificaciones de usuario para proteger sus datos.

Lecciones

- Prevención de pérdida de datos explicada
- Políticas de prevención de pérdida de datos
- Políticas personalizadas de DLP
- Crear una política DLP para proteger documentos
- Consejos de política

MS-500T00-A
Microsoft 365 Security Administration

Laboratorio: Implementar políticas de prevención de pérdida de datos

- Administrar políticas de DLP
- Probsr las directivas MRM y DLP

Después de completar este módulo, los estudiantes podrán:

- Describir la prevención de pérdida de datos (DLP, por sus siglas en inglés).
- Usar plantillas de políticas para implementar políticas DLP para la información de uso común.
- Configurar las reglas correctas para proteger el contenido.
- Describir cómo modificar las reglas existentes de las políticas DLP.
- Configurar la opción de anulación de usuario a una regla DLP.
- Explicar cómo SharePoint Online crea propiedades rastreadas a partir de documentos.

Módulo 11: Seguridad de aplicaciones en la nube

Este módulo se centra en la seguridad de las aplicaciones en la nube en Microsoft 365. El módulo explicará el descubrimiento de la nube, los conectores de la aplicación, las políticas y las alertas. Aprenderá cómo funcionan estas características para proteger sus aplicaciones en la nube.

Lecciones

- Seguridad de aplicaciones en la nube explicada
- Uso de información de seguridad de aplicaciones en la nube

Después de completar este módulo, los estudiantes podrán:

- Describir Cloud App Security.
- Explicar cómo implementar Cloud App Security.
- Controlar sus aplicaciones en la nube con políticas.
- Usar el Catálogo de aplicaciones en la nube.
- Usar el panel de Cloud Discovery.
- Administrar permisos de aplicaciones en la nube.

MS-500T00-A
Microsoft 365 Security Administration

Módulo 12: Cumplimiento en Microsoft 365

Este módulo se centra en el gobierno de datos en Microsoft 365. El módulo le presentará al Administrador de cumplimiento y analizará el Reglamento Global de Protección de Datos (GDPR).

Lecciones

- Plan de requisitos de cumplimiento
- Construir muros éticos en Exchange Online
- Administrar la retención en el correo electrónico
- Solucionar problemas de gobernanza de datos

Después de completar este módulo, los estudiantes podrán:

- Planificar los roles de seguridad y cumplimiento.
- Describir lo que debe tener en cuenta para RGPD.
- Describir qué es un muro ético en Exchange y cómo funciona.
- Trabajar con etiquetas de retención en buzones
- Describir las políticas de retención con mensajes de correo electrónico y carpetas de correo electrónico.
- Explicar cómo se calcula la edad de retención de los elementos.
- Reparar las políticas de retención que no funcionan como se esperaba.

Módulo 13: Archivado y Retención

Este módulo explica conceptos relacionados con la retención y el archivo de datos para Microsoft 365, incluidos Exchange y SharePoint.

Lecciones

- Archivado en Microsoft 365
- Retención en Microsoft 365
- Políticas de retención en el Centro de cumplimiento de Microsoft 365
- Archivo y retención en Exchange
- Gestión de registros locales en SharePoint

MS-500T00-A
Microsoft 365 Security Administration

Laboratorio: Cumplimiento y retención

- Inicializar cumplimiento
- Configurar etiquetas y políticas de retención

Después de completar este módulo, los estudiantes podrán:

- Describir la diferencia entre el Archivo local y la Gestión de registros.
- Explicar cómo se archivan los datos en Exchange.
- Explicar cómo funciona una política de retención.
- Crear una política de retención.
- Activar y desactivar el archivado local.
- Crear etiquetas de retención útiles.

Módulo 14: Búsqueda de contenido e investigación

Este módulo se centra en la búsqueda de contenido y las investigaciones. El módulo cubre cómo usar eDiscovery para realizar investigaciones avanzadas de datos de Microsoft 365. También cubre los registros de auditoría y analiza las solicitudes de sujetos de datos de GDPR.

Lecciones

- Búsqueda de contenido
- Auditoría de investigaciones de registro
- eDiscovery avanzado

Laboratorio: Administrar búsquedas e investigaciones

- Investigar sus datos de Microsoft 365
- Realizar una solicitud del interesado

Después de completar este módulo, los estudiantes podrán:

- Describir cómo usar la búsqueda de contenido.
- Diseñar una búsqueda de contenido.
- Configurar el filtrado de permisos de búsqueda.

MS-500T00-A
Microsoft 365 Security Administration

- Configurar políticas de auditoría.
- Introducir los criterios para buscar en el registro de auditoría.
- Describir eDiscovery avanzado en Microsoft 365.
- Ver el registro avanzado de eventos de exhibición de documentos electrónicos.