Microsoft 365 Security Administration

MS-500T00

Detalles del Curso

Audiencia(s):	Profesional de TI(s)
Tecnología:	Microsoft 365
Duración:	40 Horas
Material Didáctico:	Oficial (Ingles)

Sobre este Curso

En este curso, aprenderá a proteger el acceso de los usuarios a los recursos de su organización. El curso cubre la protección con contraseña del usuario, la autenticación multifactor, cómo habilitar Azure Identity Protection, cómo configurar y usar Azure AD Connect, y le presenta el acceso condicional en Microsoft 365. Aprenderá sobre tecnologías de protección contra amenazas que ayudan a proteger su Microsoft. 365 entorno. Específicamente, aprenderá sobre 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 el curso, aprenderá acerca de las tecnologías de protección de la información que ayudan a proteger su entorno Microsoft 365. El curso analiza el contenido gestionado por derechos de información, cifrado de mensajes, así como etiquetas, políticas y reglas que respaldan la prevención de pérdida de datos y la protección de la información. Por último, aprenderá sobre el archivo 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 in situ para SharePoint, la retención de correo electrónico y cómo realizar búsquedas de contenido que respalden las investigaciones de eDiscovery.

Perfil de Audiencia

El administrador de seguridad de Microsoft 365 colabora con el administrador de Microsoft 365 Enterprise, las partes interesadas del negocio y otros administradores de cargas de trabajo para planificar e implementar estrategias de seguridad y para garantizar que las soluciones cumplan con las políticas y regulaciones de la organización. Esta función protege de forma proactiva los entornos empresariales de Microsoft 365. Las responsabilidades incluyen responder a las amenazas, implementar, administrar y

monitorear las 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 y los entornos híbridos de Microsoft 365. Este rol tiene fuertes habilidades y experiencia en protección de identidad, protección de información, protección contra amenazas, administración de seguridad y gobernanza de datos.

Contenido del Curso

Módulo 1: Gestión de usuarios y grupos

Este módulo explica cómo administrar cuentas de usuario y grupos en Microsoft 365. Le presenta el concepto zero trust, así como la autenticación. El módulo sienta las bases para el resto del curso.

Lecciones

- Conceptos de gestión de identidades y accesos
- El modelo Zero Trust
- Planeación de la solución de identidad y autenticación
- Cuentas y roles de usuario
- Gestión de contraseñas

Laboratorio: Inicialice su inquilino - usuarios y grupos
Laboratorio : Gestión de contraseñas

Módulo 2: Sincronización y protección de identidades

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

Lecciones

- Planeación de la sincronización de directorios
- Configurar y administrar identidades sincronizadas
- Protección de identidad de Azure AD

Laboratorio: Implementar la sincronización de identidades

Módulo 3: Gestión de identidades y accesos

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

Lecciones

- Administración de aplicaciones
- Gobernanza de la identidad
- Administrar el acceso a los dispositivos
- Control de acceso basado en roles (RBAC)
- Soluciones para el acceso externo
- Gestión de identidades privilegiadas

Laboratorio: Usar el acceso condicional para habilitar MFA
Laboratorio: Configurar la administración de identidades privilegiadas

Módulo 4: Seguridad en Microsoft 365

Este módulo explica las diversas amenazas de ciberataque que existen. A continuación, le presenta las soluciones de Microsoft utilizadas para mitigar esas amenazas. El módulo termina 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
- Soluciones de seguridad de Microsoft
- Puntuación segura

Laboratorio: Usar Microsoft Secure Score

Módulo 5: Protección contra amenazas

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, Microsoft Defender for Identity y Microsoft Defender for Endpoint.

Lecciones

- Protección de Exchange Online (EOP)
- Microsoft Defender para Office 365
- Administrar archivos adjuntos seguros
- Administrar enlaces seguros

- Microsoft Defender para identidad
- Microsoft Defender para endpoint

Laboratorio: Administrar los servicios de seguridad de Microsoft 365

Módulo 6: Gestión 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.

Lecciones

- Panel de seguridad
- Investigación y respuesta a amenazas
- Azure Sentinel
- Análisis avanzado de amenazas

Laboratorio : Uso de Attack Simulator

Módulo 7: Seguridad de aplicaciones en la nube de Microsoft

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 aplicaciones, las políticas y las alertas. Aprenderá cómo funcionan estas características para proteger sus aplicaciones en la nube.

Lecciones

- Implementar la seguridad de las aplicaciones en la nube
- Usar la información de seguridad de las aplicaciones en la nube

Módulo 8: Movilidad

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

Lecciones

- Gestión de aplicaciones móviles (MAM)
- Administración de dispositivos móviles (MDM)
- Implementar servicios de dispositivos móviles
- Inscribir dispositivos en Mobile Device Management

Laboratorio : Administración de dispositivos

Módulo 9: Protección y gobernanza de la información

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

Lecciones

- Conceptos de protección de la información
- Gobierno y gestión de registros
- Etiquetas de sensibilidad
- Archivado en Microsoft 365
- Retención en Microsoft 365
- Directivas de retención en el Centro de cumplimiento de Microsoft 365
- Archivado y retención en Exchange
- Administración de registros en tiempo real en SharePoint

Laboratorio : Archiving y Retención

Módulo 10: Gestión de derechos y cifrado

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

Lecciones

- Administración de derechos de información (IRM)
- Extensión de correo de Internet multipropósito segura (S-MIME)
- Cifrado de mensajes de Office 365

Laboratorio: Configurar el cifrado de mensajes de Office 365

Módulo 11: Prevención de pérdida de datos

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

Lecciones

- Fundamentos de la prevención de pérdida de datos
- Crear una directiva DLP
- Personalizar una directiva DLP
- Crear una directiva DLP para proteger documentos
- Consejos de política

Laboratorio: Implementar políticas de prevención de pérdida de datos

Módulo 12: Gestión del cumplimiento

Este módulo explica el Centro de cumplimiento en Microsoft 365. Discute los componentes de la puntuación de cumplimiento.

Lecciones

- Centro de cumplimiento

Módulo 13: Gestión de riesgos internos

Este módulo se centra en la funcionalidad relacionada con el riesgo interno dentro de Microsoft 365. Cubre no solo la gestión de riesgos internos en el centro de cumplimiento, sino también las barreras de información y la administración de acceso privilegiado.

Lecciones

- Riesgo interno
- Acceso privilegiado
- Barreras de la información
- Construyendo muros éticos en Exchange Online

Laboratorio : Gestión de acceso privilegiado

Módulo 14: Descubrir y responder

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 los interesados de GDPR.

Lecciones

- Búsqueda de contenido
- Investigaciones de registros de auditoría
- Exhibición de documentos electrónicos avanzada

Laboratorio : Administrar la búsqueda y la investigación

Al Finalizar este Curso

Después de completar este curso, los estudiantes podrán:

- Administre el acceso de usuarios y grupos en Microsoft 365.
- Explique y administre Azure Identity Protection.
- Planifique e implemente Azure AD Connect.
- Administre identidades de usuarios sincronizadas.
- Explique y use el acceso condicional.
- Describir los vectores de amenazas de ataques cibernéticos.
- Explique las soluciones de seguridad para Microsoft 365.
- Utilice Microsoft Secure Score para evaluar y mejorar su postura de seguridad.
- Configure varios servicios avanzados de protección contra amenazas para Microsoft 365.
- Planifique e implemente dispositivos móviles seguros.
- Implementar la gestión de derechos de información.
- Proteja los mensajes en Office 365.
- Configure las políticas de prevención de pérdida de datos.
- Implemente y administre la seguridad de las aplicaciones en la nube.
- Implemente la protección de la información de Windows para los dispositivos.
- Planifique e implemente un sistema de almacenamiento y retención de datos.
- Cree y gestione una investigación de eDiscovery.
- Gestionar las solicitudes de los sujetos de datos del RGPD.
- Explique y use etiquetas de confidencialidad.