MS-500: Microsoft 365 Security Administration

Duración: **30 Horas**

INTRODUCCION:

En esta formación los asistentes aprenderán a asegurar el acceso de los usuarios a los recursos de su organización. Este curso cubre la protección de contraseña del usuario, la autenticación multifactor, cómo habilitar Azure Identity Protection, cómo configurar Active Directory Federation Services, cómo configurar y usar Azure AD Connect, y también presenta el Conditional Access. Se aprenderán soluciones para administrar el acceso externo a un sistema Microsoft 365.

Los asistentes también aprenderán diversas tecnologías de protección contra amenazas para proteger un entorno Microsoft 365. Concretamente, aprenderán sobre los vectores de amenazas, Secure Score, la protección de Exchange Online, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection y a usar Microsoft 365 Threat Intelligence.

Los asistentes también aprenderán sobre las diferentes tecnologías de protección de la información que ayudan a proteger un entorno Microsoft 365, y lo haremos discutiendo sobre el contenido de Information Rights Management, el cifrado de mensajes, las etiquetas, políticas y reglas que definan la prevención de pérdida de datos y la protección de la información. Por último, en esta parte del curso explicaremos la implementación de Microsoft Cloud App Security.

Para finalizar se aprenderá sobre el archivado y la retención en Microsoft 365, así como sobre la gobernanza de datos y la realización de búsquedas e investigaciones de contenido. Se tratará sobre las políticas y etiquetas de retención de datos, In-Place Records Management para SharePoint, la retención de correo electrónico y cómo realizar búsquedas de contenido que admitan investigaciones con casos de eDiscovery. El curso también da las directrices necesarias para que una empresa pueda prepararse para el Reglamento Global de Protección de Datos (GDPR).

DIRIGIDO A:

Esta formación va dirigida a aquellas personas que deseen aprender sobre el rol de Microsoft 365 Security Administrator. Este rol colabora con el de Microsoft 365 Enterprise Administrator, stakeholders y otros administradores de cargas de trabajo para planificar e implementar estrategias de seguridad y garantizar que las soluciones aplicadas cumplan con las políticas y regulaciones de la empresa.

OBJETIVOS:

- Administrar el acceso de usuarios y grupos en Microsoft 365.
- Explicar y administrar Azure Identity Protection.
- Planifique e implemente Azure AD Connect.
- Gestionar identidades de usuario sincronizadas.

- Explicar y usar el acceso condicional.
- Describir los vectores de amenazas de ciberataques.
- Explicar las soluciones de seguridad para Microsoft 365.
- Use 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.
- Mensajes seguros en Office 365.
- Configurar políticas de prevención de pérdida de datos.
- Implemente y administre Cloud App Security.
- Implemente la protección de información de Windows para dispositivos.
- Planifique e implemente un sistema de archivo y retención de datos.
- Crear y administrar una investigación de descubrimiento electrónico.
- Gestionar solicitudes de sujetos de datos GDPR.
- Explicar y usar etiquetas de sensibilidad.

EXAMEN:

Este curso oficial es el recomendado por Microsoft para la preparación del siguiente examen de certificación:

- **MS-500: Microsoft 365 Security Administration.**

REQUISITOS:

Es recomendable que el alumno tenga los siguientes conocimientos previos para garantizar un correcto seguimiento del curso:

- Conocimientos básicos de Microsoft Azure.
- Experiencia con dispositivos con 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.

CONTENIDO:

MS-500T01-A: Administración de la identidad y el acceso de Microsoft 365
Módulo 1: Seguridad de usuario y grupo.

- Cuentas de usuario en Microsoft 365.
- Roles de administrador y grupos de seguridad en Microsoft 365.
- Administración de contraseñas en Microsoft 365.
- Protección de identidad de Azure AD.

Módulo 2: Sincronización de identidades.

- Introducción a la sincronización de identidades.
- Planificación de Azure AD Connect.
- Implementación de Azure AD Connect.
- Administración de identidades sincronizadas.

Módulo 3: Identidades Federadas.

- Introducción a las identidades federadas.
- Planificación de una implementación de AD FS.
- Implementación de AD FS.

Módulo 4: Gestión de accesos.

- Acceso condicional.
- Administración del acceso a dispositivos.
- Control de acceso basado en roles (RBAC).
- Soluciones para el acceso externo.

MS-500T02-A: Implementación de microsoft 365 protección contra amenazas.
Módulo 1: Seguridad en Microsoft 365.

- Vectores de amenazas y violaciones de datos.
- Soluciones de seguridad para Microsoft 365.
- Microsoft Secure Score.

Módulo 2: Protección contra amenazas avanzada.

- Protección de Exchange Online.
- Protección contra amenazas avanzada de Office 365.
- Gestión de archivos adjuntos seguros.
- Gestión de enlaces seguros.
- Protección contra amenazas avanzada de Azure.
- Protección contra amenazas avanzada de Windows Defender.

Módulo 3: Inteligencia de amenazas.

- Inteligencia de amenazas de Microsoft 365.
- Uso del panel de seguridad.
- Configuración de análisis avanzados de amenazas.

Módulo 4: Movilidad.

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

MS-500T03-A: Implementación de Microsoft 365 Information Protection.
Módulo 1: Protección de la información.

- Gestión de los derechos de la información.
- Extensión segura de correo de Internet multipropósuspos.
- Cifrado de mensajes de Office 365.
- Azure Information Protection.

- Protección avanzada de la información.
- Protección de la información de Windows.

Módulo 2: Prevención de pérdida de datos

- Explicación de la prevención de pérdida de datos
- Políticas de prevención de pérdida de datos
- Políticas personalizadas de DLP
- Creación de una directiva dlp para proteger documentos.
- Consejos de política.

Módulo 3: Seguridad de aplicaciones en la nube.

- Explicación de la seguridad de las aplicaciones en la nube.
- Uso de la información de seguridad de aplicaciones en la nube.
- Seguridad de aplicaciones en la nube de Office 365.

MS-500T04-A: Administración de cumplimiento integrado de Microsoft 365.
Módulo 1: Archiving y Retención.

- Archivo en Microsoft 365.
- Retención en Microsoft 365.
- Políticas de retención en el Centro de Seguridad y Cumplimiento.
- Archiving y retención en Exchange.
- Administración de registros in situ en SharePoint.

Módulo 2: Gobernanza de datos en Microsoft 365.

- Planificación de las necesidades de seguridad y cumplimiento.
- Construcción de muros éticos en Exchange Online.
- Administrar la retención en el correo electrónico.
- Solución de problemas de gobernanza de datos.
- Análisis y Telemetría.

Módulo 3: Gestión de la búsqueda y las investigaciones.

- Búsqueda de contenido en el Centro de seguridad y cumplimiento.
- Investigaciones de registro de auditoría.
- Exhibición avanzada de eDiscovery.