TEMARIO

Microsoft 365 Security Administration

Microsoft 365

Microsoft CERTIFIED ASSOCIATE

MS-500

SIV & DB CLOUD

EXPERIENCIA Y TECNOLOGIA

CONTÁCTENOS

+57 316 3956090 contactenos@siv.com.co www.siv.com.co

+57 315 2653920 comercial@siv.com.co www.dbcloud.co

Microsoft 365 Security Administration

Examen MS-500

Descripción del 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.

Perfil de Audiencia

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.

Prerrequisitos

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 administración de dispositivos móviles.

DESCRIPCION MODULOS DE CAPACITACION

Módulo 1: Administración de usuarios y grupos

Este módulo explica cómo administrar cuentas de usuario y grupos en Microsoft 365. Presenta el concepto de Confianza cero y la autenticación. El módulo establece las bases para el resto del curso.

Lecciones

- Conceptos de administración de identidades y acceso
- Modelo de confianza cero
- Planeamiento de la solución de identidad y autenticación
- Roles y cuentas de usuario
- Administración de contraseñas.

Laboratorio : Inicialización del inquilino: usuarios y grupos

- Configuración del inquilino de Microsoft 365
- Administración de usuarios y grupos

Laboratorio : Administración de contraseñas

- Configuración del autoservicio de restablecimiento de contraseña (SSPR) para cuentas de usuario en Azure AD
- Implementación de Smart Lock de Azure AD.

Después de completar este módulo, los estudiantes podrán:

- Crear y administrar cuentas de usuario.
- Describir y usar roles de administrador de Microsoft 365.
- Planear directivas de contraseña y autenticación con contraseña.

- Describir los conceptos de seguridad de Confianza cero.
- Explicar el modelo de Confianza cero.

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 en la administración de la sincronización de directorios para garantizar que las personas adecuadas se conecten a su sistema Microsoft 365.

Lecciones

- Planeamiento de la sincronización de directorios
- Configuración y administración de identidades sincronizadas
- Azure AD Identity Protection.

Laboratorio : Implementación de la sincronización de identidades

- Configuración de la organización para la sincronización de identidades.

Después de completar este módulo, los estudiantes podrán:

- Explicar la sincronización de directorios.
- Planear la sincronización de directorios.
- Describir y usar Azure AD Connect.
- Configurar los requisitos previos de Azure AD Connect.
- Administrar usuarios y grupos con la sincronización de directorios.
- Describir la federación de Active Directory.
- Habilitación de Azure Identity Protection.

Módulo 3: Administración de identidades y 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. Analizamos la gobernanza de identidades como concepto y sus componentes.

Lecciones

- Administración de aplicaciones
- Identity Governance
- Administración del acceso al dispositivo
- Control de acceso basado en roles (RBAC)

- Soluciones de acceso externo
- Privileged Identity Management

Laboratorio : Uso del acceso condicional para habilitar MFA

- Piloto de autenticación MFA (requiere MFA para aplicaciones específicas)
- Acceso condicional de MFA (realizar una implementación de MFA)

Laboratorio : Configuración de Privileged Identity Management

- Administración de recursos de Azure
- Asignación de roles de directorio
- Activación y desactivación de roles de PIM
- Roles de directorio
- Flujos de trabajo de recursos de PIM
- Visualización del historial de auditoría de los roles de Azure AD en PIM

Después de completar este módulo, los estudiantes podrán:

- Describir el concepto de acceso condicional.
- Describir y usar directivas de acceso condicional.
- Planear el cumplimiento de dispositivos.
- Configurar usuarios y grupos condicionales.
- Configurar el control de acceso basado en roles.
- Describir los conceptos de la gobernanza de identidades.
- Configurar y usar Privileged Identity Management.

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 e infracciones de datos
- Estrategia y principios de seguridad.
- Soluciones de seguridad de Microsoft
- Puntuación segura.

Laboratorio : Uso de Puntuación de seguridad de Microsoft

- Mejora de la puntuación de seguridad en el Centro de seguridad de Microsoft 365.

Después de completar este módulo, los estudiantes podrán:

- Describir varias técnicas que usan los atacantes 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 EOP y Microsoft Defender para Office 365.
- Describir los beneficios de Puntuación segura y qué tipo de servicios se pueden analizar.
- Describir cómo usar Puntuación segura para identificar brechas en su posición de seguridad actual de Microsoft 365.

Módulo 5: Protección contra amenazas

Este módulo explica las diversas tecnologías y servicios de protección contra amenazas disponibles para Microsoft 365. El módulo trata la protección de mensajes mediante Exchange Online Protection, Microsoft Defender for Identity y Microsoft Defender para punto de conexión.

Lecciones

- Exchange Online Protection (EOP)
- Microsoft Defender para Office 365
- Administración de datos adjuntos seguros
- Administración de vínculos seguros
- Microsoft Defender for Identity
- Microsoft Defender para punto de conexión

Laboratorio : Administración de servicios de seguridad de Microsoft 365

- Implementación de directivas de Microsoft Defender

Después de completar este módulo, los estudiantes podrán:

- Describir la canalización antimalware a medida que Exchange Online Protection analiza el correo electrónico.
- Describir cómo se usa la característica Datos adjuntos seguros para bloquear el malware de día cero en datos adjuntos de correo electrónico y documentos.
- Describir cómo la característica Vínculos seguros protege a los usuarios de direcciones URL maliciosas insertadas en el correo electrónico y los documentos a los que apuntan.

- Configurar Microsoft Defender for Identity.
- Configure Microsoft Defender para punto de conexión.

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.

Lecciones

- Panel de seguridad
- Investigación de amenazas y respuesta a ellas
- Azure Sentinel
- Advanced Threat Analytics

Laboratorio : Uso del simulador de ataques

- Realización de un ataque simulado de suplantación de identidad (phishing) de Spear
- Realización de ataques de contraseña simulados

Después de completar este módulo, los estudiantes podrán:

- Describir cómo se puede usar el Explorador de amenazas para investigar amenazas y ayudar a proteger el inquilino.
- Describir cómo el Panel de seguridad 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 ataques de Microsoft 365.
- Describir cómo se puede usar Azure Sentinel para Microsoft 365.

Módulo 7: Microsoft Cloud Application Security

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

- Implementación de Cloud Application Security
- Uso de información de Cloud Application Security

Después de completar este módulo, los estudiantes podrán:

- Describir Cloud App Security.
- Explicar cómo implementar Cloud App Security.
- Controlar las aplicaciones en la nube con directivas.
- Usar el catálogo de aplicaciones en la nube.
- Usar el panel de Cloud Discovery.
- Administrar los permisos de aplicaciones en la nube.

Módulo 8: 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

- Administración de aplicaciones móviles (MAM)
- Administración de dispositivos móviles (MDM)
- Implementación de servicios para dispositivos móviles
- Registro de dispositivos en la administración de dispositivos móviles

Laboratorio : Administración de dispositivos

- Habilitación de la administración de dispositivos
- Configuración de Azure AD para Intune
- Creación de directivas de cumplimiento y acceso condicional

Después de completar este módulo, los estudiantes podrán:

- Describir las consideraciones de las aplicaciones móviles.
- Gestionar dispositivos con MDM.
- Configurar dominios para MDM.
- Administrar directivas de seguridad de dispositivos.
- Inscribir dispositivos en MDM.
- Configurar un rol de administrador de inscripción 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 cómo crear políticas, editar reglas y personalizar notificaciones de usuario para proteger sus datos.

Lecciones

- Conceptos de la protección de la información
- Gobernanza y administración de registros
- Etiquetas de confidencialidad
- Archivo en Microsoft 365
- Retención en Microsoft 365
- Directivas de retención en el Centro de cumplimiento de Microsoft 365
- Archivo y retención en Exchange
- Administración de registros locales en SharePoint.

Laboratorio : Archivado y retención

- Inicialización del cumplimiento
- Configuración de etiquetas y directivas de retención

Después de completar este módulo, los estudiantes podrán:

- Configurar las etiquetas de confidencialidad.
- Configurar el archivo y la retención en Microsoft 365.
- Planear y configurar la administración de registros.

Módulo 10: Derechos de administración 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

- Information Rights Management (IRM)
- Extensión segura de correo multipropósito de Internet (S-MIME)
- Cifrado de mensajes de Office 365

Laboratorio : Configuración del cifrado de mensajes de Office 365

- Configuración del cifrado de mensajes de Office 365
- Validación de la administración de derechos de la 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 11: Prevención de la 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

- Aspectos básicos de la prevención de la pérdida de datos
- Crear una directiva DLP
- Personalización de una directiva DLP
- Creación de una directiva DLP para proteger documentos
- Consejos de directiva

Laboratorio : Implementación de directivas de prevención de la pérdida de datos

- Administración de directivas DLP
- Prueba de directivas MRM y DLP

Después de completar este módulo, los estudiantes podrán:

- Describir la prevención de pérdida de datos (DLP).
- Usar plantillas de directiva para implementar directivas DLP para la información de uso común.
- Configurar las reglas correctas para proteger el contenido.
- Describir cómo modificar las reglas existentes de las directivas DLP.
- Configurar la opción de invalidación de usuarios como una regla DLP.
- Explicar cómo SharePoint Online crea propiedades rastreadas a partir de documentos.

Módulo 12: Administración del cumplimiento

En este módulo se explica el Centro de cumplimiento de Microsoft 365. Se describen los componentes de la puntuación de cumplimiento.

Lecciones

- Centro de cumplimiento.

Después de completar este módulo, los estudiantes podrán:

- Describir cómo usar la puntuación de cumplimiento para tomar decisiones organizativas.
- Describir cómo se usan las evaluaciones para determinar la puntuación de cumplimiento.

Módulo 13: Administración de riesgos internos

Este módulo se centra en la funcionalidad relacionada con el riesgo interno dentro Microsoft 365. No solo abarca la administración de riesgos internos en el centro de cumplimiento, sino también las barreras de información y la administración del acceso con privilegios.

Lecciones

- Riesgo interno
- Acceso con privilegios
- Barreras de información
- Construcción de muros éticos en Exchange Online

Laboratorio : Privileged Access Management

- Configuración de la administración del acceso con privilegios y procesamiento de una solicitud

Después de completar este módulo, los estudiantes podrán:

- Explicar y configurar la administración de riesgos internos en Microsoft 365.
- Configurar y aprobar solicitudes de acceso con privilegios de administradores globales.
- Configurar y usar barreras de información para cumplir con las regulaciones de la organización.
- Construir muros éticos en Exchange Online.
- Configurar la Caja de seguridad del cliente.

Módulo 14: Detección y respuesta

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 las investigaciones del registro
- eDiscovery avanzado

Laboratorio: Administración de búsqueda e investigación

- Investigación de los datos de Microsoft 365
- Realización de una solicitud del interesado

Después de completar este módulo, los estudiantes podrán:

- Realizar búsquedas de contenido en Microsoft 365.
- Realizar y auditar investigaciones del registro.
- Configurar Microsoft 365 para el registro de auditoría.
- Usar la versión avanzada de eDiscovery.

DESCRIPCION CAPACITACION

Duración de la Capacitación

La capacitación tiene una intensidad de 32 horas.

Fechas y Horario Capacitación

La capacitación en horario nocturno de 6:30 P.M. A 9:30 P.M. hora de Colombia 3 veces por semana.

Plataforma Capacitación

Los alumnos se integran a la plataforma Microsoft Teams teniendo acceso siempre a cada clase, así como a los videos de toda la capacitación**.**

Instructor

Se dispone de un Instructor certificado y calificado con muchos años de experiencia en la implementación de soluciones avanzadas y docencia.

Certificados de Asistencia

Cada alumno recibirá el certificado digital de asistencia al finalizar el entrenamiento.