SC-500T00-A | Implementación de controles de seguridad de extremo a extremo para cargas de trabajo en la nube e IA

La adopción de la nube y la inteligencia artificial está transformando la forma en que las organizaciones desarrollan, despliegan y gestionan sus servicios digitales. Sin embargo, esta evolución también introduce nuevos desafíos de seguridad que requieren profesionales capaces de proteger identidades, datos, infraestructuras, aplicaciones y cargas de trabajo de IA de forma integral.

El curso oficial **SC-500T00-A** de Microsoft te prepara para diseñar, implementar y administrar controles de seguridad de extremo a extremo en entornos Microsoft Azure y Microsoft 365, incluyendo la protección de soluciones de Inteligencia Artificial y agentes autónomos. A través de formación práctica y laboratorios guiados, desarrollarás las competencias necesarias para fortalecer la postura de seguridad de tu organización utilizando las tecnologías de seguridad de Microsoft.

Objetivos Didácticos

Al finalizar este curso serás capaz de:

- Diseñar e implementar estrategias de seguridad para entornos Microsoft Azure y Microsoft 365.
- Proteger identidades y controlar el acceso a recursos mediante Microsoft Entra ID y Azure Key Vault.
- Implementar controles de seguridad para infraestructuras cloud, redes, almacenamiento, bases de datos y recursos de proceso.
- Proteger aplicaciones, datos y cargas de trabajo de Inteligencia Artificial frente a amenazas y accesos no autorizados.
- Supervisar y mejorar continuamente la postura de seguridad mediante las herramientas de Microsoft Security.
- Detectar y responder a amenazas utilizando las capacidades de Microsoft Defender.
- Aplicar controles de cumplimiento normativo y buenas prácticas de seguridad en entornos cloud, híbridos y multicloud.
- Prepararte para la certificación **Microsoft Certified: Cloud and AI Security Engineer Associate (beta)**.

¿A quién está dedicado este curso?

Este curso está dirigido a ingenieros de seguridad, administradores de Azure, arquitectos cloud y profesionales de ciberseguridad que desean implementar una estrategia integral de protección para entornos Microsoft Azure, Microsoft 365 y cargas de trabajo de Inteligencia Artificial. También es una excelente opción para quienes buscan especializarse en la protección de infraestructuras cloud y prepararse para la certificación **Microsoft Certified: Cloud and AI Security Engineer Associate**.

¿Por qué debería hacer este curso?

La seguridad ya no consiste únicamente en proteger servidores o redes. Hoy es imprescindible asegurar identidades, datos, aplicaciones, infraestructuras cloud y soluciones basadas en IA mediante una estrategia unificada.
Con este curso adquirirás competencias prácticas para implementar controles de seguridad de extremo a extremo utilizando las tecnologías de Microsoft, una habilidad cada vez más demandada

por organizaciones que están acelerando su transformación digital y la adopción de la Inteligencia Artificial.

Audiencia

Este curso está orientado a profesionales responsables de proteger sistemas, datos e infraestructuras en entornos cloud e híbridos mediante tecnologías de seguridad de Microsoft.

Es especialmente recomendable para:

- Ingenieros de Seguridad (Security Engineers).
- Administradores de Microsoft Azure.
- Arquitectos Cloud y de Seguridad.
- Especialistas en Microsoft Entra ID.
- Administradores de Microsoft 365.
- Ingenieros DevSecOps.
- Analistas de operaciones de seguridad (SOC).
- Profesionales que trabajan con Microsoft Defender, Microsoft Purview y Azure AI.
- Técnicos que desean especializarse en la protección de cargas de trabajo de Inteligencia Artificial y prepararse para la certificación oficial de Microsoft.

Requisitos previos

Para obtener el máximo aprovechamiento del curso se recomienda disponer de:

- Experiencia práctica en la administración de Microsoft Azure y entornos híbridos.
- Conocimientos de redes, almacenamiento y recursos de proceso (compute) en Azure.
- Familiaridad con Microsoft Entra ID.
- Conocimientos básicos de administración de Microsoft 365.
- Conocimientos generales de ciberseguridad, gestión de identidades y protección de datos.
- Interés por la seguridad aplicada a soluciones de Inteligencia Artificial y entornos cloud.

Modalidad

Aula virtual en directo.

Duración

4 días

Temario del curso

1. **Protección del acceso a los recursos mediante Microsoft Entra**
   - 1.1. Administración e implementación de métodos de autenticación en microsoft Entra ID
   - 1.2. Implementación y configuración de Privileged Identity Management (PIM)
   - 1.3. Autenticación del complemento de API para agentes declarativos con API protegidas

2. **Proteja Azure Key Vault con una defensa en profundidad para la nube y las cargas de trabajo de IA**
   - 2.1. Configuración y protección de Azure Key Vault
   - 2.2. Administración de claves y secretos en Azure Key Vault
   - 2.3. Administración de certificados y supervisión de Azure Key Vault
   - 2.4. Protección de Azure Key Vault con Microsoft Defender para la nube

3. **Aplicación de la gobernanza de seguridad y el cumplimiento normativo**
   - 3.1. Imponer la gobernanza con Azure Policy y bloqueos de recursos
   - 3.2. Configuración de controles de seguridad y recomendaciones de corrección en Defender for Cloud
   - 3.3. Evaluación del cumplimiento normativo en Defender for Cloud
   - 3.4. Administración y asignación de roles de RBAC de tamaño adecuado para privilegios mínimos
   - 3.5. Protección de datos de copia de seguridad con características de seguridad de Azure Backup
   - 3.6. Implementación de controles de seguridad en la infraestructura como código

4. **Implementación de la seguridad para Azure Storage para el ingeniero de seguridad de la nube e inteligencia artificial**
   - 4.1. Descripción de los servicios de almacenamiento de Azure
   - 4.2. Implementación de la seguridad y administración del acceso para Azure Storage
   - 4.3. Configuración de la seguridad de red para Azure Storage
   - 4.4. Implementación de Microsoft Defender para Storage

5. **Implementación de la seguridad para bases de datos de Azure SQL**
   - 5.1. Configuración de la seguridad de nivel de plataforma para Azure SQL
   - 5.2. Configuración de auditoría para Azure SQL Database y SQL Managed Instance
   - 5.3. Implementación de Microsoft Defender para bases de datos