SC-100T00 Microsoft Cybersecurity Architect

Liderar la protección digital de una organización requiere una visión estratégica y conocimientos avanzados en ciberseguridad. Este programa formativo está diseñado para profesionales que desean **diseñar e implementar arquitecturas de seguridad integradas**, alineadas con las prioridades del negocio. La certificación **Microsoft Certified: Cybersecurity Architect Expert** acredita tu capacidad para coordinar soluciones de protección en entornos complejos y altamente regulados.

Objetivos Didácticos

- Diseñar una estrategia de ciberseguridad integral basada en el modelo Zero Trust.
- Planificar soluciones de seguridad que abarquen identidades, dispositivos, aplicaciones, datos, redes y cargas de trabajo en la nube.
- Integrar herramientas clave de Microsoft como Defender, Sentinel, Purview y Entra en una arquitectura coherente.
- Recomendar mejoras técnicas que equilibren las necesidades de seguridad, cumplimiento y eficiencia operativa.
- Prepararte para la certificación oficial Microsoft Certified: Cybersecurity Architect Expert.

Audiencia

- Profesionales con experiencia en seguridad que desean evolucionar hacia un perfil estratégico y de liderazgo técnico.
- Arquitectos de soluciones, responsables de IT y expertos en cumplimiento que necesitan definir arquitecturas seguras y resilientes.
- Personas con certificaciones como SC-200, SC-300 o AZ-500 que buscan una credencial de nivel experto.

Requisitos previos

- Experiencia consolidada en áreas de seguridad, cumplimiento o gestión de identidades en entornos Microsoft.
- Se recomienda haber completado formaciones previas como SC-200, SC-300 o AZ-500.
- Conocimientos sólidos sobre modelos de seguridad en la nube, Zero Trust y diseño de arquitecturas empresariales.

Modalidad

Aula virtual en directo.

Duración

2 días

Temario del curso

1. **Diseño de soluciones que se alineen con los procedimientos recomendados de seguridad y las prioridades**

    1.1. Introducción a los marcos de procedimientos recomendados y la Confianza cero
    1.2. Diseñar soluciones de seguridad que se alineen con Cloud Adoption Framework (CAF) y Well-Architected Framework (WAF)
    1.3. Diseño de soluciones que se alineen con la Arquitectura de referencia de ciberseguridad de Microsoft (MCRA) y Microsoft Cloud Security Benchmark (MCSB)
    1.4. Diseño de una estrategia de resistencia para ransomware y otros ataques en función de los procedimientos recomendados de seguridad de Microsoft
    1.5. Caso práctico: Diseño de soluciones que se alineen con los procedimientos recomendados de seguridad y las prioridades

2. **Diseño de funcionalidades de operaciones de seguridad, identidad y cumplimiento**

    2.1. Diseño de soluciones para el cumplimiento normativo
    2.2. Diseño de soluciones para la administración de identidades y acceso
    2.3. Diseño de soluciones para proteger el acceso con privilegios
    2.4. Diseño de soluciones para operaciones de seguridad
    2.5. Caso práctico: Diseño de funcionalidades de operaciones de seguridad, identidad y cumplimiento

3. **Diseño de soluciones de seguridad para aplicaciones y datos**

    3.1. Diseñar soluciones para proteger Microsoft 365
    3.2. Diseño de soluciones para proteger aplicaciones
    3.3. Diseño de soluciones para proteger los datos de una organización
    3.4. Caso práctico: diseño de soluciones de seguridad para aplicaciones y datos

4. **Diseño de soluciones de seguridad para infraestructura**

    4.1. Especificación de los requisitos para proteger los servicios SaaS, PaaS e IaaS
    4.2. Diseño de soluciones para la administración de la posición de seguridad en entornos híbridos y multinube
    4.3. Diseño de soluciones para proteger los puntos de conexión de cliente y servidor
    4.4. Diseño de soluciones para la seguridad de red
    4.5. Caso práctico: Diseño de soluciones de seguridad para la infraestructura