Microsoft Cybersecurity Architect (SC-100)

Detalles del curso:

Duración: 24 h.

Modalidad: Aula virtual

Certificación: Oficial

Información e inscripción:

685 457 610 - 615 844 193

formacion@laberit.com

LÄBERIT | CENTRO DE FORMACIÓN TIC.

Microsoft Cybersecurity Architect (SC-100)

LÁBERIT CENTRO DE FORMACIÓN TIC

Introducción

Se trata de un curso avanzado de nivel de experto. Aunque no es necesario asistir, se recomienda encarecidamente que los alumnos hayan aprobado otra certificación de nivel de técnico auxiliar en la cartera seguridad, cumplimiento e identidad (como AZ-500, SC-200 o SC-300) antes de asistir a esta clase. Este curso prepara a los alumnos con la experiencia para diseñar y evaluar estrategias de ciberseguridad en las siguientes áreas: Confianza cero; gobernanza, riesgo y cumplimiento (GRC), operaciones de seguridad (SecOps) y datos y aplicaciones. Los alumnos también aprenderán a diseñar soluciones siguiendo los principios de confianza cero y a especificar los requisitos de seguridad para la infraestructura en la nube en diferentes modelos de servicio (SaaS, PaaS, IaaS).

¿Por qué hacer este curso?

Vivimos en una era en la que las amenazas cibernéticas evolucionan constantemente, y las organizaciones necesitan profesionales capaces de diseñar estrategias de seguridad robustas y adaptativas. Este curso te prepara para asumir ese rol, brindándote las habilidades necesarias para proteger los activos y operaciones de una empresa en entornos híbridos y multinube.

Además, completar esta formación te acerca a obtener la certificación **Microsoft Certified: Cybersecurity Architect Expert**, una credencial reconocida que puede abrirte puertas en el ámbito de la ciberseguridad.

¿En qué consiste la formación en Microsoft Cybersecurity Architect?

Este curso avanzado de cuatro días se centra en el diseño y evaluación de estrategias de ciberseguridad en áreas clave como:

- Confianza cero (Zero Trust)
- Gobernanza, riesgo y cumplimiento (GRC)
- Operaciones de seguridad (SecOps)
- Seguridad de datos y aplicaciones

Aprenderás a especificar requisitos de seguridad para infraestructuras en la nube bajo diferentes modelos de servicio (SaaS, PaaS, IaaS) y a diseñar soluciones que sigan los principios de confianza cero. Se recomienda tener experiencia previa en áreas como identidad

y acceso, protección de plataformas, operaciones de seguridad, protección de datos y aplicaciones, así como en implementaciones híbridas y en la nube.

¿A quién va dirigido?

Este curso es para ingenieros de seguridad en la nube con experiencia que han aprobado una certificación anterior en la cartera seguridad, cumplimiento e identidad. Concretamente, los alumnos deben tener experiencia y conocimientos avanzados en una amplia gama de áreas de ingeniería de seguridad, como la identidad y el acceso, la protección de plataformas, las operaciones de seguridad, la protección de datos y la protección de aplicaciones. También deben tener experiencia con implementaciones híbridas y en la nube. En su lugar, los alumnos principiantes deben realizar el curso SC-900: Conceptos básicos de seguridad, cumplimiento e identidad de Microsoft.

Objetivos didácticos

El objetivo general es dotarte de los conocimientos y habilidades necesarios para trabajar Al finalizar el curso, estarás capacitado para:

- Diseñar soluciones que se alineen con las mejores prácticas y prioridades de seguridad.
- Diseñar operaciones de seguridad, identidad y capacidades de cumplimiento.
- Diseñar soluciones de seguridad para infraestructuras.
- Diseñar soluciones de seguridad para aplicaciones y datos

Metodología

El curso combina sesiones teóricas con prácticas, utilizando un enfoque basado en proyectos y retos reales. Se fomenta la participación de los asistentes, promoviendo el aprendizaje colaborativo y la aplicación de los conocimientos adquiridos en situaciones prácticas.

Microsoft Cybersecurity Architect (SC-100)

Salidas profesionales u opciones de promoción profesional

Este curso está dirigido a ingenieros de seguridad en la nube con experiencia que buscan avanzar hacia roles de arquitectura de ciberseguridad. Al completar la formación y obtener la certificación correspondiente, podrás aspirar a posiciones como:

- Arquitecto de ciberseguridad
- Arquitecto de soluciones de seguridad en la nube
- Consultor de seguridad en entornos híbridos y multinube
- Especialista en gobernanza, riesgo y cumplimiento (GRC)

Estas posiciones son altamente demandadas en sectores que priorizan la seguridad de la información y la resiliencia frente a amenazas cibernéticas.

Programa

1. **SC-100: Diseño de soluciones que se alineen con los procedimientos recomendados de seguridad y las prioridades**
    - Introducción a los procedimientos recomendados y la Confianza cero
    - Diseñar soluciones de seguridad que se alineen con Cloud Adoption Framework (CAF) y Well-Architected Framework (WAF)
    - Diseño de soluciones que se alineen con la Arquitectura de referencia de ciberseguridad de Microsoft (MCRA) Y Microsoft Cloud Security Benchmark (MCSB)
    - Diseño de una estrategia de resistencia para ransomware y otros ataques en función de los procedimientos recomendados de seguridad de Microsoft
    - Caso práctico: Diseño de soluciones que se alineen con los procedimientos recomendados de seguridad y las prioridades

2. **SC-100: Diseño de funcionalidades de operaciones de seguridad, identidad y cumplimiento**
    - Diseño de soluciones para el cumplimiento normativo
    - Diseño de soluciones para la administración de identidades y acceso
    - Diseño de soluciones para proteger el acceso con privilegios
    - Diseño de soluciones para operaciones de seguridad

- Caso práctico: Diseño de funcionalidades de operaciones de seguridad, identidad y cumplimiento

3. SC-100: Diseño de soluciones de seguridad para aplicaciones y datos

- Diseñar soluciones para proteger Microsoft 365
- Diseño de soluciones para proteger aplicaciones
- Diseño de soluciones para proteger los datos de una organización
- Caso práctico: diseño de soluciones de seguridad para aplicaciones y datos

4. SC-100: Diseño de soluciones de seguridad para infraestructura

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

LÁBERIT | CENTRO DE FORMACIÓN TIC.

Acreditado:

Microsoft Imagine Academy
Program Member

CertiProf® | Partner

Fundación Estatal
PARA LA FORMACIÓN EN EL EMPLEO

Networking Academy
CISCO

Linux Professional Institute

Microsoft
Technology Associate

Pearson VUE
Authorised
Test Centre

CERTIPORT
A PEARSON VUE BUSINESS
AUTHORIZED TESTING CENTER

Microsoft
Office Specialist
Authorized Testing Center

LABORA
Servei Valencià d'Ocupació i Formació

Avenida Cataluña, 11, bajo derecha. 46020 -Valencia
960 075 817 (Ext. 257) (Ext. 276) | formacion@laberit.com
formacion.laberit.com