The DevSecOps Company

Microsoft Partner

SC-100T00
Microsoft Cybersecurity Architect

Información general.

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).

Duración.

4 Días.

Perfil del público.

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.

Examen.

SC-100: Microsoft Cybersecurity Architect.

Temario.

Módulo 1: Introducción a los marcos de procedimientos recomendados y la Confianza cero.

Conozca qué son los procedimientos recomendados y cómo los usan los arquitectos de ciberseguridad, así como algunos marcos clave de procedimientos recomendados para las funcionalidades de ciberseguridad de Microsoft. También obtendrá información sobre el concepto de Confianza cero y cómo empezar a trabajar con la Confianza cero en una organización.

- Introducción a los procedimientos recomendados.
- Introducción a la Confianza cero.
- iniciativas de Confianza cero.
- Pilares tecnológicos de la Confianza cero, parte 1.
- Pilares tecnológicos de la Confianza cero, parte 2.

Al término de este módulo, sabrá hacer lo siguiente:

- Comprenda cómo usar los procedimientos recomendados como arquitecto de ciberseguridad.
- Comprenda el concepto de Confianza cero y cómo se puede usar para modernizar la ciberseguridad de las organizaciones.
- Comprenda cuándo usar los diferentes marcos de procedimientos recomendados, como MCRA, CAF y WAF.

Módulo 2: Diseño de soluciones que se alineen con Cloud Adoption Framework (CAF) y el Marco de buena arquitectura (WAF).

Obtendrá información sobre Cloud Adoption Framework (CAF) y el Marco de buena arquitectura (WAF) y cómo puede usarlos para diseñar soluciones más seguras.

- Definición de una estrategia de seguridad.
- Introducción a Cloud Adoption Framework.
- Metodología de seguridad de Cloud Adoption Framework.
- Introducción a las zonas de aterrizaje de Azure.
- Diseño de la seguridad con zonas de aterrizaje de Azure.
- Introducción al Marco de buena arquitectura.
- Pilar de seguridad del Marco de buena arquitectura.

Al final de este módulo, podrá hacer lo siguiente:

- Comprenda el marco Cloud Adoption Framework y cómo se puede usar para acelerar y proteger la migración de una organización a la nube.
- Comprenda el Marco de buena arquitectura y cómo se puede usar para diseñar soluciones en la nube que sigan sólidos principios de diseño, incluida la seguridad.

Módulo 3: Diseño de soluciones que se alineen con la Arquitectura de referencia de ciberseguridad de Microsoft (MCRA) y Microsoft Cloud Security Benchmark (MCSB).

Obtendrá información sobre la Arquitectura de referencia de ciberseguridad de Microsoft (MCRA) y Microsoft Cloud Security Benchmark (MCSB) y cómo puede utilizarlos para diseñar soluciones más seguras.

- Introducción a la Arquitectura de referencia de ciberseguridad de Microsoft y el punto de referencia de seguridad en la nube.
- Diseñar soluciones con procedimientos recomendados para funcionalidades y controles.
- Diseño de soluciones con procedimientos recomendados para la protección contra ataques.

Al término de este módulo, podrá:

Obtendrá información sobre la Arquitectura de referencia de ciberseguridad de Microsoft (MCRA) y Microsoft Cloud Security Benchmark (MCSB) para diseñar soluciones más seguras.

Módulo 4: Diseño de una estrategia de resistencia para ciberamenazas comunes, como el ransomware.

Obtendrá información sobre ciberamenazas comunes, como el ransomware, y para qué tipos de patrones de ataque se debe preparar una organización.

- Patrones comunes de ciberamenazas y ataques.
- Compatibilidad con la resistencia empresarial.
- Protección contra ransomware.
- Configuraciones para copias de seguridad y restauración seguras.
- Actualizaciones de seguridad.

Al término de este módulo, sabrá hacer lo siguiente:

- Comprender las ciberamenazas comunes, como el ransomware.
- Saber cómo admitir la resistencia empresarial
- Diseñar configuraciones para copias de seguridad y restauración seguras.
- Diseñar soluciones para administrar actualizaciones de seguridad.

Módulo 5: Caso práctico: Diseño de soluciones que se alineen con los procedimientos recomendados de seguridad y las prioridades.

Aplique sus aptitudes de arquitecto de ciberseguridad en un escenario empresarial real en el área de operaciones de seguridad, identidad y cumplimiento. Analizará los requisitos de diseño, responderá a preguntas conceptuales y técnicas y diseñará una solución para satisfacer las necesidades empresariales.

- Descripción del caso práctico.
- Respuestas de caso práctico.
- Tutorial conceptual.
- Tutorial técnico.

Aprenderá a:

- Análisis de los requisitos empresariales.
- Cómo hacer coincidir las aptitudes técnicas para satisfacer esas necesidades.
- Cómo diseñar soluciones cohesivas que incorporen todas las funciones necesarias.

Módulo 6: Diseño de soluciones para el cumplimiento normativo.

Aprenderá a interpretar y traducir los requisitos normativos en soluciones técnicas. También aprenderá a usar las funcionalidades que se encuentran en Microsoft Purview, Microsoft Priva y Defender for Cloud para el cumplimiento.

- Introducción al cumplimiento normativo.
- Traducción de los requisitos de cumplimiento en una solución de seguridad.
- Abordar los requisitos de cumplimiento con Microsoft Purview.
- Abordar los requisitos de cumplimiento con Microsoft Priva.
- Abordar los requisitos de seguridad y cumplimiento con Azure Policy.
- Evaluar el cumplimiento de la infraestructura con Defender for Cloud.

Al final de este módulo, podrá hacer lo siguiente:

- Traducción de los requisitos de cumplimiento en una solución de seguridad.
- Abordar los requisitos de cumplimiento con Microsoft Purview.
- Diseño de una solución para abordar los requisitos de privacidad con Microsoft Priva.
- Diseño de soluciones Azure Policy para abordar los requisitos de seguridad y cumplimiento.
- Evaluar el cumplimiento de la infraestructura con Microsoft Defender for Cloud.

Módulo 7: Diseño de soluciones para la administración de identidades y acceso.

Obtendrá información sobre varias estrategias para administrar identidades y el acceso a los recursos, incluidos escenarios híbridos y multinube, identidades externas y acceso condicional.

- Introducción a la administración de identidades y acceso.
- Diseño de estrategias de acceso en entornos de nube, híbridos y multinube (incluido Microsoft Entra ID).
- Diseño de una solución para identidades externas.
- Diseño de estrategias modernas de autenticación y autorización.
- Alineación del acceso condicional y la Confianza cero.
- Especificación de requisitos para proteger Active Directory Domain Services (AD DS).
- Diseño de una solución para administrar secretos, claves y certificados.

Al término de este módulo, podrá:

- Diseño de estrategias de acceso en la nube, híbridas y multinube
- Diseño de una solución para Microsoft Azure Active Directory (Azure AD), parte de Microsoft Entra
- Diseño de una solución para identidades externas
- Diseño de estrategias modernas de autenticación y autorización
- Especificación de los requisitos para proteger Active Directory Domain Services
- Diseño de una solución para administrar secretos, claves y certificados

Módulo 8: Diseño de soluciones para proteger el acceso con privilegios.

Aprenderá técnicas avanzadas para diseñar soluciones que administren el acceso con privilegios de forma eficaz.

- Introducción al acceso con privilegios.
- Modelo de acceso empresarial.
- Diseño de soluciones de gobernanza de identidad.
- Diseño de una solución para proteger la administración de inquilinos.
- Diseño de una solución para la administración de derechos de infraestructura en la nube (CIEM).
- Diseño de una solución para estaciones de trabajo de acceso con privilegios y servicios bastión.

Al término de este módulo, podrá:

- Descripción del acceso con privilegios y el modelo de acceso empresarial.
- Diseño de soluciones de gobernanza de identidad.
- Diseño de una solución para proteger la administración de inquilinos en la nube.
- Diseño de la administración de derechos de infraestructura en la nube.

Módulo 9: Diseño de soluciones para operaciones de seguridad.

Aprenderá técnicas para diseñar funcionalidades de operaciones de seguridad, como el registro, la auditoría, la Administración de eventos e información de seguridad (SIEM), la Orquestación de la seguridad y la respuesta automatizada (SOAR) y los flujos de trabajo de seguridad.

- Introducción a las operaciones de seguridad (SecOps).
- Diseño de funcionalidades de operaciones de seguridad en entornos híbridos y multinube.
- Diseño del registro y la auditoría centralizados.
- Diseño de soluciones de Administración de eventos e información de seguridad (SIEM).
- Diseño de soluciones para detección y respuesta.
- Diseño de una solución para la Orquestación de seguridad, automatización y respuesta (SOAR).
- Diseño de flujos de trabajo de seguridad.
- Diseño de la cobertura de detección de amenazas.

Al término de este módulo, podrá:

- Diseñar funcionalidades de operaciones de seguridad en entornos híbridos y multinube.
- Diseñar el registro y la auditoría centralizados.
- Diseño de soluciones de Administración de eventos e información de seguridad (SIEM).
- Diseñar una solución para la detección y respuesta que incluye Detección y respuesta extendidas (XDR).
- Diseño de una solución para la orquestación de seguridad, automatización y respuesta (SOAR).
- Diseñar flujos de trabajo de seguridad.
- Diseñar y evaluar la detección de amenazas con el marco MITRE ATT&CK.

Módulo 10: Caso práctico: diseño de funcionalidades de operaciones de seguridad, identidad y cumplimiento.

Aplique sus aptitudes de arquitecto de ciberseguridad en un escenario empresarial real en el área de operaciones de seguridad, identidad y cumplimiento. Analizará los requisitos de diseño, responderá a preguntas conceptuales y técnicas y diseñará una solución para satisfacer las necesidades empresariales.

- Descripción del caso práctico.
- Respuestas del caso práctico.
- Tutorial conceptual.
- Tutorial técnico.

Aprenderá a:

- Análisis de los requisitos empresariales.
- Cómo hacer coincidir las aptitudes técnicas para satisfacer esas necesidades.
- Cómo diseñar soluciones cohesivas que incorporen todas las funciones necesarias.

Módulo 11: Diseñar soluciones para proteger Microsoft 365.

Aprenderá a diseñar soluciones de seguridad para Exchange, Sharepoint, OneDrive y Teams.

- Introducción a la seguridad de Exchange, SharePoint, OneDrive y Teams.
- Evaluación de la posición de seguridad para las cargas de trabajo de colaboración y productividad.
- Diseño de una solución de Microsoft Defender XDR.
- Diseño de configuraciones y prácticas operativas para Microsoft 365.

Al término de este módulo, podrá:

- Evaluación de la posición de seguridad para las cargas de trabajo de colaboración y productividad.
- Diseño de una solución de Microsoft Defender XDR.
- Diseño de configuraciones y prácticas operativas para Microsoft 365.

Módulo 12: Diseño de soluciones para proteger aplicaciones.

Aprenderá a proteger las aplicaciones, las API y el proceso de desarrollo mediante técnicas como la administración de posiciones, el modelado de amenazas y el acceso seguro para las identidades de carga de trabajo.

- Introducción a la seguridad de las aplicaciones.
- Diseño e implementación de estándares para proteger el desarrollo de aplicaciones.

- Evaluación de la posición de seguridad de las carteras de aplicaciones existentes.
- Evaluación de amenazas de aplicación con modelado de amenazas.
- Diseño de la estrategia de ciclo de vida de seguridad para aplicaciones.
- Acceso seguro para identidades de carga de trabajo.
- Diseño de una solución para la administración y seguridad de API.
- Diseño de una solución para el acceso seguro a las aplicaciones.

Al término de este módulo, podrá:

- Evaluación de la posición de seguridad de las carteras de aplicaciones existentes.
- Evaluación de amenazas a aplicaciones críticas para la empresa mediante el modelado de amenazas.
- Diseño e implementación de una estrategia de ciclo de vida completo para la seguridad de las aplicaciones.
- Diseño e implementación de estándares y prácticas para proteger el proceso de desarrollo de aplicaciones.
- Diseño de una solución para la identidad de la carga de trabajo para autenticarse y acceder a los recursos en la nube de Azure.
- Diseño de una solución para la administración y seguridad de API.
- Diseño de una solución para el acceso seguro a las aplicaciones.

Módulo 13: Diseño de soluciones para proteger los datos de una organización.

Obtenga información sobre cómo diseñar soluciones que protejan los datos de una organización mediante funcionalidades como Microsoft Purview, Defender para SQL y Defender para Storage.

- Introducción a la seguridad de los datos.
- Diseño de una solución para la detección y clasificación de datos mediante Microsoft Purview.
- Diseño de una solución para la protección de los datos.
- Diseño de la seguridad de datos para cargas de trabajo de Azure.
- Diseño de la seguridad para Azure Storage.
- Diseño de una solución de seguridad con Microsoft Defender para SQL y Microsoft Defender para Storage.

Al término de este módulo, podrá:

- Diseño de una solución para la detección y clasificación de datos mediante Microsoft Purview.
- Especificación de prioridades para mitigar las amenazas a los datos.
- Diseño de una solución para proteger los datos en reposo, en tránsito y en uso.
- Diseño de una solución de seguridad para datos de cargas de trabajo de Azure.
- Diseño de una solución de seguridad para datos de Azure Storage.
- Diseño de una solución de seguridad que incluye Microsoft Defender para SQL y Microsoft Defender para Storage.

Módulo 14: Caso práctico: diseño de soluciones de seguridad para aplicaciones y datos.

Aplique sus aptitudes de arquitecto de ciberseguridad en un escenario empresarial real en el área de protección de aplicaciones y datos. Analizará los requisitos de diseño, responderá a preguntas conceptuales y técnicas y diseñará una solución para satisfacer las necesidades empresariales.

- Descripción del caso práctico.
- Respuestas del caso práctico.
- Tutorial conceptual.
- Tutorial técnico.

Aprenderá a:

- Análisis de los requisitos empresariales.
- Cómo hacer coincidir las aptitudes técnicas para satisfacer esas necesidades.
- Cómo diseñar soluciones cohesivas que incorporen todas las funciones necesarias.

Módulo 15: Especificación de los requisitos para proteger los servicios SaaS, PaaS e IaaS.

Obtenga información sobre cómo analizar los requisitos de seguridad para diferentes ofertas en la nube (SaaS, PaaS e IaaS), cargas de trabajo de IoT, cargas de trabajo de IoT, cargas de trabajo web y contenedores.

- Introducción a la seguridad de SaaS, PaaS e IaaS.
- Especificación de las líneas de base de seguridad para los servicios SaaS, PaaS e IaaS.
- Especificación de los requisitos de seguridad para cargas de trabajo web.
- Especificar los requisitos de seguridad para contenedores y la orquestación de contenedores.

Al término de este módulo, podrá:

- Especificación de las líneas de base de seguridad para los servicios SaaS, PaaS e IaaS
- Especificación de requisitos de seguridad para cargas de trabajo de IoT
- Especificación de los requisitos de seguridad para cargas de trabajo web
- Especificar los requisitos de seguridad para contenedores y la orquestación de contenedores.

Módulo 16: Diseño de soluciones para la administración de la posición de seguridad en entornos híbridos y multinube.

Aprenderá a diseñar soluciones de administración de la posición de seguridad que se integran en escenarios híbridos y multinube mediante las funcionalidades de Microsoft Defender for Cloud, Azure Arc y Microsoft Cloud Security Benchmark (MCSB).

- Introducción a la administración de la posición en entornos híbridos y multinube.
- Evaluación de la posición de seguridad mediante Microsoft Cloud Security Benchmark.
- Diseño de la administración de la posición integrada y la protección de la carga de trabajo.
- Evaluación de la posición de seguridad mediante Microsoft Defender for Cloud.
- Evaluación de la posición con la puntuación de seguridad de Microsoft Defender for Cloud.
- Diseño de las protecciones de las cargas de trabajo en la nube con Microsoft Defender for Cloud.
- Integración de entornos híbridos y multinube con Azure Arc.
- Diseño de una solución para administrar la superficie expuesta a ataques externos.

Al término de este módulo, podrá:

- Evaluación de la posición de seguridad mediante Microsoft Cloud Security Benchmark, Microsoft Defender for Cloud y las puntuaciones de seguridad.
- Diseño de soluciones integradas de administración de la posición de seguridad y protección de cargas de trabajo en entornos híbridos y multinube.
- Diseño de soluciones de protección de cargas de trabajo en la nube que usan Microsoft Defender for Cloud.

Módulo 17: Diseño de soluciones para proteger los puntos de conexión de cliente y servidor.

Aprenderá a analizar los requisitos de seguridad para distintos tipos de puntos de conexión, incluidos servidores, clientes, IoT, OT, dispositivos móviles y dispositivos insertados. Estos requisitos tendrán en cuenta diferentes plataformas y sistemas operativos y establecerán estándares para la protección de puntos de conexión, el refuerzo de la seguridad y la configuración.

- Introducción a la seguridad de los puntos de conexión.
- Especificación de los requisitos de seguridad del servidor.
- Especificación de los requisitos para dispositivos móviles y clientes.
- Especificación de los requisitos de seguridad de Internet de las cosas (IoT) y los dispositivos insertados.
- Protección de la tecnología operativa (OT) y los sistemas de control industrial (ICS) con Microsoft Defender para IoT.
- Especificación de las líneas de base de seguridad para los puntos de conexión del servidor y del cliente.
- Diseño de una solución para el acceso remoto seguro.

Al término de este módulo, podrá:

- Especificar los requisitos de seguridad para servidores.
- Especificar los requisitos de seguridad para dispositivos móviles y clientes.
- Especificación de los requisitos de seguridad para dispositivos IoT y sistemas insertados.
- Diseño de una solución para proteger la tecnología operativa (OT) y los sistemas de control industrial (ICS) mediante Microsoft Defender para IoT.
- Especificar las líneas base de seguridad para los puntos de conexión de servidor y de cliente.
- Diseño de una solución para el acceso remoto seguro.

Módulo 18: Diseño de soluciones para la seguridad de red.

Aprenderá a diseñar soluciones de red seguras mediante técnicas como la segmentación de la red, el filtrado del tráfico, la supervisión de la red y la administración de posiciones.

- Diseñar soluciones para la segmentación de la red.
- Diseñar soluciones para el filtrado del tráfico con grupos de seguridad de red.
- Diseñar soluciones para la administración de posiciones de la red.
- Diseñar soluciones para la supervisión de la red.

Al término de este módulo, podrá:

- Diseñar soluciones para la segmentación de la red.
- Diseñar soluciones para filtrar el tráfico con grupos de seguridad de red.
- Diseñar soluciones para medir la posición de la red.
- Diseñar soluciones para la supervisión de la red.

Módulo 19: Caso práctico: Diseño de soluciones de seguridad para la infraestructura.

Aplique sus aptitudes de arquitecto de ciberseguridad en un escenario empresarial real en el área de seguridad de la infraestructura. Analizará los requisitos de diseño, responderá a preguntas conceptuales y técnicas y diseñará una solución para satisfacer las necesidades empresariales.

- Descripción del caso práctico.
- Respuestas de caso práctico.
- Tutorial conceptual.
- Tutorial técnico.

Aprenderá a:

- Análisis de los requisitos empresariales.
- Cómo hacer coincidir las aptitudes técnicas para satisfacer esas necesidades.
- Cómo diseñar soluciones cohesivas que incorporen todas las funciones necesarias.