Microsoft Partner

SC-100T00
Microsoft Cybersecurity Architect

Información general.

Este es un curso avanzado, de nivel experto que prepara a los estudiantes con la experiencia necesaria para diseñar y evaluar estrategias de ciberseguridad en las siguientes áreas: Confianza Cero, Cumplimiento de Riesgos de Gobernanza (GRC), operaciones de seguridad (SecOps) y datos y aplicaciones. Los estudiantes también aprenderán a diseñar y diseñar soluciones usando principios de confianza cero y a especificar requisitos de seguridad para infraestructuras en la nube en diferentes modelos de servicio (SaaS, PaaS, IaaS).

Duración.

4 Días.

Perfil del público.

Este curso está dirigido a ingenieros experimentados en seguridad en la nube que han obtenido una certificación previa en el ámbito de la cartera de seguridad, cumplimiento e identidad. En concreto, los estudiantes deben tener experiencia y conocimientos avanzados en una amplia variedad de áreas de ingeniería de seguridad, incluyendo identidad y acceso, protección de plataformas, operaciones de seguridad, protección de datos y protección de aplicaciones. También deberían tener experiencia con implementaciones híbridas y en la nube. Los estudiantes principiantes deberían cursar el curso SC-900: Introduction to Microsoft Security, Compliance, and Identity.

Examen.

SC-100: Microsoft Cybersecurity Architect.

Temario.

Ruta de aprendizaje: Diseña soluciones que se alineen con las mejores prácticas y prioridades de seguridad.

En esta ruta aprendes a utilizar las mejores prácticas críticas de seguridad de Microsoft para mejorar la postura de seguridad de una organización, aplicar los principios de Confianza Cero y minimizar el riesgo de ataques emergentes. Los marcos de trabajo tratados incluyen el Marco de Adopción en la Nube (CAF), el Marco Bien Arquitectado (WAF) y la Arquitectura de Referencia de Ciberseguridad de Microsoft (MCRA).

Módulo 1: Introducción a Zero Trust y marcos de buenas prácticas.

Aprendes sobre las mejores prácticas y antipatrones en seguridad, el concepto de Zero Trust y sus principios rectores, así como marcos clave de buenas prácticas como CAF, WAF, MCRA y MCSB. También aprendes sobre el marco de adopción Zero Trust y cómo se relacionan entre sí.

- Describe antipatrones y mejores prácticas.
- Describe el concepto de Confianza Cero.
- Describe los marcos.
- Describe el marco de adopción de Zero Trust.
- Describe cómo se relacionan los marcos entre sí.

Módulo 2: Diseña soluciones de seguridad que se alineen con el Marco de Adopción en la Nube (CAF) y el Marco Bien Arquitecto (WAF).

Aprenderás sobre el Cloud Adoption Framework (CAF) y el Well-Architected Framework (WAF) y cómo puedes utilizarlos para diseñar soluciones más seguras.

- Entiende el Marco de Adopción en la Nube.
- Comprende la metodología segura del Marco de Adopción en la Nube.
- Entender las zonas de aterrizaje de Azure.
- Diseña seguridad con zonas de aterrizaje Azure.
- Entiende el marco bien arquitectado.
- Entiende el pilar de seguridad del Framework Bien Arquitectado.
- Evalúa una estrategia de seguridad.
- Definir una estrategia de seguridad.
- Recomienda soluciones para la seguridad y la gobernanza.
- Diseña procesos DevSecOps seguros.
- Diseña una estrategia para la adopción segura de la IA.

Módulo 3: Diseñar soluciones que se alineen con la Arquitectura de Referencia de Ciberseguridad de Microsoft (MCRA) y el benchmark de seguridad en la nube de Microsoft (MCSB).

Aprendes sobre los marcos de seguridad de Microsoft —el Marco de Adopción de Seguridad (SAF), la Arquitectura de Referencia de Ciberseguridad de Microsoft (MCRA) y el Microsoft Cloud Security Benchmark (MCSB)— y cómo utilizarlos para diseñar soluciones seguras que protejan contra amenazas internas, ataques externos, compromisos en la cadena de suministro y riesgos específicos de IA.

- Describe la Arquitectura de Referencia de Ciberseguridad de Microsoft.
- Describe el Microsoft Cloud Security Benchmark.
- Soluciones de diseño con las mejores prácticas de capacidades y controles.
- Diseñar soluciones con las mejores prácticas para protegerse contra ataques internos, externos y de la cadena de suministro.
- Diseña soluciones de IA que se alineen con el Microsoft Cloud Security Benchmark.
- Diseñar soluciones que se alineen con el marco de adopción Zero Trust.

Módulo 4: Diseñar una estrategia de resiliencia ante ransomware y otros ataques basada en las mejores prácticas de seguridad de Microsoft.

Aprendes sobre amenazas cibernéticas comunes como el ransomware y qué tipos de patrones de ataque debe afrontar una organización.

- Ciberamenazas comunes y patrones de ataque.
- Apoyar la resiliencia empresarial.
- Diseñar soluciones para mitigar ataques de ransomware, incluyendo la priorización de BCDR y el acceso privilegiado.
- Soluciones de diseño para la continuidad del negocio y recuperación ante desastres (BCDR), incluyendo copias de seguridad seguras y restauración.
- Evaluar soluciones para actualizaciones de seguridad.

Ruta de aprendizaje: Diseña capacidades de operaciones de seguridad, identidad y cumplimiento normativo.

En esta ruta prendes a diseñar soluciones para operaciones de seguridad (SecOps), gestión de identidad y accesos, acceso privilegiado y cumplimiento normativo.

Módulo 5: Soluciones de diseño para el cumplimiento normativo.

Aprende a diseñar soluciones de seguridad que respondan a los requisitos de cumplimiento normativo en entornos multicloud. Aprenderás a traducir los requisitos de cumplimiento en controles de seguridad, utilizar Microsoft Purview Compliance Manager para el cumplimiento multicloud incluyendo la gobernanza de IA, diseñar soluciones Azure Policy y evaluar el cumplimiento con Microsoft Defender for Cloud.

- Traducir los requisitos de cumplimiento en controles de seguridad.
- Consideraciones de cumplimiento de la IA.
- Diseñar una solución para cumplir con los requisitos de cumplimiento utilizando Microsoft Purview.
- Abordar los requisitos de seguridad y cumplimiento con la Política de Azure.
- Evalúa y valida la alineación con los estándares regulatorios y benchmarks utilizando Microsoft Defender for Cloud.

KeD es una empresa sustentable, Por favor no imprimas este documento si no es necesario.

Módulo 6: Soluciones de diseño para la gestión de identidad y acceso.

Diseña soluciones de gestión de identidad y acceso que protejan los recursos organizativos y faciliten la productividad. Aprende a diseñar estrategias de acceso para diferentes modelos de despliegue, permitir una colaboración externa segura, implementar autenticación moderna y proteger la infraestructura de identidad.

- Diseñar una solución para el acceso a recursos SaaS, PaaS, IaaS, híbridos y multicloud.
- Diseñar una solución para Microsoft Entra ID, incluyendo entornos híbridos y multicloud.
- Diseñar una solución para identidades externas.
- Diseñar estrategias modernas de autenticación y autorización.
- Diseñar una solución para identidades de agentes usando Microsoft Entra Agent ID.
- Diseñar políticas de Acceso Condicional para agentes de IA.
- Validar la alineación de políticas de Acceso Condicional con una estrategia de Confianza Cero.
- Especificar los requisitos para asegurar los Servicios de Dominio de Active Directory.
- Diseñar una solución para gestionar secretos, claves y certificados.

Módulo 7: Diseñar soluciones para asegurar el acceso privilegiado.

Se aprenden técnicas avanzadas para diseñar soluciones que aseguran el acceso privilegiado utilizando principios de Zero Trust, el Modelo de Acceso Empresarial y capacidades de gobernanza Microsoft Entra ID, incluyendo consideraciones para cargas de trabajo de IA y entornos multicloud.

- Acceso privilegiado seguro.
- Asignación privilegiada de roles de diseño utilizando el Modelo de Acceso Empresarial.
- Evalúa la seguridad y la gobernanza con soluciones Microsoft Entra ID.
- Diseña una solución para asegurar la administración de los inquilinos.
- Diseñar una solución para la gestión de derechos de infraestructura en la nube.
- Diseñar una solución para estaciones de trabajo de acceso privilegiado y acceso remoto.
- Evalúa una solución de gestión de revisión de acceso.

Módulo 8: Soluciones de diseño para operaciones de seguridad.

Aprendes técnicas para diseñar capacidades de operaciones de seguridad como registros, auditorías, gestión de información y eventos de seguridad (SIEM), orquestación de seguridad y respuesta automatizada (SOAR) y flujos de trabajo de seguridad.

- Describe la función de las operaciones de seguridad (SecOps).
- Monitorización de diseño para soportar entornos híbridos y multicloud.
- Diseñar soluciones para apoyar la gestión centralizada de registros y auditorías.
- Soluciones de diseño para detección y respuesta que incluyen detección y respuesta extendida (XDR) y gestión de información y eventos de seguridad (SIEM).
- Diseñar una solución para orquestación, automatización y respuesta de seguridad (SOAR).
- Diseñar y evaluar flujos de trabajo de seguridad, incluyendo respuesta a incidentes, caza de amenazas y gestión de incidentes.
- Diseñar y evaluar la cobertura de detección de amenazas utilizando matrices MITRE ATT&CK, incluyendo Cloud, Enterprise, Mobile e ICS.

Módulo 9: Modernización de la seguridad de identidad y datos (Estudio de caso interactivo).

Aplica tus habilidades de arquitecto de ciberseguridad en un escenario empresarial real centrado en la seguridad de identidad y datos. Analizar los requisitos de diseño, responder a preguntas conceptuales y técnicas y diseñar una solución que satisfaga las necesidades del negocio.

- Estudio de caso interactivo.
- Aspectos destacados de estudios de caso interactivos.

Módulo 10: Modernización del control de acceso de usuarios y resiliencia a amenazas (Estudio de caso interactivo).

Aplica tus habilidades de arquitecto de ciberseguridad en un escenario empresarial real centrado en el control de acceso de usuarios y la resiliencia a amenazas. Analizar los requisitos de diseño, responder a preguntas conceptuales y técnicas y diseñar una solución que satisfaga las necesidades del negocio.

KeD® es una marca registrada ante el Instituto Mexicano de la Propiedad Intelectual

- Estudio de caso interactivo.
- Aspectos destacados de estudios de caso interactivos.

Ruta de aprendizaje: Diseñar soluciones de seguridad para aplicaciones y datos.

En esta ruta aprende a diseñar soluciones para proteger datos y aplicaciones, incluyendo: Microsoft 365, desarrollo de aplicaciones, portafolios de aplicaciones existentes, descubrimiento y clasificación de datos con Microsoft Purview y seguridad de datos para cargas de trabajo de Azure.

Módulo 11: Evalúa soluciones para proteger Microsoft 365.

Aprendes a evaluar soluciones de seguridad para proteger Microsoft 365.

- Evalúa la postura de seguridad para la productividad y las cargas de trabajo de colaboración utilizando métricas.
- Evalúa cómo Microsoft Defender para Office 365 y Microsoft Defender para Aplicaciones en la Nube protegen las cargas de trabajo de productividad.
- Evalúa cómo Microsoft Intune protege y gestiona los endpoints.
- Evalúa soluciones para proteger datos en Microsoft 365 utilizando Microsoft Purview.
- Evalúa cómo la seguridad de los datos y los controles de cumplimiento de los datos protegen los datos organizacionales utilizados por Microsoft 365 Copilot.

Módulo 12: Soluciones de diseño para asegurar aplicaciones.

Aprendes a proteger aplicaciones, APIs y el proceso de desarrollo utilizando técnicas como la gestión de posturas, el modelado de amenazas y el acceso seguro para las identidades de cargas de trabajo.

- Diseñar e implementar estándares para asegurar el desarrollo de aplicaciones.
- Diseña una estrategia de ciclo de vida completo para la seguridad de las aplicaciones.
- Evaluar la postura de seguridad de las carteras de aplicaciones existentes.
- Evaluar amenazas de aplicaciones mediante modelado de amenazas.
- Acceso seguro para las identidades de cargas de trabajo.
- Diseñar una solución para la gestión y seguridad de las APIs.
- Diseñar una solución para el acceso seguro a las aplicaciones.
- Mapear tecnologías a los requisitos de seguridad de las aplicaciones.

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

Aprendes a diseñar soluciones que protegen los datos de una organización utilizando capacidades como Microsoft Purview, Defender for SQL, Defender for Storage.

- Principios y marcos de diseño de seguridad de datos.
- Evaluar soluciones para el descubrimiento y clasificación de datos.
- Especificar prioridades para mitigar amenazas a los datos.
- Evalúa soluciones para el cifrado de datos en reposo y en tránsito, incluyendo Azure KeyVault y el cifrado de infraestructura.
- Seguridad de datos de diseño para cargas de trabajo Azure.
- Diseñar seguridad para los datos utilizados en cargas de trabajo de IA.
- Design security for Azure Storage.
- Diseñar una solución de seguridad con Microsoft Defender para SQL y Microsoft Defender para almacenamiento.

Módulo 14: Proteger aplicaciones y datos (Estudio de caso interactivo).

Aplica tus habilidades de arquitecto de ciberseguridad en un escenario empresarial real centrado en proteger aplicaciones y datos. Analizar los requisitos de diseño, responder a preguntas conceptuales y técnicas y diseñar una solución que satisfaga las necesidades del negocio.

- Estudio de caso interactivo.
- Aspectos destacados de estudios de caso interactivos.

Ruta de aprendizaje: Diseñar soluciones de seguridad para infraestructuras.

En esta ruta aprendes a diseñar soluciones para la seguridad de

KeD es una empresa sustentable, Por favor no imprimas este documento si no es necesario.

infraestructuras. Estas soluciones de infraestructura incluyen especificar requisitos para diferentes modelos de nube, diseñar soluciones para la gestión de posturas en entornos híbridos y multicloud, y asegurar endpoints.

Módulo 15: Especificar los requisitos para asegurar los servicios SaaS, PaaS e IaaS.

Aprendes a analizar los requisitos de seguridad para diferentes ofertas de nube (SaaS, PaaS e IaaS), cargas de trabajo IoT, cargas web, contenedores y cargas de trabajo de IA.

- Especificar líneas de seguridad para servicios SaaS, PaaS e IaaS.
- Especificar requisitos de seguridad para cargas de trabajo IoT.
- Especificar requisitos de seguridad para cargas de trabajo web.
- Especificar requisitos de seguridad para contenedores y orquestación de contenedores.
- Especificar requisitos de seguridad para cargas de trabajo de IA.
- Evaluar la seguridad de las cargas de trabajo de Microsoft Foundry.

Módulo 16: Soluciones de diseño para la gestión de postura de seguridad en entornos híbridos y multicloud.

Aprendes a diseñar soluciones de gestión de postura de seguridad que se integren en escenarios híbridos y multicloud utilizando capacidades de Microsoft Defender for Cloud, Azure Arc y Microsoft Cloud Security Benchmark (MCSB).

- Evalúa la postura de seguridad utilizando Microsoft Defender for Cloud, incluyendo el benchmark de seguridad en la nube de Microsoft.
- Evalúa la postura de seguridad utilizando Microsoft Secure Score.
- Diseña soluciones integradas de gestión de postura que incluyan Microsoft Defender for Cloud en entornos híbridos y multicloud.
- Selecciona soluciones de protección de carga de trabajo en la nube en Microsoft Defender for Cloud.
- Diseña una solución para integrar entornos híbridos y multicloud utilizando Azure Arc.
- Diseñar una solución para la gestión de superficies de ataque externas de Microsoft Defender.
- Especificar requisitos y prioridades para un proceso de gestión de postura que utilice rutas de ataque Microsoft Security Exposure Management.

Módulo 17: Diseñar soluciones para asegurar los puntos finales de servidor y cliente.

Aprendes a analizar los requisitos de seguridad para diferentes tipos de endpoints, incluyendo servidores, clientes, IoT, OT, móviles y dispositivos embebidos. Estos requisitos tienen en cuenta diferentes plataformas y sistemas operativos y establecen estándares para la protección, endurecimiento y configuración de endpoints.

- Introducción a la seguridad de endpoints.
- Especificar los requisitos de seguridad para los servidores.
- Especificar los requisitos de seguridad para dispositivos móviles y clientes.
- Especificar los requisitos de seguridad para dispositivos IoT y sistemas embebidos.
- Evalúa soluciones para asegurar tecnología operativa (OT) y sistemas de control industrial (ICS) utilizando Microsoft Defender para IoT.
- Especificar líneas base de seguridad para los endpoints de servidor y cliente.
- Diseñar una solución para el acceso remoto seguro.
- Evaluar soluciones de soluciones de contraseñas de administrador local de Windows (LAPS).

Módulo 18: Soluciones de diseño para la seguridad de redes.

Aprendes a diseñar soluciones de red seguras utilizando técnicas como segmentación de red, filtrado de tráfico, monitorización de red y gestión de posturas.

- Evalúa los diseños de redes para alinearlos con los requisitos de seguridad y las mejores prácticas.
- Soluciones de diseño para segmentación de red.
- Soluciones de diseño para filtrado de tráfico con grupos de seguridad de red.
- Soluciones de diseño para la gestión de la postura de la red.
- Soluciones de diseño para la monitorización de redes.

KeD® es una marca registrada ante el Instituto Mexicano de la Propiedad Intelectual

- Evalúa soluciones que utilicen Microsoft Entra Internet Access.
- Evalúa soluciones que utilicen Microsoft Entra Private Access.

Módulo 19: Asegurar endpoints e infraestructura (Estudio de caso interactivo).

Aplica tus habilidades de arquitecto de ciberseguridad en un escenario empresarial real centrado en la seguridad de endpoints e infraestructuras. Analizar los requisitos de diseño, responder a preguntas conceptuales y técnicas y diseñar una solución que satisfaga las necesidades del negocio.

- Estudio de caso interactivo.
- Aspectos destacados de estudios de caso interactivos.