Microsoft Partner

SC-900T00
Introduction to Microsoft Security, Compliance, and Identity

Información general.

Este curso proporciona conocimientos introductorios sobre conceptos de seguridad, cumplimiento normativo e identidad, así como soluciones relacionadas de Microsoft basadas en la nube.

Duración.

1 Día.

Perfil del público.

El público de este curso busca obtener una introducción a la seguridad, el cumplimiento normativo y la identidad (SCI) en servicios de Microsoft basados en la nube y relacionados. El contenido de este curso se ajusta al ámbito objetivo del examen SC-900. Los candidatos deben estar familiarizados con Microsoft Azure y Microsoft 365 y comprender cómo las soluciones de seguridad, cumplimiento e identidad de Microsoft pueden abarcar estas áreas para ofrecer una solución integral y completa. Antes de asistir a este curso, los estudiantes deben tener:

- Comprensión general de los conceptos de redes y computación en la nube.
- Conocimientos generales de informática o cualquier experiencia general trabajando en un entorno informático.
- Comprensión general de Microsoft Azure y Microsoft 365.

Examen.

SC-900: Microsoft Security, Compliance, and Identity Fundamentals.

Temario.

Ruta de aprendizaje: Introducción a los conceptos de seguridad, cumplimiento e identidad.

Descubre conceptos fundamentales para soluciones de seguridad, cumplimiento e identidad, incluyendo responsabilidad compartida, Zero Trust, residencia de datos, el papel de los proveedores de identidad y más.

Módulo 1: Describe conceptos de seguridad y cumplimiento.

Infórmate sobre conceptos comunes de seguridad y cumplimiento que son fundamentales para las soluciones de Microsoft. Los temas incluyen la responsabilidad compartida y los modelos Zero Trust, el cifrado, la residencia y soberanía de datos, entre otros.

- Introducción.
- Describe el modelo de responsabilidad compartida.
- Describe la defensa en profundidad.
- Describe el modelo de Zero Trust.
- Describe el cifrado y el hashing.
- Describe los conceptos de gobernanza, riesgo y cumplimiento (GRC).

Módulo 2: Describe conceptos de identidad.

Aprende sobre los conceptos clave de autenticación y autorización, por qué la identidad es el nuevo perímetro de seguridad, cómo los proveedores de identidad permiten la autenticación moderna y el inicio de sesión único, el papel de los servicios de directorio y

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

Microsoft Entra ID, y cómo la federación extiende la confianza más allá de los límites organizativos.

- Definir autenticación y autorización.
- Define identidad como el perímetro de seguridad principal.
- Describe el papel del proveedor de identidad.
- Describe el concepto de servicios de directorio y Active Directory.
- Describe el concepto de federación.

Ruta de aprendizaje: Introducción a Microsoft Entra.

Microsoft Entra ID es la solución de gestión de identidad y acceso basada en la nube de Microsoft. Infórmate sobre los servicios y principios de identidad de Microsoft Entra, autenticación segura, capacidades de gestión de accesos, así como protección y gobernanza de identidad.

Módulo 3: Describe los tipos de función e identidad del ID de Microsoft Entra.

Microsoft Entra ID es la solución de gestión de identidad y acceso en la nube de Microsoft que conecta a las personas con sus aplicaciones, dispositivos y datos. Infórmate sobre las funciones y tipos de identidad soportados por Microsoft Entra ID, incluyendo las identidades de agentes para IA, identidad híbrida e identidades externas.

- Describe Microsoft Entra.
- Describe Microsoft Entra ID.
- Describe tipos de identidades.
- Describe el ID del Agente Microsoft Entra.
- Describe la identidad híbrida.
- Describe identidades externas.

Módulo 4: Describe las capacidades de autenticación del ID Microsoft Entra.

Aprende sobre las capacidades de autenticación de Microsoft Entra ID, incluida la autenticación multifactor, y cómo mejoran la seguridad. También aprenderás sobre el restablecimiento de contraseñas de autoservicio (SSPR) y las capacidades de protección y gestión de contraseñas.

- Describe los métodos de autenticación.
- Describe la autenticación multifactor.
- Describe el restablecimiento de contraseña de autoservicio.
- Describe las capacidades de protección y gestión de contraseñas.

Módulo 5: Describe las capacidades de gestión de acceso de Microsoft Entra.

Una función clave de Microsoft Entra es gestionar el acceso. Descubre la solución Security Service Edge (SSE) de Microsoft, el acceso condicional y cómo los roles de Microsoft Entra y el control de acceso basado en roles (RBAC) ayudan a las organizaciones a gestionar el acceso.

- Describe el acceso condicional.
- Describe el acceso seguro global en Microsoft Entra.
- Describe los roles de Microsoft Entra y el control de acceso basado en roles (RBAC).

Módulo 6: Describe las capacidades de protección de identidad y gobernanza de Microsoft Entra.

Microsoft Entra ofrece capacidades de protección de identidad y gobernanza. Infórmate sobre estas capacidades, sus casos de uso y sus beneficios.

- Describe la gobernanza de Microsoft Entra ID.
- Describe las revisiones de acceso.
- Describe la gestión de los derechos.
- Describe las capacidades de la Gestión de Identidad Privilegiada.
- Describe la Protección de ID de Microsoft Entra.
- Describe el ID verificado de Microsoft Entra.
- Describe la integración de Microsoft Entra con Microsoft Security Copilot.

Ruta de aprendizaje: Introducción a las soluciones de seguridad de Microsoft.

Infórmate sobre las capacidades de seguridad en Microsoft. Los temas tratados incluirán capacidades de red y plataforma como Azure, gestión de seguridad Azure y Sentinel. Aprenderás sobre protección contra amenazas con Microsoft Defender XDR y la gestión de seguridad de Microsoft 365.

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

Módulo 7: Describe Microsoft Security Copilot.

Se te introduce algo de terminología básica, cómo Microsoft Security Copilot procesa los prompts, los elementos de un prompt efectivo y cómo habilitar la solución.

- Familiarízate con Microsoft Security Copilot.
- Describe la terminología de Microsoft Security Copilot.
- Describe cómo Microsoft Security Copilot procesa las solicitudes de aviso.
- Describe los elementos de un prompt efectivo.
- Describe cómo habilitar Microsoft Security Copilot.

Módulo 8: Describe los servicios de seguridad de infraestructura central en Azure.

Infórmate sobre las capacidades que Azure ofrece para proteger tu red, máquinas virtuales y tus datos.

- Describe la protección DDoS de Azure.
- Describe Azure Firewall.
- Describe el cortafuegos de aplicaciones web.
- Describe la segmentación de red en Azure.
- Describe los grupos de seguridad de red de Azure.
- Describe Azure Bastion.
- Describe Azure Key Vault.

Módulo 9: Describe las capacidades de gestión de seguridad en Azure.

Conoce Microsoft Defender for Cloud y las capacidades que combina para proteger tu nube mediante políticas de seguridad, estándares, recomendaciones, puntuación segura, planes mejorados de protección de carga de trabajo y capacidades de seguridad en IA.

- Describe Microsoft Defender for Cloud.
- Describe cómo las políticas, estándares y recomendaciones de seguridad mejoran la postura de seguridad en la nube.
- Describe la gestión de la postura de seguridad en la nube.
- Describe la seguridad mejorada de Microsoft Defender for Cloud.
- Describe la gestión de la seguridad DevOps.

Módulo 10: Describe las capacidades de seguridad de Microsoft Sentinel.

Descubre Microsoft Sentinel: una solución escalable y nativa en la nube de gestión de información y eventos de seguridad (SIEM) y orquestación, automatización y respuesta de seguridad (SOAR). Explora cómo las capacidades de IA y aprendizaje automático ayudan a los equipos de seguridad a detectar, investigar y responder a amenazas. También te presentarán Microsoft Security Copilot y cómo se integra con Microsoft Sentinel.

- Definir los conceptos de SIEM y SOAR.
- Describe las capacidades de detección y mitigación de amenazas en Microsoft Sentinel.
- Describe la integración de Microsoft Sentinel con Microsoft Security Copilot.

Módulo 11: Describe la protección contra amenazas con Microsoft Defender XDR.

Protégete contra amenazas cibernéticas con Microsoft Defender XDR en endpoints, identidades, correo electrónico y aplicaciones.

- Describe los servicios de Microsoft Defender XDR.
- Describe Microsoft Defender para Office 365.
- Describe Microsoft Defender para Endpoint.
- Describe Microsoft Defender para aplicaciones en la nube.
- Describe Microsoft Defender para la identidad.
- Describe la gestión de vulnerabilidades de Microsoft Defender.
- Describe la inteligencia de amenazas de Microsoft Defender.
- Describe la gestión de la exposición a la seguridad de Microsoft.
- Describe el portal Microsoft Defender.
- Describe la integración de Copilot con Microsoft Defender XDR.

Ruta de aprendizaje: Introducción a Microsoft Purview y a los principios de privacidad de Microsoft.

Infórmate sobre soluciones de cumplimiento normativo en Microsoft. Los temas tratados incluirán el portal de cumplimiento de Microsoft Purview, la protección y gobernanza de la información en Microsoft 365, Insider Risk, auditoría y soluciones de eDiscovery. También se abordan las capacidades de gobernanza de recursos de Azure.

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

Módulo 12: Describe el portal Service Trust de Microsoft y los principios de privacidad.

¡Microsoft funciona con la confianza! Aquí exploras el Portal de Confianza de Servicios para encontrar contenido sobre cómo Microsoft cumple con nuestro compromiso de confianza. También aprendes sobre los principios de privacidad de Microsoft.

- Describe las ofertas del portal Service Trust.
- Describe los principios de privacidad de Microsoft.

Módulo 13: Describe las soluciones de seguridad de datos de Microsoft Purview.

Describe las soluciones de seguridad de datos de Microsoft Purview.

- Describe las capacidades de clasificación de datos de Microsoft Purview Information Protection.
- Describe las etiquetas de sensibilidad y las políticas en Microsoft Champview Information Protection.
- Describe la prevención de pérdida de datos en Microsoft Champview.
- Describe la gestión de riesgos internos en el ámbito de Microsoft.
- Describe la protección adaptativa en el ámbito de Microsoft.
- Describe la gestión de la postura de seguridad de los datos.
- Describe las investigaciones de seguridad de datos de Microsoft Purview.

Módulo 14: Describe las soluciones de cumplimiento de datos de Microsoft Purview.

Descubre cómo las soluciones de cumplimiento de datos de Microsoft Purview ayudan a las organizaciones a gestionar los requisitos de riesgos y normativas.

- Describe al Responsable de Cumplimiento.
- Describe el cumplimiento de la comunicación.
- Describe eDiscovery.
- Describe la auditoría en el ámbito de Microsoft.
- Describir la gestión del ciclo de vida de los datos.
- Describe la gestión de registros de Microsoft Purview.

Módulo 15: Describe las soluciones de gobernanza de datos de Microsoft Champview.

Infórmate sobre las soluciones de gobernanza de datos de Microsoft Purview, incluyendo Data Map y Unified Catalog, que ayudan a garantizar la calidad, seguridad y cumplimiento de los datos, al tiempo que aceleran la creación de valor.

- Describe los conceptos y beneficios de la gobernanza de datos.
- Describe el mapa de datos de Microsoft Purview.
- Describe el Catálogo Unificado de Microsoft Purview.