The DevOps Company

Microsoft Partner

SC-900T00
Microsoft Security, Compliance, and Identity Fundamentals

Sobre este curso.

Este curso proporciona conocimientos de nivel básico sobre los conceptos de seguridad, cumplimiento e identidad y las soluciones de Microsoft relacionadas basadas en la nube.

Duración.

1 Día.

Perfil del público.

El público de este curso busca familiarizarse con los aspectos básicos de la seguridad, el cumplimiento y la identidad (SCI) en los entornos basados en la nube y servicios de Microsoft relacionados. El contenido de este curso se alinea con el dominio del objetivo de examen SC-900. Esta certificación va dirigida a aquellos que buscan familiarizarse con los fundamentos de seguridad, cumplimiento e identidad (SCI) a través de los servicios basados en cloud y relacionados con Microsoft.

Requisitos previos.

Antes de asistir a este curso, los estudiantes deben tener:

- Descripción general de los conceptos relativos a la informática en la nube y las redes.
- Conocimientos generales de TI o experiencia general trabajando en un entorno de TI.
- Descripción general de Microsoft Azure y Microsoft 365.

Examen.

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

Temario.

Módulo 1: Descripción de conceptos de seguridad y cumplimiento.

Obtenga información sobre los conceptos comunes de seguridad y cumplimiento que son fundamentales para las soluciones de Microsoft. Entre estos temas, se incluyen los modelos de responsabilidad compartida y confianza cero, el cifrado, la residencia de datos y la soberanía de datos, etc.

- Descripción del modelo de responsabilidad compartida.
- Descripción de la defensa en profundidad.
- Descripción del modelo de Confianza cero.
- Descripción del cifrado y el código hash.
- Descripción de los conceptos de cumplimiento.

Tras finalizar este módulo, podrá:

- Describir la responsabilidad compartida y los modelos de seguridad para una defensa en profundidad
- Describir el modelo de Confianza cero, el cifrado y hash.
- Describir algunos conceptos básicos de cumplimiento

Módulo 2: Descripción de los conceptos de identidad.

Conozca los conceptos clave de autenticación y autorización, y por qué la identidad es importante para proteger los recursos corporativos. También aprenderá sobre servicios relacionados con la identidad.

- Definición de autenticación y autorización.
- Definición de identidad como perímetro de seguridad principal.
- Descripción del rol del proveedor de identidades.
- Descripción del concepto de servicios de directorio y Active Directory.
- Descripción del concepto de federación.

Tras finalizar este módulo, podrá:

- Entienda la diferencia entre autenticación y autorización.
- Describir el concepto de identidad como perímetro de seguridad.
- Describir los servicios relacionados con la identidad.

Módulo 3: Descripción de los servicios y los tipos de identidad de Azure AD.

Azure Active Directory (Azure AD) es un servicio de administración de acceso y de identidades basado en la nube de Microsoft. Obtenga información sobre Azure AD, sus servicios y los tipos de identidades que admite.

- Descripción de Azure Active Directory.
- Descripción de las ediciones de Azure AD disponibles.
- Descripción de los tipos de identidad de Azure AD.
- Descripción de los tipos de identidades externas.
- Descripción del concepto de identidad híbrida.

Tras finalizar este módulo, podrá:

- Describir cómo funciona Azure AD.
- Describir los tipos de identidades que admite Azure AD.

Módulo 4: Describir las funcionalidades de autenticación de Azure AD.

Obtenga información sobre las funcionalidades de autenticación de Azure AD, la autenticación multifactor y cómo estas mejoran la seguridad. Aquí también encontrará información sobre las funcionalidades de administración y protección de contraseñas de Azure AD.

- Describir los métodos de autenticación de Azure AD.
- Describir la autenticación multifactor (MFA) en Azure AD.
- Descripción del autoservicio de restablecimiento de contraseña (SSPR) en Azure AD.
- Descripción de las funcionalidades de administración y protección de contraseñas de Azure AD.

Después de completar este módulo, podrá:

- Describir los métodos de autenticación de Azure AD.
- Descripción de la autenticación multifactor en Azure AD.
- Describir las funcionalidades de administración y protección de contraseñas de Azure AD.

Módulo 5: Describir las funcionalidades de administración de acceso de Azure AD.

Una función clave de Azure AD es administrar el acceso. Obtenga información sobre las funcionalidades de administración de acceso, sus casos de uso y ventajas.

- Descripción del acceso condicional en Azure AD.
- Descripción de las ventajas de los roles de Azure AD y el control de acceso basado en roles.

Tras finalizar este módulo, podrá:

- Describir el acceso condicional en Azure AD.
- Describir las ventajas de los roles de Azure AD y el control de acceso basado en roles.

Módulo 6: Descripción de las funcionalidades de gobernanza y protección de identidades de Azure AD.

Azure AD proporciona funcionalidades de protección y gobernanza de identidades. Obtenga información sobre estas funcionalidades, sus casos de uso y sus ventajas.

- Describir la gobernanza de identidades en Azure AD.
- Descripción de qué son la administración de derechos y las revisiones de acceso.
- Descripción de las funcionalidades de Privileged Identity Management.
- Descripción de Azure AD Identity Protection.

Tras finalizar este módulo, podrá:

- Describir las funcionalidades de gobernanza de identidades en Azure.
- Describir Privileged Identity Management.
- Describir las capacidades de Azure Identity Protection.

Módulo 7: Descripción de las funcionalidades básicas de seguridad en Azure.

Obtenga información sobre las funcionalidades que admite Azure para proteger la red, las VM y los datos.

- Descripción de la protección contra DDoS de Azure.
- Descripción de Azure Firewall.
- Descripción de Web Application Firewall.
- Descripción de la segmentación de red en Azure.
- Descripción de los grupos de seguridad de red de Azure.
- Descripción del acceso JIT y Azure Bastion.
- Descripción de las maneras en que Azure cifra los datos.

Tras finalizar este módulo, podrá:

- Describir cómo las funcionalidades de seguridad de Azure pueden proteger la red.
- Describir cómo Azure puede proteger sus VM.
- Describir cómo el cifrado de Azure puede proteger sus datos.

Módulo 8: Descripción de las funcionalidades de administración de seguridad de Azure.

Obtenga información sobre la administración de la posición de seguridad en la nube y cómo Microsoft Defender for Cloud protege la nube mediante la puntuación de seguridad, las recomendaciones y las características mejoradas que protegen las cargas de trabajo en la nube. También obtendrá información sobre las líneas de base de seguridad en Azure.

- Descripción de la administración de la posición de seguridad en la nube.
- Descripción de Microsoft Defender for Cloud.
- Descripción de la seguridad mejorada de Microsoft Defender for Cloud.
- Descripción de Azure Security Benchmark y las líneas de base de seguridad para Azure.

Después de completar este módulo, podrá:

- Describa la administración de la posición de seguridad en la nube.
- Descripción de las funcionalidades de Microsoft Defender for Cloud.
- Reconocer Azure Security Benchmark y las líneas de base de seguridad de Azure.

Módulo 9: Descripción de las funcionalidades de seguridad de Microsoft Sentinel.

Obtenga información sobre Microsoft Azure Sentinel, una solución de administración de eventos de información de seguridad (SIEM) y respuesta automatizada de orquestación de seguridad (SOAR) que es escalable y nativa de la nube.

- Definición de los conceptos de SIEM y SOAR.
- Descripción de cómo Microsoft Sentinel proporciona administración contra amenazas integrada.
- Descripción de los costos de Sentinel.

Tras finalizar este módulo, podrá:

- Describir los conceptos de seguridad de SIEM y SOAR.
- Describir cómo Microsoft Sentinel proporciona administración contra amenazas integrada.
- Describir los modelos de precios de Microsoft Sentinel.

Módulo 10: Descripción de la protección contra amenazas con Microsoft 365 Defender.

Obtenga más información acerca de Microsoft 365 Defender, un conjunto unificado de defensa de la empresa que coordina la detección, la prevención, la investigación y la respuesta a través de los puntos de conexión, las identidades, el correo electrónico y las aplicaciones para proporcionar protección integrada frente a ataques sofisticados.

- Describir los servicios de Microsoft 365 Defender.
- Describir Microsoft Defender for Office 365.
- Describir Microsoft Defender para punto de conexión.
- Descripción de Microsoft Defender for Cloud Apps.
- Describir Microsoft Defender for Identity.
- Descripción del portal de Microsoft 365 Defender.

Después de completar este módulo, podrá:

- Describir el servicio de Microsoft 365 Defender.
- Describir cómo Microsoft 365 Defender proporciona protección integrada frente a ataques sofisticados.
- Describirá y explorará el portal de Microsoft 365 Defender.

Módulo 11: Descripción del Portal de confianza de servicios y de la privacidad en Microsoft.

¡Microsoft se basa en la confianza! Aquí explorará el Portal de confianza de servicios para ver contenido sobre cómo brinda Microsoft nuestro compromiso de confianza. También obtendrá información sobre Microsoft Priva, una solución para ayudar a cumplir los objetivos de privacidad.

- Descripción del Portal de confianza de servicios.
- Describir los principios de privacidad de Microsoft.
- Descripción de Microsoft Priva.

Después de completar este módulo, podrá:

- Describir las ofertas del Portal de confianza de servicios.
- Describir los principios de privacidad de Microsoft.
- Describir Microsoft Priva.

Módulo 12: Descripción de las capacidades de administración de cumplimiento en Microsoft Purview.

Explore el Portal de cumplimiento de Microsoft Purview, el portal para que las organizaciones administren sus necesidades de cumplimiento. Obtenga información sobre el Administrador de cumplimiento y la puntuación de cumplimiento, que pueden ayudar a administrar, simplificar y mejorar el cumplimiento en toda su organización.

- Descripción del Portal de cumplimiento de Microsoft Purview.
- Descripción del Administrador de cumplimiento.
- Descripción del uso y las ventajas de la puntuación de cumplimiento.

Después de completar este módulo, podrá:

- Describir el Portal de cumplimiento de Microsoft Purview.
- Describir el Administrador de cumplimiento.
- Describir el uso y las ventajas de la puntuación de cumplimiento.

Módulo 13: Descripción de la protección de la información y la administración del ciclo de vida de los datos en Microsoft Purview.

La protección de la información y la administración del ciclo de vida de los datos en Microsoft Purview ayudan a las organizaciones a clasificar, proteger y conservar sus datos donde residen y dondequiera que vayan. Obtenga información sobre las capacidades de clasificación de datos, la prevención de pérdida de datos y la gestión de registros.

- Conocimiento, protección y gobernanza de los datos.
- Descripción de las funcionalidades de clasificación de datos del portal de cumplimiento.
- Descripción de las directivas y las etiquetas de confidencialidad.
- Descripción de la prevención de la pérdida de datos.
- Descripción de las directivas y las etiquetas de retención.
- Descripción de la administración de registros.

Después de completar este módulo, podrá:

- Describir las características de clasificación de los datos.
- Describir la administración de registros.
- Describir la prevención de pérdida de datos.

Módulo 14: Descripción de las capacidades de riesgo interno en Microsoft Purview.

Los riesgos internos son una preocupación principal para las organizaciones. Estos riesgos pueden ser difíciles de identificar y mitigar. Obtenga información sobre cómo Microsoft Purview permite a las organizaciones identificar, analizar y corregir los riesgos internos antes de causar daños.

- Descripción de la gestión de riesgos internos.
- Descripción del cumplimiento de comunicaciones.
- Descripción de las barreras de información.

Después de completar este módulo, podrá:

- Descripción de la gestión de riesgos internos
- Descripción del cumplimiento de comunicaciones
- Descripción de las barreras de información

Módulo 15: Descripción de las funcionalidades de eDiscovery y de auditoría de Microsoft Purview.

Es posible que las organizaciones necesiten identificar, recopilar o auditar información por motivos legales, normativos o empresariales. Obtenga información sobre cómo las funcionalidades de eDiscovery y de auditoría de Microsoft Purview ayudan a las organizaciones a encontrar datos pertinentes rápidamente.

- Descripción de las soluciones de eDiscovery de Microsoft Purview.
- Descripción de las soluciones de auditoría de Microsoft Purview.

Después de completar este módulo, podrá:

- Describir las funcionalidades de eDiscovery de Microsoft Purview.
- Describir las funcionalidades de auditoría de Microsoft Purview.

Módulo 16: Descripción de las funcionalidades de la gobernanza de recursos en Azure.

Las funcionalidades de gobernanza de Azure proporcionan mecanismos y procesos para que las organizaciones mantengan el control sobre sus aplicaciones y recursos. Obtenga información sobre cómo Azure Policy, Blueprints y Microsoft Purview ayudan a las organizaciones a controlar sus recursos y aplicaciones.

- Descripción de Azure Policy.
- Descripción del uso de Azure Blueprints.
- Describir las funcionalidades en el portal de gobernanza de Microsoft Purview.

Después de completar este módulo, podrá:

- Describir Azure Policy.
- Describir Azure Blueprints.
- Describir Microsoft Purview.