

Cloud Security

Código: CIS-CS-001

Propuesta de Valor: CISCO

Duración: 40 Horas



Aprenda a desarrollar un programa holístico de seguridad en la nube en relación con los estándares aceptados a nivel mundial. utilizando la Guía de seguridad de Cloud Security Alliance (CSA) V.4 y las recomendaciones de Agencia de la Unión Europea para la Ciberseguridad (ENISA). También se le presentará a CSA herramienta de gobernanza, riesgo y cumplimiento para la nube: Cloud Controls Matrix (CCM).



AUDIENCIA

- Este curso de nivel introductorio a la seguridad en la nube está dirigido a estudiantes inscritos en programas de grado en tecnología en instituciones de educación superior y profesionales de TI que desean seguir una carrera en seguridad en la nube.



PRE REQUISITOS

- No se requiere experiencia laboral oficial, sin embargo, es útil que los asistentes tengan al menos una comprensión básica de los fundamentos de seguridad como firewalls, desarrollo seguro, cifrado y administración de identidad y acceso que se pueden aprender tomando el Cisco Networking Academy Introducción a los cursos de Cybersecurity y Cybersecurity Essentials.



OBJETIVOS

- El objetivo de este curso es despertar el interés del alumno en la seguridad en la nube y familiarizar el estudiante con los conceptos universales de computación en la nube. Además, el curso ofrece estudiantes con una base de conocimientos sobre la teoría de la seguridad de la computación en la nube y estudiantes familiarizados con amenazas de seguridad y mejores prácticas para proteger la nube.

 **CERTIFICACIÓN DISPONIBLE**

- Este curso prepara a los estudiantes para tomar el examen de certificado para obtener su CCSK.
- Este curso también proporciona posibles créditos de educación profesional continua (CPE).

 **CONTENIDO****1. ARQUITECTURA DE LA NUBE**

- 1.1. INTRODUCCIÓN A LA COMPUTACIÓN EN LA NUBE
- 1.2. INTRODUCCIÓN Y ARQUITECTURA DE LA NUBE
- 1.3. CARACTERÍSTICAS ESENCIALES DE LA NUBE
- 1.4. MODELOS DE SERVICIOS EN LA NUBE
- 1.5. MODELOS DE IMPLEMENTACIÓN EN LA NUBE
- 1.6. RESPONSABILIDADES COMPARTIDAS

2. SEGURIDAD DE LA INFRAESTRUCTURA PARA LA NUBE

- 2.1. INTRODUCCIÓN AL MÓDULO
- 2.2. INTRODUCCIÓN A LA SEGURIDAD DE LA INFRAESTRUCTURA PARA LA INFORMÁTICA EN LA NUBE
- 2.3. REDES DEFINIDAS POR SOFTWARE
- 2.4. SEGURIDAD DE LA RED EN LA NUBE
- 2.5. PROTECCIÓN DE LAS CARGAS DE TRABAJO INFORMÁTICAS
- 2.6. SEGURIDAD DEL PLANO DE GESTIÓN
- 2.7. CONTINUIDAD COMERCIAL Y RECUPERACIÓN ANTE DESASTRES (BCDR)

3. GESTIÓN DE RIESGOS Y SEGURIDAD EN LA NUBE

- 3.1. INTRODUCCIÓN AL MÓDULO
- 3.2. GOBERNANZA
- 3.3. GESTIÓN DE RIESGOS DE SEGURIDAD EN LA NUBE
- 3.4. CUMPLIMIENTO
- 3.5. PROBLEMAS LEGALES EN LA NUBE
- 3.6. AUDITORÍA
- 3.7. HERRAMIENTAS CSA

4. SEGURIDAD DE DATOS PARA LA COMPUTACIÓN EN LA NUBE

- 4.1. INTRODUCCIÓN AL MÓDULO
- 4.2. ALMACENAMIENTO DE DATOS EN LA NUBE

- 4.3. PROTECCIÓN DE DATOS EN LA NUBE
- 4.4. CIFRADO PARA IAAS
- 4.5. CIFRADO PARA PAAS Y SAAS
- 4.6. GESTIÓN DE CLAVES DE CIFRADO
- 4.7. OTRAS OPCIONES DE SEGURIDAD DE DATOS
- 4.8. CICLO DE VIDA DE LA SEGURIDAD DE LOS DATOS

5. SEGURIDAD DE APLICACIONES Y GESTIÓN DE IDENTIDADES PARA CLOUD COMPUTING

- 5.1. INTRODUCCIÓN AL MÓDULO
- 5.2. CICLO DE VIDA DEL DESARROLLO DE SOFTWARE SEGURO (SSDLC)
- 5.3. PRUEBAS Y EVALUACIÓN
- 5.4. DEVOPS
- 5.5. OPERACIONES SEGURAS
- 5.6. DEFINICIONES DE ADMINISTRACIÓN DE IDENTIDAD Y ACCESO
- 5.7. ESTÁNDARES DE IAM
- 5.8. IAM EN LA PRÁCTICA

6. OPERACIONES DE SEGURIDAD EN LA NUBE

- 6.1. INTRODUCCIÓN AL MÓDULO
- 6.2. SELECCIÓN DE UN PROVEEDOR DE NUBE
- 6.3. RESPUESTA A INCIDENTES
- 6.4. CONCEPTOS BÁSICOS DE SECAAS
- 6.5. CATEGORÍAS Y RECOMENDACIONES DE SECAAS
- 6.6. CONSIDERACIONES DEL DOMINIO 14
- 6.7. PREPARACIÓN PARA EL EXAMEN CCSK

★ BENEFICIOS

- Al finalizar el curso, usted podrá comprender los componentes de infraestructura en la nube.