Certified Cloud Security Engineer

CCSE

Certified Cloud Security Engineer (C|CSE) es un programa de certificación en seguridad multicloud, diseñado por expertos de la industria. Proporciona una visión integral de la seguridad en la nube y permite a los profesionales de ciberseguridad aplicar habilidades prácticas para crear, operar y defender sus entornos, independientemente de la infraestructura seleccionada.

Nuestro enfoque único en el diseño del plan de estudios permite que el contenido del C|CSE se alinee con las herramientas y técnicas de seguridad más recientes para las plataformas AWS, Azure y GCP, así como para arquitecturas privadas e híbridas. Este diseño hace que el programa C|CSE sea una combinación perfecta de formación con enfoque neutral respecto al proveedor, junto con instrucción específica y laboratorios prácticos, ofreciendo a los profesionales de ciberseguridad una experiencia de aprendizaje imparcial.

C|CSE ofrece un enfoque práctico, con más de 85 laboratorios para garantizar que los candidatos adquieran experiencia práctica que puedan aplicar inmediatamente en el entorno laboral para anticipar y superar los retos de la seguridad en la nube.

Dado que las organizaciones almacenan y procesan más datos que nunca en múltiples entornos de nube, la seguridad multi-nube es esencial para las iniciativas de ciberseguridad de las organizaciones. Según una proyección de Markets and Markets, se espera que el mercado de la seguridad multi-nube crezca hasta alcanzar los 10 500 millones de dólares en 2027, generando una demanda significativa en sectores como BFSI, salud, telecomunicaciones, tecnología, comercio minorista, comercio electrónico y otras industrias.

Objetivos del curso

- Planificar, implementar y ejecutar la seguridad de la plataforma en la nube para una organización.
- Acceder de forma segura a los recursos en la nube mediante la gestión de identidades y accesos (IAM).
- Evaluar y controlar la arquitectura de red en la nube de la organización mediante la integración de diversos controles de seguridad que ofrece el proveedor de servicios.
- Evaluar las técnicas de almacenamiento en la nube y las amenazas para los datos guardados, y comprender cómo proteger los datos en la nube frente a ataques.
- Implementar y gestionar la seguridad en la nube en diversas plataformas, como AWS, Azure y GCP.
- Comprender el modelo de responsabilidad compartida del proveedor de servicios.

- Evaluar diversos estándares de seguridad en la nube, programas de cumplimiento y funcionalidades ofrecidas por AWS, Azure y GCP, y realizar auditorías de seguridad de la computación en la nube.
- Implementar servicios de detección y respuesta ante amenazas, proporcionados por Azure, AWS y GCP para identificar riesgos en los servicios en la nube de una organización.
- Evaluar y mitigar riesgos de seguridad, amenazas y vulnerabilidades en plataformas de nube.
- Integrar las mejores prácticas para proteger los componentes de la infraestructura en la nube (red, almacenamiento, virtualización y gestión).
- Proteger las aplicaciones en la nube de la organización mediante la comprensión del ciclo de vida del desarrollo de software seguro de las aplicaciones en la nube y la implementación de controles de seguridad adicionales para mejorar la seguridad de las aplicaciones alojadas en la nube.
- Diseñar e implementar un marco GRC, un plan de respuesta ante incidentes en la nube y un plan de continuidad del negocio para los servicios en la nube.
- Utilizar los servicios y herramientas de seguridad disponibles en Azure, AWS y GCP para proteger el entorno en la nube de la organización.
- Comprender las implicaciones legales asociadas con la computación en la nube para proteger a las organizaciones.
- Implementar controles y estándares operativos para construir, operar, gestionar y mantener la infraestructura de nube.
- Comprender e implementar medidas de seguridad para entornos de nube privada, multiusuario e híbrida.

Perfil de la audiencia

El curso Certified Cloud Security Engineer (C|CSE) del EC-Council está diseñado por profesionales en seguridad en la nube, en colaboración con reconocidos expertos en la materia, para ofrecer una combinación de conceptos de seguridad en la nube, tanto independientes del proveedor como específicos de cada plataforma. Los conceptos independientes del proveedor se centran en prácticas, tecnologías, marcos de trabajo y principios de seguridad en la nube. En cambio, los

contenidos específicos de cada proveedor proporcionan habilidades prácticas que se requieren para configurar plataformas específicas, como Amazon Web Services (AWS), Azure y Google Cloud Platform (GCP). Esto proporciona a los candidatos una combinación equilibrada de conocimientos teóricos y habilidades prácticas. Además, los temas avanzados incluyen módulos sobre la protección de la infraestructura en la nube mediante la implementación de normativas y estándares para mantener la seguridad. El curso de seguridad en la nube del EC-Council está alineado con los roles y responsabilidades reales de los profesionales en seguridad en la nube, y es ideal tanto para principiantes como para especialistas en ciberseguridad con experiencia.

- Seguridad de Red: Administrador / Ingeniero / Analista
- Ciberseguridad: Ingeniero / Analista
- Nube: Administrador / Analista / Ingeniero
- Profesionales de seguridad de la información
- Profesionales certificados en CND

O cualquier otro rol que implique administración, gestión u operación de redes o entornos en la nube.

ESQUEMA DEL CURSO

Módulo 01: Introducción a la Seguridad en la Nube

Este módulo proporciona una comprensión básica de la computación en la nube y sus modelos de servicio, incluyendo las diversas amenazas y vulnerabilidades que se encuentran en la nube. Se destacan factores clave para la evaluación de proveedores de servicios y la comprensión del modelo de responsabilidad compartida en materia de seguridad. Comprender el modelo de responsabilidad compartida ofrecido por el proveedor de servicios en la nube es fundamental para configurar el entorno de la nube de manera segura y proteger los recursos organizacionales.

Módulo 02: Seguridad de Plataforma e Infraestructura en la Nube

Este módulo explica los componentes clave y las tecnologías que conforman la arquitectura de la nube, así como las diversas técnicas implicadas en la protección de los elementos multiusuario, virtualizados, físicos y lógicos del entorno de la nube. Se presentan las configuraciones necesarias para proteger el centro de datos físico. Los usuarios aprenderán las mejores prácticas para asegurar las cargas de trabajo, los recursos informáticos y las redes en la nube. Este módulo muestra el uso de distintos servicios y herramientas proporcionados para la seguridad de la red y cómputo en Azure, AWS y Google Cloud.

Módulo 03: Seguridad de Aplicaciones en la Nube

Este módulo se enfoca en la protección de aplicaciones en la nube, desde su diseño hasta su implementación. Explica los cambios en el Ciclo de Vida del Desarrollo de Software Seguro (SSDLC) en la nube. Muestra cómo las funciones de gestión de identidades y accesos (IAM) de los proveedores de servicios permiten implementar mecanismos de autenticación y autorización, y restringen el acceso no autorizado a los recursos en la nube. Enseña la implementación de controles de seguridad a lo largo del ciclo de desarrollo de software. Este módulo resalta la integración de la seguridad en DevOps y en el modelo de integración y entrega continua (CI/CD) para el desarrollo e implementación de aplicaciones en la nube. Este módulo muestra el uso de diversos servicios y herramientas de seguridad para aplicaciones en Azure, AWS y Google Cloud.

Módulo 04: Seguridad de los Datos en la Nube

La seguridad de los datos es la principal preocupación a la hora de migrar a la nube. Este módulo cubre los fundamentos del almacenamiento de datos en la nube, su ciclo de vida y los distintos controles para proteger los datos en reposo y en tránsito. Este módulo incluye características de almacenamiento de datos y diversas herramientas y servicios para proteger la información almacenada en Azure, AWS y Google Cloud.

Módulo 05: Seguridad Operativa en la Nube

Este módulo incluye los controles de seguridad para crear, implementar, operar, gestionar y mantener la infraestructura física y lógica de los entornos en la nube. Abarca los servicios, características y herramientas que AWS, Azure y Google Cloud proporcionan para la seguridad operativa.

Módulo 06: Pruebas de Penetración en la Nube

Este módulo muestra cómo implementar una metodología integral de pruebas de penetración para evaluar la seguridad de la infraestructura en la nube de una organización.

Presenta los distintos servicios y herramientas utilizados para realizar pruebas de penetración en AWS, Azure y Google Cloud.

Módulo 07: Detección y Respuesta ante Incidentes en la Nube

Un plan de respuesta ante incidentes (IR) es esencial para prevenir brechas de seguridad en la nube. Este módulo describe el ciclo de vida de la respuesta ante incidentes y destaca las consideraciones que deben tener en cuenta los responsables de la respuesta en cada fase del plan IR en un entorno de nube. Se resalta el uso de SOAR para automatizar la respuesta ante incidentes en la nube. Este módulo explora las capacidades de respuesta ante incidentes que ofrecen AWS, Azure y Google Cloud. También demuestra diversas herramientas y servicios para la detección y respuesta a incidentes.

Módulo 08: Investigación Forense en la Nube

El acceso a los datos forenses y el proceso de investigación forense en un entorno de computación en la nube difieren del proceso de investigación forense en redes. Este módulo destaca varios retos forenses en la nube y metodologías de recopilación de datos. Se muestra cómo investigar

incidentes de seguridad en la nube utilizando diversas herramientas proporcionadas por AWS, Azure y Google Cloud.

Módulo 09: Continuidad del Negocio y Recuperación ante Desastres en la Nube

La Continuidad del Negocio y la Recuperación ante Desastres (BC/DR) son fundamentales en la nube, dado que los recursos son gestionados por terceros. Este módulo enseña el papel del plan de continuidad del negocio y recuperación ante desastres en la nube. Explica las herramientas de copia de seguridad y recuperación, así como los servicios y características que ofrecen proveedores de servicios como AWS, Azure y Google Cloud para preparar y gestionar las interrupciones del servicio con el fin de garantizar la continuidad del negocio.

Módulo 10: Gobernanza, Gestión de Riesgos y Cumplimiento Normativo en la Nube

Este módulo abarca las normas, políticas y aspectos legales relacionados con la nube. Destaca diversas cuestiones legales y de cumplimiento normativo que se plantean en un entorno de nube. Analiza diversos estándares de seguridad y la planificación de auditorías en la nube. Muestra las características, servicios y herramientas disponibles en Azure, AWS y Google Cloud para facilitar el cumplimiento y la auditoría.

Módulo 11: Estándares, Políticas y Cuestiones Legales en la Nube

Este módulo destaca los estándares, políticas y cuestiones legales relacionadas con la nube. Destaca diversos aspectos legales y de cumplimiento que se plantean en un entorno de nube. Analiza diversas normas de seguridad y planificación de auditorías en la nube. Se presentan las funcionalidades, servicios y herramientas que ofrecen Azure, AWS y Google Cloud para apoyar los procesos de cumplimiento y auditoría.

Debido a las constantes actualizaciones de los contenidos de los cursos por parte del fabricante, el contenido de este temario puede variar con respecto al publicado en el sitio oficial, sin embargo, Netec siempre entregará la versión actualizada de éste.