CCSP Certified Cloud Security Professional

Duración: 40 Hrs.

Acerca de CCSP

(ISC)2 y la *Cloud Security Alliance* (CSA) desarrollaron la certificación de Profesional Certificado en Seguridad en la Nube (CCSP) para asegurar que las y os profesionales de seguridad en la nube tengan los conocimientos, habilidades y destrezas necesarias en el diseño, implementación, arquitectura, operaciones, controles y cumplimiento de los marcos regulatorios de seguridad en la nube.

Objetivos

- Describir los componentes físicos y virtuales e identificar las principales tecnologías de los sistemas basados en la nube.
- Definir las funciones y responsabilidades de los clientes, proveedores, socios, corredores y los diversos profesionales técnicos que apoyan los entornos de computación en nube.
- Identificar y explicar las cinco características necesarias para satisfacer la definición del NIST de computación en nube.
- Diferenciar entre los diversos modelos y marcos de prestación de servicios que se incorporan a la arquitectura de referencia de la computación en nube.
- Discutir las estrategias para salvaguardar los datos, clasificar los datos, garantizar la privacidad, asegurar el cumplimiento de los organismos reguladores y trabajar con las autoridades durante las investigaciones judiciales.
- Realizar un contraste entre el análisis forense en el centro de datos corporativo y los entornos de computación en nube.
- Evaluar y aplicar los controles de seguridad necesarios para garantizar la confidencialidad, la integridad y la disponibilidad en la computación en nube.
- Comparar una variedad de estrategias de continuidad de negocio/recuperación de desastres basadas en la nube y seleccionar una solución apropiada para los requerimientos específicos del negocio.
- Realizar un análisis de las diferencias entre las mejores prácticas de base y el estándar de la industria.
- Desarrollar acuerdos de nivel de servicio (SLA) para entornos de computación en la nube.
- Realizar evaluaciones de riesgos de los entornos basados en nubes existentes y propuestos.

CCSP Certified Cloud Security Professional

Duración: 40 Hrs.

Perfiles Interesados

- Arquitecto(a) de la nube
- Director(a) de Seguridad de la Información CISO
- Ingeniero(a)/Desarrollador(a)/Gerente(a)
- DevOps
- Arquitecto(a) Enterprise
- Negociador(a) de contratos de TI
- Gestor(a) de riesgos y conformidad de TI
- Administrador(a) de seguridad
- Analista de seguridad
- Arquitecto(a) de seguridad
- Consultor(a) de seguridad
- Ingeniero(a) de seguridad
- Director(a) de seguridad
- Arquitecto(a) de sistemas
- Ingeniero(a) de sistemas
- SecOps

¿Qué Incluye, este curso?

MODALIDAD VIRTUAL

- Examen de certificación
- Guía de estudio oficial digital
- Examen de práctica oficial
- Manual digital de participante
- Material digital complementario
- Constancia digital de participación oficial de (ISC)2

Requisitos de experiencia

Conocimientos generales de Tecnologías de Nube y Ciberseguridad

REQUISITOS DE CERTIFICACIÓN

- Aprobar el examen CCSP.
- 5 años de experiencia laboral acumulada en tecnología de la información, de los cuales 3 años deben ser en seguridad de la información y 1 año en 1 o más de los 6 dominios del CCSP CBK.
    - La obtención del certificado CCSK de CSA puede sustituir a un año de experiencia en uno o más de los seis ámbitos del CCSP CBK.
    - La obtención de la credencial CISSP de (ISC)2 puede sustituir a todo el requisito de experiencia CCSP

- Un candidato que no tenga la experiencia requerida puede convertirse en Asociado de (ISC)^2 aprobando el examen CSSLP. El Asociado de (ISC)2 tendrá entonces 6 años para obtener los 5 años de experiencia requerida.

➢ Cubrir la cuota de membresía de 125.00 USD.

Los certificados CCSP son válidos por tres años.
Una vez obtenida la certificación, se convierte en un miembro de la (ISC)2.
Para mantener un certificado, se requiere de un mínimo de 30 créditos de Educación Profesional Continua (CPE) cada año, es decir, un total de 90 CPE en el periodo de 3 años y el pago de una cuota de mantenimiento anual (AMF*) de 125 USD.

❖ Los miembros sólo pagan un único AMF de 125.00 USD independientemente del número de certificaciones que obtengan. La cuota para asociados es de 50.00 USD.

BENEFICIOS PERSONALES Y EMPRESARIALES
Obtener la certificación CCSP brinda credibilidad y diferenciación instantánea.
Como organización, contar con profesionales certificados en CCSP garantiza que cuenta con controles adecuados de seguridad en la nube, reduce el riesgo a través de contratos y SLAs con proveedores de servicios en la nube. Además, si está en busca de una certificación de un SGSI se beneficia en gran medida al tener en su equipo a profesionales con conocimientos sobre estándares de seguridad en la nube, permitiéndole ganar nuevos negocios.

Temario:

1. **Conceptos de nubes, arquitectura y diseño**
   a. Entender los conceptos de computación en la nube
   b. Describir la arquitectura de referencia de la nube
   c. Comprender los conceptos de seguridad relevantes para la computación en la nube
   d. Comprender los principios de diseño de la computación segura en la nube
   e. Evaluar los proveedores de servicios de nube

2. **Seguridad de datos en la nube**
    a. Describir los conceptos de datos de las nubes
    b. Diseñar e implementar arquitecturas de almacenamiento de datos en la nube
    c. Diseñar y aplicar tecnologías y estrategias de seguridad de datos
    d. Implementar el descubrimiento de datos
    e. Implementar la clasificación de datos
    f. Diseñar e implementar la gestión de derechos de información (IRM)
    g. Planificar y aplicar políticas de retención, eliminación y archivo de datos
    h. Diseñar e implementar la auditabilidad, trazabilidad y responsabilidad de los eventos de datos

3. **Seguridad de la plataforma en la nube y de la infraestructura**
    a. Comprender los componentes de la infraestructura de la nube
    b. Diseñar un centro de datos seguro
    c. Analizar los riesgos asociados a la infraestructura de la nube
    d. Controles de seguridad del diseño y del plan
    e. Planificar la recuperación de desastres (DR) y la continuidad de las actividades (BC)

4. **Seguridad de aplicaciones en la nube**
    a. Formación y sensibilización en materia de seguridad de las aplicaciones
    b. Describir el proceso del ciclo de vida del desarrollo de software seguro (SDLC)
    c. Aplicar el Ciclo de Vida del Desarrollo de Software Seguro (SDLC)
    d. Aplicar el aseguramiento y la validación del software de la nube
    e. Usar software seguro y verificado
    f. Comprender los detalles de la arquitectura de las aplicaciones en la nube
    g. Diseñar soluciones apropiadas de gestión de identidad y acceso (IAM)

5. **Operaciones de seguridad en la nube**
    a. Implementar y construir la infraestructura física y lógica para el entorno de la nube
    b. Operar la infraestructura física y lógica del entorno de la nube
    c. Gestionar la infraestructura física y lógica del entorno de la nube
    d. Aplicar controles y normas operacionales (por ejemplo, Biblioteca de Infraestructura de Tecnología de la Información (ITIL), Organización

Internacional de Normalización/Comisión Electrotécnica Internacional (ISO/ CEI) 20000-1)

e. Apoyar la investigación forense digital
f. Gestionar la comunicación con las partes pertinentes
g. Gestionar las operaciones de seguridad

6. Jurídico, riesgo y cumplimiento

a. Articular los requisitos legales y los riesgos únicos en el entorno de la nube
b. Entender los asuntos de privacidad
c. Comprender el proceso de auditoría, las metodologías y las adaptaciones necesarias para un entorno de nubes