CCSP – Certified Cloud Security Professional

Este curso de preparación oficial para la certificación CCSP® **proporciona una revisión integral del conocimiento necesario para comprender la computación en la nube y sus riesgos de seguridad de la información y estrategias de mitigación**.

Te ayudará a revisar y actualizar tus conocimientos e identificar áreas que necesitas estudiar para el examen CCSP. **El contenido se alinea y cubre de manera integral los seis dominios del Cuerpo Común de Conocimientos (CBK®) de ISC2 CCSP**, lo que garantiza la relevancia en todas las disciplinas en el campo de la ciberseguridad.

Como partners de formación de ISC2 ofrecemos el material educativo oficial desarrollado por ISC2®, para garantizar que tu capacitación sea relevante y esté actualizada. Nuestros instructores son expertos en seguridad verificados y han completado una capacitación intensiva para enseñar contenido ISC2.

Objetivos Didácticos

Después de completar este curso, el candidato será capaz de:

- Comprender los marcos legales y norma que afectan los servicios en la nube.
- Reconocer los fundamentos de los mandatos regulatorios y legislativos sobre la privacidad de datos.
- Evaluar riesgos, vulnerabilidades, amenazas y ataques en el entorno de la nube.
- Evaluar el diseño y plan de controles de seguridad de la infraestructura de la nube.
- Evaluar lo necesario para gestionar las operaciones de seguridad.
- Comprender qué controles y estándares operativos implementar.
- Describir los tipos de modelos de implementación de la nube en los tipos de modelos de nube “como servicio” disponibles actualmente.
- Identificar terminología clave y definiciones asociadas relacionadas con la tecnología de la nube. Ser capaz de establecer una terminología común para su uso dentro de un equipo o grupo de trabajo.
- Construir un business case para la adopción de la nube y ser capaz de determinar con las unidades de negocio los beneficios de la nube y las estrategias de migración a la nube.

Audiencia

Este curso de capacitación está dirigido a profesionales que tengan al menos cinco años de experiencia en TI a tiempo completo, incluidos tres años en seguridad de la información y al menos un año en seguridad en la nube, y que estén buscando la certificación CCSP para mejorar la credibilidad y la movilidad profesional. El curso es ideal para quienes trabajan en puestos tales como, entre otros:

- Consultor de seguridad
- Arquitecto de sistemas
- Ingeniero de sistemas
- Gerente de seguridad
- Arquitecto de seguridad
- Ingeniero de seguridad
- Administrador de seguridad
- Arquitecto empresarial

Dominios del curso

- Dominio 1. Conceptos, arquitectura y diseño de la nube
- Dominio 2. Gobernanza de la nube: Legal, Riesgo y Cumplimiento
- Dominio 3. Seguridad de los datos en la nube
- Dominio 4. Seguridad de infraestructura y plataforma en la nube
- Dominio 5. Seguridad de aplicaciones en la nube
- Dominio 6. Operaciones de seguridad en la nube

Metodología

Aula virtual en directo.

Duración

5 días (35 horas)

Temario del curso

1. **Conceptos, arquitectura y diseño de la nube**

- Establecer las características esenciales de la computación en la nube.
- Describir los servicios fundamentales de computación en la nube.
- Describir las arquitecturas de referencia de la computación en la nube.
- Explicar las actividades de computación en la nube.
- Comparar capacidades y modelos de servicios en la nube
- Describir los modelos de implementación de la nube.
- Resumir las características económicas de la computación en la nube.
- Evaluar las métricas de ROI y KPI de la computación en la nube
- Resumir los conceptos de seguridad de la computación en la nube.
- Describir las consideraciones de seguridad clave para cada modelo de servicio.
- Analizar documentos clave de relaciones contractuales con proveedores de servicios en la nube.

2. **Gobernanza de la nube: Legal, Riesgo y Cumplimiento**

- Explicar los problemas relacionados con los conflictos de leyes internacionales.
- Interpretar pautas para análisis forense digital.
- Identificar los fundamentos de los mandatos regulatorios/ legislativos de privacidad de datos.
- Resumir el proceso de auditoría, las metodologías y las adaptaciones listas para la nube.
- Describir la gestión de riesgos relacionados con los servicios en la nube.
- Identificar las actividades de debida diligencia/ diligencia relacionadas con los contratos de servicios.

3. **Seguridad de datos en la nube**

- Discutir conceptos de seguridad de datos en la nube.
- Describir la criptografía
- Explicar las tecnologías de clasificación y descubrimiento de datos.
- Interpretar arquitecturas de almacenamiento de datos en la nube.
- Analizar la gestión de derechos de información.

- Evaluar las estrategias de seguridad de datos en la nube.
- Comparar soluciones para políticas de retención, eliminación y archivo de datos en la nube
- Explicar conceptos básicos de seguridad en la nube.

4. **Seguridad de la infraestructura y la plataforma en la nube**

- Comparar los componentes de la infraestructura de la nube.
- Seleccionar prácticas estándar para implementar un diseño de centro de datos seguro.
- Evaluar riesgos, vulnerabilidades, amenazas y ataques en el entorno de la nube.
- Descubra componentes para planificar e implementar controles de seguridad.
- Evaluar el diseño y plan de controles de seguridad de la infraestructura de la nube.
- Evaluar soluciones apropiadas de gestión de identidad y acceso (IAM)
- Recomendar estándares de continuidad del negocio y recuperación ante desastres (BCDR)

5. **Seguridad de las aplicaciones en la nube**

- Explicar soluciones de capacitación y concientización para la seguridad de aplicaciones.
- Evaluar los desafíos en el proceso del ciclo de vida de desarrollo de software seguro (SDLC)
- Seleccionar un modelo de amenaza para proteger el desarrollo de software.
- Demostrar la garantía y validación del software en la nube.
- Elegir software seguro verificado.
- Explicar los detalles de una arquitectura de aplicación en la nube.

6. **Operaciones de seguridad en la nube**

- Analizar qué se utiliza para gestionar y operar la infraestructura física y lógica de una nube.
- ambiente
- Discutir controles y estándares operativos.
- Identificar metodologías para apoyar la ciencia forense digital.
- Identificar necesidades críticas de comunicación con las partes relevantes.
- Definir la auditabilidad, trazabilidad y responsabilidad de los eventos de datos relevantes para la seguridad.
- Seleccionar requisitos para implementar operaciones seguras-