

La certificación de referencia mundial para diseñar, gestionar y proteger datos, aplicaciones e infraestructura en entornos de nube.

¿Por qué debería asistir?

CCSP, de ISC2, acredita que el profesional tiene el conocimiento técnico y la experiencia necesarios para diseñar, gestionar y asegurar datos, aplicaciones e infraestructura en la nube aplicando las mejores prácticas, políticas y procedimientos de ciberseguridad. Es una credencial de alcance mundial, independiente de proveedores, pensada para quienes lideran la adopción segura de servicios en la nube y gestionan su riesgo y cumplimiento.

Este curso recorre los 6 dominios del Common Body of Knowledge (CBK) de CCSP según el exam outline vigente desde el 1 de agosto de 2026, que incorpora la seguridad de la inteligencia artificial y el aprendizaje automático (IA/ML), la protección de los datos de entrenamiento, Zero Trust y la cadena de suministro de software. Con el material oficial de ISC2, casos prácticos, preguntas de práctica y discusión guiada por un instructor autorizado, los participantes desarrollan el criterio que evalúa el examen CCSP.

5 días	6	100–150	Casos	Avanzado
DURACIÓN	DOMINIOS	ÍTEMS DEL EXAMEN	PRÁCTICOS Y PREGUNTAS	NIVEL



¿Quién debería participar?

Arquitectos y diseñadores de seguridad en la nube
Profesionales que diseñan arquitecturas seguras en IaaS, PaaS y SaaS, públicas, privadas o híbridas.

Ingenieros y administradores de sistemas en la nube
Responsables de implementar, operar y endurecer plataformas, contenedores e infraestructura como código.

CISO, gerentes y consultores de seguridad
Líderes que definen la estrategia, la gobernanza y la gestión de proveedores de servicios en la nube.

Auditores, analistas de riesgo y cumplimiento
Especialistas que evalúan controles, contratos, privacidad y requisitos regulatorios en la nube.

Objetivos de aprendizaje

- Comprender los conceptos, la arquitectura de referencia y los principios de diseño seguro de la computación en la nube.
- Evaluar proveedores de servicios en la nube y aplicar el modelo de responsabilidad compartida.
- Diseñar estrategias de protección de datos: cifrado, clasificación, IRM, retención y trazabilidad, incluidos los datos de IA/ML.
- Proteger la plataforma y la infraestructura de la nube, y planificar la continuidad del negocio y la recuperación ante desastres.
- Integrar la seguridad en el ciclo de vida del desarrollo de aplicaciones en la nube y en sus soluciones de IAM.
- Operar, monitorear y mantener la infraestructura física y lógica de la nube con controles y estándares operativos.
- Dar soporte a la respuesta a incidentes y a la investigación forense digital en entornos de nube.
- Gestionar los requisitos legales, la privacidad, la auditoría y los contratos con proveedores de nube.

Áreas de habilidad

Arquitectura de nube | Responsabilidad compartida | Seguridad de IA/ML | Cifrado y gestión de claves | Clasificación de datos | Contenedores e IaC | Continuidad y recuperación | SDLC seguro | IAM y Zero Trust | Operaciones de seguridad | Forense digital | Privacidad y contratos

Programa del curso

Duración: 5 días

Modalidades de formación

- **Presencial** — En aula, con instructor
- **Online** — En vivo, con instructor
- **Híbrida** — Aula y online combinadas

Módulo	Contenido
Dominio 1 Día 1	**1 Conceptos, arquitectura y diseño de la nube (17 %)** Conceptos de computación en la nube; arquitectura de referencia; conceptos de seguridad relevantes para la nube; principios de diseño seguro; evaluación de proveedores de servicios en la nube (CSP); comprensión de la inteligencia artificial y el aprendizaje automático (IA/ML).
Dominio 2 Día 2	**2 Seguridad de los datos en la nube (20 %)** Conceptos de datos en la nube; arquitecturas de almacenamiento; tecnologías y estrategias de seguridad de datos; descubrimiento y clasificación; gestión de derechos de información (IRM); retención, eliminación y archivo; auditabilidad y trazabilidad; protección de los datos de IA/ML.
Dominio 3 Día 3	**3 Seguridad de la plataforma e infraestructura en la nube (17 %)** Componentes de la infraestructura y la plataforma de nube; diseño de un centro de datos seguro; análisis de riesgos de infraestructura y plataformas; planificación e implementación de controles de seguridad; continuidad del negocio (BC) y recuperación ante desastres (DR).
Dominios 4 · 5 Día 4	**4 Seguridad de las aplicaciones en la nube (16 %)** Concienciación; SDLC seguro; garantía y validación del software; software verificado; arquitectura de aplicaciones en la nube; soluciones de IAM. **5 Operaciones de seguridad en la nube (17 %)** Construcción, operación y mantenimiento de la infraestructura física y lógica; controles operativos; forense digital; comunicación con las partes; gestión de operaciones de seguridad.
Dominio 6 Día 5	**6 Aspectos legales, riesgo y cumplimiento (13 %)** Requisitos legales y riesgos propios de la nube; privacidad; auditoría adaptada a la nube; implicaciones para la gestión de riesgos empresariales; externalización y diseño de contratos de nube. Cierre del curso: repaso integral de los 6 dominios, preguntas de práctica y estrategia para el examen CCSP.

Los dominios y sus pesos siguen el exam outline oficial de CCSP vigente desde el 1 de agosto de 2026. El reparto por día es orientativo y el instructor puede ajustarlo según el avance del grupo.

Examen y certificación

Título	Certified Cloud Security Professional (CCSP) – Exam Outline 2026
Dominios	6 dominios del CBK de CCSP
Ítems	100 a 150
Formato	Adaptativo (CAT); preguntas de opción múltiple
Duración	Hasta 3 horas
Aprobación	700 de 1000
Idioma	Inglés, chino, alemán y japonés
Plataforma	Centros de pruebas autorizados de Pearson VUE

Requisitos de elegibilidad

- Mínimo de **5 años** de experiencia laboral acumulada, remunerada y a tiempo completo en TI, de los cuales **3 años** en seguridad de la información y **1 año** en uno o más de los 6 dominios del CBK de CCSP.
- El certificado CCSK de Cloud Security Alliance sustituye 1 año de experiencia en los dominios; una certificación **CISSP** activa sustituye todo el requisito de experiencia.
- Quien aprueba el examen sin la experiencia requerida se convierte en **Associate of ISC2** y dispone de 6 años para acumularla.
- Tras aprobar: solicitud de endoso avalada por un miembro certificado de ISC2 y aceptación del Código de Ética de ISC2.

Ruta profesional ISC2

CCSP es la especialización de ISC2 en seguridad de la nube: complementa la base de CC y SSCP y el liderazgo de CISSP, cuya certificación activa exime del requisito de experiencia. Junto a CSSLP y CGRC, forma las especializaciones de ISC2.



Información general

- Material oficial de ISC2 para CCSP, incluido con el curso.
- Instructor autorizado por ISC2 y Savant Consultores como ISC2 Official Training Partner.
- Certificación acreditada por ANAB según ISO/IEC 17024.
- Vigencia de 3 años: 90 créditos CPE por ciclo y cuota anual de mantenimiento (AMF) de US$135.

ISC2 OFFICIAL TRAINING PARTNER

CCSP Certified Cloud Security Professional
ISC2 Certification