CCSP®

Certified Cloud Security Professional

An (ISC)² Certification

Esquema **del examen de certificación**

Fecha efectiva: 1 de Agosto de 2022.

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

Sobre CCSP

(ISC)² ha desarrollado la credencial de *Certified Cloud Security Professional* (CCSP) para garantizar que los profesionales de seguridad en la nube tengan los conocimientos, habilidades y capacidades necesarias en el diseño de la seguridad en la nube, la implementación, la arquitectura, las operaciones, los controles y el cumplimiento de los marcos normativos. Un CCSP aplica la experiencia en seguridad de la información a un entorno de computación en la nube y acredita competencia en arquitectura, diseño, operaciones y orquestación de servicios de seguridad en la nube. Dicha aptitud profesional se mide en función de un conjunto de conocimientos reconocidos globalmente.

Los temas incluidos en el Conjunto común de conocimientos (Common Body of Knowledge (CBK)) de CCSP garantizan su relevancia en todas las disciplinas en el campo de la seguridad en la nube. Los estudiantes que obtienen la certificación logran competencia en los siguientes seis dominios:

- Conceptos, arquitectura y diseño en la nube.
- Seguridad de datos en la nube
- Plataforma y seguridad de infraestructura en la nube
- Seguridad de aplicaciones en la nube
- Operaciones de seguridad en la nube
- Asuntos jurídicos, riesgo y cumplimiento normativo

Requisitos de experiencia previa

Los candidatos deben tener un mínimo de cinco años de experiencia laboral acumulada remunerada previa en tecnologías de la información, de los cuales tres años deben ser en seguridad de la información y un año en uno o más de los seis dominios del CBK de CCSP. La obtención del certificado CCSK de CSA equivale a un año de experiencia en uno o más de los seis dominios del CBK de CCSP. La obtención de la credencial CISSP de (ISC)² es equivalente por completo al requisito de experiencia previa como CCSP.

Un candidato que no tenga la experiencia requerida para convertirse en CCSP puede convertirse en Asociado de (ISC)² al aprobar el examen CCSP. El Asociado de (ISC)² tendrá seis años para obtener los cinco años de experiencia requeridos. Puede conocer más acerca de los requisitos de experiencia previa de CCSP y cómo dar cuenta de los trabajos de tiempo parcial y prácticas en www.isc2.org/Certifications/CCSP/experience-requirements.

Acreditación

CCSP cumple con los estrictos requisitos de la norma ANSI/ISO/IEC 17024.

Análisis de tareas laborales (JTA)

(ISC)² tiene la obligación con sus miembros de mantener la relevancia del CCSP. Realizado a intervalos regulares, el Análisis de tareas laborales (JTA) es un proceso metódico y crítico para determinar las tareas que realizan los profesionales de seguridad que se dedican a la profesión definida por el CCSP. Los resultados del JTA se utilizan para actualizar el examen. Este proceso garantiza que los candidatos sean evaluados en las áreas temáticas actuales y relevantes para las funciones y responsabilidades de los profesionales de seguridad de la información en ejercicio que se centran en las tecnologías de la nube.

Información del examen CCSP

Duración del examen	4 horas
Cantidad de preguntas	150
Formato de las preguntas	Opción múltiple
Calificación necesaria para aprobar	700 de 1000 puntos
Disponibilidad del examen	Inglés, Japonés, Chino, Coreano, Alemán, Español
Centro de examen	Pearson VUE Testing Center

Ponderación del examen para CCSP

Temas	Ponderación
1. Conceptos, arquitectura y diseño en la nube.	17%
2. Seguridad de datos en la nube	20%
3. Plataforma y seguridad de infraestructura en la nube	17%
4. Seguridad de aplicaciones en la nube	17%
5. Operaciones de seguridad en la nube	16%
6. Asuntos jurídicos, riesgo y cumplimiento normativo	13%
Total:	**100.**

Dominio 1:
Conceptos, arquitectura y diseño en la nube.

1.1 Comprender los conceptos de computación en la nube

» Definiciones de computación en la nube.

» Funciones y responsabilidades de computación en la nube (por ejemplo: cliente de servicios en la nube, proveedor de servicios en la nube, socio de servicios en la nube, agente de servicios en la nube, regulador).

» Características clave de la computación en la nube (por ejemplo: autoservicio bajo demanda, acceso a la red, multi-cliente, elasticidad y escalabilidad rápidas, agrupamiento de recursos, servicio medido).

» Tecnologías de construcción de bloques (por ejemplo: virtualización, almacenamiento, redes, bases de datos, orquestación).

1.2 Describir la arquitectura de referencia en la nube

» Actividades de computación en la nube

» Capacidades de servicios en la nube (por ejemplo: tipos de capacidad de aplicación, tipos de capacidad de plataforma, tipos de capacidad de infraestructura)

» Categorías de servicios en la nube (por ejemplo: Software como servicio (SaaS), Infraestructura como servicio (IaaS), Plataforma como servicio (PaaS))

» Modelos de implementación en la nube (por ejemplo: pública, privada, híbrida, comunidad, nube múltiple)

» Consideraciones compartidas en la nube (por ejemplo: interoperabilidad, portabilidad, reversibilidad, disponibilidad, seguridad, privacidad, resiliencia, desempeño, gobernabilidad, mantenimiento y versionado, acuerdos de niveles de servicio (SLA), capacidad de auditoría, impacto regulatorio, externalización)

» Impacto de tecnologías relacionadas (por ejemplo: ciencia de datos, aprendizaje automático, inteligencia artificial (AI), blockchain, Internet de las cosas (IoT), contenedores, computación cuántica, edge computing, computación confidencial, DevSecOps)

1.3 Comprender los conceptos de seguridad relevantes para la computación en la nube

» Administración de claves y cifrado

» Identidad y control de acceso (por ejemplo: acceso de usuario, acceso privilegiado, acceso de servicios)

» Sanitización de medios y datos (por ejemplo: sobre-escritura, borrado criptográfico)

» Seguridad en la red (por ejemplo: grupos de seguridad en la red, inspección de tráfico, geovallado, redes de confianza cero (Zero Trust))

» Seguridad de virtualización (por ejemplo: seguridad del hipervisor, seguridad de contenedores, computación efímera, tecnología sin servidor)

» Amenazas comunes

» Higiene de la seguridad (por ejemplo: parches, nivel mínimo de actualizaciones)

1.4 Comprender principios de diseño de seguridad de la computación en la nube

» Ciclo de vida de la seguridad de datos en la nube

» Plan de continuidad de negocios (BC) y plan de recuperación ante desastres (DR)

» Análisis del impacto en el negocio (BIA) (por ejemplo: análisis de costo/beneficio, retorno de la inversión (ROI))

» Requisitos funcionales de seguridad (por ejemplo: portabilidad, interoperabilidad, dependencia de un proveedor)

» Consideraciones y responsabilidades de seguridad para diferentes categorías de nubes (por ejemplo: Software como servicio (SaaS), Infraestructura como servicio (IaaS), Plataforma como servicio (PaaS))

» Patrones de diseño en la nube (por ejemplo: Principios de seguridad SANS, Well-Architected Framework, Cloud Security Alliance (CSA), arquitectura de la empresa)

» Seguridad de DevOps

1.5 Evaluar proveedores de servicio en la nube

» Verificación contra criterios (por ejemplo: Organización Internacional de Normalización (ISO)/Comisión Electrotécnica Internacional (IEC) 27017, Estándar de Seguridad de la Información de la Industria de las Tarjetas de Pago (PCI DSS))

» Certificaciones de producto de sistema/subsistema (por ejemplo: Criterios comunes (CC), Estándares federales de procesamiento de la información (FIPS) 140-2)

Dominio 2: Seguridad de datos en la nube

2.1 Describir conceptos de datos en la nube

- Fases del ciclo de vida de datos en la nube
- Dispersión de datos
- Flujo de datos

2.2 Diseñar e implementar arquitecturas de almacenamiento de datos en la nube

- Tipos de almacenamiento (por ejemplo: a largo plazo, efímero, en bruto)
- Amenazas a los tipos de almacenamiento

2.3 Diseñar y aplicar tecnologías y estrategias de seguridad de datos

- Encriptación y administración de claves
- Hashing
- Ofuscación de datos (por ejemplo: enmascaramiento, anonimización)
- Tokenización
- Prevención de pérdida de datos (DLP)
- Administración de claves, secretos y certificados

2.4 Implementar descubrimiento de datos

- Datos estructurados
- Datos no estructurados
- Datos semiestructurados
- Ubicación de datos

2.5 Planear e implementar clasificación de datos

- Políticas de clasificación de datos
- Mapeo de datos
- Etiquetado de datos

2.6 Diseñar e implementar la gestión de derechos de la información (IRM)

- Objetivos (por ejemplo: derechos sobre los datos, aprovisionamiento, modelos de acceso)
- Herramientas apropiadas (por ejemplo: expedición y revocación de certificados)

2.7 Planear e implementar la retención de datos, políticas de archivo y borrado

- Políticas de retención de datos
- Procedimientos y mecanismos de borrado de datos
- Procedimientos y mecanismos de archivo de datos
- Retención legal

2.8 Diseñar e implementar la auditabilidad, trazabilidad y responsabilidad de los eventos de datos

- Definición de fuente de eventos y requisitos de atributos de eventos (por ejemplo: identidad, dirección de protocolos de internet (IP) , geolocalización)
- Registro, almacenamiento y análisis de eventos de datos
- Cadena de custodia y no repudio

Dominio 3: Plataforma y seguridad de infraestructura en la nube

3.1 Comprender la infraestructura de datos y los componentes de la plataforma

- Entorno físico
- Redes y comunicación
- Cómputo
- Virtualización
- Almacenamiento
- Plano de administración

3.2 Diseñar un centro de datos seguro

- Diseño lógico (por ejemplo: partición de usuario, control de acceso)
- Diseño físico (por ejemplo: ubicación, compra y construcción)
- Diseño ambiental (por ejemplo: calefacción, ventilación y refrigeración (HVAC), conectividad de rutas multi-proveedor)
- Diseño resiliente

3.3 Analizar riesgos asociados con la infraestructura y plataforma en la nube

- Evaluación de riesgos (por ejemplo: identificación, análisis)
- Vulnerabilidades, amenazas y ataques en la nube
- Estrategias de mitigación de riesgo

3.4 Plan e implementación de controles de seguridad

- Protección física y ambiental (por ejemplo: en el local)
- Protección del sistema, el almacenamiento y la comunicación
- Identificación, autenticación y autorización en entornos en la nube
- Mecanismos de auditoría (por ejemplo: recopilación de registros, correlación, captura de paquetes)

3.5 Planear la continuidad del negocio (BC) y la recuperación ante desastres (DR)

- Estrategia de continuidad del negocio (BC)/recuperación ante desastres (DR)
- Requisitos del negocio (por ejemplo: tiempo objetivo de recuperación (RTO), punto objetivo de recuperación (RPO), nivel de servicio de recuperación)
- Creación, implementación y prueba del plan

Dominio 4:
Seguridad de aplicaciones en la nube

4.1 Abogar por la formación y la concienciación para la seguridad de las aplicaciones

- Fundamentos del desarrollo en la nube
- Dificultades comunes
- Vulnerabilidades comunes de la nube (por ejemplo: Proyecto abierto de seguridad de aplicaciones web (OWASP) Top-10, SANS Top-25).

4.2 Describir el proceso del ciclo de vida de desarrollo del software (SDLC)

- Requisitos del negocio
- Fases y metodologías (por ejemplo: diseño, código, prueba, mantenimiento, waterfall vs. agile).

4.3 Aplicar el ciclo de vida de desarrollo seguro del software (SDLC)

- Riesgos específicos de la nube
- Modelado de amenazas (por ejemplo: Suplantación de identidad, manipulación, repudio, Divulgación de información, denegación de servicio, elevación del privilegio (STRIDE), Daño potencial, Reproducibilidad, Capacidad de aprovechamiento, Usuarios afectados, Capacidad de descubrimiento (DREAD), Arquitectura, amenazas, ataques de superficies y mitigaciones (ATASM), Proceso para la Simulación de Ataques y Análisis de Amenazas (PASTA))
- Evitar vulnerabilidades comunes durante el desarrollo
- Código seguro (por ejemplo: Proyecto abierto de seguridad de aplicaciones web (OWASP), Estándares de Verificación de Seguridad de las Aplicaciones (ASVS), Foro de garantía de software para la excelencia en el código (SAFECode))
- Gestión de configuración de software y versiones.

4.4 Aplicar la seguridad y validación de software en la nube

- Pruebas funcionales y no funcionales
- Metodologías de pruebas de seguridad (por ejemplo: pruebas de caja blanca, pruebas de caja negra, pruebas estáticas y pruebas dinámicas, análisis de composición de software (SCA), prueba de seguridad interactiva de aplicación (IAST))
- Aseguramiento de la calidad (QA)
- Prueba de caso de abuso

4.5 Utilización de software con seguridad verificada

- Securización de interfaces de programación de aplicación (API)
- Gestión de cadena de suministro (por ejemplo: evaluación del proveedor)
- Gestión del software de terceros (por ejemplo: licenciamiento)
- Validación de software de código abierto

4.6 Comprender los detalles de la arquitectura de aplicaciones en la nube

- Componentes de seguridad adicionales (por ejemplo: Cortafuegos de aplicaciones web (WAF), Monitoreo de actividad de base de datos (DAM), Cortafuegos de lenguaje de marcas extensibles (XML), Puerta de enlace a la interfaz de programación de aplicaciones (API))
- Cifrado
- Entorno de pruebas (Sandboxing)
- Virtualización de aplicaciones y orquestación (por ejemplo: micro servicios, contenedores)

4.7 Diseñar soluciones para una gestión de identidades y acceso (IAM) apropiada

- Identidad federada
- Proveedores de identidad (IdP)
- Inicio de sesión único (SSO)
- Autenticación multifactor
- Agente de seguridad de acceso a la nube (CASB)
- Administración de secretos

Dominio 5:
Operaciones de seguridad en la nube

5.1 Construir e implementar infraestructura física y lógica para el entorno en la nube

- Requisitos de configuración de Hardware de seguridad específicos (por ejemplo: módulo de seguridad de hardware (HSM) y módulo de plataforma confiable (TPM))
- Instalación y configuración de herramientas de gestión
- Requisitos de configuración de seguridad específicos de hardware virtual (por ejemplo: red, almacenamiento, memoria, unidad central de procesamiento (CPU), hipervisor tipo 1 y 2)
- Instalación de conjuntos de herramientas de virtualización en sistema operativo (OS) invitado

5.2 Operar y mantener la infraestructura física y lógica para el entorno de nube

- Control de acceso para acceso remoto y acceso local (por ejemplo: Protocolo de escritorio remoto (RDP), acceso seguro a terminal, Intérprete de ordenes segura (SSH), mecanismos de acceso basados en consola, host bastión, cliente virtual)
- Configuración de red segura (por ejemplo: Red virtual de área local (VLAN), Seguridad en la capa de transporte (TLS), Protocolo de configuración dinámica de host (DHCP), Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC), Red privada virtual (VPN))
- Controles de seguridad de red (por ejemplo: cortafuegos, sistema de detección de intrusos (IDS), sistema de prevención de intrusos (IPS), sistema de señuelo, evaluaciones de vulnerabilidad, grupos de seguridad de red, host bastión)
- Endurecimiento del sistema operativo (OS) a través de la aplicación de lineamientos, monitoreo y soluciones (por ejemplo: Windows, Linux, VMware).
- Gestión de parches
- Estrategia de infraestructura como código (IaC)
- Disponibilidad de host en clúster (por ejemplo: programación de recursos distribuidos, optimización dinámica, clúster de almacenamiento, modo de mantenimiento, alta disponibilidad (HA))
- Disponibilidad de sistema operativo (OS) invitado
- Rendimiento y monitoreo de capacidades (por ejemplo: red, cómputo, almacenamiento, tiempo de respuesta)
- Monitoreo de hardware (por ejemplo: disco, unidad central de procesamiento (CPU), velocidad del ventilador, temperatura)
- Configuración de host y respaldo de sistema operativo (OS) invitado y restaurar funciones
- Plano de administración (por ejemplo: planificación, orquestación, mantenimiento)

5.3 Implementar controles operacionales y estándares (por ejemplo: Biblioteca de Infraestructura de Tecnologías de Información (ITIL), Organización Internacional de Normalización/Comisión Electrotécnica Internacional (ISO/IEC) 20000-1)

- » Gestión de cambio
- » Gestión de continuidad
- » Gestión de seguridad de la información
- » Gestión de mejora continua del servicio
- » Gestión de incidentes
- » Gestión de problema
- » Gestión de versiones
- » Gestión de implementación
- » Gestión de configuración
- » Gestión de nivel de servicio
- » Gestión de disponibilidad
- » Gestión de capacidad

5.4 Soporte forense digital

- » Metodologías de recolección de datos forenses
- » Gestión de evidencia
- » Recolectar, adquirir y preservar evidencia digital

5.5 Gestionar la comunicación entre las partes relevantes

- » Proveedores
- » Clientes
- » Socios
- » Reguladores
- » Otras partes interesadas

5.6 Gestión de operaciones de seguridad

- » Centro de operaciones de seguridad (SOC)
- » Monitoreo inteligente de controles de seguridad (cortafuegos, sistema de detección de intrusos (IDS), sistema de prevención de intrusos (IPS), sistema de señuelos, grupos de seguridad de red, inteligencia artificial (AI))
- » Captura de registros y análisis (por ejemplo: Gestión de evento e información de seguridad (SIEM), gestión de registro)
- » Gestión de incidentes
- » Evaluaciones de vulnerabilidades

Dominio 6:
Asuntos jurídicos, riesgo y cumplimiento normativo

6.1 Articular los requisitos legales y los riesgos únicos dentro del entorno de la nube

- Legislación internacional conflictiva
- Evaluación de riesgos legales específicos de la computación en la nube
- Marco legal y directrices
- eDiscovery (por ejemplo: Organización Internacional de Normalización/Comisión Electrotécnica Internacional (ISO/IEC) 27050, guía de Cloud Security Alliance (CSA)
- Requisitos forenses

6.2 Comprender problemas relativos a la privacidad

- Diferencias entre datos privados contractuales y regulados (por ejemplo: información médica protegida (PHI), información personal identificable (PII))
- Legislación específica de cada país con respecto a los datos privados (por ejemplo: información médica protegida (PHI), información personal identificable (PII))
- Diferencias jurisdiccionales con respecto a la privacidad de datos
- Requisitos de privacidad estándar (por ejemplo: Organización Internacional de Normalización/Comisión Electrotécnica Internacional (ISO/IEC) 27018, Principios de Privacidad generalmente aceptados (GAPP), Reglamento General de Protección de Datos (GDPR))
- Evaluaciones de impacto sobre la privacidad (PIA)

6.3 Comprender procesos de auditoría, metodologías y adaptaciones necesarias para un entorno de nube

- Controles de auditoría internos y externos
- Impacto de los requisitos de auditoría.
- Identificar los desafíos de aseguramiento de la virtualización y la nube
- Tipos de reportes de auditoría (por ejemplo: Declaración de Estándares para Compromisos de Atestiguamiento (SSAE), Control de organizaciones de servicio (SOC), Estándar Internacional para Compromisos de Aseguramiento (ISAE))
- Restricciones de las declaraciones de alcance de la auditoría (por ejemplo: Declaración de Estándares para Compromisos de Atestiguamiento (SSAE), Estándar Internacional para Compromisos de Aseguramiento (ISAE))
- Análisis de brecha (por ejemplo: análisis de control, nivel básico)
- Planificación de la auditoría
- Sistema interno de gestión de seguridad de la información
- Sistema interno de controles de seguridad de la información
- Políticas (por ejemplo: organizacional, funcional, computación en la nube)
- Identificación y participación de las partes interesadas
- Requisitos de cumplimiento especiales para las industrias altamente reguladas (por ejemplo: Corporación norteamericana de fiabilidad eléctrica /Protección de infraestructura crítica (NERC/CIP), Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA), Tecnología de la información sanitaria para la salud económica y clínica (HITECH), Industria de las tarjetas de pago (PCI))
- Impacto del modelo de distribución de tecnología de la información (TI) (por ejemplo: diversas ubicaciones geográficas y cruzar jurisdicciones legales)

6.4 Comprender las implicaciones de la nube para la gestión del riesgo empresarial

- Evaluar los programas de gestión de riesgos de los proveedores (por ejemplo: controles, metodologías, políticas, perfil de riesgo, apetito por el riesgo)
- Diferencias entre propietario/controlador de datos y custodio/procesador de datos
- Requisitos de transparencia regulatoria (por ejemplo: notificación de incumplimiento, Sarbanes-Oxley (SOX), Reglamento General de Protección de Datos (GDPR))
- Gestión del riesgo (por ejemplo: evitar, mitigar, transferir, compartir, aceptar)
- Diferentes marcos de gestión de riesgo
- Métricas para gestión de riesgo
- Evaluación del entorno de riesgo (por ejemplo: servicio, proveedor, infraestructura, negocio)

6.5 Comprender el diseño de contratación y subcontratación en la nube

- Requisitos del negocio (por ejemplo: acuerdo de nivel de servicio (SLA), acuerdo marco de servicios (MSA), declaración de trabajo (SOW))
- Gestión de proveedores (por ejemplo: evaluación de proveedores, dependencia del proveedor, viabilidad del proveedor, garantía)
- Gestión de contratos (por ejemplo: derechos de auditoría, métricas, definiciones, finalización, litigios, seguridad, cumplimiento, acceso a datos/nube, seguro de riesgo cibernético)
- Gestión de la cadena de suministro (por ejemplo: Organización Internacional de Normalización/Comisión Electrotécnica Internacional (ISO/IEC) 27036)

Información adicional del examen

Referencias suplementarias

Se alienta a los candidatos a complementar su educación y experiencia revisando los recursos relevantes que pertenecen al CBK e identificando áreas de estudio que pueden necesitar atención adicional.

Puede encontrar la lista completa de referencias suplementarias en www.isc2.org/certifications/References.

Políticas y procedimientos para tomar el examen

(ISC)² recomienda que los candidatos a CCSP revisen las políticas y procedimiento para tomar el examen con anterioridad a registrarse para el mismo. Lea la información completa en www.isc2.org/Register-for-Exam.

Información legal

Por cualquier consulta relacionada con las políticas legales de (ISC)², por favor contacte con el Departamento legal de (ISC)² en legal@isc2.org.

Consultas a:

(ISC)² Americas
Tel: +1-727-785-0189
Correo electrónico: info@isc2.org

(ISC)² Asia-Pacific
Tel: +852-5803-5662
Correo electrónico: isc2asia@isc2.org

(ISC)² EMEA
Tel: +44 (0)203-960-7800
Correo electrónico: info-emea@isc2.org