Certified
in Cybersecurity

ISC2 Certification

Esquema del examen de certificación

Fecha efectiva: 1 de septiembre de 2026

ISC2

Acerca de la Certificación en Ciberseguridad

La certificación *Certified in Cybersecurity* (CC) le demostrará a los empleadores que usted posee los conocimientos, habilidades y competencias básicas necesarias para un puesto de ciberseguridad de nivel inicial o junior. Indicará su comprensión de las prácticas recomendadas, políticas y procedimientos básicos de seguridad, así como su disposición y capacidad para aprender más y crecer en el trabajo.

El examen cubre cinco áreas.

- Principios de seguridad
- Gobernanza de la seguridad
- Conceptos de Gestión de Identidades y Accesos (IAM)
- Conceptos de seguridad en redes y en la nube
- Operaciones de seguridad y respuesta ante incidentes

Requerimientos de experiencia previa

No existen requisitos previos específicos para realizar el examen. Se recomienda que los candidatos cuenten con conocimientos básicos de Tecnologías de la Información (TI). No se requiere experiencia laboral en ciberseguridad ni ningún título o diploma formal. El siguiente paso en la carrera profesional de los candidatos sería obtener certificaciones del ISC2 de nivel de experto, las cuales requieren experiencia en el campo.

Acreditación

CC cumple los requisitos estrictos de la norma ISO/IEC 17024 del Consejo Nacional de Acreditación (ANAB) del Instituto Estadounidense de Normas Nacionales (ANSI).

Análisis de tareas laborales (JTA)

ISC2 tiene la obligación con sus miembros de mantener la relevancia de la certificación CC. Realizado a intervalos regulares, el análisis de tareas laborales (JTA por sus siglas en inglés) es un proceso metódico y crítico para determinar las tareas que llevan a cabo los profesionales de seguridad que ejercen la profesión definida por la certificación CC. Los resultados del JTA se utilizan para actualizar el examen. Este proceso garantiza que los candidatos sean evaluados en las áreas temáticas pertinentes a los roles y responsabilidades de los profesionales en ejercicio de la seguridad de la información.

Información sobre el examen CAT de CC

El examen de CC usa pruebas adaptativas computarizadas (CAT por sus siglas en inglés) para todos los exámenes en inglés, chino simplificado, japonés, alemán y español moderno. Puede obtener más información sobre el examen CAT de CC en www.ISC2.org/certifications/computerized-adaptive-testing

Duración del examen	2 horas
Número de preguntas	100 - 125
Formato de las preguntas	Preguntas de opción múltiple y avanzadas
Calificación necesaria para aprobar	700 de 1000 puntos
Disponibilidad del examen	Inglés, chino, japonés, alemán, español
Centro de examen	Pearson VUE Testing Center

Ponderación del examen CAT de CC

Áreas	Ponderación promedio
1. Principios de seguridad	24%
2. Gobernanza de la seguridad	17.3%
3. Conceptos de Gestión de Identidades y Accesos (IAM)	20%
4. Conceptos de seguridad en redes y en la nube	21.3%
5. Operaciones de seguridad y respuesta ante incidentes	17.3%
	Total: 100%

Área 1: Principios de seguridad

1.1 Comprender los conceptos de ciberseguridad

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticación, autorización y contabilidad (AAA)
- No repudio
- Privacidad

1.2 Comprender los conceptos de gestión de riesgos

- Ciclo de vida de la gestión de riesgos
- Procesos de gestión de riesgos

1.3 Comprender los conceptos de gobernanza

- Leyes y normas
- Marcos y directrices
- Políticas, normas (por ejemplo, Organización Internacional de Normalización (ISO), Centro para la Seguridad en Internet), procedimientos

1.4 Comprender los controles de ciberseguridad

- Controles técnicos
- Controles administrativos
- Controles físicos

1.5 Mantener una conducta profesional y ética

- Código de conducta profesional
- Cuidado y diligencia debidos
- Código de Ética del ISC2

Área 2: Gobernanza de la seguridad

2.1 Plan de gobernanza, riesgo y cumplimiento (GRC)

- Propósito
- Importancia
- Marcos y herramientas

2.2 Comprender la redundancia

- Continuidad del negocio (BC)
- Recuperación ante desastres (DR)

2.3 Comprender la concienciación en materia de seguridad

- Cultura organizativa (por ejemplo, importancia de la seguridad, liderazgo en materia de seguridad).
- Propósitos y conceptos (por ejemplo, ingeniería social, protección de contraseñas)

2.4 Medir la efectividad de la ciberseguridad

- Métricas clave, Indicadores clave de riesgo (KRI)
- Cuadros de mando, tarjetas de calificación, informes

Área 3: Conceptos de Gestión de Identidades y Accesos (IAM)

3.1 Comprender la gestión del ciclo de vida de identidades

- Definición de roles
- Provisión
- Revisión
- Desprovisión
- Marcos y herramientas

3.2 Comprender los controles lógicos de acceso

- Principio de privilegios mínimos (PoLP)
- Separación de funciones (SoD)
- Modelos de control de acceso

Área 4: Conceptos de seguridad en redes y en la nube

4.1 Comprender la seguridad de la red

- Conceptos (por ejemplo, modelo de Interconexión de Sistemas Abiertos (OSI), modelo de Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP), Protocolo de Internet versión 4 (IPv4), Protocolo de Internet versión 6 (IPv6), Red Privada Virtual (VPN))
- Cortafuegos (por ejemplo, puertos, aplicaciones)
- Conexiones inalámbricas (por ejemplo, Wi-Fi, Bluetooth)
- Sistemas empotrados (por ejemplo, Sistemas de Control Industrial (ICS)), Internet de las cosas (IoT)

4.2 Comprender la arquitectura de seguridad de la red

- Comprensión de la segmentación de la red (por ejemplo, zonas de cortafuegos, redes virtuales de área local (VLAN), microsegmentación).
- Defensa a profundidad
- Confianza cero (ZT)

4.3 Comprender la seguridad en la nube

- Características (por ejemplo, acceso amplio a la red, elasticidad rápida, servicio medido, autoservicio bajo demanda, agrupación de recursos)
- Modelos de servicio
- Modelos de implementación
- Modelo de seguridad compartida (por ejemplo, roles y responsabilidades)

Área 5:

Operaciones de seguridad y respuesta ante incidentes

5.1 Comprender la seguridad de los datos

» Tratamiento de datos (por ejemplo, clasificación, etiquetado, enmascaramiento y saneamiento)
» Cifrado (por ejemplo, cifrado simétrico, cifrado asimétrico, hashing, criptografía resistente al quantum)

5.2 Comprender las operaciones de seguridad

» Registro y monitoreo de eventos de seguridad
» Triaje de eventos de seguridad (por ejemplo, casos de uso de incidentes, priorización, correlación)
» Actores de la amenaza (por ejemplo, tipos, motivaciones)
» Inteligencia sobre ciberamenazas
» Marcos de amenazas

5.3 Comprender la respuesta ante incidentes (IR)

» Política de tratamiento de datos que aplica el Plan de Respuesta ante Incidentes (IRP)
» Ejercicios de respuesta ante incidentes (IR) (por ejemplo, pruebas, ejercicios de escritorio)

5.4 Comprender la protección de activos

» Gestión del ciclo de vida de los activos (por ejemplo, software y dispositivos al final de su vida útil)
» Gestión de configuraciones y cambios

5.5 Comprender las pruebas de seguridad

» Pruebas de preparación en seguridad (por ejemplo, equipos azul, púrpura y rojo)
» Pruebas de aplicaciones (por ejemplo, exploración de vulnerabilidades, análisis estático, análisis dinámico, modelos de amenazas).
» Pruebas de penetración física (por ejemplo, phishing, filtración de personas no autorizados por accesos físicos, suplantación de identidades)

Información adicional sobre el examen

Referencias complementarias

Se sugiere a los candidatos que complementen su formación y experiencia revisando los recursos pertinentes relacionados con el esquema del examen de CC e identificando las áreas de estudio que puedan requerir atención adicional.

Consulte la lista completa de referencias complementarias en ISC2.org/certifications/References.

Políticas y procedimientos para tomar el examen

ISC2 recomienda que los candidatos revisen las políticas y procedimientos del examen antes de inscribirse. Lea el desglose completo de esta información importante en ISC2.org/Register-for-Exam.

Información legal

Si tiene alguna pregunta relacionada con las políticas legales de ISC2, comuníquese con el Departamento Legal de ISC2 a través del correo legal@isc2.org.

¿Alguna pregunta?

Comuníquese con el área de Servicios para Candidatos del ISC2 en su región:

Américas

Teléfono: +1 866 331 ISC2 (4722), presione 1
Correo electrónico: membersupport@isc2.org

Asia-Pacífico

Tel: +852 5803 5662
Correo electrónico: isc2asia@isc2.org

Europa, Oriente Medio y África

Teléfono: +44 203 960 7800
Correo electrónico: info-emea@isc2.org