CC SM

Certified in Cybersecurity

Certificación de ISC2

Esquema del examen de certificación

Fecha de entrada en vigor: 1 de octubre de 2025

ISC2

Acerca de la certificación *Certified in Cybersecurity*

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
- Conceptos de continuidad de negocio (CN), recuperación ante desastres (DR) y respuesta ante incidentes
- Conceptos de control de acceso
- Seguridad de las redes
- Operaciones de seguridad

Requisitos de experiencia previa

No existen requisitos previos específicos para realizar el examen. Se recomienda que los candidatos tengan 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 de ISC2 de nivel de experto, que 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 (ATL)

ISC2 tiene la obligación con sus miembros de mantener la relevancia de la certificación CC. Realizado a intervalos regulares, el análisis de tareas laborales (ATL) 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 ATL se utilizan para actualizar el examen. Este proceso garantiza que los candidatos sean evaluados en las áreas temáticas relevantes para los roles y responsabilidades de los profesionales en ejercicio de la seguridad de la información en la actualidad.

Información sobre el examen PAC de CC

El examen de CC usa pruebas adaptativas computarizadas (PAC) para todos los exámenes en inglés, chino simplificado, japonés, alemán y español moderno. Puede obtener más información sobre el examen PAC 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 PAC de CC

Áreas	Ponderación media
1. Principios de seguridad	26 %
2. Conceptos de continuidad de negocio (CN), recuperación ante desastres (DR) y respuesta ante incidentes	10 %
3. Conceptos de control de acceso	22 %
4. Seguridad de las redes	24 %
5. Operaciones de seguridad	18 %
	Total: 100 %

Área 1: Principios de seguridad

1.1 Comprender los conceptos de seguridad de la protección de la información

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticación (ej., métodos de autenticación, autenticación multifactor (MFA))
- No repudio
- Privacidad

1.2 Comprender el proceso de gestión de riesgos

- Gestión de riesgos (ej: prioridades de riesgos, tolerancia al riesgo)
- Identificación, evaluación y tratamiento de riesgos

1.3 Comprender los controles de seguridad

- Controles técnicos
- Controles administrativos
- Controles físicos

1.4 Comprender el Código de ética de ISC2

- Código de conducta profesional

1.5 Comprender los procesos de gobernanza

- Políticas
- Procedimientos
- Normas
- Leyes y reglamentaciones

Área 2:
Conceptos de continuidad de negocio (CN), recuperación ante desastres (DR) y respuesta ante incidentes

2.1 Comprender la continuidad del negocio (CN)

- Propósito
- Importancia
- Componentes

2.2 Comprender la recuperación ante desastres (DR)

- Propósito
- Importancia
- Componentes

2.3 Comprender la respuesta ante incidentes

- Propósito
- Importancia
- Componentes

Área 3:
Conceptos de control de acceso

3.1 Comprender los controles de acceso físico

- Controles de seguridad física (ej., sistemas de tarjetas de identificación, puertas de acceso, diseño ambiental)
- Monitoreo (ej., guardias de seguridad, circuito cerrado de televisión (CCTV), sistemas de alarma, registros)
- Personal autorizado vs. personal no autorizado

3.2 Comprender los controles lógicos de acceso

- Principio del menor privilegio
- Segregación de funciones
- Control de acceso discrecional (DAC)
- Control de acceso obligatorio (MAC)
- Control de acceso basado en roles (RBAC)

Área 4: Seguridad de las redes

4.1 Comprender las redes informáticas

- Redes (ej., 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), Wi-Fi)
- Puertos
- Aplicaciones

4.2 Comprender las amenazas y los ataques a la red

- Tipos de amenazas (ej., ataque distribuido de denegación de servicio (DDoS), virus, gusanos, troyanos, intermediarios (MITM), canales laterales)
- Identificación (ej., sistema de detección de intrusos (SDI), sistema de detección de intrusos en el host (SIDH), sistema de detección de intrusos en la red (SDIR))
- Prevención (ej., antivirus, escáneres, cortafuegos, sistema de prevención de intrusos (SPI))

4.3 Comprender la infraestructura de seguridad de la red

- Local (ej., energía, centro de datos/cuartos de cableado, calefacción, ventilación y aire acondicionado (HVAC), condiciones ambientales, supresión de incendios, redundancia, memorando de entendimiento (MOU)/memorando de acuerdo (MOA))
- De diseño (ej., segmentación de redes, zonas desmilitarizadas (DMZ), redes virtuales de área local (VLAN), redes privadas virtuales (VPN), microsegmentación, defensa en profundidad, control de acceso de red (NAC), segmentación para sistemas integrados, Internet de las cosas (IoT))
- En la nube (ej., acuerdos de nivel de servicio (SLA), proveedor de servicio gestionado (MSP), software como servicio (SaaS), infraestructura como servicio (IaaS), plataforma como servicio (PaaS), nube híbrida)

Área 5: Operaciones de seguridad

5.1 Comprender la seguridad de los datos

- Cifrado (ej., simétrico, asimétrico, algoritmos hash)
- Tratamiento de los datos (ej., destrucción, retención, clasificación, etiquetado)
- Registro y monitoreo de eventos de seguridad

5.2 Comprender el refuerzo del sistema

- Gestión de la configuración (ej., líneas base, actualizaciones, parches)

5.3 Comprender las prácticas recomendadas en políticas de seguridad

- Política de gestión de datos
- Política de contraseñas
- Política de uso aceptable (AUP)
- Política de "traiga su propio dispositivo" (*Bring Your Own Device*, BYOD)
- Política de gestión del cambio (ej., documentación, aprobación, reversión)
- Política de privacidad

5.4 Comprender la capacitación sobre concienciación en materia de seguridad

- Propósitos y conceptos (ej., ingeniería social, protección de contraseñas)
- Importancia

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 de examen de CC e identificando las áreas de estudio que puedan requerir atención adicional.

Consulte la lista completa de referencias complementarias en www.isc2.org/certifications/References.

Políticas y procedimientos de 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 www.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 de ISC2 en su región:

América

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