Certified in Cybersecurity

An (ISC)² Certification

Esquema **del examen de certificación**

Fecha efectiva: 29 de Agosto de 2022

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

Acerca de la Certificación en Ciberseguridad

La certificación en ciberseguridad (CC) demostrará a los empleadores que tiene los conocimientos básicos, las habilidades y las capacidades necesarias para un puesto de ciberseguridad de nivel inicial o junior. Señalará su comprensión de las mejores prácticas, políticas y procedimientos fundamentales de seguridad, así como su disposición y capacidad para aprender más y crecer en la función.

El examen cubre cinco dominios.

- Principios de seguridad
- Conceptos de continuidad del negocio (BC), recuperación ante desastres (DR) y respuesta ante incidentes
- Conceptos de Control de Acceso
- Seguridad de Red
- Operaciones de seguridad

Requisitos de experiencia previa

No existen requisitos previos específicos para rendir el examen. Se recomienda que los candidatos tengan conocimientos básicos de tecnología de la información (TI). No se requiere experiencia laboral en ciberseguridad ni ningún diploma/título educativo formal. El siguiente paso en la carrera del candidato sería obtener certificaciones de nivel experto (ISC)² , que requieren experiencia en el campo.

Análisis de tareas laborales (JTA)

(ISC)² tiene la obligación con sus miembros de mantener la relevancia del CC. 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 CC. 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 la actualidad.

Información del examen CC

Duración del examen	2 horas
Cantidad de preguntas	100
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 CC

Dominios	Ponderación promedio
1. Principios de seguridad	26%
2. Continuidad del negocio (BC), Recuperación ante Desastres (DR) y Conceptos de Respuesta ante Incidentes	10%
3. Conceptos de Control de Acceso	22%
4. Seguridad de Red	24%
5. Operaciones de Seguridad	18%
Total:	**100%**

Dominio 1:
Principios de seguridad

1.1 Comprender los conceptos de seguridad de la información

» Confidencialidad
» Integridad
» Disponibilidad
» Autenticación (ej: métodos de autenticación, autenticación multifactor (MFA))
» No rechazo
» No repudio

1.2 Comprender el proceso de gestión de riesgo

» Gestión del riesgo (ej: prioridad de riesgos, tolerancia de riesgos)
» Identificación, evaluación y tratamiento del riesgo

1.3 Comprender controles de seguridad

» Controles técnicos
» Controles administrativos
» Controles físicos

1.4 Comprender el Código de Ética (ISC)²

» Código de conducta profesional

1.5 Comprender procesos de gobernanza

» Políticas
» Procedimientos
» Estándares
» Regulaciones y leyes

Dominio 2:

Conceptos de Continuidad del Negocio (BC), Recuperación ante Desastres (DR) y Respuesta ante Incidentes

2.1 Comprender la continuidad del negocio(BC)

» Propósito
» Importancia
» Componentes

2.2 Comprender la recuperación ante desastres (DR)

» Propósito
» Importancia
» Componentes

2.3 Comprender los conceptos de Respuesta ante incidentes

» Respuesta
» Importancia
» Componentes

Dominio 3:

Conceptos de Control de Acceso

3.1 Comprender los controles de acceso físico

» Controles de seguridad físicos (ej. sistema de identificación con tarjetas, puerta de entrada, diseño ambiental)
» Monitoreo (ej. guardias de seguridad, circuito cerrado de televisión (CCTV), sistema de alarma, registros)
» Personal autorizado versus personal no autorizado

3.2 Comprender los controles de acceso lógicos

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

Dominio 4:
Seguridad de Red

4.1 Comprender redes informáticas

» Redes (ej. modelo de Interconexión de sistemas abiertos (OSI), modelo Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP), Protocolo de internet versión 4 (IPv4), Protocolo de internet versión 6 (IPv6), WiFi)

» Puertos

» Aplicaciones

4.2 Comprender las amenazas y los ataques de red

» Tipos de amenazas (ej. denegación de servicio distribuido (DDOS), virus, gusano, troyano, intermediario (MITM), canal lateral)

» Identificación (ej. sistema de detección de intrusos (IDS), sistema de detección de intrusos en un host (HIDS), sistema de detección de intrusos de red (NIDS))

» Prevención (ej. antivirus, escaneos, cortafuegos, sistema de prevención de intrusos (IPS))

4.3 Comprender la infraestructura de seguridad de red

» En las instalaciones (ej. energía, centro/armario de datos, calefacción, ventilación, aire acondicionado (HVAC), ambiente, extinción de incendios, redundancia, memorándum de entendimiento (MOU)/ memorandum de acuerdo (MOA))

» Diseño (ej. segmentación de redes (zona desmilitarizada (DMZ), red virtual de área local (VLAN), red privada virtual (VPN), micro segmentación), defensa en profundidad, Control de Acceso de Red (NAC) (segmentación de sistemas integrados, Internet de las Cosas (IoT))

» Nube (ej. Acuerdo de Nivel de Servicio (SLA), Proveedor de Servicio Gestionado (MSP), Software como Servicio (SaaS), Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS), híbrido)

Dominio 5:
Operaciones de seguridad

5.1 Comprender la seguridad de datos

» Cifrado (ej. simétrico, asimétrico, hashing)
» Gestión de datos (ej. destrucción, retención, clasificación, etiquetado)
» Registro y monitoreo de eventos de seguridad

5.2 Comprender el fortalecimiento del sistema

» Gestión de configuración (ej. nivel de base, actualizaciones, parches)

5.3 Comprender las mejores prácticas en políticas de seguridad

» Política de gestión de datos
» Política de contraseñas
» Política de uso aceptable (AUP)
» Política de traer tu propio dispositivo (BYOD)
» Política de gestión de cambio (ej. documentación, aprobación, reversión)
» Política de privacidad

5.4 Comprender formación en concientización en materia de seguridad

» Propósito/conceptos (ej. ingeniería social, protección de claves)
» Importancia

Información adicional del examen

Políticas y Procedimientos Para Tomar el Examen

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

Información Legal

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

Consultas Generales:

Contacte con el servicio a candidatos (ISC)² de su región:

Américas

Teléfono: +1-866-331-ISC2 (4722)
Correo electrónico: info@isc2.org

Asia y Pacífico

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

Europa, Medio Oriente y África

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