CISSP®

Certified Information Systems Security Professional

ISC2 Certification

Esquema del **Examen de Certificación**

Fecha efectiva: 15 de abril de 2024

ISC2™

Acerca de la certificación CISSP

La certificación del Certified Information Systems Security Professional (CISSP) es la certificación más reconocida a nivel mundial en el mercado de seguridad de la información. La certificación CISSP valida a profundidad el conocimiento y la experiencia técnica y administrativa de un profesional de seguridad de la información para diseñar, desarrollar y gestionar de manera efectiva la postura general en temas de seguridad que posee una organización.

El amplio espectro de temas incluidos en el cuerpo de conocimientos de la certificación CISSP garantiza su relevancia multidisciplinaria en el campo de la seguridad de la información. Los candidatos seleccionados son competentes en los siguientes ocho dominios:

- Seguridad y gestión del riesgo
- Seguridad de activos
- Arquitectura e ingeniería de la seguridad
- Seguridad de comunicaciones y redes
- Gestión de identidades y accesos (IAM)
- Evaluación y pruebas de seguridad
- Operaciones de seguridad
- Seguridad del desarrollo de software

Requerimientos de experiencia

Los candidatos deben tener un mínimo de cinco años de experiencia acumulada a tiempo completo en dos o más de los ocho dominios del esquema actual del examen para la certificación CISSP. Obtener un título universitario (licenciatura o maestría) en ciencias de la computación, tecnología de la información (TI) o campos relacionados puede equiparar hasta un año de la experiencia requerida. De igual manera, una acreditación adicional de la lista aprobada por la ISC2 puede equiparar hasta un año de la experiencia requerida. El trabajo a tiempo parcial y las pasantías también cuentan para el requisito de experiencia.

Un candidato que no cuente con la experiencia requerida para convertirse en un CISSP puede convertirse en un socio de la ISC2 al aprobar con éxito el examen de certificación CISSP. El socio de la ISC2 tendrá seis años para obtener los cinco años de experiencia requeridos. Puede obtener más información sobre los requerimientos de experiencia para el CISSP y cómo contabilizar el trabajo a tiempo parcial y las pasantías en www.isc2.org/Certifications/CISSP/experience-requirements.

Acreditación

La certificación CISSP fue la primera acreditación en el campo de la seguridad de la información que cumplió con los estrictos requisitos impuestos por la norma ANSI/ISO/IEC 17024.

Análisis de tareas laborales (JTA)

La ISC2 tiene la obligación con sus miembros de mantener la relevancia la certificación CISSP CISSP. 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 participan en la profesión definida por el CISSP. Los resultados del JTA 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 de seguridad de la información de la actualidad.

Información de los exámenes CAT para la certificación CISSP

El examen para la certificación CISSP utiliza pruebas adaptativas por computadora (CAT) para todos los exámenes en inglés, alemán, español moderno, japonés y chino simplificado. Puede obtener más información sobre las pruebas CAT para la certificacción CISSP en www.isc2.org/certificatons/CISSP-CAT.

Duración del examen	3 horas
Número de preguntas	100 - 150
Formato de las preguntas	Opciones múltiples y preguntas avanzadas innovadoras
Nota mínima de aprobación	700 de 1000 puntos
Disponibilidad de idiomas del examen	Chino, inglés, alemán, japonés, español
Centro de pruebas	Centros de pruebas PPC y PVTC (Pearson VUE) seleccionados y autorizados por la ICS2

Pesos de las pruebas CAT para la certificación CISSP

Dominios	Peso promedio
1. Seguridad y gestión del riesgo	16%
2. Seguridad de activos	10%
3. Arquitectura e ingeniería de la seguridad	13%
4. Seguridad de comunicaciones y redes	13%
5. Gestión de identidades y accesos (IAM)	13%
6. Evaluación y pruebas de seguridad	12%
7. Operaciones de seguridad	13%
8. Seguridad del desarrollo de software	10%
Total:	**100%**

Dominio 1: Seguridad y gestión del riesgo

1.1 Comprender, respetar y promover la ética profesional

- Código de ética profesional de la ISC2
- Código de ética organizacional

1.2 Comprender y aplicar conceptos de seguridad

- Confidencialidad, integridad y disponibilidad, autenticidad y no repudio (los 5 pilares de la seguridad de la información)

1.3 Evaluar y aplicar principios de gobernanza de la seguridad

- Alineación de la función de seguridad con las estrategias, metas, la misión y los objetivos comerciales
- Procesos organizacionales (por ejemplo: adquisiciones, cesiones, comités de gobernanza)
- Roles y responsabilidades organizacionales
- Marcos de control de seguridad (por ejemplo: la Organización Internacional de Normalización (ISO), el Instituto Nacional de Estándares y Tecnología (NIST), los Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT), la Arquitectura de Seguridad Empresarial Aplicada de Sherwood (SABSA), la Industria de Tarjetas de Pago (PCI), el Programa Federal de Gestión de Autorizaciones y Riesgos (FedRAMP))
- Debida diligencia/cuidado

1.4 Comprender los problemas legales, regulatorios y de cumplimiento relacionados con la seguridad de la información en un contexto holístico

- Delitos cibernéticos y filtraciones de datos
- Requerimientos de licenciamiento y propiedad intelectual
- Controles de importación/exportación
- Flujo de datos transfronterizos
- Temas relacionados con la privacidad (por ejemplo: el Reglamento General de Protección de Datos (GDPR), la Ley de Privacidad del Consumidor de California, la Ley de Protección de Información Personal, la Ley de Protección de Información Personal)
- Requerimientos contractuales, legales, de la industria y regulatorios

1.5 Comprender los requerimientos para los tipos de investigación (por ejemplo: estándares administrativos, penales, civiles, regulatorios y de la industria)

1.6 Desarrollar, documentar e implementar políticas, normas, procedimientos y directrices de seguridad

1.7 Identificar, analizar, evaluar, priorizar e implementar requerimientos de continuidad del negocio (BC)

- Análisis de impactos al negocio (BIA)
- Dependencias externas

1.8 Contribuir e implementar políticas y procedimientos de seguridad para el personal

- Selección y contratación de candidatos
- Acuerdos laborales y requerimientos derivados de políticas
- Procesos de incorporación, transferencias y desvinculaciones
- Acuerdos y controles de proveedores, consultores y contratistas

1.9 Comprender y aplicar conceptos de gestión de riesgos

- Identificación de amenazas y vulnerabilidades
- Análisis, evaluación y alcance de riesgos
- Respuesta y tratamiento de riesgos (por ejemplo: seguros para ciberseguridad)
- Tipos de controles aplicables (por ejemplo: preventivos, de detección, correctivos)
- Evaluaciones de control (por ejemplo: seguridad y privacidad)
- Monitoreo y mediciones continuas
- Informes (por ejemplo: internos, externos)
- Mejoras continuas (por ejemplo: modelos de madurez de riesgo)
- Marcos de riesgo (por ejemplo: la Organización Internacional de Normalización (ISO), el Instituto Nacional de Estándares y Tecnología (NIST), los Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT), la Arquitectura de Seguridad Empresarial Aplicada de Sherwood (SABSA), la Industria de Tarjetas de Pago (PCI))

1.10 Comprender y aplicar conceptos y metodologías de modelado de amenazas

1.11 Aplicar conceptos de gestión de riesgos de la cadena de suministro (SCRM)

- Riesgos asociados con la adquisición de productos y servicios de proveedores (por ejemplo: manipulación de productos, falsificaciones, implantes)
- Mitigación de riesgos (por ejemplo: evaluación y monitoreo de terceros, requerimientos mínimos de seguridad, requerimientos de nivel de servicio, raíz de confianza de silicio, función físicamente no clonable, lista de materiales de software)

1.12 Establecer y mantener un programa de concientización, educación y capacitación en materia de seguridad

- Métodos y técnicas para aumentar la conciencia y la capacitación (por ejemplo: ingeniería social, phishing, defensores de la seguridad, gamificación)
- Revisiones periódicas de contenido para incluir tecnologías y tendencias emergentes (por ejemplo: criptomonedas, inteligencia artificial (IA), blockchain)
- Evaluación de la efectividad del programa

Dominio 2: Seguridad de activos

2.1 Identificar y clasificar la información y los activos

- Clasificación de datos
- Clasificación de activos

2.2 Establecer requerimientos de información y manejo de activos

2.3 Aprovisionamiento de información y activos de forma segura

- Propiedad de la información y de los activos
- Inventario de activos (por ejemplo: tangibles, intangibles)
- Gestión de activos

2.4 Gestión del ciclo de vida de los datos

- Roles de datos (es decir, propietarios, controladores, custodios, procesadores, usuarios/sujetos)
- Recopilación de datos
- Ubicación de datos
- Mantenimiento de datos
- Retención de datos
- Remanencia de datos
- Destrucción de datos

2.5 Garantizar la retención adecuada de activos (por ejemplo: fin de vida útil (EOL), fin de soporte)

2.6 Determinar los controles de seguridad de los datos y los requerimientos de cumplimiento

- Estados de los datos (por ejemplo: en uso, en tránsito, en reposo)
- Definición del alcance y personalización
- Selección de normas
- Métodos de protección de datos (por ejemplo: gestión de derechos digitales (DRM), prevención de pérdida de datos (DLP), agente de seguridad de acceso a la nube (CASB))

Dominio 3: Arquitectura e ingeniería de la seguridad

3.1 Investigar, implementar y gestionar procesos de ingeniería utilizando principios de diseño seguros

- Modelos de amenazas
- Privilegios mínimos
- Defensa a profundidad
- Valores seguros predeterminados
- Fallas seguras
- Segregación de funciones (SoD)
- Mantenerlo simple y pequeño
- Confianza cero o confianza con verificación
- Privacidad por diseño
- Responsabilidad compartida
- Borde de servicio de acceso seguro

3.2 Comprender los conceptos fundamentales de los modelos de seguridad (por ejemplo: Biba, Modelo estrella, Bell-LaPadula)

3.3 Seleccionar controles basados en los requerimientos de seguridad de los sistemas

3.4 Comprender las capacidades de seguridad de los sistemas de información (por ejemplo: protección de la memoria, módulo de plataforma segura (TPM), cifrado/descifrado)

3.5 Evaluar y mitigar las vulnerabilidades de las arquitecturas, diseños y elementos de la solución de seguridad

- Sistemas basados en el cliente
- Sistemas basados en el servidor
- Sistemas de bases de datos
- Sistemas criptográficos
- Sistemas de control industrial (ICS)
- Sistemas basados en la nube (por ejemplo: software como un servicio (SaaS), infraestructura como un servicio (IaaS), plataforma como un servicio (PaaS))
- Sistemas distribuidos
- Internet de las cosas (IoT)
- Microservicios (por ejemplo: interfaz de programación de aplicaciones (API))
- Contenedorización
- Sistemas sin servidores
- Sistemas embebidos
- Sistemas informáticos de alto rendimiento
- Sistemas informáticos del borde
- Sistemas virtualizados

3.6 Seleccionar y determinar soluciones criptográficas

- Ciclo de vida criptográfico (por ejemplo: claves, selección de algoritmos)
- Métodos criptográficos (por ejemplo: curvas simétricas, asimétricas, elípticas, cuánticas)
- Infraestructura de clave pública (PKI) (por ejemplo: distribución de claves cuánticas)
- Prácticas clave de gestión (por ejemplo: rotación)
- Firmas digitales y certificados digitales (por ejemplo: no repudio, integridad)

3.7 Comprender los métodos de ataques criptoanalíticos

- Fuerza bruta
- Sólo texto cifrado
- Texto plano conocido
- Análisis de frecuencias
- Texto cifrado seleccionado
- Ataques de implementación
- Canal lateral
- Inyección de fallas
- Momento preciso
- Intermediario (MITM)
- Pasar el hash
- Explotación de Kerberos
- Secuestro de datos

3.8 Aplicar principios de seguridad al diseño de sitios e instalaciones

3.9 Diseñar controles de seguridad del sitio y de las instalaciones

- Armarios de cableado/instalaciones de distribución intermedia
- Salas de servidores/centros de datos
- Instalaciones de almacenamiento de medios
- Almacenamiento de evidencia
- Seguridad de áreas restringidas y de trabajo
- Servicios públicos y calefacción, ventilación y aire acondicionado (HVAC)
- Temas ambientales (por ejemplo: desastres naturales, provocados por el hombre)
- Prevención, detección y extinción de incendios
- Energía (por ejemplo: redundante, respaldo)

3.10 Gestión del ciclo de vida del sistema de información

- Necesidades y requerimientos de las partes interesadas
- Análisis de requerimientos
- Diseño arquitectónico
- Desarrollo/implementación
- Integración
- Verificación y validación
- Transición/despliegue
- Operaciones y mantenimiento/sostenimiento
- Retiro/disposición

Dominio 4: Seguridad de comunicaciones y redes

4.1 Aplicar principios de diseño seguro en arquitecturas de red

- Modelos de interconexión de sistema abierto (OSI) y protocolo de control de transmisión/protocolo de Internet (TCP/IP)
- Protocolo de Internet (IP) versión 4 y 6 (IPv6) (por ejemplo: unidifusión, difusión, multidifusión, difusión directa)
- Protocolos seguros (por ejemplo: seguridad del Protocolo de Internet (IPSec), intérprete de órdenes seguras (SSH), capa de conexión segura (SSL)/seguridad de la capa de transporte (TLS))
- Implicaciones de los protocolos multicapa
- Protocolos convergentes (por ejemplo: interfaz de pequeños sistemas de cómputo en Internet (iSCSI), voz sobre el Protocolo de Internet (VoIP), InfiniBand sobre Ethernet, Compute Express Link)
- Arquitectura de transporte (por ejemplo: topología, datos/control/plano de gestión, corte/almacenamiento y reenvío)
- Métricas de rendimiento (por ejemplo: ancho de banda, latencia, fluctuación, rendimiento, relación señal-ruido)
- Flujos de tráfico (por ejemplo: norte-sur, este-oeste)
- Segmentación física (por ejemplo: dentro de banda, fuera de banda, con espacio de aire)
- Segmentación lógica (por ejemplo: redes virtuales de área local (VLAN), redes privadas virtuales (VPN), enrutamiento y reenvío virtual, dominio virtual)
- Microsegmentación (por ejemplo: superposiciones/encapsulación de red; cortafuegos distribuidos, enrutadores, sistema de detección de intrusos (IDS)/sistema de prevención de intrusos (IPS), confianza cero)
- Redes perimetrales (por ejemplo: entrada/salida, emparejamiento)
- Redes inalámbricas (por ejemplo: Bluetooth, Wi-Fi, Zigbee, satélite)
- Redes celulares/móviles (por ejemplo: 4G, 5G)
- Redes de distribución de contenidos (CDN)
- Redes definidas por software (SDN), (por ejemplo: interfaz de programación de aplicaciones (API), red de área amplia definida por software, virtualización de funciones de red)
- Nube privada virtual (VPC)
- Monitoreo y gestión (por ejemplo: observabilidad de la red, configuración/flujo de tráfico, gestión de capacidades, detección y manejo de fallas)

4.2 Componentes de red seguros

- Operación de infraestructura (por ejemplo: energía redundante, garantía, soporte)
- Medios de transmisión (por ejemplo: seguridad física de los medios, calidad de propagación de la señal)
- Sistemas de control de accesos a la red (NAC) (por ejemplo: soluciones físicas y virtuales)
- Seguridad de puntos finales (por ejemplo: basada en host)

4.3 Implementar canales de comunicación seguros según diseño

- Voz, video y colaboración (por ejemplo: conferencias, salas de Zoom)
- Acceso remoto (por ejemplo: funciones administrativas de red)
- Comunicaciones de datos (por ejemplo: redes de retorno, satélite)
- Conectividad de terceros (por ejemplo: proveedores de telecomunicaciones, soporte de hardware)

Dominio 5: Gestión de identidades y accesos (IAM)

5.1 Control del acceso físico y lógico a los activos

- Información
- Sistemas
- Dispositivos
- Instalaciones
- Aplicaciones
- Servicios

5.2 Diseño de una estrategia de identificación y autenticación (por ejemplo: personas, dispositivos y servicios)

- Grupos y roles
- Autenticación, autorización y contabilización (AAA) (por ejemplo: autenticación multifactorial (MFA), autenticación sin contraseña)
- Gestión de sesiones
- Registro, comprobación y establecimiento de identidades
- Gestión de identidades federadas (FIM)
- Sistemas de gestión de credenciales (por ejemplo: bóveda de contraseñas)
- Inicio único de sesión (SSO)
- Justo a tiempo

5.3 Identidad federada con un servicio de terceros

- En el sitio
- Nube
- Híbrido

5.4 Implementación y gestión de mecanismos de autorización

- Control de accesos basado en roles (RBAC)
- Control de accesos basado en reglas
- Control de accesos obligatorios (MAC)
- Control de accesos discrecionales (DAC)
- Control de accesos basado en atributos (ABAC)
- Control de accesos basado en riesgos
- Acceder a la aplicación de políticas (por ejemplo: punto de decisión de políticas, punto de aplicación de políticas)

5.5 Gestión del ciclo de vida del aprovisionamiento de identidades y accesos

- Revisión de accesos a la cuenta (por ejemplo: usuario, sistema, servicio)
- Aprovisionamiento y desaprovisionamiento (por ejemplo: altas/bajas y traslados)
- Gestión de cuentas de servicio
- Definición y transición de roles (por ejemplo: personas asignadas a roles nuevos)
- Escalación de privilegios (por ejemplo: uso de sudo, auditoría de su uso)

5.6 Implementación de sistemas de autenticación

Dominio 6: Evaluación y pruebas de seguridad

6.1 Diseño y validación de estrategias de evaluación, prueba y auditoría

- Internas (por ejemplo: dentro del control de la organización)
- Externas (por ejemplo: fuera del control de la organización)
- De terceros (por ejemplo: fuera del control de la empresa)
- Ubicación (por ejemplo: local, en la nube, híbrida)

6.2 Realización de pruebas de control de seguridad

- Evaluación de vulnerabilidades
- Pruebas de penetración (por ejemplo: ejercicios de equipos rojo, azul y/o morado)
- Revisiones de registros
- Transacciones sintéticas/puntos de referencia
- Revisiones y pruebas de código
- Pruebas de casos de usos indebidos
- Análisis de cobertura
- Pruebas de interfaz (por ejemplo: interfaz del usuario, interfaz de la red, interfaz de programación de aplicaciones (API))
- Simulaciones de ataques de violaciones
- Controles de cumplimiento

6.3 Recopilación de datos de procesos de seguridad (por ejemplo: técnicos y administrativos)

- Administración de cuentas
- Revisión y aprobación gerencial
- Indicadores clave de desempeño y riesgo
- Datos de verificación de copias de respaldo
- Capacitación y concientización
- Recuperación ante desastres (DR) y Continuidad del negocio (BC)

6.4 Análisis de los resultados de las pruebas y generación de informes

- Remediación
- Manejo de excepciones
- Divulgación ética

6.5 Realización o facilitación de auditorías de seguridad

- Internas (por ejemplo: dentro del control de la organización)
- Externas (por ejemplo: fuera del control de la organización)
- De terceros (por ejemplo: fuera del control de la empresa)
- Ubicación (por ejemplo: local, en la nube, híbrida)

Dominio 7: Operaciones de seguridad

7.1 Comprender y cumplir con las investigaciones

- Recopilación y manejo de evidencias
- Generación de informes y documentación
- Técnicas de investigación
- Herramientas, tácticas y procedimientos de análisis forense digital
- Artefactos (por ejemplo: datos, computadoras, redes, dispositivos móviles)

7.2 Realizar actividades de registro y monitoreo

- Detección y prevención de intrusos (IDPS)
- Información de la seguridad y gestión de eventos (SIEM)
- Monitoreo y ajustes continuos
- Monitoreo de salidas
- Gestión de registros
- Inteligencia de amenazas (por ejemplo: fuentes de amenazas, búsqueda de amenazas)
- Análisis de comportamiento de usuarios y entidades (UEBA)

7.3 Realizar gestiones de configuración (CM) (por ejemplo: aprovisionamiento, definición de líneas base, automatización)

7.4 Aplicar conceptos fundamentales de operaciones de seguridad

- Necesidad de saber/privilegios mínimos
- Segregación de funciones (SoD) y responsabilidades
- Gestión de cuentas con privilegios
- Rotación de trabajos
- Acuerdos de nivel de servicio (SLA)

7.5 Aplicar protección de recursos

- Administración de medios
- Técnicas de protección de medios
- Datos en reposo/datos en tránsito

7.6 Gestionar incidentes

- Detección
- Respuesta
- Mitigación
- Generación de Informes
- Recuperación
- Remediación
- Lecciones aprendidas

7.7 Operar y mantener medidas de detección y prevención

- Cortafuegos (por ejemplo: próxima generación, aplicaciones web, redes)
- Sistemas de detección de intrusos (IDS) y sistemas de prevención de intrusos (IPS)
- Listas blancas/listas negras
- Servicios de seguridad proporcionados por terceros
- Ambientes aislados de pruebas
- Sistemas/redes señuelo
- Programas anti-software malicioso
- Herramientas basadas en aprendizaje automático e inteligencia artificial (IA)

7.8 Implementar y soportar la gestión de parches y vulnerabilidades

7.9 Comprender y participar en los procesos de gestión del cambio

7.10 Implementar estrategias de recuperación

- Estrategias de almacenamiento de respaldos (por ejemplo: almacenamiento en la nube, en el sitio, fuera del sitio)
- Estrategias del sitio de recuperación (por ejemplo: acuerdos de capacidad de recursos, sitios fríos vs sitios calientes)
- Sitios de procesamiento múltiple
- Resiliencia del sistema, alta disponibilidad (HA), calidad de servicio (QoS) y tolerancia a fallas

7.11 Implementar procesos de recuperación ante desastres (DR)

- Respuesta
- Personal
- Comunicaciones (por ejemplo: métodos)
- Evaluación
- Restauración
- Capacitación y concientización
- Lecciones aprendidas

7.12 Realizar pruebas de planes de recuperación ante desastres (DRP)

- Ejercicios de lectura/mesa
- Recorridos
- Simulaciones
- En paralelo
- Interrupción total
- Comunicaciones (por ejemplo: partes interesadas, estado de las pruebas, reguladores)

7.13 Participar en la planificación y en ejercicios de continuidad del negocio (BC)

7.14 Implementar y gestionar la seguridad física

- Controles de seguridad perimetrales
- Controles de seguridad internos

7.15 Abordar las preocupaciones de seguridad y protección del personal

- Viajes
- Capacitación y concientización sobre seguridad (por ejemplo: amenazas internas, impactos en las redes sociales, fatiga de la autenticación de dos factores (2FA))
- Gestión de emergencias
- Coacción

Dominio 8: Seguridad del desarrollo de software

8.1 Comprender e integrar la seguridad en el ciclo de vida del desarrollo de software (SDLC)

- Metodologías de desarrollo (por ejemplo: Agile, Waterfall, DevOps, DevSecOps, Scaled Agile Framework)
- Modelos de madurez (por ejemplo: modelo de madurez de capacidades (CMM), modelo de madurez de garantía de software (SAMM))
- Operación y mantenimiento
- Gestión del cambio
- Equipo de productos integrados

8.2 Identificar y aplicar controles de seguridad en ecosistemas de desarrollo de software

- Lenguajes de programación
- Bibliotecas
- Juegos de herramientas
- Ambiente de desarrollo integrado
- Tiempo de ejecución
- Integración continua y entrega continua (CI/CD)
- Gestión de configuración de software (CM)
- Repositorios de código
- Pruebas de seguridad de aplicaciones (por ejemplo: pruebas estáticas de seguridad de aplicaciones(SAST), pruebas dinámicas de seguridad de aplicaciones (DAST), análisis de composición de software, pruebas interactivas de seguridad de aplicaciones (IAST))

8.3 Evaluar la efectividad de la seguridad del software

- Auditoría y registro de cambios
- Análisis y mitigación de riesgos

8.4 Evaluar el impacto en la seguridad del software adquirido

- Producto comercial listo para usar (COTS)
- Código fuente abierto
- Terceros
- Servicios administrados (por ejemplo: aplicaciones empresariales)
- Sistemas en la nube (por ejemplo: software como un servicio (SaaS), infraestructura como un servicio (IaaS), plataforma como un servicio (PaaS))

8.5 Definir y aplicar guías y estándares de codificación segura

- Debilidades y vulnerabilidades de seguridad a nivel de código fuente
- Seguridad de las interfaces de programación de aplicaciones (API)
- Prácticas de codificación segura
- Seguridad definida por software

Información adicional sobre el examen

Referencias complementarias

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

La lista completa de referencias complementarias se encuentra disponible en www.isc2.org/certifications/References.

Políticas y procedimientos del examen

La ISC2 recomienda que los candidatos revisen las políticas y procedimientos del examen antes de registrarse para el examen. El desglose completo de esta importante información se encuentra disponible en isc2.org/register-for-exam.

Información legal

Si tiene alguna pregunta relacionada con las políticas legales de la ISC2, comuníquese con el Departamento Legal de la ISC2 en legal@isc2.org.

¿Alguna pregunta?

Comuníquese con los Servicios para Candidatos de la ISC2 en su región:

Continente americano
Teléfono: +1.866.331.ISC2 (4722), presione 1
Correo electrónico: membersupport@isc2.org

Asia-Pacífico
Teléfono: +(852) 5803-5662
Correo electrónico: isc2asia@isc2.org

Europa, Medio Oriente y África
Teléfono: +44 (0)203-960-7800
Correo electrónico: info-emea@isc2.org

ISC2