



Certified Information Systems Security Professional

ISC2 Certification

Esquema del examen de certificación

Fecha efectiva: 15 de abril de 2027



ISC2



Acerca de CISSP

La certificación Certified Information Systems Security Professional (CISSP) es la más reconocida a nivel mundial en el mercado de la seguridad de la información. La certificación CISSP valida los amplios conocimientos técnicos y de gestión, así como la experiencia de los profesionales de la seguridad de la información para diseñar, desarrollar y gestionar eficazmente la postura general de seguridad de una organización.

El amplio espectro de temas incluidos en el temario del examen para obtener la certificación CISSP garantiza su pertinencia en todas las disciplinas del ámbito de la seguridad de la información. Los candidatos que obtengan esta certificación serán competentes en las siguientes ocho áreas:

- Gobernanza de la seguridad y gestión de riesgos
- Seguridad de los activos
- Arquitectura e ingeniería de la seguridad
- Seguridad de las comunicaciones y redes
- Gestión de identidades y accesos (IAM)
- Evaluación y pruebas de seguridad
- Operaciones de seguridad
- Seguridad en el desarrollo de software

Requerimientos de experiencia previa

Los candidatos deben tener un mínimo de cinco años de experiencia acumulada a tiempo completo en dos o más de las ocho áreas del esquema actual del examen para obtener la certificación CISSP. La obtención de un título de educación superior (licenciatura o maestría) en ciencias de la computación, tecnologías de la información (TI) o campos relacionados puede convalidar hasta un año de la experiencia requerida. Asimismo, una credencial adicional incluida en la lista aprobada por ISC2 puede convalidar hasta un año de la experiencia exigida. Solo se puede eximir un año de experiencia. El trabajo a tiempo parcial y las pasantías también pueden contar para el requisito de experiencia.

Un candidato que no cuente con la experiencia necesaria para obtener la certificación CISSP puede convertirse en Asociado de ISC2 si aprueba satisfactoriamente el examen para la CISSP. Posteriormente, el Asociado de ISC2 dispondrá de seis años para adquirir los cinco años de experiencia requeridos. Puede obtener más información sobre los requisitos de experiencia de CISSP y cómo contabilizar el trabajo a tiempo parcial y las prácticas en www.isc2.org/Certifications/CISSP/experience-requirements.

Acreditación

La CISSP fue la primera credencial en el ámbito de la seguridad de la información en cumplir los estrictos requerimientos de la norma ISO/IEC 17024 de la Junta Nacional de Acreditación de ANSI (ANAB)

Análisis de tareas laborales (JTA)

ISC2 tiene la obligación ante sus miembros de mantener la pertinencia y vigencia de la certificación CISSP. Realizado periódicamente, el análisis de tareas laborales (JTA) es un proceso metódico y riguroso destinado a determinar las tareas que desempeñan los profesionales de la seguridad que ejercen dentro del ámbito profesional definido por CISSP. 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 la versión CAT del examen para la CISSP

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

Duración del examen	3 horas
Número de preguntas	100 - 150
Formato de las preguntas	Preguntas de opción múltiple y avanzadas
Calificación necesaria para aprobar	700 de 1000 puntos
Idiomas disponibles para el examen	Alemán, chino, español, inglés, japonés
Centro de evaluación	Centros de evaluación Pearson PPC y PVT Select autorizados por ISC2

Ponderaciones para la versión CAT del examen para la CISSP

Áreas	Ponderación promedio
1. Gobernanza de la seguridad y gestión de riesgos	13.6%
2. Seguridad de los activos	12%
3. Arquitectura e ingeniería de la seguridad	12.8%
4. Seguridad de las comunicaciones y redes	12.8%
5. Gestión de identidades y accesos (IAM)	13.6%
6. Evaluación y pruebas de seguridad	11.2%
7. Operaciones de seguridad	12.8%
8. Seguridad en el desarrollo de software	11.2%
Total: 100%	



Área 1: Gobernanza de la seguridad y gestión de riesgos

1.1 Comprender, respetar y promover la ética profesional

- » Código de ética profesional de ISC2
- » Ética en la inteligencia artificial (AI)
- » Código de ética de la organización

1.2 Comprender y aplicar los conceptos de seguridad

- » Confidencialidad, integridad, disponibilidad, autenticidad y no repudio

1.3 Evaluar, aplicar y mantener los principios de gobernanza de la seguridad

- » Alineación de la función de seguridad con la estrategia, las metas, la misión y los objetivos de negocio
- » Procesos organizacionales (por ejemplo, adquisiciones, desinversiones, comités de gobernanza)
- » Roles y responsabilidades organizacionales
- » Marcos de controles de seguridad (por ejemplo, Organización Internacional de Normalización (ISO), Instituto Nacional de Estándares y Tecnología (NIST), Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT), Arquitectura de Seguridad Empresarial Aplicada de Sherwood (SABSA), Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS), Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP))
- » Cuidado y diligencia debidos

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

- » Ciberdelitos y filtraciones de datos
- » Requisitos de licencias y propiedad intelectual
- » Controles de importación/exportación
- » Flujo transfronterizo de datos
- » Aspectos relacionados con la privacidad (por ejemplo, Reglamento General de Protección de Datos (RGPD), Ley de Privacidad del Consumidor de California, Ley de Protección de la Información Personal, Ley de Protección de la Información Personal y Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA))
- » Requisitos contractuales, legales, regulatorios y de estándares de la industria

1.5 Comprender los requisitos correspondientes a los distintos tipos de investigación (administrativa, penal, civil y regulatoria)

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

1.7 Identificar, analizar, evaluar, priorizar e implementar los requisitos de Continuidad del Negocio (BC)

- » Análisis de impacto en el negocio (BIA)
- » Dependencias externas



1.8 Contribuir a la aplicación y el cumplimiento de las políticas y procedimientos de seguridad del personal

- » Evaluación y contratación de candidatos
- » Contratos laborales y requisitos basados en políticas
- » Procesos de incorporación, transferencias y desvinculación del personal
- » Acuerdos y controles de proveedores, consultores y contratistas (por ejemplo, acuerdos de nivel de servicio (SLA))

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, seguro de ciberseguridad, estrategias de mitigación de riesgos)
- » Tipos de controles aplicables (por ejemplo, preventivos, de detección, correctivos)
- » Evaluaciones de controles (por ejemplo, seguridad y privacidad)
- » Monitoreo y medición continuos
- » Informes (por ejemplo, internos, externos)
- » Mejora continua (por ejemplo, modelado de madurez)
- » Marcos de gestión de riesgos (por ejemplo, Organización Internacional de Normalización (ISO), Instituto Nacional de Estándares y Tecnología (NIST), Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT), Arquitectura de Seguridad Empresarial Aplicada de Sherwood (SABSA), Industria de Tarjetas de Pago (PCI) y Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA))

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 y prestadores (por ejemplo, manipulación de productos, falsificaciones, implantes y riesgos para la reputación)
- » Medidas de mitigación de riesgos (por ejemplo, evaluación y monitoreo de terceros, requisitos mínimos de seguridad, requisitos de nivel de servicio, raíz de confianza de silicio, función físicamente inclonable y lista de materiales de software (SBOM))

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

- » Métodos y técnicas para aumentar la concientización y la capacitación (por ejemplo, promotores de seguridad y gamificación)
- » Revisiones periódicas del contenido para incluir tecnologías y tendencias emergentes (por ejemplo, criptomonedas, inteligencia artificial (IA) y cadenas de bloques)
- » Evaluación de la efectividad del programa y participación de las partes interesadas



Área 2: Seguridad de los activos

2.1 Identificar y clasificar información y activos

- » Clasificación de datos
- » Clasificación de activos

2.2 Establecer requisitos de manejo de información y activos

- » Físicos
- » Digitales/electrónicos
- » Destrucción segura de medios
- » Cifrado de datos (por ejemplo, en reposo, en tránsito/movimiento)

2.3 Proveer información y activos de manera segura

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

2.4 Gestionar el ciclo de vida de los datos

- » Política de gestión de 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 una gestión de activos adecuada (por ejemplo, fin de vida útil (EOL), fin de soporte (EOS))

- » Política de gestión de activos
- » Retención de activos
- » Retiro de activos

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

- » Estados de los datos (por ejemplo, en uso, en tránsito, en reposo)
- » Definición del alcance y adaptación
- » Selección de estándares y controles
- » 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) y Plataforma de Protección de Aplicaciones Nativas de la Nube (CNAPP))



Área 3: Arquitectura e ingeniería de la seguridad

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

- » Modelado de amenazas
- » Principio de privilegios mínimos (PoLP)
- » Defensa en profundidad (DiD)
- » Configuraciones predeterminadas seguras
- » Fallar de manera segura
- » Separación de funciones (SoD)
- » Principios de mantenerlo simple y pequeño
- » Confianza cero (ZT)
- » Privacidad desde el diseño (por ejemplo, tecnologías de mejora de la privacidad)
- » Responsabilidad compartida
- » Servicio de acceso seguro en el borde (SASE)
- » Marco de arquitectura bien diseñada
- » Rotación de funciones
- » Integridad de dos personas

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

3.3 Seleccionar controles con base en los requisitos de seguridad de los sistemas

3.4 Comprender las capacidades de seguridad de los sistemas de información (por ejemplo, protección de memoria, Módulo de Plataforma Segura (TPM), Módulo de Seguridad de Hardware (HSM), cifrado/descifrado)

3.5 Evaluar y mitigar las vulnerabilidades de las arquitecturas, diseños y componentes de las soluciones de seguridad

- » Sistemas basados en el cliente
- » Sistemas basados en servidor
- » Sistemas de bases de datos
- » Sistemas criptográficos
- » Tecnología operacional (OT) y 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), informática sin servidor (Serverless), Función como un servicio (FaaS))
- » Sistemas distribuidos
- » Internet de las cosas (IoT)
- » Microservicios y contenerización
- » Sistemas embebidos
- » Sistemas de computación de alto rendimiento
- » Sistemas de computación en el borde
- » Sistemas virtualizados
- » Riesgo de la cadena de suministro
- » Sistemas autónomos
- » Computación cuántica

3.6 Seleccionar y determinar soluciones criptográficas

- » Ciclo de vida criptográfico (por ejemplo, claves, selección de algoritmos)
- » Métodos criptográficos (por ejemplo, simétricos, asimétricos, de curva elíptica, poscuánticos)
- » Infraestructura de clave pública (PKI) (por ejemplo, distribución de claves)
- » Prácticas de gestión de claves (por ejemplo, rotación, gestión de accesos)
- » Firmas digitales y certificados digitales (por ejemplo, no repudio, integridad)



3.7 Comprender los métodos de ataques criptoanalíticos

- » Ataques de fuerza bruta
- » Ataques de dolo texto cifrado
- » Ataques de texto en claro conocido
- » Análisis de frecuencia
- » Ataques de texto cifrado elegido
- » Ataques de implementación
- » Canal lateral
- » Inyección de fallos
- » Ataques de temporización
- » Ataques de intermediarios (MITM)
- » Pass the Hash
- » Explotación de Kerberos
- » Ransomware
- » Ataques de día cero
- » Amenazas de inteligencia artificial (AI)
(por ejemplo, AI adversaria, envenenamiento de modelos de AI, ataques mediante deepfakes)

3.8 Aplicar principios de seguridad al diseño de sitios e instalaciones

3.9 Diseñar controles de seguridad de sitios e instalaciones

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

3.10 Administrar el ciclo de vida de los sistemas de información

- » Necesidades y requisitos de las partes interesadas
- » Análisis de requisitos
- » Diseño de arquitectura seguro
- » Desarrollo/Implementación
- » Integración
- » Verificación y validación
- » Revisión de seguridad continua
- » Transición/despliegue
- » Operaciones y mantenimiento/sustentación
- » Retiro/eliminación segura



Área 4: Seguridad de las comunicaciones y redes

4.1 Aplicar principios de diseño seguro en arquitecturas de red

- » Modelos de Interconexión de Sistemas Abiertos (OSI) y de Protocolo de Control de Transmisiones/Protocolo de Internet (TCP/IP)
- » Protocolo de Internet versión 4 (IPv4) y 6 (IPv6) (por ejemplo, unicast, broadcast, multicast, anycast)
- » Protocolos seguros (por ejemplo, Seguridad del Protocolo de Internet (IPSec), Secure Shell (SSH), Capa de Sockets Seguros (SSL)/Seguridad de la Capa de Transporte (TLS))
- » Implicaciones de los protocolos multicapa
- » Protocolos convergentes (por ejemplo, Interfaz de Sistemas de Computadoras Pequeñas de Internet (iSCSI), Voz sobre Protocolo de Internet (VoIP), InfiniBand sobre Ethernet, Compute Express Link)
- » Arquitectura de transporte (por ejemplo, topología, planos de datos/control/gestión, conmutación directa/almacenamiento y reenvío)
- » Métricas de rendimiento (por ejemplo, ancho de banda, latencia, jitter, rendimiento efectivo, relación señal-ruido)
- » Flujos de tráfico (por ejemplo, norte-sur, este-oeste)
- » Segmentación física (por ejemplo, en banda, fuera de banda, aislada (air-gapped))
- » Segmentación lógica (por ejemplo, Redes de Área Local Virtuales (VLAN), Redes Privadas Virtuales (VPN), Enrutamiento y Reenvío Virtuales, Dominio Virtual)
- » Microsegmentación (por ejemplo, superposición/encapsulación de redes, cortafuegos distribuidos, routers, Sistema de Detección de Intrusiones (IDS)/Sistema de Prevención de Intrusiones (IPS), Confianza Cero)
- » Redes de borde (por ejemplo, tráfico de entrada/salida, interconexión entre pares (peering))
- » Redes inalámbricas (por ejemplo, Bluetooth, Wi-Fi, Zigbee, satélite)
- » Redes celulares/móviles (por ejemplo, 4G, 5G)
- » Redes de distribución de contenido (CDN)
- » Redes definidas por software (SDN), (por ejemplo, interfaz de programación de aplicaciones (API), red de área amplia definida por software (SDWAN), virtualización de funciones de red)
- » Nube privada virtual (VPC)
- » Monitoreo y gestión (por ejemplo, observabilidad de la red, flujo/modelado de tráfico, gestión de capacidad, detección y manejo de fallas)
- » Seguridad definida por software

4.2 Asegurar los componentes de red

- » Operación de la 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 acceso 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 el diseño

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



Área 5: Gestión de identidades y accesos (IAM)

5.1 Gestionar el acceso físico y lógico a los activos (por ejemplo, aprovisionar, controlar, revisar, revocar)

- » Información
- » Sistemas
- » Dispositivos
- » Instalaciones
- » Aplicaciones
- » Servicios
- » Identidades

5.2 Diseñar la estrategia de identificación y autenticación (por ejemplo, personas, dispositivos y servicios)

- » Grupos y roles
- » Autenticación, autorización y contabilidad (AAA)
- » Gestión de sesiones
- » Registro, verificación y establecimiento de la identidad
- » Gestión de identidades federadas (FIM)
- » Sistemas de gestión de credenciales (por ejemplo, bóveda de contraseñas)
- » Inicio único de sesión (SSO)
- » Justo a tiempo
- » Autenticación sin contraseña (por ejemplo, Identidad rápida en línea (FIDO), WebAuthn, claves de acceso, datos biométricos)

5.3 Identidad federada con un servicio de terceros

- » En las instalaciones
- » En la nube
- » Híbrido

5.4 Implementar y gestionar mecanismos de autorización

- » Control de acceso basado en roles (RBAC)
- » Control de acceso basado en reglas (RuBAC)
- » Control de acceso obligatorio (MAC)
- » Control de acceso discrecional (DAC)
- » Control de acceso basado en atributos (ABAC)
- » Control de acceso adaptable al riesgo (RAdAC)
- » Aplicación de políticas de acceso (por ejemplo, punto de decisión de políticas, punto de aplicación de políticas)

5.5 Gestionar el ciclo de vida del aprovisionamiento de identidades y accesos

- » Revisión de acceso a cuentas (por ejemplo, usuario, sistema, servicio)
- » Aprovisionamiento y desaprovisionamiento (incorporación/desvinculación y transferencias)
- » Definición y transición de roles (por ejemplo, personas asignadas a nuevos roles)
- » Escalada de privilegios (por ejemplo, uso de grupos de administradores/sudo, auditoría de su uso, Principio de Mínimo Privilegio (PoLP))
- » Gestión de cuentas de servicio

5.6 Implementar sistemas de autenticación y autorización



Área 6: Evaluación y pruebas de seguridad

6.1 Diseñar y validar estrategias de evaluación, prueba y auditoría

- » Interno (por ejemplo, bajo el control de la organización)
- » Externo (por ejemplo, fuera del control de la organización)
- » Terceros (por ejemplo, fuera del control de la empresa)
- » Ubicación (por ejemplo, local, nube, híbrido)

6.2 Realizar pruebas de controles de seguridad

- » Evaluación de vulnerabilidades
- » Pruebas de penetración
- » Revisiones de registros
- » Transacciones sintéticas/benchmarks
- » Revisión de código y pruebas
- » Pruebas de casos de mal uso
- » Análisis de cobertura
- » Pruebas de interfaz (por ejemplo, interfaz de usuario, interfaz de red, interfaz de programación de aplicaciones (API))
- » Simulaciones de ataque
- » Verificaciones de cumplimiento

6.3 Recopilar datos de procesos de seguridad (por ejemplo, técnicos, administrativos)

- » Gestión de cuentas
- » Revisión y aprobación por parte de la gerencia
- » Indicadores clave de rendimiento y de riesgo
- » Datos de verificación de copias de seguridad
- » Capacitación y concienciación
- » Recuperación ante desastres (DR) y continuidad del negocio (BC)

6.4 Analizar los resultados de las pruebas/auditorías y generar informes

- » Remediación
- » Gestión de excepciones
- » Divulgación responsable

6.5 Realizar o facilitar auditorías de seguridad

- » Interno (por ejemplo, bajo el control de la organización)
- » Externo (por ejemplo, fuera del control de la organización)
- » Terceros (por ejemplo, fuera del control de la empresa)
- » Ubicación (por ejemplo, en las instalaciones, nube, híbrido)



Área 7: Operaciones de seguridad

7.1 Comprender y cumplir con las investigaciones

- » Recopilación y manejo de pruebas
- » Técnicas de investigación
- » Informes y documentación
- » 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 intrusiones (IDPS)
- » Gestión de eventos e información de seguridad (SIEM)
- » Orquestación, automatización y respuesta de seguridad (SOAR)
- » Monitoreo continuo y ajuste
- » Monitoreo de egreso (por ejemplo, prevención de pérdida de datos (DLP))
- » Gestión de registros (logs)
- » Inteligencia de amenazas (por ejemplo, fuentes de amenazas, búsqueda de amenazas)
- » Análisis de comportamiento de usuarios y entidades (UEBA)

7.3 Realizar la gestión de la configuración (CM) (por ejemplo, aprovisionamiento, establecimiento de líneas base, automatización)

- » Necesidad de conocer/privilegios mínimos
- » Segregación de funciones (SoD) y responsabilidades
- » Gestión de cuentas con privilegios
- » Rotación de puestos

7.4 Aplicar conceptos fundamentales de operaciones de seguridad (por ejemplo, defensa en profundidad (DiD))

- » Gestión de medios
- » Técnicas de protección de medios (por ejemplo, archivado, cifrado, eliminación/reutilización)
- » Estados de los datos (por ejemplo, en uso, en tránsito, en reposo)

7.5 Aplicar protección de recursos

- » Detección
- » Respuesta
- » Mitigación
- » Presentación de informes
- » Recuperación
- » Remediación
- » Lecciones aprendidas

7.6 Realizar la gestión de incidentes



7.7 Operar y mantener medidas de detección y preventivas

- » Cortafuegos (por ejemplo, de última generación, de aplicaciones web, de red)
- » Sistemas de detección de intrusos (SDI) y sistemas de prevención de intrusos (SPI)
- » Lista de permitidos/Lista de denegados
- » Servicios de seguridad proporcionados por terceros (por ejemplo, servicios de mitigación de denegación de servicio distribuido (DDoS), proveedor de servicios de seguridad gestionados)
- » Creación de entornos aislados (sandboxing)
- » Sistemas/redes señuelo (honeypots/honeynets)
- » Protección de puntos finales (por ejemplo, antimalware, detección y respuesta de puntos finales (EDR), detección y respuesta extendidas (XDR))
- » Herramientas basadas en aprendizaje automático (ML) e inteligencia artificial (AI)

7.8 Implementar y dar soporte a la gestión basada en parches y vulnerabilidades

7.9 Comprender y participar en los procesos de gestión de cambios

7.10 Implementar estrategias de recuperación

- » Estrategias de almacenamiento de copias de seguridad (por ejemplo, almacenamiento en la nube, local, externo, inmutable, cifrado)
- » Estrategias de sitios de recuperación (por ejemplo, frío frente a templado frente a caliente, acuerdos de capacidad de recursos)
- » Múltiples sitios de procesamiento
- » Resiliencia del sistema, alta disponibilidad (HA), calidad de servicio (QoS) y tolerancia a fallos

7.11 Implementar procesos de recuperación ante desastres (DR)

- » Respuesta
- » Personal
- » Comunicaciones (por ejemplo, métodos, priorización)
- » Evaluación
- » Restauración
- » Capacitación y concienciación
- » Lecciones aprendidas
- » Métricas (por ejemplo, línea base, tiempo medio de resolución)
- » (MTTR), tiempo medio entre fallos (MTBF))

7.12 Probar los planes de recuperación ante desastres (DRP)

- » Revisión documental/ejercicios de escritorio
- » Recorridos
- » Simulaciones
- » Interrupción completa en paralelo
- » Comunicaciones (por ejemplo, internas/externas)

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

7.14 Implementar y gestionar la seguridad física

- » Controles de seguridad externos
- » Controles de seguridad internos

7.15 Implementar y gestionar la seguridad física

- » Viajes
- » Capacitación y concientización sobre seguridad
- » Gestión de emergencias
- » Coacción



Área 8: Seguridad en el 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, Cascada, DevOps, DevSecOps, Marco Ágil Escalado)
- » Modelos de madurez (por ejemplo, Modelo de Madurez de Capacidades (CMM), Modelo de Madurez de Aseguramiento de Software (SAMM))
- » Operación y mantenimiento
- » Gestión del cambio
- » Equipo de producto integrado
- » Requisitos del Marco de Desarrollo de Software Seguro (SSDF) y de la Lista de Materiales de Software (SBOM)
- » Desplazamiento a la izquierda (Shift left)

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

- » Lenguajes de programación (por ejemplo, con seguridad de memoria, orientados a objetos)
- » Bibliotecas
- » Conjuntos de herramientas
- » Ambiente de desarrollo integrado
- » Tiempo de ejecución
- » Integración continua y entrega continua (CI/CD)
- » Software de gestión de la configuración (GC)
- » Repositorios de código
- » Pruebas de seguridad de aplicaciones (por ejemplo, pruebas estáticas de seguridad de aplicaciones (SAST), pruebas dinámicas de seguridad de aplicaciones (DAST))

8.3 Evaluar la eficacia 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

- » Productos comerciales listos para usar (COTS)
- » Código abierto (por ejemplo, análisis de composición de software (SCA))
- » De terceros
- » Servicios gestionados (por ejemplo, aplicaciones empresariales)
- » Servicios en la nube (por ejemplo, Software como un servicio (SaaS), Infraestructura como un servicio (IaaS), Plataforma como un servicio (PaaS), Función como un servicio (FaaS))

8.5 Definir y aplicar pautas 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



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 para la certificación CISSP e identificando las áreas de estudio que puedan necesitar atención adicional.

Consulte la lista completa de referencias adicionales en www.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 de ISC2 en su región:

América

Tel: +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

Tel: +44 203-960-7800

Email: info-emea@isc2.org