CISSP®

Certified Information Systems Security Professional

An (ISC)² Certification

Descripción del **examen de certificación**

Fecha de entrada en vigor: 1 de mayo de 2021

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

Acerca del CISSP

El Profesional certificado en seguridad de sistemas de información (Certified Information Systems Security Professional, CISSP) es la certificación más reconocida a nivel mundial en el mercado de la seguridad de la información. El CISSP valida el profundo conocimiento técnico y de gestión de un profesional de la seguridad de la información, y su experiencia para diseñar, organizar y gestionar eficazmente la postura general de seguridad de una organización.

El amplio abanico de temas incluidos en el cuerpo común de conocimiento (, CBK®) del CISSP garantiza su relevancia en todas las disciplinas del campo de la seguridad de la información. Los candidatos aptos serán competentes en estos ocho dominios:

- Gestión de la seguridad y el riesgo
- Seguridad de activos
- Arquitectura e ingeniería de la seguridad
- Seguridad de la red y la comunicación
- Gestión de identidades y acceso (IAM)
- Evaluación y pruebas de seguridad
- Operaciones de seguridad
- Seguridad en el desarrollo de software

Requisitos de experiencia

Los candidatos deben contar con un mínimo de cinco años de experiencia laboral pagada acumulada en dos o más de los ocho dominios del CBK del CISSP. La posesión de un título universitario de cuatro años o de un título extranjero equivalente o de otra credencial de la lista aprobada del (ISC)² convalidará un año de la experiencia requerida. La formación académica solo podrá convalidar un año de experiencia.

Los candidatos que no cuenten con la experiencia requerida para convertirse en CISSP pueden asociarse al (ISC)² aprobando el examen CISSP. El asociado del (ISC)² tendrá, a partir de ese momento, seis años para acumular los cinco años de experiencia requerida. Puede encontrar más información acerca de los requisitos de experiencia del CISSP y de cómo reconocer trabajos a tiempo parcial y prácticas en www.isc2.org/Certifications/CISSP/experience-requirements.

Acreditación

El CISSP fue la primera credencial en el campo de la seguridad de la información en cumplir los rigurosos requisitos de la norma ANSI/ISO/IEC 17024.

Análisis de tareas de trabajo (JTA)

El (ISC)² tiene la obligación con sus miembros de mantener la relevancia del CISSP. Realizado a intervalos regulares, el análisis de tareas de trabajo (JTA) es un proceso metódico y crítico que consiste en determinar las tareas realizadas por los profesionales de la seguridad que participan en la profesión definida por el CISSP. Los resultados del JTA se utilizan para actualizar el examen. Este proceso garantiza que se evalúe a los candidatos en áreas de conocimiento relevantes para los roles y responsabilidades de los profesionales de la seguridad de la información de hoy en día.

Información del examen CISSP CAT

El examen CISSP utiliza pruebas adaptativas computarizadas (CAT) para todos los exámenes en inglés. Los exámenes CISSP de todos los demás idiomas se administran como exámenes lineales de formulario. Puede encontrar más información acerca del CISSP CAT 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 innovadoras avanzadas
Calificación para aprobar	700 de 1000 puntos
Idiomas disponibles para el examen	Inglés
Centro examinador	Centros examinadores de PPC and PVTC Select Pearson VUE autorizados por el (ISC)²

Peso de cada dominio en el CISSP CAT

Dominios	Peso promedio
1. Gestión de la seguridad y el riesgo	15 %
2. Seguridad de activos	10 %
3. Arquitectura e ingeniería de la seguridad	13 %
4. Seguridad de la red y la comunicación	13 %
5. Gestión de identidades y acceso (IAM)	13 %
6. Evaluación y pruebas de seguridad	12 %
7. Operaciones de seguridad	13 %
8. Seguridad en el desarrollo de software	11 %
Total:	**100 %**

Información del examen lineal de CISSP

Duración del examen	6 horas
Número de preguntas	250
Formato de las preguntas	Opciones múltiples y preguntas innovadoras avanzadas
Calificación para aprobar	700 de 1000 puntos
Idiomas disponibles para el examen	Francés, alemán, portugués brasileño, español moderno, japonés, chino simplificado y coreano
Centro examinador	Centros examinadores de PPC and PVTC Select Pearson VUE autorizados por el (ISC)²

Peso de cada dominio en el examen CISSP lineal

Dominios	Peso
1. Gestión de la seguridad y el riesgo	15 %
2. Seguridad de activos	10 %
3. Arquitectura e ingeniería de la seguridad	13 %
4. Seguridad de la red y la comunicación	13 %
5. Gestión de identidades y acceso (IAM)	13 %
6. Evaluación y pruebas de seguridad	12 %
7. Operaciones de seguridad	13 %
8. Seguridad en el desarrollo de software	11 %
Total:	**100 %**

Dominio 1: Gestión de la seguridad y el riesgo

1.1 Comprender, cumplir y promover la ética profesional

- Código de ética profesional del (ISC)²
- Código de ética de la organización

1.2 Comprender y aplicar conceptos de seguridad

- Confidencialidad, integridad y disponibilidad, autenticidad y no repudio

1.3 Evaluar y aplicar principios de gobernanza de seguridad

- Adaptación de la función de seguridad a la estrategia, las metas, la misión y los objetivos del negocio
- Procesos organizativos (p. ej., adquisiciones, desinversiones, comités de dirección)
- Roles y responsabilidades de la organización
- Marcos de control de seguridad
- Debido cuidado/Diligencia debida

1.4 Determinar el cumplimiento y otros requisitos

- Requisitos contractuales, legales, estándares de la industria y requisitos regulatorios
- Requisitos de privacidad

1.5 Comprender problemas legales y regulatorios que pertenecen al campo de la seguridad de la información en un contexto holístico

- Delitos cibernéticos y vulneración de datos
- Requisitos de concesión de licencias y propiedad intelectual (IP)
- Controles de importación/exportación
- Flujo de datos transfronterizos
- Privacidad

1.6 Comprender los requisitos para los distintos tipos de investigación (p. ej., administrativa, criminal, civil, regulatoria, de estándares de la industria)

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

1.8 Identificar, analizar y priorizar los requisitos de continuidad del negocio (BC)

- Análisis del impacto al negocio (BIA)
- Desarrollar y documentar el alcance y el plan

1.9 Contribuir a las políticas y procedimientos de seguridad del personal y hacer que se cumplan

- Cribado y contratación de candidatos
- Acuerdos y políticas de empleo
- Incorporaciones, traslados y procesos de rescisión
- Acuerdos y controles con proveedores, consultoras y contratistas
- Requisitos de políticas de cumplimiento
- Requisitos de políticas de privacidad

1.10 Comprender y aplicar conceptos de gestión de riesgos

- Identificar amenazas y vulnerabilidades
- Gestión/Análisis de riesgos
- Respuesta ante riesgos
- Selección e implementación de contramedidas
- Tipos aplicables de controles (p. ej., preventivo, de detección, correctivo)
- Evaluaciones de control (seguridad y privacidad)
- Monitorización y medición
- Informes
- Mejora continua (p. ej., creación de modelos de madurez de riesgo)
- Marcos de riesgo

1.11 Comprender y aplicar conceptos y metodologías de modelado de amenazas

1.12 Aplicar conceptos de gestión de riesgos de la cadena de suministros (SCRM)

- Riesgos asociados al hardware, software, y servicios
- Monitorización y evaluación de terceros
- Requisitos mínimos de seguridad
- Requerimiento de nivel de servicio

1.13 Establecer y mantener un programa de concienciación, educación y capacitación en seguridad

- Métodos y técnicas para concienciar y capacitar (p. ej., ingeniería social, suplantación de identidad, programas de campeones de seguridad, ludificación)
- Revisiones de contenido periódicas
- Evaluación de la efectividad del programa

Dominio 2: Seguridad de activos

2.1 Identificar y clasificar información y activos

» Clasificación de datos
» Clasificación de activos

2.2 Establecer requisitos del manejo de información y activos

2.3 Aprovisionar recursos de forma segura

» Propiedad de la información y de los activos
» Inventario de activos (p. ej., tangibles, intangibles)
» Gestión de activos

2.4 Gestionar el ciclo de vida de los datos

» Roles de datos (p. ej., propietarios, responsables, custodios, encargados, usuarios/sujetos)
» Recopilación de datos
» Localización de datos
» Mantenimiento de datos
» Retención de datos
» Persistencia de datos
» Destrucción de datos

2.5 Asegurar la retención de activos adecuada (p. ej., fin de vida útil [EOL], fin de soporte [EOS])

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

» Estados de los datos (p. ej., en uso, en tránsito, en reposo)
» Alcance y ajuste
» Selección de estándares
» Métodos de protección de datos (p. ej., gestión digital de derechos [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 por medio de principios de diseño seguro

- Modelado de amenazas
- Mínimo privilegio
- Defensa en profundidad
- Predeterminados seguros
- Control seguro de errores
- Segregación de funciones (SoD)
- Keep it simple
- Zero Trust
- Privacidad por diseño
- Trust but verify
- Responsabilidad compartida

3.2 Comprender los conceptos fundamentales de los modelos de seguridad (p. ej., los modelos Biba, Star y Bell-LaPadula)

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

3.4 Comprender las capacidades de seguridad de los sistemas de la información (IS) (p. ej., protección de memoria, módulo de plataforma de confianza [TPM], cifrado/descifrado)

3.5 Evaluar y mitigar las vulnerabilidades de las arquitecturas, diseños y soluciones 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 (p. ej., software como servicio [SaaS], infraestructura como servicio [IaaS], plataforma como servicio [PaaS])
- Sistemas distribuidos
- Internet de las cosas (IoT)
- Microservicios
- Creación de contenedores
- Sin servidor
- Sistemas incrustados
- Sistemas de computación de alto rendimiento (HPC)
- Sistemas de computación perimetral o Edge Computing
- Sistemas virtualizados

3.6 Seleccionar y determinar soluciones criptográficas

- Ciclo de vida criptográfico (p ej., claves, selección de algoritmos)
- Métodos criptográficos (p. ej., simétricos, asimétricos, curvas elípticas, cuanto)
- Infraestructura de clave pública (PKI)
- Prácticas de gestión de claves
- Firmas digitales y certificados digitales
- No repudio
- Integridad (p. ej., hashing)

3.7 Comprender los métodos de ataque criptoanalíticos

- Fuerza bruta
- Solo texto cifrado
- Texto sin formato conocido
- Análisis de frecuencia
- Texto cifrado elegido
- Ataques de implementación
- Canal lateral
- Inserción de errores
- Sincronización
- Intermediario (MITM)
- Pasar el hash
- Explotación de Kerberos
- Ransomware

3.8 Aplicar principios de seguridad al diseño de recintos e instalaciones

3.9 Diseñar controles de seguridad de recintos e instalaciones

- Armarios de cableado/Instalaciones de distribución intermedia
- Salas de servidores/Centros de datos
- Instalaciones de almacenamiento multimedia
- Almacenamiento de pruebas
- Seguridad restringida y del área de trabajo
- Utilidades y calefacción, ventilación y aire acondicionado (HVAC)
- Cuestiones medioambientales
- Prevención, detección y extinción de incendios
- Alimentación (p. ej., redundante, de respaldo)

Dominio 4: Seguridad de la red y la comunicación

4.1 Evaluar e implementar principios de diseño seguro en arquitecturas de red

- Modelos de interconexión de sistemas abiertos (OSI) y de protocolo de control de transmisión/protocolo de Internet (TCP/IP)
- Redes de protocolo de Internet (IP) (p. ej., seguridad del protocolo de Internet [IPSec], protocolo de Internet [IP] v 4/6)
- Protocolos seguros
- Implicaciones de los protocolos multicapa
- Protocolos convergentes (p. ej., canal de fibra sobre Ethernet [FCoE], interfaz de pequeños sistemas de cómputo en Internet [iSCSI], voz sobre protocolo de Internet [VoIP])
- Microsegmentación (p. ej., redes definidas por software [SDN], red de área local extensible virtual [VXLAN], encapsulación, red de área amplia definida por software [SD-WAN])
- Redes inalámbricas (p. ej., Li-Fi, Wi-Fi, Zigbee, satélite)
- Redes móviles (p. ej., 4G, 5G)
- Redes de distribución de contenidos (CDN)

4.2 Componentes de red segura

- Operación de hardware (p. ej., alimentación redundante, garantía, soporte)
- Medios de transmisión
- Dispositivos de control de acceso de red (NAC)
- Seguridad del Endpoint

4.3 Implementar canales de comunicación seguros de acuerdo al diseño

- Voz
- Colaboración multimedia
- Acceso remoto
- Comunicaciones de datos
- Redes virtualizadas
- Conectividad de terceros

Dominio 5: Gestión de identidades y acceso (IAM)

5.1 Controlar el acceso físico y lógico a los activos

- Información
- Sistemas
- Dispositivos
- Instalaciones
- Aplicaciones

5.2 Gestionar la identificación y autenticación de personas, dispositivos y servicios

- Implementación de gestión de identidad (IdM)
- Autenticación multifactor (MFA) / única
- Responsabilidad
- Gestión de sesiones
- Registro, revisión y establecimiento de identidad
- Gestión federada de identidades (FIM)
- Sistemas de gestión de credenciales
- Inicio de sesión único (SSO)
- Just-In-time (JIT)

5.3 Identidad federada con un servicio de terceros

- On-premise (en local)
- Nube
- Híbrido

5.4 Implementar y gestionar mecanismos de autorización

- Control de acceso basado en roles (RBAC)
- Control de acceso basado en reglas
- Control de acceso obligatorio (MAC)
- Control de acceso discrecional (DAC)
- Control de acceso basado en atributos (ABAC)
- Control de acceso basado en riesgos

5.5 Gestionar la identidad y el acceso que aprovisionan el ciclo de vida

- Revisión del acceso a la cuenta (p. ej., usuario, sistema, servicio)
- Aprovisionamiento y desaprovisionamiento (p. ej., activar/desactivar integraciones y transferencias)
- Definición de roles (p. ej., nuevos roles asignados a personas)
- Elevación de privilegios (p. ej., cuentas de servicio gestionado, uso del comando sudo, minimizar su uso)

5.6 Implementar sistemas de autenticación

- OpenID Connect (OIDC)/Autorización abierta (Oauth)
- Lenguaje de marcado para confirmaciones de seguridad (SAML)
- Kerberos
- Servicio de autenticación remota de llamadas de usuarios (RADIUS)/Sistema plus de control de acceso del controlador de acceso a terminales (TaCACS+)

Dominio 6: Evaluación y pruebas de seguridad

6.1 Diseñar y validar estrategias de evaluación, prueba y auditoría

- Internas
- Externas
- De terceros

6.2 Dirigir pruebas de control de seguridad

- Evaluación de vulnerabilidad
- Prueba de penetración
- Revisiones de registros
- Transacciones sintéticas
- Prueba y revisión de código
- Prueba de caso de uso indebido (misuse case)
- Análisis de cobertura de prueba
- Prueba de interfaz
- Simulaciones de ataques Breach
- Comprobaciones de cumplimiento

6.3 Recopilar datos de procesos de seguridad (p. ej., técnicos y administrativos)

- Gestión de cuenta
- Revisión y aprobación de gestión
- Indicadores clave de rendimiento y riesgo
- Datos de verificación de respaldo
- Formación y capacitación
- Recuperación ante desastres (DR) y continuidad de negocio (BC)

6.4 Analizar resultados de pruebas y generar informes

- Reparación
- Manejo de la excepción
- Divulgación ética

6.5 Dirigir o facilitar auditorías de seguridad

- Internas
- Externas
- De terceros

Dominio 7: Operaciones de seguridad

7.1 Comprender y apoyar las investigaciones

- Recopilar y manejar pruebas
- Informes y documentación
- Técnicas investigativas
- Herramientas, tácticas y procedimientos de la ciencia forense digital
- Artefactos (p. ej., ordenador, red, dispositivo móvil)

7.2 Dirigir actividades de registro y monitorización

- Prevención y detección de intrusos
- Gestión de eventos e información de seguridad (SiEM)
- Monitorización continua
- Monitorización de salida
- Gestión de registro
- Inteligencia de amenazas (p. ej., fuentes de amenazas, búsqueda de amenazas)
- Análisis de comportamiento de usuarios y entidades (UEBA)

7.3 Realizar la gestión de la configuración (CM) (p. ej., aprovisionamiento, creación de líneas de base, automatización)

7.4 Aplicar conceptos fundamentales de operaciones de seguridad

- Necesidad de saber/Mínimo privilegio
- Segregación de funciones (SoD) y responsabilidades
- Gestión de cuenta privilegiada
- Rotación de tareas
- Acuerdos de nivel de servicio (SLAs)

7.5 Aplicar la protección de recursos

- Gestión multimedia
- Técnicas de protección de medios

7.6 Dirigir la gestión de incidencias

- Detección
- Respuesta
- Mitigación
- Informes
- Recuperación
- Reparación
- Lecciones aprendidas

7.7 Operar y mantener medidas de detección y preventivas

- Cortafuegos (p. ej., de próxima generación, aplicación web, red)
- Sistema de detección de intrusos (IDS) y sistemas de prevención de intrusiones (IPS)
- Lista blanca/Lista negra
- Servicios de seguridad proporcionados por terceros
- Entorno aislado (sandboxing)
- Honeypots/Honeynets
- Anti-malware
- Herramientas basadas en aprendizaje automático e inteligencia artificial (IA)

7.8 Implementar y apoyar la gestión de revisión y vulnerabilidad

7.9 Comprender los procesos de modificación de gestión y participar en ellos

7.10 Implementar estrategias de recuperación

- Estrategias de almacenamiento de respaldo
- Estrategias de sitios de recuperación
- Múltiples sitios de procesamiento
- Resistencia del sistema, alta disponibilidad (HA), calidad del servicio (QoS) y tolerancia a fallos

7.11 Implementar procesos de recuperación ante desastres (DR)

- Respuesta
- Personal
- Comunicaciones
- Evaluación
- Restauración
- Formación y capacitación
- Lecciones aprendidas

7.12 Probar los planes de recuperación ante desastres (DRP)

- Lectura/Trabajo en la mesa
- Tutoriales
- Simulación
- Paralelo
- Interrupción completa

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

7.14 Implementar y gestionar seguridad física

- Controles de seguridad perimetral
- Controles de seguridad interna

7.15 Abordar preocupaciones relativas a la protección y a la seguridad del personal

- Viajes
- Capacitación y concienciación en seguridad
- Gestión de emergencias
- Coacción

Dominio 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 (p. ej., Agile, Waterfall, DevOps, DevSecOps)
- Modelos de madurez (p. ej., Modelo de capacidad y madurez [CMM], Modelo de madurez de garantía de seguridad [SAMM])
- Operación y mantenimiento
- Gestión de modificaciones
- Equipo integrado de producto (IPT)

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

- Lenguajes de programación
- Bibliotecas
- Conjuntos de herramientas
- Entorno de desarrollo integrado (IDE)
- Tiempo de ejecución
- Integración continua y entrega continua (CI/CD)
- Orquestación de seguridad, automatización y respuesta (SOAR)
- Gestión de la configuración del software (SCM)
- Repositorios de código
- Pruebas de seguridad de aplicaciones (p. ej., pruebas de seguridad de aplicaciones estáticas [SAST], pruebas de seguridad de aplicaciones dinámicas [DAST])

8.3 Evaluar la efectividad de la seguridad del software

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

8.4 Evaluar el impacto en la seguridad del software adquirido

- Listo para la comercialización (COTS)
- Código abierto
- De terceros
- Servicios gestionados (p. ej., software como servicio [SaaS], infraestructura como servicio [IaaS], plataforma como servicio [PaaS])

8.5 Definir y aplicar directrices y normas de codificación seguras

- Debilidades y vulnerabilidades de seguridad en el nivel de código fuente
- Seguridad de interfaces empresariales seguras de programación de aplicaciones (APIs)
- Prácticas de codificación segura
- Seguridad definida por software

Información adicional del examen

Referencias complementarias

Se anima a los candidatos a complementar su formación académica y su experiencia mediante los recursos pertinentes que se enmarquen dentro del CBK y de la identificación de áreas de estudio que puedan necesitar especial atención.

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

Políticas y procedimientos del examen

El (ISC)² recomienda que los candidatos al CISSP repasen los procedimientos y políticas del examen antes de inscribirse. Puede leer el desglose completo de esta información importante en www.isc2.org/Register-for-Exam.

Información legal

Si tiene cualquier pregunta relacionada con las políticas legales del (ISC)², póngase en contacto con el Departamento Legal del (ISC)² en legal@isc2.org.

¿Tiene alguna pregunta?

(ISC)² Candidate Services
311 Park Place Blvd, Suite 400
Clearwater, FL 33759

(ISC)² Américas
Tel.: +1 866 331 ISC2 (4722)
Correo electrónico: info@isc2.org

(ISC)² Asia Pacífico
Tel.: +(852) 28506951
Correo electrónico: isc2asia@isc2.org

(ISC)² EMEA
Tel.: +44 (0)203 300 1625
Correo electrónico: info-emea@isc2.org