CISSP®

Certified Information Systems Security Professional

Esquema del examen de Certificación

Fecha efectiva: Abril 2018

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

Acerca de CISSP

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

El amplio espectro de temas incluidos en el conjunto de conocimientos de CISSP (Common Body of Knowledge - CBK) asegura su relevancia en todas las disciplinas en el campo de la seguridad de la información. Los candidatos aptos son competentes en los siguientes 8 dominios:

- Seguridad y gestión de riesgos
- Seguridad de activos
- Arquitectura de seguridad e ingeniería
- Comunicación y seguridad de red
- Gestión de identidad y acceso (IAM)
- Evaluación de seguridad y pruebas
- Operaciones de seguridad
- Seguridad de desarrollo de software

Requisitos de experiencia

Los candidatos tienen que tener un mínimo de 5 años de experiencia laboral acumulada a tiempo completo en 2 o más de los 8 dominios del CISSP CBK. Obtener un título universitario de 4 años o equivalente regional o una credencial adicional de la lista aprobada (ISC)² satisfará 1 año de la experiencia requerida. El crédito educativo solo satisfará 1 año de experiencia.

Un candidato que no tenga la experiencia requerida para convertirse en un CISSP puede convertirse en un Asociado de (ISC)² al aprobar con éxito el examen CISSP. El Asociado de (ISC)² tendrá 6 años para obtener la experiencia requerida de 5 años.

Acreditación

CISSP fue la primera credencial en el campo de la seguridad de la información en cumplir con los estrictos requisitos de ANSI/ISO/IEC Standard 17024.

Análisis de las áreas de trabajo

(ISC)² tiene la obligación con sus miembros de mantener la relevancia del CISSP. Realizado a intervalos regulares, el análisis de las áreas de trabajo 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 se utilizan para actualizar el examen. Este proceso asegura que los candidatos sean evaluados en las áreas temáticas relevantes para los roles y responsabilidades de los profesionales de la seguridad de la información de hoy en día.

CISSP CAT Información del examen

El examen CISSP usa Pruebas Adaptativas Computerizadas (CAT) para todos los exámenes en inglés. Los exámenes CISSP en todos los otros idiomas se administran como exámenes lineales con formularios. Puede obtener más información sobre CISSP CAT en www.isc2.org/certificatons/CISSP-CAT.

Duración del examen	3 horas
Número de preguntas	100 - 150
Formato de la pregunta	Múltiples opciones y preguntas innovadoras avanzadas
Calificación para aprobar	700 de 1000 puntos
Disponibilidad del idioma del examen	Inglés
Centro de prueba	(ISC)² Authorized PPC and PVTC Select Pearson VUE Testing Centers

CISSP CAT Pesos del examen

Dominios	Peso promedio
1. Seguridad y gestión de riesgos	15%
2. Seguridad de activos	10%
3. Arquitectura de seguridad e ingeniería	13%
4. Comunicación y seguridad de red	14%
5. Gestión de identidad y acceso (IAM)	13%
6. Evaluación de seguridad y pruebas	12%
7. Operaciones de seguridad	13%
8. Seguridad de desarrollo de software	10%
Total:	**100%**

CISSP Información del examen lineal

Duración del examen	6 horas
Número de preguntas	250
Formato de la pregunta	Múltiples opciones y preguntas innovadoras avanzadas
Calificación para aprobar	700 de 1000 puntos
Disponibilidad del idioma del examen	Francés, alemán, portugués brasileño, español, japonés, chino simplificado, coreano
Centro de prueba	(ISC)² Authorized PPC and PVTC Select Pearson VUE Testing Centers

CISSP Pesos del examen lineal

Dominios	Peso
1. Seguridad y gestión de riesgos	15%
2. Seguridad de activos	10%
3. Arquitectura de seguridad e ingeniería	13%
4. Comunicación y seguridad de red	14%
5. Gestión de identidad y acceso (IAM)	13%
6. Evaluación de seguridad y pruebas	12%
7. Operaciones de seguridad	13%
8. Seguridad de desarrollo de software	10%
Total:	**100%**

Dominio 1: Seguridad y Gestión de riesgos

1.1 Comprender y aplicar conceptos de confidencialidad, integridad y disponibilidad

1.2 Evaluar y aplicar principios de gobierno de la seguridad

- Alineación de la función de seguridad con la estrategia comercial, las metas, la misión y los objetivos
- Procesos de la organización (por ejemplo, adquisiciones, desinversiones, comités de gobierno)
- Roles y responsabilidades de la organización
- Marcos de controles de seguridad
- Debido cuidado/Debida diligencia (Due care/due diligence)
- Determinar los requisitos de cumplimiento

1.3 Determinar los requisitos de cumplimiento

- Requisitos contractuales, legales, estándares industriales y regulatorios
- Requisitos de privacidad

1.4 Comprender las cuestiones legales y regulatorias relacionadas con la seguridad de la información en un contexto global

- Ciberdelitos y filtración de datos
- Requisitos de licencias y propiedad intelectual
- Controles de importación/exportación
- Flujo de datos transfronterizos
- Privacidad

1.5 Comprender, adherirse a, y promover la ética profesional

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

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

1.7 Identificar, analizar y priorizar los requisitos de continuidad del negocio

- Desarrollar y documentar el alcance y el plan
- Análisis de impacto en el negocio (BIA)

1.8 Contribuir y hacer cumplir las políticas y procedimientos de seguridad de personal

- Comprobación de los candidatos y contratación
- Acuerdos y políticas laborales
- Procesos de incorporación y finalización
- Acuerdos y controles de proveedores, consultores y contratistas
- Requisitos de la política de cumplimiento
- Requisitos de la política de privacidad

1.9 Comprender y aplicar conceptos de gestión de riesgos

- Identificar amenazas y vulnerabilidades
- Evaluación de riesgos/análisis
- Respuesta a los riesgos
- Selección e implementación de contramedidas
- Tipos de controles aplicables (por ejemplo, preventivo, de detención, correctivo)
- Evaluación del control de seguridad
- Monitorización y medición
- Valoración de activos
- Informes
- Mejora continua
- Marcos de riesgo

1.10 Comprender y aplicar conceptos y metodologías de modelado de amenazas

- Metodologías de modelado de amenazas
- Conceptos de modelado de amenazas

1.11 Aplicar conceptos de gestión basados en el riesgo a la cadena de suministro

- Riesgos asociados con hardware, software y servicios
- Evaluación y seguimiento de terceros
- Requisitos mínimos de seguridad
- Requisitos de nivel de servicio

1.12 Establecer y mantener un programa de concienciación, educación y capacitación sobre seguridad

- Métodos y técnicas para presentar concienciación y capacitación
- Revisiones de contenido periódico
- Evaluación de efectividad del programa

Dominio 2: Seguridad de activos

2.1 Identificar y clasificar información y activos

- Clasificación de datos
- Clasificación de activos

2.2 Determinar y mantener la información y la propiedad de activos

2.3 Proteger la privacidad

- Propietarios de datos
- Procesadores de datos
- Remanencia de datos
- Limitación en la recogida de datos

2.4 Asegurar la retención adecuada de activos

2.5 Determinar los controles de seguridad de datos

- Comprender los estados de datos
- Alcance y ajuste
- Selección de estándares
- Métodos de protección de datos

2.6 Establecer requisitos de gestión de activos e información

Dominio 3: Arquitectura de seguridad e ingeniería

3.1 Implementar y gestionar procesos de ingeniería utilizando principios de diseño seguro

3.2 Comprender los conceptos fundamentales de los modelos de seguridad

3.3 Seleccionar controles basados 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 de confianza (TPM), cifrado / descifrado)

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

- Sistemas basados en cliente
- Sistemas basados en servidor
- Sistemas de bases de datos
- Sistemas criptográficos
- Sistemas de control industrial (ICS)
- Sistemas basados en la nube
- Sistemas distribuidos
- Internet de las cosas (IoT)

3.6 Evaluar y mitigar las vulnerabilidades en sistemas basados en web

3.7 Evaluar y mitigar las vulnerabilidades en sistemas móviles

3.8 Evaluar y mitigar vulnerabilidades en dispositivos integrados

3.9 Aplicar criptografía

- Ciclo de vida criptográfico (por ejemplo, gestión de claves, selección de algoritmos)
- Métodos criptográficos (por ejemplo, curvas elípticas simétricas, asimétricas)
- Infraestructura de clave pública (PKI)
- Métodos de gestión de claves
- Firmas digitales
- No repudio
- Integridad (por ejemplo, hashing)
- Comprender los métodos de ataques criptoanalíticos
- Gestión de derechos digitales (DRM)

3.10 Aplicar principios de seguridad al diseño de recintos y las instalaciones

3.11 Implementar controles de seguridad en recintos e instalaciones

- Armarios de cableado / instalaciones de distribución
- Salas de servidores / centros de datos
- Instalaciones de almacenamiento de medios
- Almacenamiento de evidencias
- Seguridad restringida y del área de trabajo
- Servicios públicos y calefacción, ventilación y aire acondicionado (HVAC)
- Cuestiones ambientales
- Prevención, detección y supresión de incendios

Dominio 4: Comunicación y seguridad de red

4.1 Implementar 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)
- Redes de Protocolo de Internet (IP)
- Implicaciones de los protocolos multicapa
- Protocolos convergentes
- Redes definidas por software
- Conexiones inalámbricas

4.2 Componentes de red seguros

- Funcionamiento del hardware
- Medios de transmisión
- Dispositivos de control de acceso a la red (NAC)
- Seguridad en endpoints
- Redes de distribución de contenido

4.3 Implementar canales de comunicación seguros según el diseño

- Voz
- Colaboración multimedia
- Acceso remoto
- Transmisión de datos
- Redes virtualizadas

Dominio 5: Gestión de identidad y acceso (IAM)

5.1 Control de acceso físico y lógico a los activos

- Información
- Sistemas
- Dispositivos
- Instalaciones

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

- Implementación de gestión de identidades
- Autenticación única / multifactor
- Responsabilidad
- Gestión de sesiones
- Registro y prueba de identidad
- Gestión de identidad federada (FIM)
- Sistemas de gestión de credenciales

5.3 Integrar la identidad como un servicio de terceros

- En las instalaciones
- En la nube
- Federado

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)

5.5 Gestionar el ciclo de vida de acceso y aprovisionamiento

- Revisión de acceso de usuario
- Revisión del acceso a la cuenta del sistema
- Aprovisionamiento y desaprovisionamiento

Dominio 6: Evaluación de seguridad y pruebas

6.1 Diseñar y validar estrategias de evaluación, prueba y auditoría

- Internas
- Externas
- De terceros

6.2 Realizar pruebas de control de seguridad

- Evaluación de vulnerabilidades
- Pruebas de penetración
- Revisiones de registros
- Transacciones sintéticas
- Revisión y prueba de código
- Prueba de caso de uso indebido
- Análisis de cobertura de prueba
- Pruebas de interfaz

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

- Gestión de cuentas
- Revisión y aprobación por parte de la dirección
- Indicadores clave de rendimiento y riesgo
- Datos de verificación de respaldo
- Capacitación y concienciación
- Recuperación de desastres (DR) y continuidad del negocio (BC)

6.4 Analizar resultados de prueba y generación de informes

6.5 Realizar o facilitar auditorías de seguridad

- Internas
- Externas
- De terceros

Dominio 7: Operaciones de seguridad

7.1 Comprender y apoyar las investigaciones

- Recopilación y gestión de evidencias
- Informes y documentación
- Técnicas de investigación
- Procedimientos, tácticas y herramientas forenses digitales

7.2 Comprender los requisitos para los tipos de investigación

- Administrativo
- Criminal
- Civil
- Regulatorio
- Estándares de la industria

7.3 Realizar actividades de registro y monitorización

- Detección y prevención de intrusiones
- Información de seguridad y gestión de eventos (SIEM)
- Monitorización continua
- Control de salida

7.4 Aprovisionamiento de recursos de forma segura

- Inventario de activos
- Gestión de activos
- Gestión de la configuración

7.5 Comprender y aplicar conceptos de operaciones de seguridad fundamentales

- Necesidad de saber / menor privilegio
- Separación de tareas y responsabilidades
- Gestión de cuentas privilegiadas
- Rotación de tareas
- Ciclo de vida de la información
- Acuerdos de nivel de servicio (SLA)

7.6 Aplicar técnicas de protección de recursos

- Gestión de medios
- Gestión de activos de hardware y software

7.7 Realizar gestión de incidentes

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

7.8 Operar y mantener medidas de detectivas y preventivas

- Cortafuegos
- Sistemas de detección y prevención de intrusiones
- Listas blancas / listas negra
- Servicios de seguridad proporcionados por terceros
- Sandboxing
- Honeypots/honeynets
- Anti-malware

7.9 Implementar y soportar la gestión de parches y vulnerabilidades

7.10 Comprender y participar en los procesos de gestión de cambios

7.11 Implementar estrategias de recuperación

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

7.12 Implementar procesos de recuperación de desastres (DR)

- Respuesta
- Personal
- Comunicaciones
- Evaluación
- Restauración
- Capacitación y concienciación

7.13 Prueba de Planes de Recuperación ante Desastres (DRP)

- Read-through/tabletop
- Walkthrough
- Simulación
- Paralelas
- Interrupción completa

7.14 Participar en la planificación y ejercicios de Continuidad del Negocio (BC)

7.15 Implementar y administrar la seguridad física

- Controles de seguridad perimetrales
- Controles de seguridad internos

7.16 Tratar las preocupaciones de seguridad y protección del personal

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

Dominio 8: Seguridad de desarrollo de software

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

- Metodologías de desarrollo
- Modelos de madurez
- Operación y mantenimiento
- Gestión del cambio
- Equipo de producto integrado

8.2 Identificar y aplicar controles de seguridad en entornos de desarrollo

- Seguridad de los entornos de software
- Gestión de la configuración como parte del código seguro
- Seguridad de los repositorios de código

8.3 Evaluar la efectividad de la seguridad del software

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

8.4 Evaluar el impacto de seguridad del software adquirido

8.5 Definir y aplicar pautas y normas de programación segura

- Debilidades de seguridad y vulnerabilidades en el nivel de código fuente
- Seguridad de las interfaces de programación de aplicaciones
- Prácticas seguras de programación

Información adicional del examen

Referencias suplementarias

Se alienta a los candidatos a complementar su educación y experiencia mediante la revisión de los recursos relevantes que pertenecen al CBK y la identificación de áreas de estudio que pueden necesitar atención adicional.

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

Políticas y procedimientos del examen

(ISC)² recomienda que los candidatos CISSP revisen las políticas y procedimientos de los exámenes antes de registrarse para el examen. Lea el desglose completo de esta información importante en www.isc2.org/Register-for-Exam.

Información legal

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

¿Alguna pregunta?

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

(ISC)² Americas
Tel: +1.866.331.ISC2 (4722)
Email: info@isc2.org

(ISC)² Asia Pacific
Tel: +(852) 28506951
Email: isc2asia@isc2.org

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