

ISC2 · CIBERSEGURIDAD

EXAM OUTLINE 2024

Certified Information Systems Security Professional (CISSP)

Exam Outline vigente desde el 15 de abril de 2024

La certificación de referencia mundial para diseñar, implementar y gestionar un programa de ciberseguridad de primer nivel en la organización.

¿Por qué debería asistir?

CISSP, de ISC2, acredita que el profesional tiene el conocimiento técnico y la experiencia de gestión necesarios para dirigir la seguridad de la información de una organización. Es una certificación acreditada por ANAB conforme a ISO/IEC 17024, reconocida por empresas y gobiernos de todo el mundo, y suele exigirse para puestos de liderazgo como CISO, arquitecto de seguridad o gerente de seguridad de la información.

Este curso recorre los 8 dominios del Common Body of Knowledge (CBK) de ISC2 según el exam outline vigente: desde la gestión de riesgos, la gobernanza y el cumplimiento hasta la arquitectura de seguridad, las redes, la gestión de identidades, las operaciones y el desarrollo seguro de software. Con el material oficial de ISC2, casos prácticos, preguntas de práctica y discusión guiada por un instructor autorizado, los participantes refuerzan la visión estratégica y el criterio de liderazgo que evalúa el examen CISSP.

5 días	8	100–150	Casos	Avanzado
DURACIÓN	DOMINIOS	ÍTEMS DEL EXAMEN	PRÁCTICOS Y PREGUNTAS	NIVEL

Certified Information Systems Security Professional

ISC2 Certification

¿Quién debería participar?

CISO, directores y gerentes de seguridad
Responsables de definir la estrategia, la gobernanza y el programa de seguridad de la información.

Arquitectos e ingenieros de seguridad
Profesionales que diseñan e implementan arquitecturas, redes y controles de seguridad.

Consultores, auditores y analistas de riesgo
Especialistas que evalúan controles, riesgos y cumplimiento normativo en las organizaciones.

Gerentes de TI y administradores de seguridad
Personas con experiencia en seguridad que buscan una certificación de liderazgo reconocida mundialmente.

Objetivos de aprendizaje

- Aplicar principios de gobernanza, cumplimiento, ética y gestión de riesgos para alinear la seguridad con los objetivos del negocio.
- Clasificar, proteger y gestionar los activos de información durante todo su ciclo de vida.
- Diseñar arquitecturas seguras aplicando principios de ingeniería de seguridad y criptografía.
- Proteger las comunicaciones y la infraestructura de red con controles y diseños seguros.
- Gestionar identidades, autenticación, autorización y el ciclo de vida de los accesos.
- Planificar y ejecutar evaluaciones, pruebas y auditorías de seguridad, e interpretar sus resultados.
- Dirigir operaciones de seguridad: monitoreo, respuesta a incidentes, recuperación y continuidad.
- Integrar la seguridad en el ciclo de vida del desarrollo de software y evaluar su eficacia.

Áreas de habilidad

Gobernanza de seguridad | Gestión de riesgos | Cumplimiento y ética | Clasificación de activos | Arquitectura segura | Criptografía | Seguridad de redes | IAM y Zero Trust | Pruebas y auditoría | Respuesta a incidentes | Continuidad y recuperación | Desarrollo seguro

Programa del curso

Duración: 5 días

Modalidades de formación

- **Presencial** — En aula, con instructor
- **Online** — En vivo, con instructor
- **Híbrida** — Aula y online combinadas

Módulo	Contenido
Dominio 1 **Día 1**	**1 Seguridad y gestión de riesgos (16 %)** Ética profesional; confidencialidad, integridad y disponibilidad; gobernanza; cumplimiento legal y regulatorio; investigaciones; políticas y procedimientos; continuidad del negocio; seguridad del personal; gestión de riesgos; modelado de amenazas; riesgo de la cadena de suministro; concienciación y formación.
Dominios 2 · 3 **Día 2**	**2 Seguridad de los activos (10 %)** Clasificación de la información; manejo, inventario y ciclo de vida de los activos; retención; controles de protección de datos. **3 Arquitectura e ingeniería de seguridad (13 %)** Principios de diseño seguro; modelos de seguridad; vulnerabilidades de arquitecturas; criptografía; seguridad física.
Dominios 4 · 5 **Día 3**	**4 Seguridad de las comunicaciones y redes (13 %)** Principios de arquitectura de red segura; componentes de red seguros; canales de comunicación seguros. **5 Gestión de identidades y accesos (IAM) (13 %)** Control de acceso físico y lógico; identificación y autenticación; federación; autorización; ciclo de vida del acceso.
Dominios 6 · 7 **Día 4**	**6 Evaluación y pruebas de seguridad (12 %)** Estrategias de evaluación y auditoría; pruebas de controles; datos de procesos; análisis e informe de resultados. **7 Operaciones de seguridad (13 %)** Investigaciones; registro y monitoreo; gestión de incidentes y cambios; recuperación ante desastres; seguridad física.
Dominio 8 **Día 5**	**8 Seguridad en el desarrollo de software (10 %)** Seguridad en el ciclo de vida del desarrollo (SDLC); controles en ecosistemas de desarrollo; eficacia de la seguridad del software; software adquirido; codificación segura. Cierre del curso: repaso integral de los 8 dominios, preguntas de práctica y estrategia para el examen CISSP.

Los dominios y sus pesos siguen el exam outline oficial de CISSP vigente desde el 15 de abril de 2024. El reparto por día es orientativo y el instructor puede ajustarlo según el avance del grupo.

Examen y certificación

Título	Certified Information Systems Security Professional (CISSP) – Exam Outline 2024
Dominios	8 dominios del CBK de ISC2
Ítems	100 a 150
Formato	Adaptativo (CAT) en todos los idiomas; opción múltiple e ítems innovadores avanzados
Duración	3 horas
Aprobación	700 de 1000
Idioma	Español, inglés, alemán, japonés y chino simplificado
Plataforma	Centros de pruebas autorizados de Pearson VUE

Requisitos de elegibilidad

- Mínimo de **5 años** de experiencia laboral acumulada, remunerada y a tiempo completo en **2 o más** de los 8 dominios del CBK. Cuentan el trabajo a tiempo parcial y las pasantías.
- Exención de **1 año** de experiencia con un título universitario (licenciatura o maestría) en informática, TI o un campo afín, o con una credencial de la lista aprobada por ISC2 (máximo 1 año en total).
- Quien aprueba el examen sin la experiencia requerida se convierte en **Associate of ISC2** y dispone de 6 años para acumularla.
- Tras aprobar: solicitud de endoso avalada por un miembro certificado de ISC2 y aceptación del Código de Ética de ISC2.

Ruta profesional ISC2

CISSP es la certificación insignia de ISC2: parte de CC y SSCP, y da paso a las concentraciones de arquitectura (ISSAP), ingeniería (ISSEP) y gestión (ISSMP). CCSP, CSSLP y CGRC la complementan como especializaciones.



Información general

- Material oficial de ISC2: eTextbook de CISSP y libro de preguntas de estudio.
- Instructor autorizado por ISC2 y Savant Consultores como ISC2 Official Training Partner.
- Certificación acreditada por ANAB según ISO/IEC 17024 y aprobada bajo DoDM 8140.03.
- Vigencia de 3 años: 120 créditos CPE por ciclo y cuota anual de mantenimiento (AMF) de US$135.



