

Profesional Certificado En Seguridad De Sistemas De Información (CISSP)

Código: ISC2-003

Propuesta de Valor: ISC2

Duración: 40 Horas



Certified Information Systems Security Professional (CISSP) es la certificación más reconocida a nivel mundial en el mercado de la seguridad de la información. CISSP valida el profundo conocimiento técnico y gerencial y la experiencia de un profesional de seguridad de la información para diseñar, diseñar y administrar de manera efectiva la postura general de seguridad de una organización.

Este curso está diseñado para profesionales de seguridad de la información con profundos conocimientos y experiencia técnica y gerencial para diseñar, diseñar y administrar de manera efectiva la postura general de seguridad de una organización. Dirigido por un instructor autorizado (ISC)², este seminario de capacitación proporciona una revisión integral de los conceptos de seguridad de los sistemas de información y las mejores prácticas de la industria.



AUDIENCIA

El curso es ideal para quienes trabajan en puestos como:

- Director de información
- Director de seguridad de la información
- Jefe de Tecnología
- Gerente/Oficial de Cumplimiento
- Director de seguridad
- Arquitecto de información
- Especialista en TI/Director/Gerente



PRE REQUISITOS

Los candidatos deben tener un mínimo de cinco años de experiencia laboral remunerada acumulada en dos o más de los ocho dominios del CISSP CBK.

- Seguridad y Gestión de Riesgos
- Seguridad de activos
- Arquitectura e ingeniería de seguridad
- Comunicación y Seguridad de la Red
- Gestión de acceso e identidad (IAM)

- Evaluación y pruebas de seguridad
- Operaciones de seguridad
- Seguridad de desarrollo de software

OBJETIVOS

- Aplicar conceptos y métodos fundamentales relacionados con los campos de la tecnología de la información y la seguridad.
- Alinear los objetivos operativos generales de la organización con las funciones e implementaciones de seguridad.
- Determinar cómo proteger los activos de la organización a lo largo de su ciclo de vida.
- Aprovechar los conceptos, principios, estructuras y estándares utilizados para diseñar, implementar, monitorear y proteger los sistemas operativos, equipos, redes, aplicaciones y los controles utilizados para hacer cumplir varios niveles de confidencialidad, integridad y disponibilidad.
- Aplicar principios de diseño de seguridad para seleccionar mitigaciones apropiadas para vulnerabilidades presentes en arquitecturas y tipos de sistemas de información comunes.
- Explicar la importancia de la criptografía y los servicios de seguridad que puede brindar en la era digital y de la información actual.
- Evaluar los elementos de seguridad física relativos a las necesidades de seguridad de la información.
- Evaluar los elementos que componen la seguridad de las comunicaciones y redes en relación con las necesidades de seguridad de la información.

CERTIFICACIÓN DISPONIBLE

- Este curso es preparación para el examen: **Certified Information Systems Security Professional (CISSP)**.
- Puntuación de 70% o más en la evaluación final.
- Certificación oficial de **ISC2**.

CONTENIDO

1. EL ENTORNO DE SEGURIDAD DE LA INFORMACIÓN
2. SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN
3. GESTIÓN DE ACCESO E IDENTIDAD
4. ARQUITECTURA E INGENIERÍA DE SEGURIDAD
5. COMUNICACIÓN Y SEGURIDAD DE LA RED
6. SEGURIDAD EN EL DESARROLLO DE SOFTWARE
7. EVALUACIÓN Y PRUEBAS DE SEGURIDAD
8. OPERACIONES DE SEGURIDAD
9. PONIENDO TODO JUNTO

★ BENEFICIOS

- Al finalizar el curso, los participantes aplicarán conceptos de seguridad de sistemas de información para mitigar el riesgo de vulnerabilidades de software y sistemas a lo largo de los ciclos de vida de los sistemas.