Curso taller
CISSP® - Certified Information Systems Security Professional

Objetivo

CISSP (Certified Information Systems Security Professional) es un certificado para profesionales de Seguridad de la Información, de (ISC)², la institución líder mundial, que tiene el mayor número de profesionales certificados y es la única presente en mas de 130 países. Ideal para los que buscan visibilidad, carrera internacional y crecimiento profesional.

El CISSP es uno de los más valorizados certificados del mercado porque abarca un contenido neutro, comprobando que los profesionales certificados, independientemente de la tecnología, tienen una comprensión amplia y maestría sobre el área de Seguridad de la Información, al gestionar un equipo en los retos de su cotidiano.

Temario

Los aspectos que debe dominar aquel que pretenda certificarse como CISSP cubre los 10 dominios de conocimiento que requiere el (ISC)² al candidato y son los que se tratan en el curso de preparación para el examen. Estos 10 dominios son los siguientes:

- **I. Prácticas de Gestión de la Seguridad:** Identificación de los activos de una organización y desarrollo, documentación e implementación de políticas, estándares, procedimientos y guías:
  - Conceptos y objetivos
  - Gestión del riesgo
  - Procedimientos y políticas.
  - Clasificación de la información
  - Responsabilidades y roles en la seguridad de la información
  - Concienciación en la seguridad de la información

- **II. Arquitectura y Modelos de Seguridad:** Conceptos, principios, estructuras y estándares empleados para diseñar, monitorizar y asegurar sistemas, equipos, redes, aplicaciones y controles usados para reforzar los diversos niveles de la disponibilidad, integridad y confidencialidad:
  - Conceptos de control y seguridad
  - Modelos de seguridad
  - Criterios de evaluación
  - Seguridad en entornos cliente/servidor y host
  - Seguridad y arquitectura de redes
  - Arquitectura de la seguridad IP

- **III. Sistemas y Metodología de Control de Acceso:** Conjunto de mecanismos que permiten crear una arquitectura segura para proteger los activos de los sistemas de información:
  - Conceptos y tópicos
  - Identificación y autenticación
  - Equipo de e-security.
  - Single sign-on.
  - Acceso centralizado / descentralizado / distribuido.
  - Metodologías de control.
  - Monitorización y tecnologías de control de acceso.

- **IV. Seguridad en el Desarrollo de Aplicaciones y Sistemas:** Define el entorno donde se diseña y desarrolla el software y engloba la importancia crítica del software dentro de la seguridad de los sistemas de información:
  - Definiciones
  - Amenazas y metas de seguridad
  - Ciclo de vida
  - Arquitecturas seguras
  - Control de cambios
  - Medidas de seguridad y desarrollo de aplicaciones
  - Bases de datos y data warehousing
  - Knowledge-based systems

- **V. Seguridad de las Operaciones:** Usado para identificar los controles sobre el hardware, medios y los operadores y administrador con privilegios de acceso a algún tipo de recurso:
  - Recursos
  - Privilegios
  - Mecanismos de control
  - Abusos potenciales
  - Controles apropiados
  - Principios
- **VI. Criptografía:** Los principios, medios y métodos de protección de la información para asegurar su integridad, confidencialidad y autenticidad:
  - Historia y definiciones
  - Aplicaciones y usos de la criptografía
  - Protocolos y estándares
  - Tecnologías básicas
  - Sistemas de encriptación
  - Criptografía simétrica / asimétrica
  - Firma digital
  - Seguridad en el correo electrónico e Internet empleando encriptación
  - Gestión de claves

- Public key infrastructure (PKI)
- Ataques y criptoanálisis
- Cuestiones legales en la exportación de criptografía

- **VII. Seguridad Física:** Técnicas de protección de instalaciones, incluyendo los recursos de los sistemas de información:
  - Gestión de las instalaciones
  - Seguridad del personal
  - Defensa en profundidad
  - Controles físicos
- **VIII. Seguridad en Internet, Redes y Telecomunicaciones:** Incluye los dispositivos de la red, los métodos de transmisión, formatos de transporte, medidas de seguridad y autenticación:
  - Gestión de la seguridad en la comunicaciones:
  - Protocolos de red
  - Identificación y autenticación
  - Comunicación de datos
  - Seguridad de Internet y Web
  - Métodos de ataque
  - Seguridad en Multimedia

- **IX. Recuperación ante Desastres y Planificación de la Continuidad del Negocio:** Dirige la preservación del negocio en el caso de producirse situaciones de parada para la restauración de las operaciones:
  - Conceptos de recuperación ante desastres y de negocio
  - Procesos de planificación de la recuperación
  - Gestión del software
  - Análisis de Vulnerabilidades
  - Desarrollo, mantenimiento y testing de planes
  - Prevención de desastres

- **X. Leyes, investigaciones y Ética:** Engloba las leyes y regulaciones de los crímenes informáticos, las técnicas y medidas de investigación, recuperación de evidencias y códigos éticos:
  - Leyes y regulaciones
  - Gestión de incidentes
  - Gestión de la respuesta ante incidentes
  - Conducción de investigaciones
  - Ética en la seguridad de la información
  - Código ético del (ISC)²

Tiempo: 40 horas.

Instructores Certificados.