

# CISSP BOOTCAMP

CISSP001

CISSP: Certified Information Systems Security Professional

La certificación CISSP ha sido creada para atenuar uno de los principales problemas en el área de seguridad informática, el cual es estar seguros que la persona que se dice conocedora dentro de esta área cuente con los conocimientos necesarios. La (ISC)<sup>2</sup> (International Information Systems Security Certification Consortium) es un organismo independiente creado para realizar la certificación de profesionales en seguridad informática. Ellos son los encargados de crear el examen CISSP.

Creada en 1989 como un consorcio de líderes de la industria sin ánimo de lucro, (ISC)<sup>2</sup> se dedica a ofrecer credibilidad reconocida internacionalmente a los profesionales de la seguridad de la información en cada nivel y en cada especialidad de la seguridad de la información.

## Descripción:

Curso preparatorio INTERNACIONAL de dedicación Full Time durante una semana para certificar CISSP. Se profundizan y actualizan todos los aspectos que involucra la certificación, realizando este seminario que lo prepara para rendir exitosamente la certificación CISSP

I-SEC Education Center ha alcanzado hasta la fecha una efectividad de 100 % de aprobados entre los participantes del Bootcamp que han aplicado para certificarse.

Los instructores que dictarán el curso son todos certificados CISSP.

## ¿A quién esta dirigido?:

Dirigido especialmente a Profesionales de Áreas de Sistemas, Consultores de Tecnología, Auditores Internos y Externos de Sistemas, Profesionales, Administradores y Responsables de Seguridad Informática que deseen validar sus Conocimientos con la certificación de seguridad de mayor prestigio y Reconocimiento a nivel mundial.

## Requisitos del Participante

- Conocimientos básicos de lo que es la seguridad informática
- Experiencia en el ramo de la seguridad informática
- Domino del idioma inglés
- Capacidad de lectura y autoestudio.

## Metodología

Se trata de un curso de preparación para el examen (Bootcamp). De 45 horas con 5 sesiones de 9 horas cada una. Realizándose un test con ejercicios de similares características y temática al examen.

## Material:

Contenido académico del Seminario (Presentaciones) y material de trabajo para las compañías (Planillas, documentos soportes, tableros de control y seguimiento) y documentación relacionada con la certificación.

## Temario:

### 1. Prácticas de Gestión de la Seguridad

Identificación de los recursos de información, desarrollo, documentación e implementación de políticas, normas, procedimientos y directrices.

- Conceptos y objetivos
- Gestión de riesgo
- Políticas y procedimientos
- Clasificación de la información
- Papeles de seguridad de la información y responsabilidades
- Conciencia de seguridad de la información

### 2. Arquitectura de la seguridad & Modelos

Conceptos, principios, estructuras y normas utilizadas para diseñar, controlar y asegurar sistemas operativos, equipos, redes, aplicaciones y controles utilizados para imponer varios niveles e disponibilidad, integridad y confidencialidad.

- Informática y arquitectura
- Seguridad y conceptos de control
- Modelos de seguridad

- Criterios de Evaluación
- Seguridad basada en el huésped y cliente/servidor
- Arquitectura de red y seguridad
- Arquitectura de seguridad IP

### **3. Sistemas de Control de Acceso & Metodología**

Una colección de mecanismos que funcionan juntos para crear una arquitectura de seguridad para proteger los recursos del sistema de la información.

- Conceptos y temas
- Identificación y autenticación
- Firma única
- Acceso centralizado/descentralizado/distribuido metodologías de control
- Tecnologías de control de acceso y control

### **4. Seguridad de Desarrollo de la Aplicación**

Perfila el entorno cuando se diseña y desarrolla el software y explica el papel crítico que juega el software que facilita a la hora de suministrar seguridad al sistema de información

- Definiciones
- Objetivos y amenazas de la seguridad
- Ciclo de vida del sistema
- Arquitectura de seguridad
- Control de cambio
- Medidas de desarrollo de la aplicación y de seguridad
- Bases de datos y almacenaje
- Sistemas basados en el conocimiento

### **5. Seguridad de Operaciones**

Utilizado para identificar los controles en el hardware soporte y operadores y administradores con privilegios de acceso a cualquiera de estos recursos.

- Recursos
- Privilegios
- Mecanismos de control
- Abusos de potencial
- Controles apropiados

## 6. Criptografía

Los principios, medios y métodos de información para asegurar su integridad, confidencialidad y autenticidad

- Historia y definiciones
- Aplicaciones y usos de criptografía
- Protocolos y normas
- Tecnologías básicas
- Sistemas de cifrado
- Criptografía simétrica/asimétrica
- Firmas digitales
- Seguridad de Internet y de correo utilizando criptografía
- Gestión de clave
- Infraestructura de clave pública (PKI)
- Criptoanálisis y ataques
- Asuntos de exportación

## 7. Seguridad física

Técnicas de protección para toda la instalación, incluyendo todos los recursos del sistema de información

- Gestión de instalaciones
- Seguridad del Personal
- Defensa en profundidad
- Controles físicos

## 8. Seguridad de las Telecomunicaciones, Redes e Internet

incluye las estructuras de red, los métodos de transmisión, formatos de transporte, medidas de seguridad y autenticación.

- o Gestión de seguridad de las comunicaciones
- o Protocolos de red
- o Identificación y autenticación
- o Comunicaciones de datos
- o Seguridad de Internet y de la Web.
- o Métodos de ataque
- o Seguridad Multimedia

## 9. Planificación continúa de Negocio (BCP) y recuperación de Desastre

Trata de la conservación del negocio en caso de apagones de las operaciones normales de negocio.

- Conceptos de negocio y de recuperación de desastre
- Proceso de planificación de recuperación
- Gestión de programa
- Evaluación de vulnerabilidad
- Desarrollo, mantenimiento y prueba del plan
- Prevención del desastre

## 10. Leyes, investigaciones y Ética

Trata de las leyes y normas referentes a la informática, medidas de investigación y técnicas, reunir pruebas, y código de conducta.

- Normas y leyes
- Gestión del incidente
- Gestión de respuesta del incidente
- Investigaciones de conducta
- Ética de seguridad de la información
- Código de Ética (ISC)2

### Test final de cada Módulo

- Examen final de simulación de 250 preguntas
- Workshop final de respuestas