

# CISSP Security Training

## Objetivo

---

Los objetivos del presente entrenamiento son:

- Que los asistentes conozcan acerca del (ISC)2 y de la certificación CISSP.
- Que los asistentes se familiaricen con el formato de examen utilizado por (ISC)2.
- Que los asistentes comprendan los dominios de la certificación.
- Que los asistentes se familiaricen con documentación complementaria para cada dominio.
- Que los asistentes conozcan que aspectos deben fortalecer para rendir la certificación en forma exitosa.

## Descripción

---

El curso consistirá en la explicación de los temas de cada módulo por parte de un instructor certificado seguido de la presentación de ejemplos y casos prácticos, con el objetivo de que los asistentes asimilen los conocimientos contenidos en dichos módulos.

Adicionalmente, en cada módulo el instructor presentará una serie de documentos que complementarán el contenido teórico del curso y dotará a los asistentes de información de alto valor para el desempeño de sus tareas cotidianas.

## Habilidades a adquirir

---

Al completar el entrenamiento, cada asistente conocerá los aspectos más importantes de cada módulo y tendrá experiencia en responder preguntas de características similares a las que se enfrentará en el proceso de certificación. Adicionalmente conocerá diversos recursos que le permitirán ampliar o complementar los temas vistos con el objetivo de rendir exitosamente dicha certificación.

## Pre-requisitos

---

Se recomienda que los asistentes posean conocimientos básicos de controles de Seguridad de la Información y Networking

## Duración

---

40 hs.

# CISSP Security Training

## Audiencia

---

El entrenamiento se encuentra dirigido a:

- Oficiales de Seguridad de la Información
- Administradores de sistemas
- Administradores de redes
- Profesionales de tecnología que quieran especializarse en Seguridad de la Información
- Estudiantes y entusiastas que quieran iniciarse en Seguridad de la Información

## Perfil de instructores

---

IT College y SIClabs (empresa asociada para el dictado de los cursos de Seguridad informática) ponen a disposición del cliente un equipo de profesionales altamente calificados en la temática del entrenamiento y con amplia experiencia en docencia. Para esta capacitación en particular, el instructor a cargo dispone de las siguientes cualidades:

- Títulos de Ingeniero en Informática y Especialista en Telecomunicaciones.
- Certificación CISSP otorgada por el ISC2 en el año 2009.
- Experiencia en el desarrollo de cursos de capacitación en materia de Seguridad de la Información y Networking.
- Amplia experiencia en el dictado de cursos similares, tanto en el ambiente nacional como en el ambiente internacional.
- Disertante en prestigiosos eventos de Seguridad de la Información, tanto en el ámbito nacional como internacional.
- 13 años de experiencia comprobable como profesional de Seguridad de la Información y Networking.

## Temario

---

- Gobierno de la Seguridad de la Información y Gestión del Riesgo
  - ✓ Introducción a la Seguridad de la Información
  - ✓ Gestión de la Seguridad de la Información
  - ✓ Marco Normativo
  - ✓ Gestión del Riesgo
  - ✓ Cumplimiento y Regulación
  - ✓ Computer Crime

# CISSP Security Training

- ✓ Concientización de Usuarios
- ✓ BCP / DRP
  
- Protección de Recursos
  - ✓ Política de Protección de Datos
  - ✓ Ciclo de Vida de la Información
  - ✓ Calidad de la Información
  - ✓ Estadíos de la información
  - ✓ Controles
  
- Ingeniería de Seguridad
  - ✓ Arquitectura de Computadoras
  - ✓ Mecanismos de Protección
  - ✓ Modelos de Seguridad
  - ✓ Modos de Seguridad
  - ✓ Arquitecturas Cloud
  - ✓ Guías de Evaluación
  - ✓ Certificación & Acreditación
  - ✓ Criptografía
  
- Telecomunicaciones y Seguridad de la red
  - ✓ Modelo de Referencia OSI
  - ✓ Redes de Datos
  - ✓ Métodos de Acceso
  - ✓ TCP/IP
  - ✓ Dispositivos de Red
  - ✓ Firewalls
  - ✓ Redes Privadas Virtuales (VPN)
  - ✓ Wireless LAN
  - ✓ Ataques Típicos en Red
  - ✓ Recomendaciones y Buenas Prácticas
  
- Gestión de Accesos e Identidades
  - ✓ Tipos de control de acceso
  - ✓ Implementación de control de acceso
  - ✓ Identificación, autenticación, autorización y auditoría
  - ✓ Técnicas de identificación y autenticación
  - ✓ Passwords

# CISSP Security Training

- ✓ Sistemas Biométricos
- ✓ Tokens / Tickets / Single Sign On
- ✓ Modelos de control de acceso
- ✓ Administración de control de acceso
- ✓ Monitoreo, Auditoría y Logs
- ✓ Sistemas de Detección de Intrusos (IDS)
  
- Evaluaciones de Seguridad
  - ✓ Log Management
  - ✓ Monitoreo en Arquitecturas Web
  - ✓ Monitoreo y Revisión de Código
  - ✓ Vulnerabilidades Comunes en Software
  - ✓ Vulnerability Assessment & Pentest
  - ✓ Security Operations Center (SOC)
  
- Seguridad en las Operaciones
  - ✓ Gestión administrativa
  - ✓ Controles
  - ✓ Gestión y Respuesta ante Incidentes
  - ✓ Forensia
  - ✓ Prevención de Fuga de Información
  - ✓ Malware
  - ✓ Seguridad Física y Ambiental
  
- Seguridad en el Ciclo de Vida de Desarrollo de Software
  - ✓ Conceptos Generales
  - ✓ Arquitectura de Aplicaciones
  - ✓ Lenguajes de Programación
  - ✓ Bases de Datos
  - ✓ Desarrollo de Aplicaciones
  - ✓ Modelos de Desarrollo de Aplicaciones
  - ✓ Mantenimiento y Soporte
  - ✓ Amenazas y Ataques