La Información es el activo más importante de la Organización y de las personas. La seguridad que puede lograrse por medios técnicos es
limitada y debe ser respaldada por una gestión y procedimientos
adecuados.

Para llevar adelante una adecuada gestión de la Seguridad de la Información es necesario contar con personal altamente calificado y las certificaciones internaciones ayudan a cumplir este objetivo.

Objetivos generales:
Este curso, conocido como Bootcamp CISSP 2015, está orientado a hacer conocer el cuerpo de estudio (CBK) de CISSP (Certified Information System Security Professional), la certificación de Seguridad de la Información más aceptada por los profesionales de seguridad de todo el mundo.

¿Qué es la certificación (ISC 2) CISSP?
CISSP es la Certificación de mayor reconocimiento internacional como profesional integral con el mismo valor académico y profesional en cualquier lugar y que reúne
alrededor de 30.000 profesionales en el mundo. La Certificación CISSP es entregada por organización ISC 2 , una organización sin fines de lucro dedicada a aspectos de seguridad de la información y que ha provisto Certificaciones Internacionales a profesionales desde 1992.

Es una de las pocas Certificaciones que ha logrado el Estándar ISO/IEC 17024 como □□□□□□□□□□ “General requirements for bodies operating certification of persons”.

Consta de 8 dominios de estudio (conocidos como CBK - Base Común de Conocimiento) que cubren gran parte del conocimiento y experiencia actual en seguridad de la información.

El proceso de Certificación consta de tres etapas:
• Examination (rendir un examen) para el cual este Bootcamp lo prepara.
• Certification (verificar experiencia del interesado y código de ética).
• Audit (revisión de antecedentes del interesado).

Público Objetivo
El curso está orientado a CIO, CSO, responsables y administradores de seguridad de la información, analistas de riesgo, área de auditoría.

Finalizado el curso, el asistente será capaz de:
• Conocer la Certificación CISSP
• Conocer los ocho dominios que forman parte de la Certificación CISSP
• Conocer la metodología de evaluación y los tipos de preguntas realizadas
• Rendir la Certificación (opcional y no incluida en el curso)
• Conocer los distintos tipos de análisis de seguridad

Material a entregar:
Presentaciones utilizadas durante el curso en formato impreso y digital.

Instructor:
Cristian Borghello es Licenciado en Sistemas (UTN), desarrollador, Certified Information Systems Security Professional (CISSP), Certificate of Cloud Security Knowledge (CCSK), Microsoft MVP (Most Valuable Professional) Security.
Actualmente es Director de Segu-Info y Segu-Kids y se desempeña como consultor independiente en Seguridad de la Información.
Escribe para diversos medios especializados e investiga en forma independiente sobre Seguridad Informática y de la Información.
Ha brindado cursos y dictado congresos y seminarios nacionales e internacionales sobre la temática.

Duración y Modalidad
Este curso teórico tiene una duración de 40 horas y la modalidad de cursada es presencial. También puede ser desarrollado in-company**.**

Temario
• Introducción.
• Información sobre ISC2 y la Certificación CISSP.
• Inscripción y procedimiento para la inscripción en la Certificación.

Dominio 1 - Security and Risk Management
• The Big Three
• Clasificación de la información
• Políticas de seguridad. Estándares. Normas (Guidelines). Baselines. Procedimientos
• Roles y responsabilidad
• Administración y gestión de riesgos
• Análisis Cuantitativo vs Análisis Cualitativo
• Administración y control de cambios
• Modelado de amenazas
• ISO 27000 y SGSI
• Computer Crime
• Ética
• Leyes de los EE.UU.
• Investigación y Evidencia
• Respuesta a Incidentes

Examen 20 preguntas

Dominio 2 - Asset Security
• Evaluación de Activos
• Arquitectura de Computadoras
• Mecanismos de Protección
• Modos de Seguridad

• Guías de Evaluación
• Certificación vs Acreditación
• Concientización y Awareness
• Roles y Responsabilidades
• Políticas y Prácticas de Empleo
• Tipos de Ataques

Examen 20 preguntas

Dominio 3 - Security Engineering
• Trusted Computing Base
• Criterios de evaluación
• Modelos de Seguridad
• Cloud Computing
• Historia de la Criptografía y Conceptos Básicos
• Algoritmos clásicos
• Matemática Binaria y usos de la Criptografía
• Tipos de Algoritmos
• Algoritmos de Clave Privada y Clave Pública
• Hashing
• Tipos de ataques criptográficos
• Firma Digital y HMAC
• PKI

Examen 20 preguntas

Dominio 4 - Telecommunications and Network Security
• Modelo de Referencia OSI
• Medios y Protocolos de Transmisión
• Cableado
• Topologías y Métodos de Acceso
• Protocolos TCP/IP y comparación con OSI
• Dispositivos LAN
• Tecnologías WAN
• Tecnologías Wi-Fi
• Acceso Remoto
• Protocolos Wireless
• Ataques y Abusos de Red

Examen 20 preguntas

Dominio 5 - Identity and Access Management
• Tipos de control de acceso
• Implementación de control de acceso
• Identificación, autenticación, autorización y auditoría (AAA)
• Técnicas de identificación y autenticación
• Utilización de Passwords
• Sistemas Biométricos
• Single Sign On (SSO)
• Kerberos y otros protocolos SSO
• Modelos de control de acceso
• Administración de control de acceso
• Monitoreo, Auditoria y Logs
• Sistemas de Detección de Intrusos (IDS e IPS)

Examen 20 preguntas

Dominio 6 - Security Assessment and Testing
• Amenazas y Ataques
• Análisis de Impacto de Negocio (BIA)
• Requerimientos
• Formación de un Equipo de trabajo
• Bussiness Continuity Plan (BCP)
• Tipos de Backups
• Documentación
• Testing

Examen 20 preguntas

Dominio 7 - Operations Security
• Gestión administrativa
• Evaluación de productos
• Controles
• Seguridad en servicios
• Antivirus Management
• Métodos de ataque y Auditoría
• Protección Perimetral
• Sistemas de Vigilancia y Detección
• Requerimientos de un centro de cómputos
• Prevención, Detección y Supresión de Incendios

Examen 20 preguntas

Dominio 8 - Security Software Development Lifecycle
• Paradigmas de Desarrollo de Aplicaciones
• Modelos de Desarrollo de Aplicaciones
• Software Capability Maturity Model (CMM)
• Bases de Datos
• Mantenimiento y Soporte
• Códigos Maliciosos

Examen 20 preguntas

Examen de 250 preguntas