

DIPLOMATURA

en

Seguridad de la Información y Auditoría de Sistemas

ISO 27001 – COBIT 4.0
(ESP001)

CISO Program 2008



(Única Carrera de Nivel Internacional con 5 Orientaciones Profesionales)

ISEC forma desde hace más de 5 años a nivel internacional a los más importantes líderes del sector de seguridad de la información, mediante programas de alcance regional con visión estratégica de las más que actuales tendencias del mercado.

Certifíquese **ISEC+** (Information Security Engineer Certified +) y obtenga reconocimiento internacional del más alto nivel. Este programa aplica para esta certificación.

Usted obtendrá conocimientos teóricos y prácticos, interactuando con los referentes del mercado, y disponiendo de instructores que trabajan en la temática y le aportarán una visión práctica.

Además tendrá posibilidad de realizar tesis y exposiciones en congresos internacionales (solo previa aprobación), plan de pasantías e intercambios con el exterior.

- ♦ **Única Carrera de Nivel Superior** en Latinoamérica que prepara a los **Líderes** en Seguridad de la Información.
- ♦ **Visión Estratégica** y Orientada a Resultados sobre los distintos Aspectos de la Seguridad, ya que aborda contenidos Técnicos y

Funcionales, que se aplicarán luego en **Laboratorios Prácticos con PCs**.

- ◆ Usted adquirirá una formación Integral y Profesional que le permitirá tener una visión Exhaustiva y Enfocada a los más altos Estándares Internacionales.
- ◆ Participe de este prestigioso Seminario de Reconocimiento Regional (Se dicta en 10 países y cuenta con mas de 500 graduados).
- ◆ Durante el último mes de Cursada podrá elegir una de las cinco ORIENTACIONES PROFESIONALES que más se ajuste a su perfil, con el objetivo de intensificar sus conocimientos. Estas son:
 - CISA -Auditoría (COBIT 4.1)
 - Técnicas Forenses
 - Aspectos Legales
 - Certified Ethical Hacker
 - Certificación CISSP
- ◆ Actualice, Perfeccione y Renueve sus Conocimientos con **ISEC**, una institución de reconocimiento y aval internacional.

¿A quién está dirigido?:

Responsables y profesionales de áreas de Seguridad Informática, Sistemas, IT, Auditoria.

Desarrolladores, Programadores y Peritos.

Consultores, Auditores externos e internos.

Abogados, Contadores, Ingenieros que deseen focalizar su Carrera.

Managers (Pymes y Medianas empresas).

Único programa de Capacitación Profesional en Seguridad Informática Teórico y Práctico diseñado para adquirir metodologías y herramientas de implementación y control de medidas de Seguridad de la Información de acuerdo a estándares internacionales.

Descripción General:

Lugar:

Dependiendo del país se dictarán en las oficinas de I-SEC, en Universidades o Centros de estudio
En Argentina se dictan en nuestras instalaciones, ubicadas en el Palacio San Miguel, Bartolomé Mitre 948, Ciudad Autónoma de Buenos Aires -

Carga Horaria:

Consulte por los horarios de su país

Módulo Teórico: 145 Horas

Argentina : Miércoles de 9.00 a 13.00 hs. o de 18.30 a 22.30 hs.

Peru: Segunda semana de cada mes lunes y martes de 18.00 a 22.00 hs

USA: Semana intensiva (2da. de mayo, julio, septiembre)

Módulo Práctico: (de cursada opcional, sugerimos su cursada)

Argentina: Jueves de 18.30 a 21.30 hs.

Peru: viernes y sábados de 13.00 a 18.00 hs

USA: Última semana intensiva

Ecuador-Colombia- Paraguay- Bolivia- Venezuela (consultar)

Requisitos:

Conocimientos básicos de Sistemas y/o Auditoría de Sistemas.

Experiencia laboral en áreas de Sistemas, Auditoría, Administración, TI, Legales, Desarrollo o Contraloría.

Material de Apoyo:

Módulos Impresos. CD con Manuales y Herramientas de actualización.

Kit ISEC (material de lectura + lapicera+ carpeta+ Block)

Certificado de Asistencia:

Con el cumplimiento del 75 % de las actividades obligatorias.

Temario a Desarrollar

Módulos Funcionales

MF.01. La Seguridad Informática actual

Riesgos e impacto en los Negocios

- Normas aplicables
- Enfoque ISO 17799

Taller Práctico: Implementación de un Programa Integral.

MF.02. Políticas de Seguridad

Conocer los responsables de la redacción y aprobación del Manual de Seguridad

- Identificar la estructura y los temas de seguridad que debieran incluirse
- Definir etapas para el desarrollo y posterior mantenimiento del Manual
- Conocer la metodología de implementación de las Políticas de Seguridad basados en ISO17799

Requerimientos de Normativas Internacionales

- Etapas Generales para el Desarrollo e Implementación del Manual de Gestión de Seguridad de la Información MGSÍ

Taller Práctico: Desarrollo e Implementación de Políticas de Seguridad. Entrega del Manual de Gestión de Seguridad.

MF.03. Estructura Organizacional

Conocer los Roles y Responsabilidades en la Compañía y el Perfil del personal para cada rol

- Definir Responsabilidades con Terceros y Contratados, y consideraciones particulares para Servicios de "HOSTING"
- Identificación de los requerimientos de ISO 17799
- Definición de Roles y Responsabilidades en la Compañía
- Asignación de Perfiles del personal para cada rol
- Responsabilidades con Terceros y Contratados
- Consideraciones particulares para Servicios de "HOSTING"

Taller Práctico: Implementación de los distintos roles.

MF.04. Clasificación de Información

Identificar los Requerimientos Normativos para la Clasificación de la Información y definir una Metodología Práctica de Implementación

- Marco Normativo ISO 17799
- Normativa Interna
- Metodología Práctica de Clasificación

Taller Práctico: Clasificación de Información de una Organización.

MF.05. Aspectos humanos de la seguridad

Identificar los aspectos a implementar en relación con las obligaciones, derechos y comportamiento de las personas de la compañía y terceros en el manejo de la información

- Riesgos relacionados con las personas
- Marco Normativo ISO 17799
- Metodología Práctica de:
- Administración del Personal
- Manejo de Incidentes
- Proceso Disciplinario
- Concientización

Taller Práctico: Implementación real.

MF.06. Seguridad en los Procesos Internos del área de Sistemas

Adquirir conocimientos, metodologías y herramientas para poder implementar controles en los procesos del área de Sistemas de una compañía.

- Sistemas Informáticos
- Telefonía
- Comunicaciones Satelitales
- Outsourcing de Funciones en Proveedores
- Servicios de Hosting/Housing a Terceros.

MF.07. Sistemas de Control de Accesos

Adquirir conocimientos, metodologías y herramientas para poder implementar un Sistema de Control de Accesos Lógicos a la información sensible y los recursos informáticos en una compañía.

- Requerimientos ISO 17799
 - Definición de Sistemas de Control de Accesos
 - Implementación, Plan de Monitoreo y Mejora Continua
- Taller Práctico: Desarrollo de Sistema de Permisos en un Sector Funcional de una Empresa.

MF.08. Seguridad en el Desarrollo y Mantenimiento de Sistemas

Adquirir conocimientos, metodologías y herramientas de Seguridad para el Desarrollo y Mantenimiento de Sistemas en una compañía.

- Requerimientos ISO 17799
 - Normativa relacionada
 - Implementación, Plan de Monitoreo y Mejora Continua
- Taller Práctico: Desarrollo de Entornos de Trabajo y Permisos.

MF.09. Seguridad en Sistemas Aplicativos

Adquirir conocimientos, metodologías y herramientas para los Desarrollos de Sistemas Aplicativos en una compañía.

- Requerimientos ISO 17799
 - Normativa relacionada
 - Participación en Proyectos de Desarrollo e Implementación
- Taller Práctico: Desarrollo de Controles en Sistema Aplicativo.

MF.10. Plan de Continuidad del Negocio

Adquirir conocimientos, metodologías y herramientas para poder implementar un Plan de Continuidad de los Negocios en una compañía.

- Consideraciones Generales
 - Requerimientos ISO 17799
 - Etapas de un Plan
 - Implementación, Plan de Monitoreo y Mejora Continua
- Taller Práctico: Desarrollo de un Plan de Continuidad de los Negocios.

MF.11. Marco Normativo y Legal

Adquirir conocimientos, metodologías y herramientas para poder conocer los Riesgos y Delitos Informáticos, Organismos y Normas Internacionales, Marco Legal y Regulatorio.

- Riesgos y Delitos Informáticos
- Organismos y Normas Internacionales
- Requerimientos de ISO 17799
- Marco legal
- Normativa específica del Banco Central
- Implementación, Plan de Monitoreo y Mejora Continua.

www.i-sec.org Página 6 de 9

MF.12. Auditoría de Sistemas

Adquirir conocimientos, metodologías y herramientas para poder conocer los alcances de las tareas de Auditoría de Sistemas de Información según Normas Internacionales.

- Referencia Histórica
- Tipos y enfoques de Auditoría
- Administración de Proyectos
- Administración y prevención de riesgos
- Estándares • COSO / • CoBiT • ISO 17799
- Etapas de una Auditoría / Auditoría de Sistemas
- Procedimientos a realizar en una Auditoría de Controles
- Herramientas de Auditoría
- Desarrollo de una Auditoría de Sistemas
- ANEXO : Relación entre estándares y cumplimiento de Normas Internacionales (SOX)
- Planteo de un caso práctico.

Módulos Técnicos

MT.01. Seguridad en redes

Introducción y Situación Actual

- Principales Componentes de una red de información
 - Principales Riesgos y Vulnerabilidades de las redes
 - Vulnerabilidades y consideraciones de seguridad para cada componente
- Taller Práctico: Implementación de una Red con Criterios de Seguridad.

MT.02. Seguridad en Sistemas operativos

Etapas Metodológicas

- Principales Consideraciones de seguridad
- Taller Práctico: Desarrollo de un Estándar de Seguridad para Sistemas Operativo.

MT.03. Seguridad en Equipos de Comunicación

Consideraciones de seguridad en las comunicaciones en redes:

- LAN
- WAN
- Otras Tecnologías.

MT.04. Seguridad en Servicios de Correo

Etapas Metodológicas

- Principales Consideraciones de seguridad

Taller Práctico: Desarrollo de un Estándar de Seguridad para Servicios de Correo.

MT.05. Seguridad en Bases de Datos

Conceptos Introdutorios

- Etapas Metodológicas
- Principales Consideraciones de seguridad.

MT.06. Seguridad en Plataformas Microsoft

Windows NT 4.0

- Windows 2000
- Windows 2003
- Internet Information Server
- ISA Server
- SQL Server
- Exchange Server.

www.i-sec.org Página 7 de 9

MT.07. Seguridad en plataformas UNIX

Conceptos Introdutorios

- Etapas Metodológicas
- Principales consideraciones de Seguridad.

MT.08. Seguridad en LINUX

Conceptos Introdutorios

- Etapas Metodológicas
- Principales consideraciones de Seguridad.

MT.09. Herramientas de seguridad

Conceptos Introdutorios

- Principales herramientas de seguridad disponibles en el mercado: administración centralizada, encriptación, detección de intrusos, monitoreo, auditoria, antivirus.

MT.10. Métodos avanzados de Hacking y Protección

- Metodologías de Penetration Test
- Las técnicas de Hacking actuales
- Los diferentes perfiles de los atacantes
- Principales Ataques.

MT.11. Seguridad Avanzada

- Encriptación / Certificados Digitales
- IPsec / VPN
- Honeypots
- Respuesta a Incidentes
- Otras tecnologías asociadas (Biometría)

MT.12. Seguridad en Wireless y Centrales Telefónicas

Introducción

- 802.11

- Centrales Telefónicas
- VOIP.

Laboratorios
Escaneo de Redes
Auditoría de Sistemas operativos
Asegurar Equipos de Comunicación
Diseño de redes Seguras
Auditoría de Correo Electrónico
Asegurar plataformas Microsoft
Asegurar plataformas UNIX
Asegurar LINUX
Administración de Herramientas de seguridad
Ejecución de Test de Intrusión Internos y Externos
Construcción de VPN
Asegurar Wireless y Centrales Telefónicas

www.i-sec.org Página 8 de 9

Descripción de las Especializaciones

En el transcurso del último mes de la Especialización podrá elegir por cursar una de las siguientes Especializaciones.

CISA - Auditoría (COBIT 4.1)

El alto grado de sistematización del mercado ha generado que en la actualidad se requieran profesionales que puedan comprender integralmente la problemática de los sistemas, sus vulnerabilidades, puntos críticos y como hacer frente a ellos en forma adecuada.

Esta Especialización está diseñada para a formar auditores especializados en Sistemas de Información; le permitirá adquirir conocimientos, metodologías y herramientas para conocer los alcances de las tareas de Auditoría de Sistemas de Información según Normas Internacionales ISO 27001 y COBIT 4.0 y SOX.

Técnicas Forenses

Esta Especialización lo introducirá en las más actuales tendencias de las actividades y fases de una investigación Forense Informática, desde la adquisición de la Evidencia hasta su utilización como medio probatorio en un proceso Policial/Judicial, así como también demostrar el uso y aplicación de diversas herramientas informáticas para realizar el análisis y adquisición de datos.

Los alumnos que opten por esta Especialización obtendrán el conocimiento y la metodología de trabajo de una investigación Forense Informática.

Aspectos Legales

Esta especialización apunta a que el profesional sea capaz de:

- Identificar Bienes Intangibles a proteger.
- Utilizar Regulación legal respectiva.
- Actuar conforme el Alcance de su responsabilidad como directivo o empleado.
- Aplicar las Herramientas disponibles desde aspectos funcionales y técnicos.
- Promover la utilización de los instrumentos legales que orienten a una Política de Seguridad sólida en su organización.
- Poner en práctica medidas de implementación para cumplir con los aspectos legales.

Certified Ethical Hacker

Esta especialización le brindará un amplio conocimiento y práctica real en equipos de las más actuales herramientas y técnicas de ataque y defensa,

permitiéndonos gestionar y accionar en consecuencia.

Se verán y analizarán las últimas metodologías y técnicas de ataques utilizadas

en la actualidad, como así también las metodologías de Penetration Test.

Enfoque práctico con trabajo en los equipos informáticos, desarrollando distintos tipos de ataques en distintos tipos de entornos.

Participará de casos simulados en distintos entornos.

Certificación CISSP

La seguridad de la Información se ha convertido en uno de los rubros de mayor demanda de profesionales a nivel internacional. Hoy en muchos casos es requisito contar con certificaciones que respalden sus conocimientos, por lo que usted puede elegir aplicar a la certificación ISEC+, de reconocimiento regional, para luego aplicar a CISSP de reconocimiento Internacional.

Esta especialización de alto nivel, le permitirá repasar las últimas tendencias del mercado, analizando problemáticas reales, simulaciones de test y casos de estudio basados en las pautas requeridas para certificar CISSP.

Se efectuarán simulaciones de examen a lo largo del programa.
Se encontrará preparado para rendir satisfactoriamente el examen CISSP, pudiendo adicionalmente - si lo desea - cursar con un 50% de descuento el Bootcamp de repaso. (#2)

(#1) El cupo mínimo para abrir cada una de las especializaciones es 10 alumnos.

Se podrá modificar el día de cursada dependiendo de la especialización elegida.

(#2) El descuento del 50% aplica para aquellos alumnos de la Especialización que hayan aprobado la certificación ISEC+.

**NO DEJE PASAR LA OPORTUNIDAD DE FORMARSE
JUNTO A LOS LIDERES Y REFERENTES DEL MERCADO**

SEA PARTE DE LA COMUNIDAD ISEC

**POTENCIE SU CARRERA CON UNA DIPLOMATURA DE
NIVEL INTERNACIONAL**