

# ESPECIALIZACIÓN ANUAL EN SEGURIDAD DE LA INFORMACIÓN Y AUDITORÍA DE SISTEMAS

EN UN CONTEXTO ALTAMENTE COMPETITIVO Y DE CONSTANTE  
TRANSFORMACIÓN ES INDISPENSABLE DISPONER DE...

- Herramientas eficientes para mantener el negocio operativo, aún en casos de siniestros.
- Actualmente resulta imprescindible contar con la capacitación necesaria para recuperar en tiempo y forma los servicios de tecnología informática.
- I-SEC le ofrece el más alto nivel de capacitación para que administre eficazmente sus procesos y resguarde su información.

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.

## ¿A quién esta dirigido?

Responsables del área de Seguridad Informática, Profesionales del área de Sistemas y carreras afines, Consultores de TI, Auditores externos e internos y Gerentes Generales de PYMES.

## Modalidad

### Duración:

Anual

### Lugar:

En la Escuela de Negocios de Fundación Libertad, Mitre 170 - Rosario

**Carga Horaria Total: 145 hs.**

### Desarrollo Horario:

Viernes de 9.00 a 18.00 hs

### Requisitos:

Conocimientos básicos de sistemas y/o auditoría de sistemas.

Experiencia laboral comprobable en áreas de sistemas, auditoría, administración, TI.

### **Material de Apoyo:**

Módulos Impresos. CD con Manuales y Herramientas de actualización. Material Digital

### **Certificado de Asistencia:**

Con el cumplimiento del 75 % de las actividades obligatorias.

### **Contenidos**

#### **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 MGSI

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 Informaticos
- Telefonia
- 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

#### **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 Introductorios

- 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

**MT.07.** Seguridad en plataformas UNIX

Conceptos Introductorios

- Etapas Metodológicas
- Principales consideraciones de Seguridad

**MT.08.** Seguridad en LINUX

Conceptos Introductorios

- Etapas Metodológicas
- Principales consideraciones de Seguridad

**MT.09.** Herramientas de seguridad

Conceptos Introductorios

- 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**

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

**MT.12. Seguridad en Wireless y Centrales Telefónicas**

Introducción

- 802.11
- Centrales Telefonicas
- VOIP

**Laboratorios**

- Escaneo de Redes
- Auditoria de Sistemas operativos
- Asegurar Equipos de Comunicación
- Diseño de redes Seguras
- Auditoria 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

**Informes e inscripción**

La inscripción podrá realizarse personalmente en Mitre 170, Rosario.  
Telefónicamente al 0341-4105000 o vía mail a [info@centroit.org.ar](mailto:info@centroit.org.ar)