

# SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN ISO 27001 y LEY ORGÁNICA DE PROTECCIÓN DE DATOS

PRECIO  
**390 €**

CURSOS  
BONIFICABLES 100%  
por la Fundación  
Tripartita

**24 y 26 de Noviembre y 1, 3, 10 y 15 de Diciembre**  
de 16 a 21 h.



Fundación Tripartita  
PARA LA FORMACIÓN EN EL EMPLEO

**Oficinas Centrales de Nunsys**  
Parque Tecnológico

El curso versa sobre cómo implementar una arquitectura sólida respecto a la seguridad de la información en las empresas y entidades públicas y profundiza en la norma ISO/IEC 27001, la cual ofrece, a su vez, una aproximación formal y práctica a la seguridad en el mundo de las organizaciones y aporta el enfoque necesario para establecer un Sistema de Gestión de la Seguridad de la Información en función de las necesidades de negocio. También, se hace especial hincapié en el apartado de la normativa legal, especialmente en lo que se refiere a la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD) y al nuevo reglamento de la LOPD (RC1720/2007) que son de obligatorio cumplimiento por todas las empresas y organizaciones públicas y privadas españolas, incluyendo a los autónomos. A su vez, el curso no se queda sólo en una aproximación teórica sino que se realizan supuestos prácticos a nivel de red y aplicativo (técnicas de Hacking Ético) para comprobar el estado "real" de la seguridad. Asimismo, se profundizará en el Análisis de Riesgos, que consiste en determinar las principales amenazas que puedan afectar a la infraestructura IT de nuestra organización.

## OBJETIVOS

El curso nos introduce en el mundo de la seguridad de la información (SI) aplicada a las empresas y entidades públicas y profundiza en torno a los Sistemas de Gestión de la Seguridad de la Información (Norma ISO 27001) y la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD). Establecer una guía práctica, sencilla, ágil y lógica para implantar la norma ISO 27001 en las organizaciones.

## A QUIEN VA DIRIGIDO

Ingenieros Técnicos y Superiores en carreras técnicas, Directores Financieros y de Sistemas, Administradores, y en general cualquier persona relacionada con el mundo de los sistemas de información con ganas de introducirse o ampliar conocimientos en el área de seguridad de la información.

## PREREQUISITOS

Sin prerequisites estrictos en general. Recomendable conocimientos de informática a nivel usuario para un mejor aprovechamiento de los supuestos prácticos.

## REQUERIMIENTOS TÉCNICOS

- Acceso con cuenta de administrador al equipo
- Tener instalada la herramienta de virtualización VMware Server 2.0.
- Máquina virtual instalada: Backtrack 3.0
- Máquina virtual instalada: Ubuntu 8.10 Server
- Opcional: máquina virtual instalada con sistema Windows 2003 para realizar práctica extra.
- Visor de PDF
- Acceso a Internet..

### CONTENIDO

#### MÓDULO 1.

##### **Introducción la Seguridad de la Información.**

Tema 1.1. ¿Qué es la Seguridad de la Información?

Tema 1.2. Conceptos básicos sobre Seguridad de la información

Tema 1.3. Cómo aplicar la Seguridad de la Información en la empresa

##### **Evaluación**

Cuestionario Tipo Test Módulo I

#### MÓDULO 2.

##### **Presentación de la norma ISO/IEC 27001: Sistema de Gestión de la Información (SGSI). Información (SGSI).**

##### **Contenido**

Tema 2.1. Introducción

Tema 2.2. Antecedentes

Tema 2.3. La norma ISO 27001

Tema 2.4. Metodología

Tema 2.5. Proceso de Implantación y Certificación

##### **Evaluación**

Cuestionario Tipo Test Módulo II

#### MÓDULO 3.

##### **Controles orientados a la Seguridad Organizativa y Política de Seguridad según la norma ISO 27002.**

##### **Contenido**

Tema 3.1. Introducción

Tema 3.2. Política de Seguridad

Tema 3.3. Seguridad Organizativa

3.3.1 Organización Interna

3.3.2 Terceras Partes

3.3.3 Recursos Humanos

##### **Evaluación**

Cuestionario Tipo Test Módulo III

#### MÓDULO 4.

##### **Gestión de Activos. Análisis y Gestión del Riesgo.**

##### **Contenido**

Tema 4.1. Gestión de Activos

Tema 4.2. Análisis y Gestión del Riesgo

Tema 4.3. Práctica Módulo IV. Ejercicio práctico de Análisis de Riesgos

##### **Evaluación**

Cuestionario Tipo Test Módulo IV

#### MÓDULO 5.

##### **Plan de Adecuación al Esquema Nacional de Seguridad.**

##### **Contenido**

Tema 5.1. Introducción

Tema 5.2. Seguridad operativa

5.2.2 Procedimientos Operacionales y Responsabilidades

5.2.3 Gestión de los Servicios Realizados a Terceras Partes

5.2.4 Planificación

5.2.5 Protección contra Código Malicioso y Código Móvil

5.2.6 Copias de Seguridad

5.2.7 Gestión de Medios

5.2.8 Intercambio de Información

Tema 5.3. Seguridad Lógica

5.3.1 Requerimientos del Negocio para el Control de Acceso

5.3.2 Gestión del Acceso Lógico

5.3.3 Responsables de los Usuarios

5.3.4 Control de Acceso al Sistema Operativo

##### **Evaluación**

Cuestionario Tipo Test Módulo V

Prácticas

Virtualización: VMware Server 2.0

Comandos básicos de red

Copias de seguridad

Análisis de equipos Windows con MBSA.

#### MÓDULO 6.

##### **Seguridad de Red y Aplicativos. Hacking Ético**

##### **Contenido**

Tema 6.1. Introducción

Tema 6.2. Seguridad en Red

6.2.1 Gestión de la Seguridad en la Red

6.2.2 Controles de Acceso en la Red

6.2.3 Monitorización

6.2.4 Intercambio de Información

6.2.5 Computación de Comercio Electrónico

Tema 6.3. Seguridad en Aplicativos

6.3.1 control de Acceso a las Aplicaciones y a la Información

6.3.2 Requerimientos de Seguridad de los Sistemas de Información

6.3.3 Procesado Adecuado en las Aplicaciones

6.3.4 Controles Criptográficos

6.3.5 Seguridad en los Ficheros del Sistema

6.3.6 Procedimientos de Control de Cambios

6.3.7 Gestión de Vulnerabilidades Técnicas

### **Evaluación**

Cuestionario Tipo Test Módulo VI

Prácticas

Introducción al test de intrusión

Escaneo de puertos

Certificados OpenSSL (Instalación y configuración de una CA)

Vulnerabilidades web

### **MÓDULO 7.**

#### **Controles de Seguridad de Física según norma 27002.**

##### **Contenido**

Tema 7.1. Introducción

Tema 7.2. Áreas Seguras

Tema 7.3. Seguridad del Equipo

Evaluación

Cuestionario Tipo Test Módulo VI

### **MÓDULO 8.**

#### **Controles orientados a la Gestión de Incidencias y Continuidad de Negocio según ISO 27002.**

##### **Contenido**

Tema 8.1. Introducción

Tema 8.2. Informando de los Eventos y Debilidades Referidos a la Seguridad de la Información

Tema 8.3. Gestión de los Incidentes y Mejoras en la Seguridad de la Información.

Tema 8.4. Aspectos sobre la Seguridad de la Información relativos a la Continuidad de Negocio

Negocio

**Evaluación**

Cuestión Tipo Test Módulo VIII

### **MÓDULO 9.**

#### **Controles orientados al Cumplimiento Interno. Auditoría Interna**

##### **Contenido**

Tema 9.1. Introducción

Tema 9.2. Conformidad con las Políticas y Estándares de Seguridad y Conformidad Técnica

Tema 9.3. Auditoría Interna.

Tema 9.4. Monitorización

Evaluación

Cuestionario Tipo Test Módulo V

### **MÓDULO 10.**

#### **Controles orientados al Cumplimiento Regulatorio: LOPD, Reglamento de la LOPD y LSSICE.**

##### **Contenido**

Tema 10.1. Contenidos

Tema 10.2. Conformidad con los Requisitos Legales

Tema 10.3. LOPD y Reglamento

Tema 10.4. LSSI

Evaluación

Cuestionario Tipo Test Módulo X

Práctica

Supuesto Práctico Cumplimiento Regulatorio

### **DURACIÓN**

30 horas

### **PRECIO**

**390 €** (Cursos bonificables 100% por la Fundación Tripartita)

La formación está exenta de IVA.

El precio incluye las gestiones de la bonificación, la impartición del curso y la documentación al alumno.

### **LUGAR DE REALIZACIÓN**

NUNSYS, S.L. C/ Gustave Eiffel nº3. Parque Tecnológico.- Paterna, 46980 Valencia

T. 902 881 626 - [nunsys.com](http://nunsys.com)