



# Mantenimiento Informático y Gestión de Incidentes

## Modalidad:

e-learning con una duración 56 horas

## Objetivos:

- Conocer los componentes de un PC.
- Aprender sobre la arquitectura, la carcasa y placa base de un Ordenador.
- Realizar el Montaje de un Ordenador.
- Aprender a gestionar los incidentes en temas de seguridad informática.

## Contenidos:

### UNIDAD DIDÁCTICA 1. CONCEPTOS BÁSICOS DE INFORMÁTICA

El ordenador

Hardware y Software

Los datos: Bit y Byte

El sistema operativo

- Concepto de Sistema Operativo
- Evolución histórica de los Sistemas Operativos.
- Funciones principales de un Sistema Operativo
- Clasificación de los sistemas operativos
- Ejemplos de Sistema Operativo

Los programas o aplicaciones

### UNIDAD DIDÁCTICA 2. EL PC: HARDWARE

Componentes de un PC

Los periféricos

Manejo del Teclado y del Ratón



- Manejo del Teclado
  - Manejo del Ratón
- Tecnología de los Periféricos
- El monitor
  - El teclado
  - El ratón
  - La impresora
  - El escáner
  - El módem
- Posibles problemas y su solución

### UNIDAD DIDÁCTICA 3. ARQUITECTURA, LA CARCASA Y LA PLACA BASE

- Arquitectura del PC
- La carcasa
- La placa base
- Descripción física
  - Factores de forma

### UNIDAD DIDÁCTICA 4. SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS)

- Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención
- Identificación y caracterización de los datos de funcionamiento del sistema
- Arquitecturas más frecuentes de los sistemas de detección de intrusos
- Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad
- Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS

### UNIDAD DIDÁCTICA 5. IMPLANTACIÓN Y PUESTA EN PRODUCCIÓN DE SISTEMAS IDS/IPS

- Análisis previo de los servicios, protocolos, zonas y equipos que utiliza la organización para sus procesos de negocio.
- Definición de políticas de corte de intentos de intrusión en los IDS/IPS
- Análisis de los eventos registrados por el IDS/IPS para determinar falsos positivos y caracterizarlos en las políticas de corte del IDS/IPS
- Relación de los registros de auditoría del IDS/IPS necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de intentos de intrusión
- Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS



## UNIDAD DIDÁCTICA 6. CONTROL DE CÓDIGO MALICIOSO

Sistemas de detección y contención de código malicioso

Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar

Criterios de seguridad para la configuración de las herramientas de protección frente a código malicioso

Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a código malicioso

Relación de los registros de auditoría de las herramientas de protección frente a código maliciosos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad

Establecimiento de la monitorización y pruebas de las herramientas de protección frente a código malicioso

Análisis de los programas maliciosos mediante desensambladores y entornos de ejecución controlada