

# Ciberseguridad, Criptografía Y Delitos Telematicos



**Área:** Informática  
**Modalidad:** Teleformación  
**Duración:** 0 h  
**Precio:** 420.00€

[Curso Bonificable](#)  
[Contactar](#)  
[Recomendar](#)  
[Matricularme](#)

## OBJETIVOS

Aprender los conceptos fundamentales en materia de ciberseguridad, las amenazas y vulnerabilidades más importantes y la estrategia de respuesta a los ciberataques. Comprender el hardening y la seguridad de la información. Utilizar la auditoría en la detección de intrusos. Conocer los delitos tipificados y las fichas de delitos telemáticos.

## CONTENIDOS

Tema 1. Seguridad de comunicaciones y criptografía. Conceptos básicos de criptografía. Objetivos de seguridad criptográfica. Conceptos básicos de criptografía. ¿qué es encriptación? Asegurando datos con algoritmos criptográficos. Cifrar datos almacenados en disco. Introducción a la esteganografía. Modelo del esteganosistema. Uso de la esteganografía. Clasificación de la esteganografía. El archivo digital. Sistema de ficheros esteganográfico. Tema 2. Hacking, malware y DDOS. Hacking. Malware. Historia de los virus y gusanos. Spam. Ransomware y el secuestro de información. Virus. Hoax. Bombas lógicas. Caballos de troya. Gusanos. Contramedidas. Negación de servicio. Cómo funcionan los ataques DDOS. Como trabaja bots/botnets. Ataques smurf e inundación de SYN. Teardrop. Land. Envenenamiento DNS. Ping de la muerte. Contramedidas para dos/DDOS. Peligros planteados por el secuestro de sesión. Tema 3. Hardening y seguridad de la información. Conceptos y principios de la administración de la seguridad. Mecanismos de protección. Control/gestión de cambios. Conceptos de seguridad operacional. Control de personal. Tema 4. Auditoría y detección de intrusos. Auditoría. Monitorización. Técnicas de pruebas de penetración. Actividades inapropiadas. Amenazas y contramedidas indistintas. Sistemas de detección de intrusos. Tema 5. Delitos tipificados y fichas de delitos telemáticos. Principales categorías de crímenes de ordenador. Actividad criminal a través de web. Robo de información, manipulación de datos y usurpación de web. Terrorismo. Crímenes neotradicionales: vino viejo en nuevas botellas. Lavado de dinero.

## METODOLOGIA

- **Total libertad de horarios** para realizar el curso desde cualquier ordenador con conexión a Internet, **sin importar el sitio desde el que lo haga**. Puede comenzar la sesión en el momento del día que le sea más conveniente y dedicar el tiempo de estudio que estime más oportuno.
- En todo momento contará con un **asesoramiento de un tutor personalizado** que le guiará en su proceso de aprendizaje, ayudándole a conseguir los objetivos establecidos.
- **Hacer para aprender**, el alumno no debe ser pasivo respecto al material suministrado sino que debe participar, elaborando soluciones para los ejercicios propuestos e interactuando, de forma controlada, con el resto de usuarios.
- **El aprendizaje se realiza de una manera amena y distendida**. Para ello el tutor se comunica con su alumno y lo motiva a participar activamente en su proceso formativo. Le facilita resúmenes teóricos de los contenidos y, va controlando su progreso a través de diversos ejercicios como por ejemplo: test de autoevaluación, casos prácticos, búsqueda de información en Internet o participación en debates junto al resto de compañeros.
- **Los contenidos del curso se actualizan para que siempre respondan a las necesidades reales del mercado**. El departamento multimedia incorpora gráficos, imágenes, videos, sonidos y elementos interactivos que complementan el aprendizaje del alumno ayudándole a finalizar el curso con éxito.

## REQUISITOS

Los requisitos técnicos mínimos son:

- Navegador Microsoft Internet Explorer 8 o superior, Mozilla Firefox 52 o superior o Google Chrome 49 o superior. Todos ellos tienen que tener habilitadas las cookies y JavaScript.
- Resolución de pantalla de 1024x768 y 32 bits de color o superior.