



CONTENIDO FORMATIVO CURSO TÉCNICO EN CIBERSEGURIDAD

● **FASE ON-LINE**

○ **ANÁLISIS DE INCIDENTES Y FORENSE BÁSICO: (36h de dedicación)**

- Objetivo del curso: adquirir conceptos básicos en materia de ciberseguridad. Se hará especial hincapié en ciberdelitos como el *Cyberbullying*, el *Grooming* o el fraude electrónico y estafas en Internet para la prevención, concienciación y protección a ciudadanos.
- Contenidos:
 - Unidad 0 : Bienvenido al curso
 - Unidad 1 : Introducción a la ciberseguridad
 - Unidad 2 : Informática, redes y sistemas operativos
 - Unidad 3 : Conoce los riesgos y amenazas
 - Unidad 4 : Uso seguro de las nuevas tecnologías
 - Unidad 5 : *Cyberbullying* o ciberacoso
 - Unidad 6 : *Grooming* o acoso virtual a menores
 - Unidad 7 : Pedofilia
 - Unidad 8 : Fraude electrónico y estafas en Internet
 - Unidad 9 : Extorsión
 - Unidad 10 : Robo de información
 - Unidad 11 : Prevención, concienciación y protección de los ciudadanos

○ **ANÁLISIS DE INCIDENTES Y FORENSE AVANZADO: (60h de dedicación)**

- Objetivo del curso: especialización en cuestiones relacionadas con cibercriminalidad o ciberterrorismo, adquiriendo conocimientos en materia de ciberseguridad, para la persecución de ciberdelitos y en la orientación y concienciación a ciudadanos.
- Contenidos:
 - Unidad 0 Bienvenido al curso
 - Unidad 1 Internet, estructura y funcionamiento
 - Unidad 2 Investigación tecnológica, análisis de amenazas e incidentes
 - Unidad 3 Gestión de incidentes de seguridad
 - Unidad 4 Herramientas para adquisición e introducción al análisis forense
 - Unidad 5 Análisis de artefactos Windows
 - Unidad 6 Análisis forense en dispositivos móviles (Android e iOS)
 - Unidad 7 Análisis de Malware
 - Unidad 8 Técnicas y herramientas de búsqueda de información y análisis OSINT
 - Unidad 9 Legislación y buenas prácticas de investigación

○ **ANÁLISIS DE DISPOSITIVOS MÓVILES: (56h de dedicación)**

- Objetivo del curso: La incursión de los dispositivos móviles dentro del mundo empresarial y en el privado, ha supuesto un cambio en la manera que teníamos de interactuar con internet hasta el momento, y ha propiciado la aparición de diversos perfiles orientados exclusivamente a las tecnologías móviles como experto en seguridad móvil, auditor de seguridad móvil, etc. Este curso otorga la facilidad de adquirir las competencias necesarias

en este ámbito de una manera guiada y clara, dotando al alumno de conocimientos claros y especializados para poder introducirse en el mundo de la seguridad en entornos móviles.

- Contenidos:
 - Unidad 0 Preparación de un entorno de pruebas
 - Unidad 1 Análisis de riesgos y amenazas en entornos móviles
 - Unidad 2 Estudio de las arquitecturas de tecnologías móviles
 - Unidad 3 Análisis de vulnerabilidades de dispositivos y aplicaciones
 - Unidad 4 Análisis forenses de entornos móviles
 - Unidad 5 Desarrollo seguro de aplicaciones móviles
 - Unidad 6 Contramedidas y planes de mitigación de riesgos
- **ESPECIALISTA EN CIBERSEGURIDAD INDUSTRIAL: (60h de dedicación)**
 - Objetivo del curso:
 - Familiarizarse con conceptos fundamentales de los sistemas de automatización y control industrial.
 - Aprender a identificar posibles vulnerabilidades y riesgos.
 - Conocer las principales amenazas y técnicas de ataque a este tipo de sistemas.
 - Aprender los principios de defensa e iniciativas de seguridad existentes en la actualidad.
 - Contenidos:
 - Unidad 1 Introducción a controles y sistemas de automatización
 - Unidad 2 Estudio detallado de los distintos dispositivos de control
 - Unidad 3 Estudio de los conceptos fundamentales de las comunicaciones industriales
 - Unidad 4 Sistemas SCADA, historia y otras aplicaciones
 - Unidad 5 Estudio detallado de amenazas y otras vulnerabilidades
 - Unidad 6 Presentación de iniciativas, buenas prácticas y soluciones
 - Unidad 7 Visita virtual y demostraciones de seguridad

CONOCIMIENTOS TÉCNICOS NECESARIOS PREVIOS A LA REALIZACIÓN DE LOS CURSOS DE LA FASE ON-LINE):

- Se recomienda una base tecnológica y de conocimientos en ciberseguridad para asegurar el completo aprovechamiento de las unidades y ejercicios de mayor exigencia técnica.
- Además, especificaciones particulares para los dos últimos cursos:
 - Dispositivos móviles: Conocimientos de informática, sistemas operativos, lenguajes de programación y redes de comunicaciones a nivel intermedio.
 - SCI: Conocimientos generales en informática, gestión de la seguridad y análisis de vulnerabilidades

REQUISITOS DE SW NECESARIOS PARA CURSAR LA FORMACIÓN ADECUADAMENTE:

- Al menos un dispositivos con conexión a Internet, Windows 8 con paquete office instalado, Acrobat Reader y navegadores web actualizados.
- Es necesario tener instalado VirtualBox.
- Durante los cursos además se explican otras herramientas para su instalación (todas ellas gratuitas y de fácil acceso).