# Introducción y objetivos generales

IMF Smart Education

# I. Introducción y objetivos generales

## 1.1. Introducción general del módulo

Investigar un incidente de seguridad o seguir la pista a una caída del sistema, así como al robo o espionaje de información, pueden ser tareas de suma dificultad.

En este módulo, los estudiantes aprenderán a llevar a cabo investigaciones forenses eficientes, así como a obtener resultados

óptimos de estas investigaciones y evidencias digitales para los procedimientos legales que puedan producirse.

El módulo se adentrará en las técnicas y herramientas necesarias para llevar a cabo investigaciones forenses en objetivos y localizaciones comprometidos y la extracción de acciones mediante evidencias digitales que se han hecho contra el objetivo. A lo largo del módulo, se describirán los fundamentos y objetivos del análisis forense, así como las herramientas necesarias y las implicaciones legales que conlleva.

La integridad de las evidencias es la piedra angular del análisis forense y alrededor de esta girarán cada una de las unidades de este módulo, ya que, para poder garantizar la validez de los procesos forenses, las evidencias deben ser recogidas, procesadas y analizadas de forma estandarizada y reproducible, y en las distintas unidades se ofrecerán las claves para preservar esta integridad.

**Se incluirá también el estudio del análisis forense de red y del correo electrónico, así como de sistemas de prevención de intrusiones que puedan ayudar a las organizaciones a evitar potenciales ataques.**

Además, este módulo incluye varias horas de investigación práctica y ejercicios para detectar diferentes incidentes de seguridad, como la filtración de información y las intrusiones a los equipos de trabajo, a fin de que el alumno sea capaz de localizar, preservar, analizar y detectar la información necesaria para la gestión y resolución eficaz de un ciberincidente.

CONTINUAR

## 1.2. Objetivos de la unidad

1. Formar a los alumnos para que adquieran los conocimientos necesarios para obtener las bases de la realización de análisis forense de dispositivos.

2. Dar a conocer los diferentes tipos de ataques, amenazas e incidentes de ciberseguridad a los que se enfrentan los especialistas en seguridad.

3. Evaluar el posible impacto que estos ataques e incidentes pueden tener en los dispositivos o la organización con el fin de comenzar a trabajar en el análisis de un sistema afectado tras un incidente.

4. Aprender en qué consiste un análisis forense, sus diferentes fases y métodos de trabajo, así como las principales herramientas en las que se puede apoyar en cada fase del proceso.

5. Ser conscientes de los procedimientos que los alumnos tienen que seguir desde el punto de vista legal, en caso de que tengan que participar en un análisis forense real.

6. Garantizar que el aluno aprende la información esencial sobre la adquisición de evidencias, el clonado de disco y la cadena de custodia.

7. Proveer al alumno de las nociones básicas sobre los mecanismos o procesos que dejan rastro, conocidos como artefactos, y el tipo de información o datos que proporcionan.

8. Profundizar en dos análisis forenses concretos: el de red y el de correo electrónico, y las herramientas utilizadas para llevarlos a cabo.

9. Obtener una primera aproximación sobre la gestión y análisis forense de logs en Windows.