

## MÓDULO DE FORMACIÓN 1

## CIBERSEGURIDAD: PREVENCIÓN, ANÁLISIS Y RESPUESTA A INCIDENTES DE SEGURIDAD

### OBJETIVO

Conocer y comprender las nociones fundamentales de ciberseguridad que permitan prevenir y dar respuesta a los incidentes de seguridad.

**DURACIÓN:** 49 horas

### RESULTADOS DE APRENDIZAJE

---

#### Conocimientos/ Capacidades cognitivas y prácticas

- Conocimiento del Gobierno de seguridad de una organización.
  - Gobierno de la seguridad.
  - Cumplimiento de las normas de seguridad.
- Identificación de las acciones preventivas que se deben planificar para evitar incidentes.
  - Amenazas y análisis de riesgos.
- Recolección de evidencias tras un ataque.
  - Identificación de diferentes tipos de ataques e incidentes que pueden darse en una empresa.
  - Utilización de técnicas y recursos para el análisis de datos.
- Creación de un plan de respuesta ante incidentes.
  - Respuesta a incidentes de seguridad.
  - Criptografía.
  - Plan de recuperación ante desastres.
- Práctica de hacking ético.

#### Habilidades de gestión, personales y sociales

- Adquisición de habilidades para el análisis y síntesis en la toma de decisiones en los ataques informáticos.
- Respuestas rápidas y eficaces ante ataques e incidentes que pueden producirse en la seguridad de una empresa.