



CONCIENCIACIÓN EN CIBERSEGURIDAD

DURACIÓN: 4 horas

CRÉDITOS ECTS: 0

OBJETIVOS

- Conocer los principales aspectos relacionados con la ciberseguridad, poniendo especial atención en la protección de los datos personales, el análisis de riesgos o los aspectos legales que afectan a profesionales o empresas.
- Conocer las medidas que pueden tomarse para evitar ataques y pérdidas de información.
- Aprender a evaluar los principales riesgos en ciberseguridad.
- Adquirir buenas prácticas de seguridad en el puesto de trabajo.

PROGRAMA CONTENIDOS

MÓDULO 1. TIPOS DE CIBERATAQUE

- 1. Introducción y objetivos del curso
- 2. ¿Qué ha pasado? ¿Dónde estoy?
- 3. ¿Quién ataca?
- 4. ¿Por qué ataca?
- 5. ¿Qué tipos de ataques hay?
- 5.1 Acceso físico a datos o a productos
- 5.2 Ataque a webs, sistemas o servicios online (1)
- 5.2 Ataque a webs, sistemas o servicios online (2)
- 5.3 Engaño con señuelo (1)
- 5.3 Engaño con señuelo (2)
- 5.3 Engaño con señuelo (3)

MÓDULO 2. AGUJEROS DE SEGURIDAD

- 1. Introducción y objetivos del curso
- 2. ¿Cómo me han podido atacar?
- 3. ¿Podría evitar esos ataques?
- 3.1 Medidas organizativas
- 3.2 Medidas técnicas
- 3.3 Concienciación
- 3.4 Consejos concretos para ciertos ataques

MÓDULO 3. GESTIÓN DE CRISIS Y RESPUESTA ANTE INCIDENTES

- 1. Introducción y objetivos del curso
- 2. ¿Cómo gestionamos la situación tras recibir un ataque?
- 3. Fase de preparación
- 4. Fase de identificación
- 5. Fase de contención
- 6. Fase de mitigación
- 7. Fase de recuperación
- 8. Actuaciones post-incidente

MÓDULO 4. SITUACIÓN GENERAL Y PREVISIÓN

- 1. Introducción y objetivos del curso
- 2. ¿Este ciberataque ha sido mala suerte?
- 2.1 Cibercrimen en España
- 2.2 Cibercrimen en el mundo
- 3. ¿Seguirá aumentando?