



## IFCT89. Seguridad en internet y dispositivos móviles

**Sku:** 70543IN

**Horas:** 36

### OBJETIVOS

- Obtener los conocimientos adecuados para identificar los elementos, dentro de una red o dispositivos móviles, susceptibles de ser atacados, así como los diferentes tipos de ataque que pueden sufrir, como la omnipresencia de la tecnología en nuestro entorno afecta a nuestra privacidad o que medidas de actuación se pueden acometer para minimizar el riesgo.
- Introducir los conocimientos que se adquirirán a lo largo del desarrollo del curso para asegurar su adecuada formación sobre la ciberseguridad y su impacto en internet y los dispositivos móviles que se usan diariamente (tablets, smartphones, smartwatches...).
- Introducir en la ciberseguridad y su impacto en Internet y en los dispositivos móviles que nos rodean.
- Capacitar para la identificación, valoración, prevención y mitigación de los posibles riesgos de seguridad en una red o dispositivo móvil que estén bajo su gestión.
- Concienciar en base a antecedentes en nuestra historia reciente, y a los nuevos avances que en tecnología se prevén estar, en los próximos años, al alcance de la población y de las organizaciones, poder entender, en comprender e intuir la dirección general en la que nos dirigimos en el futuro desde la perspectiva de la ciberseguridad.

### CONTENIDOS

#### **Introducción a la ciberseguridad**

Comprensión de la ciberseguridad

Los riesgos, tipos y alcance

Vectores de ataque tipos e impacto

Medidas de prevención y actuación ante posibles ataques

Revisión del contexto futuro de la ciberseguridad

#### **Ciberseguridad. Conceptos básicos**

¿Qué es la ciberseguridad?

¿Por qué aplicar la ciberseguridad?

¿Cómo impacta la ciberseguridad en internet y los dispositivos móviles?

## **Riesgos, tipos y vectores de ataque**

Qué es un riesgo y los elementos de un sistema susceptibles de ser protegidos

Tipos de riesgos

Conceptos básicos de vectores de ataque

Tipos de vectores de ataque (phishing, malware, social engineering y medidas de actuación)

Vectores de ataque: medidas de prevención y actuación generales

Vectores de ataque: medidas de prevención y generales en la gestión de redes conectadas o no a la red: cortafuegos, segmentación, monitorización, detección, registro y encriptación

Vectores de ataque: medidas de actuación específicas para los dispositivos móviles

## **Implicaciones en la ciberseguridad de la evolución de las amenazas actuales y de la adopción de nuevas tecnologías**

Gestión de ingentes cantidades de datos en sistemas cada vez más complejos

La inteligencia artificial (IA) será un componente central de todos los sistemas de ciberseguridad

La industria de la ciberseguridad se centrará en las amenazas de la guerra cibernética

Habrà más crackers con los que lidiar

Desarrollo del talento en ciberseguridad se vuelve esencial

La tecnología heredada seguirá siendo un problema

Internet de las cosas (IoT)

Supercomputación (computación cuántica)

Mayor uso de las redes autoadaptables

Generalización del uso de los gestores de seguridad para el acceso a la nube (cloud access security broker - CASB)

Análisis de amenazas internas mediante sistemas UEBA (user and entity behavior analytics)

Implantación generalizada de autenticación multifactor física en entornos críticos

El coronavirus (COVID-19) lo ha cambiado todo (teletrabajo y la ciberresiliencia)