



## IFCM026PO - SEGURIDAD INFORMATICA Y FIRMA DIGITAL

**DURACIÓN:** 50 HORAS

**MODALIDAD:** PRESENCIAL/AULA VIRTUAL

**FECHA INICIO/FIN:**

### **OBJETIVOS:**

Conocer las diferencias entre firma electrónica y firma digital, conocer los distintos certificados existentes y las amenazas sobre la autenticidad de las firmas, conocer sistemas de seguridad informática en la empresa.

Aprender los conceptos básicos de blockchain y conocer los medios para realizar certificaciones mediante esta nueva tecnología, ya que la misma constituye una importante innovación en lo referido a la gestión e intercambio informático de datos.

### **PARTICIPANTES:**

Personas trabajadoras OCUPADAS que han estado en ERTE

Personas trabajadoras DESEMPLEADAS inscritas en los servicios públicos de empleo.

Personas trabajadoras en situación de ERTE.

### **REQUISITOS DE ACCESO:**

Cualquier persona que quiera adquirir y mejorar las competencias profesionales relacionadas con los cambios tecnológicos y la transformación digital. Es recomendable disponer de:

- Habilidades básicas de comunicación lingüística que le permitan el aprendizaje y seguimiento de la formación.
- Competencias básicas en el manejo de ordenadores.
- Manejo básico en entornos microinformáticos.
- Buen manejo del ordenador y software específico.
- Conocimientos de navegación en internet

### **CONTENIDOS:**

#### **1. FIRMA ELECTRÓNICA / FIRMA DIGITAL.**

1.1 Práctica: La firma electrónica y la firma digital

#### **2. TIPOS DE CERTIFICADOS**

2.1. Certificados de Servidor (SSL: Capa de zócalos seguro)

2.2. Microsoft Server Gated Cryptography Certificates (Certificados de CGC-una extensión del protocolo SSLofrecida por Microsoft).

2.3. Certificados Canalizadores.

- 2.4. Certificados de Correo Electrónico.
- 2.5. Certificados de Valoración de páginas WEB.
- 2.6. Certificados de Sello, Fecha y Hora
- 2.7. Práctica: Aplicación de los diferentes certificados

### 3. SISTEMAS DE SEGURIDAD EN LA EMPRESA

- 3.1. Sistemas pasivos y reactivos.
- 3.2. Suplantación o spoofing:
  - 3.2.1. SET (Secure Electronic Transaction).
  - 3.2.2. PGP (Enterprise Security).
  - 3.2.3. SSL (Secure Socket Layout).
- 3.3 Práctica: Aplicación de los distintos sistemas de seguridad

#### **PARA PODER TENER SUPERADO EL CURSO HAY QUE CUMPLIR LOS SIGUIENTES REQUISITOS:**

- TENER SUPERADAS TODAS LAS PRUEBAS DE EVALUACIÓN QUE SE REALICEN DURANTE EL PROCESO DE APRENDIZAJE Y LA PRUEBA FINAL DE LA ACCIÓN FORMATIVA.