



## (IFCM026PO) Seguridad informática y firma digital.

**Sku:** PIT091

**Horas:** 50

### OBJETIVOS

**Objetivo General** • 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. **Objetivos Específicos:** • Estudiar los certificados digitales, usos y requisitos de seguridad, para ser un certificado válido. • Conocer los efectos de las TIC en la sociedad de la información. • Conocer las principales normas reguladoras en comercio electrónico y la Ley Orgánica de Protección de Datos. • Conocer los procesos para obtener un certificado en CERES. • Estudiar las normas y precauciones para alcanzar un nivel de seguridad óptimo, además de saber minimizar los riesgos a los que se exponen los equipos y la información. • Estudiar los diferentes organismos oficiales que emiten certificados, así como entender el uso de los diferentes organismos en transacciones comerciales y financieras. • Conocer las diferentes aplicaciones de la firma digital. • Comprender las ventajas que implica la utilización de un sistema seguro en la empresa. • Estudiar los tipos de certificados. • Saber aplicar el tipo de certificado necesario a cada caso según las necesidades de los usuarios. • Conocer y saber utilizar los diferentes sistemas de seguridad informática en la empresa. • Localizar las debilidades y las fortalezas del sistema y actuar en consecuencia.

### CONTENIDOS

**Unidad 1: Firma electrónica / firma digital.** • Certificado digital • Contenido y alcance. Efectos de las TIC en la sociedad de la información • Normativa reguladora. Seguridad jurídica: Normativa sobre el comercio electrónico en España • Seguridad tecnológica • Seguridad y recomendaciones. Seguridad informática: seguridad y protección • Uso de la firma digital. Organismos oficiales nacionales, autonómicos y locales. Transacciones comerciales y financieras • Necesidad de los sistemas de seguridad en la empresa **Unidad 2: Tipos de certificados.** • Certificados de servidor (SSL: Capa de puertos seguros) • Microsoft Server Gated Cryptography Certificates (Certificados de SGC, una extensión del protocolo SSL ofrecida por Microsoft) • Certificados canalizadores • Certificados de correo electrónico • Certificados de valoración de páginas web • Certificados de sello, fecha y hora **Unidad 3: Sistemas de seguridad en la empresa.** • Sistemas pasivos y reactivos •

Suplantación o spoofing