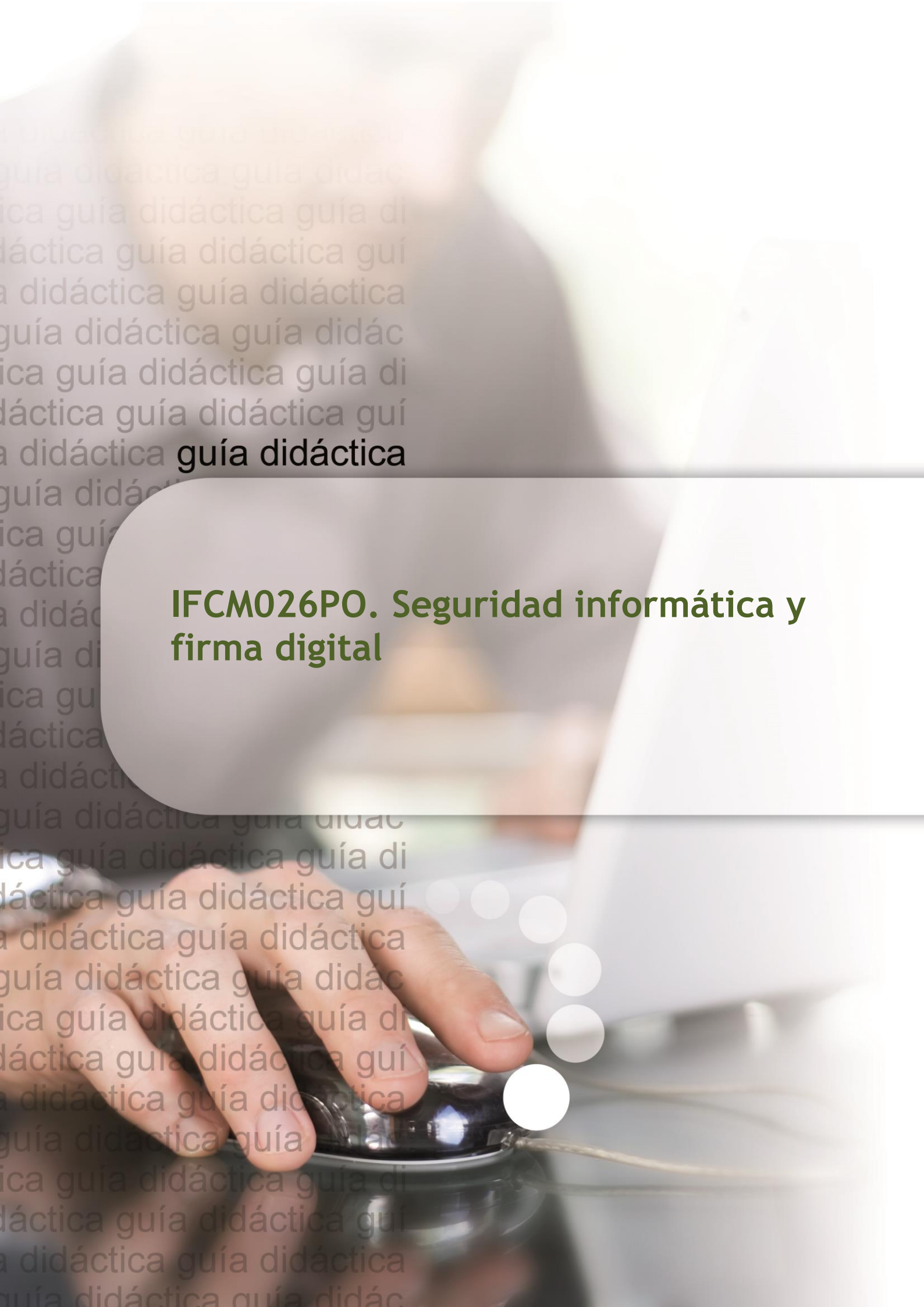


# IFCM026PO. Seguridad informática y firma digital

## 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

| 50 HORAS | IFCM026PO. Seguridad informática y firma digital |
|---|---|
| 20 horas | ❑ **Unidad 1:** Firma electrónica / firma digital.<br>• Certificado digital<br>• Contenido y alcance. Efectos de las TIC en la sociedad de la información<br>• Normativa reguladora. Seguridad jurídica: Normativa sobre el comercio electrónico en España<br>• Seguridad tecnológica<br>• Seguridad y recomendaciones. Seguridad informática: seguridad y protección<br>• Uso de la firma digital. Organismos oficiales nacionales, autonómicos y locales. Transacciones comerciales y financieras<br>• Necesidad de los sistemas de seguridad en la empresa |
| 20 horas | ❑ **Unidad 2:** Tipos de certificados.<br>• Certificados de servidor (SSL: Capa de puertos seguros)<br>• Microsoft Server Gated Cryptography Certificates (Certificados de SGC, una extensión del protocolo SSL ofrecida por Microsoft)<br>• Certificados canalizadores<br>• Certificados de correo electrónico<br>• Certificados de valoración de páginas web<br>• Certificados de sello, fecha y hora |
| 10 horas | ❑ **Unidad 3:** Sistemas de seguridad en la empresa.<br>• Sistemas pasivos y reactivos<br>• Suplantación o spoofing |
| **50 horas** | **3 unidades didácticas** |