

La manera más sencilla de que crezca  
tu organización

**CON LOS LÍDERES EN  
FORMACIÓN**



# Experto en firma electrónica y seguridad en internet

Modalidad:

e-learning con una duración 112 horas

Objetivos:

- Saber aplicar la firma electrónica y conocer la seguridad en internet.
- Adquirir las herramientas necesarias para llevar a cabo transacciones online de forma segura.
- Conocer la incorporación a la sociedad de las tecnologías de la información y las comunicaciones.
- Aprender sobre los efectos de las TIC en la sociedad de la información.

Contenidos:

## UNIDAD DIDÁCTICA 1. FIRMA ELECTRÓNICA (I)

Introducción  
Régimen Jurídico Aplicable  
Concepto de Firma electrónica  
Tipos de Firma  
Usos de la Firma Electrónica  
Formatos de la Firma Electrónica

## UNIDAD DIDÁCTICA 2. FIRMA ELECTRÓNICA (II)

Dispositivos de Firma Electrónica  
Sistemas de certificación de prestadores de servicios de certificación y dispositivos de creación de firma electrónica  
La firma electrónica como medio de prueba en juicio  
Documentos firmados electrónicamente  
Servicios de certificación  
Concepto de portadores en servicios de certificación sujetos a la Ley



La manera más sencilla de que crezca  
tu organización

**CON LOS LÍDERES EN  
FORMACIÓN**



Infracciones  
Sanciones

### UNIDAD DIDÁCTICA 3. CERTIFICADO ELECTRÓNICO

Certificado electrónico  
Entidades emisoras certificadas  
Tipo de certificado electrónico  
Clases de certificado electrónicos  
Procedimientos de obtención de un certificado electrónico de persona física  
Realizar una copia de seguridad del certificado electrónico  
La confidencialidad del certificado electrónico  
Extinción de la vigencia de los certificados electrónicos  
Suspensión de la vigencia de los certificados electrónicos  
Disposiciones comunes a la extinción y suspensión de la vigencia.

### UNIDAD DIDÁCTICA 4. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS

Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información  
Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes  
Salvaguardas y tecnologías de seguridad más habituales  
La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

### UNIDAD DIDÁCTICA 5. PLAN DE IMPLANTACIÓN DE SEGURIDAD

Determinación del nivel de seguridad existente de los sistemas frente a la necesaria en base a los requerimientos de seguridad de los procesos de negocio.  
Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información  
Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

### UNIDAD DIDÁCTICA 6. SEGURIDAD FÍSICA E INDUSTRIAL DE LOS SISTEMAS. SEGURIDAD LÓGICA DE SISTEMAS

Determinación de los perímetros de seguridad física  
Sistemas de control de acceso físico mas frecuentes a las instalaciones de la organización y a las áreas en las que estén ubicados los sistemas informáticos



La manera más sencilla de que crezca  
tu organización

**CON LOS LÍDERES EN  
FORMACIÓN**



Criterios de seguridad para el emplazamiento físico de los sistemas informáticos  
Exposición de elementos mas frecuentes para garantizar la calidad y continuidad del suministro eléctrico a los sistemas informáticos  
Requerimientos de climatización y protección contra incendios aplicables a los sistemas informáticos  
Elaboración de la normativa de seguridad física e industrial para la organización  
Sistemas de ficheros más frecuentemente utilizados  
Establecimiento del control de accesos de los sistemas informáticos a la red de comunicaciones de la organización  
Configuración de políticas y directivas del directorio de usuarios  
Establecimiento de las listas de control de acceso (ACLs) a ficheros  
Gestión de altas, bajas y modificaciones de usuarios y los privilegios que tienen asignados  
Requerimientos de seguridad relacionados con el control de acceso de los usuarios al sistema operativo  
Sistemas de autenticación de usuarios débiles, fuertes y biométricos  
Relación de los registros de auditoría del sistema operativo necesarios para monitorizar y supervisar el control de accesos  
Elaboración de la normativa de control de accesos a los sistemas informáticos