ACADEMIA INTEGRAL
CENTRO DE NUEVAS TECNOLOGIAS

# LA FORMACIÓN ES LA CLAVE DEL ÉXITO

# Guía del Curso
# Curso Práctico: Experto en Firma Electrónica y Seguridad en Internet

---

Modalidad de realización del curso: Online
Titulación: Diploma acreditativo con las horas del curso

---

## OBJETIVOS

Los rápidos avances tecnológicos y la dimensión mundial de internet han hecho que, primero las empresas y después los ciudadanos y la administración, estén haciendo cada vez mas uso de las telecomunicaciones y de las nuevas tecnologías. Está siendo verdaderamente espectacular el crecimiento de las transacciones telemáticas que se vienen realizando con contenido económico. La fórmula se ha encontrado en la "firma electrónica" y en los proveedores de "servicios de certificación". Consiste en un instrumento generado por documento electrónico relacionado con la herramienta de firma en poder del usuario, y que es capaz de permitir la comprobación de la procedencia y de la integridad de los mensajes intercambiados y ofreciendo bases para evitar su repudio. Con ello se alcanza el vínculo contractual o la autenticidad de un documento al igual que si se tratara de una firma manuscrita. Este curso le ofrece la formación sobre la firma electrónica y la seguridad en internet....

## CONTENIDOS

### UNIDAD DIDÁCTICA 1. FIRMA ELECTRÓNICA (I)

1. Introducción

2. Régimen Jurídico Aplicable
3. Concepto de Firma electrónica
4. Tipos de Firma
5. Usos de la Firma Electrónica
6. Formatos de la Firma Electrónica

## UNIDAD DIDÁCTICA 2. FIRMA ELECTRÓNICA (II)

1. Dispositivos de Firma Electrónica
2. Sistemas de certificación de prestadores de servicios de certificación y dispositivos de creación de firma electrónica
3. La firma electrónica como medio de prueba en juicio
4. Documentos firmados electrónicamente
5. Servicios de certificación
6. Concepto de portadores en servicios de certificación sujetos a la Ley
7. Infracciones
8. Sanciones

## UNIDAD DIDÁCTICA 3. CERTIFICADO ELECTRÓNICO

1. Certificado electrónico
2. Entidades emisoras certificadas
3. Tipo de certificado electrónico
4. Clases de certificado electrónicos
5. Procedimientos de obtención de un certificado electrónico de persona física
6. Realizar una copia de seguridad del certificado electrónico
7. La confidencialidad del certificado electrónico
8. Extinción de la vigencia de los certificados electrónicos
9. Suspensión de la vigencia de los certificados electrónicos
10. Disposiciones comunes a la extinción y suspensión de la vigencia.

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

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

## UNIDAD DIDÁCTICA 5. PLAN DE IMPLANTACIÓN DE SEGURIDAD

1. 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.
2. Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información
3. 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

1. Determinación de los perímetros de seguridad física
2. 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
3. Criterios de seguridad para el emplazamiento físico de los sistemas informáticos
4. Exposición de elementos mas frecuentes para garantizar la calidad y continuidad del suministro eléctrico a los sistemas informáticos
5. Requerimientos de climatización y protección contra incendios aplicables a los sistemas informáticos
6. Elaboración de la normativa de seguridad física e industrial para la organización
7. Sistemas de ficheros más frecuentemente utilizados
8. Establecimiento del control de accesos de los sistemas informáticos a la red de comunicaciones de la organización
9. Configuración de políticas y directivas del directorio de usuarios
10. Establecimiento de las listas de control de acceso (ACLs) a ficheros

11. Gestión de altas, bajas y modificaciones de usuarios y los privilegios que tienen asignados
12. Requerimientos de seguridad relacionados con el control de acceso de los usuarios al sistema operativo
13. Sistemas de autenticación de usuarios débiles, fuertes y biométricos
14. Relación de los registros de auditoría del sistema operativo necesarios para monitorizar y supervisar el control de accesos
15. Elaboración de la normativa de control de accesos a los sistemas informáticos

C/ San Lorenzo 2 - 2
29001 Málaga

Tlf: 952 215 476
Fax: 951 987 941

www.academiaintegral.com.es
E-mail: info@academiaintegral.com.es

ACADEMIA INTEGRAL
CENTRO DE NUEVAS TECNOLOGIAS