TEMARIO
IFCM012PO
LA FIRMA DIGITAL

TEMA 1. FIRMA DIGITAL

TEMA 2. CONTENIDO Y ALCANCE

TEMA 3. NORMATIVA REGULADORA

TEMA 4. SOLICITUD Y OBTENCIÓN

TEMA 5. SEGURIDAD Y RECOMENDACIONES

TEMA 6. USO DE LA FIRMA DIGITAL

TEMA 7. NECESIDAD DE SISTEMAS DE SEGURIDAD EN LA EMPRESA

OBJETIVO GENERAL

- Conocer la principal normativa legal y técnica de firma digital/electrónica; entender sus tipos y características así como las peculiaridades específicas de los certificados personales y sus aplicaciones prácticas. Comprender los conceptos básicos de seguridad en las transacciones telemáticas.

Tema 1
Firma digital

- **Firma digital**
- **Certificado digital**
- **Firma electrónica**
- **Incorporación de la sociedad a las NNTT de la Información y las Comunicaciones (TIC)**

OBJETIVOS:

- Definir la firma digital y su funcionamiento, además de establecer las diferencias con la firma digitalizada.
- Definir la firma electrónica conociendo sus variantes y su funcionamiento.
- Definir un certificado electrónico, conociendo cada uno de sus tipos.
- Introducir el concepto de las TIC.

INTRODUCCIÓN

La firma digital se ha convertido en un instrumento indispensable para hacer frente a cualquier tipo de trámite administrativo, pues nos evita tener que desplazarnos al lugar, además de otras ventajas como las siguientes:

- Los documentos que se firmen electrónicamente tendrán mayor seguridad e integridad.
- El mensaje tendrá garantizada su confidencialidad.
- Contribuye a que disminuya el almacenamiento de datos en papel, así como a una considerable reducción de papel y gastos.
- Al agilizar los trámites, se produce un aumento de la productividad y competitividad en la empresa.

En este tema desarrollaremos en profundidad el concepto de firma digital y veremos las diferencias con la firma electrónica que, aunque se suelen usar como sinónimos, engloban conceptos diferentes.

VOCABULARIO

La **criptografía** es la técnica de usar procedimientos secretos y la criptografía asimétrica se basa en el uso de dos claves:

- una pública, que se puede difundir,
- una privada, que no puede ser revelada.

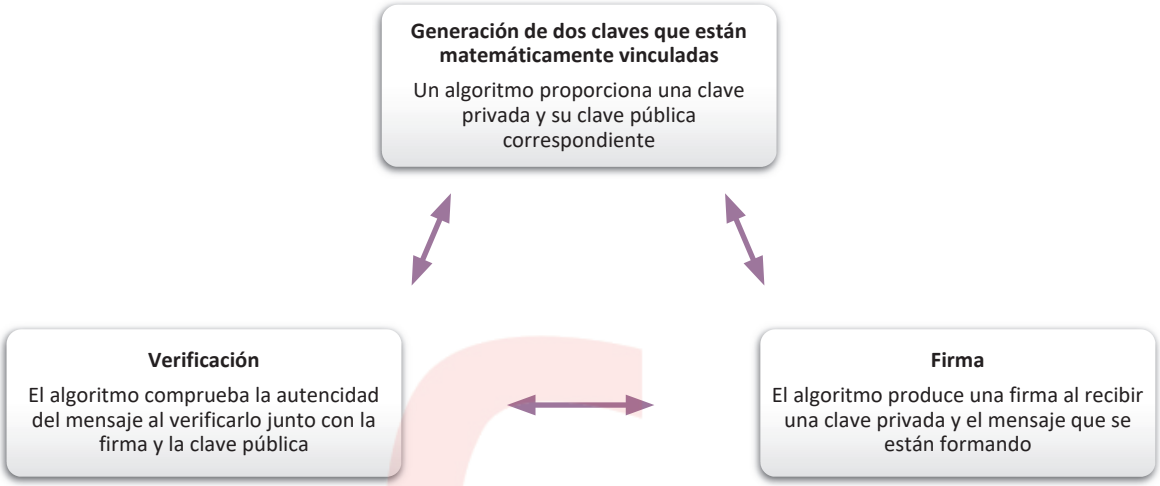
1. FIRMA DIGITAL

Este tema lo vamos a dedicar a comprender el concepto de firma digital, pero antes de profundizar en su definición debemos dejar clara la diferencia entre firma digital y firma electrónica, ya que, aunque se suelen usar como sinónimos, no son exactamente lo mismo.

De forma básica, podemos decir que la firma digital es un conjunto de métodos criptográficos y técnicos, mientras que la firma electrónica abarca un concepto mucho más amplio, que hace referencia a cuestiones legales, organizativas, técnicas, etc.

La firma digital se basa en la criptografía de clave pública (PKI: Public Key Infrastructure), conocida como criptografía asimétrica.

Para su funcionamiento, necesita que se generen tres algoritmos diferentes:



Para crear la firma digital, el software de firma crea un hash unidireccional de los datos electrónicos que se van a firmar. La clave privada se usaría para encriptar el hash, que, cifrado junto con otra información, sería la firma digital.

Un **algoritmo** es un conjunto ordenado de operaciones sistemáticas que permite hacer un cálculo y hallar la solución de un tipo de problemas.

Un **hash** es un algoritmo que consigue crear, partir de una entrada, como un texto, una contraseña o un archivo, una salida alfanumérica de longitud fija que representa un resumen de toda la información que se le ha dado.

2. CERTIFICADO DIGITAL

El certificado digital o electrónico es un documento electrónico expedido por una autoridad de certificación y su cometido es identificar a una persona, tanto física como jurídica, con dos claves: una pública y una privada. Tiene como objetivo validar y certificar que una firma electrónica se corresponde con una persona o entidad concreta.

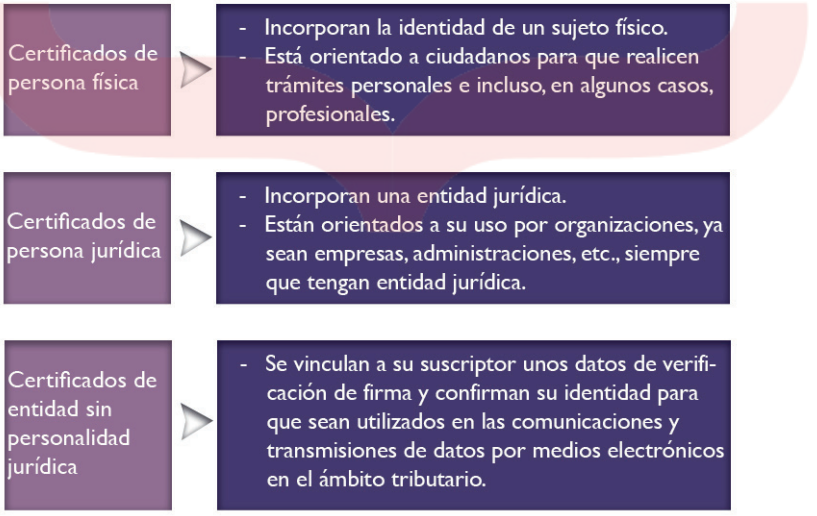
Posee la siguiente información del propietario:

- nombre
- NIF
- algoritmo y claves de firma
- fecha de expiración
- organismo que lo expide.

Hay diferentes tipos de certificados que pueden clasificarse según varios criterios que iremos viendo con detalle.

2.1 Certificados según el tipo de identidad

A partir de este criterio de identidad, los certificados se clasifican en:



El certificado de persona física, también llamado certificado de usuario, es uno de los más usados debido a que contiene los datos identificativos y permitirán al usuario identificarse en internet e intercambiar información con otras personas y organismos con garantía de que solo el usuario y el interlocutor puedan acceder a ella.

Este certificado permitirá realizar diferentes trámites de forma segura con la Administración pública y con diferentes entidades privadas a través de internet. Algunos trámites son:

- Presentación y liquidación de impuestos.
- Presentación de recursos y reclamaciones.
- Consulta e inscripción en el padrón municipal.
- Consulta de multas de circulación.
- Consulta y trámites para solicitud de subvenciones.
- Firma electrónica de documentos y formularios oficiales.

TOMA NOTA

Cualquier ciudadano español o extranjero mayor de edad o menor de edad emancipado que tenga DNI o NIE podrá obtener el certificado de forma gratuita.

2.2 Certificados según el ámbito de aplicación

Partiendo de este criterio, podemos encontrar una gran variedad de certificados. Algunos son:

- Certificado de servidor
- Certificado de pertenencia a empresa
- Certificado de representante
- Certificado de apoderado
- Certificado de sello de empresa
- Certificado de factura electrónica
- Certificado de colegiado

De los anteriores, uno de los más demandados es el certificado de representante. Se trata de un certificado para una persona física que actúa como representante legal de una organización. Puede ser de tres tipos diferentes:

- Representante para administrador único o solidario:
  - Se emite para confiar la administración de una sociedad de capital a un administrador único, una sola persona, o a varias administradores o personas que actúen de forma solidaria o conjunta.
  - Se expide a los administradores únicos o solidarios como representantes de las personas jurídicas para sus relaciones con las administraciones públicas y en la contratación de bienes o servicios.
- Representante de persona jurídica: Se expide a las personas físicas como representantes de las personas jurídicas para su uso en sus relaciones con las administraciones públicas, entidades y organismos públicos, vinculados o dependientes de las mismas.
- Representante de entidad sin personalidad jurídica: Se expide a las personas físicas como representantes de las entidades sin personalidad jurídica en al ámbito tributario.

2.3 Certificados software y certificados hardware

Encontramos, pues, dos tipos de certificados:

- **Certificado software**: se trata de un documento digital que puede guardarse en una memoria USB, en un almacén de certificados de un ordenador o en el disco duro.
- **Certificado hardware**: se trata de un certificado que se puede almacenar en una tarjeta criptográfica, que es una tarjeta que incorpora un chip electrónico donde se pueden almacenar uno o varios certificados.

Un ejemplo de tarjeta criptográfica es el DNI electrónico.

2.4 Certificados de la Administración pública

Los certificados que sirven para la identificación de la Administración y de la actuación administrativa son:

- Certificado de sede electrónica: es un certificado de servidor que identifica y autentifica al servidor como sede electrónica de una Administración pública.
- Certificado de sello electrónico: se trata del certificado utilizado para los trámites administrativos que se realizan por medios telemáticos, tanto para la identificación de servidores como para la firma de documentos electrónicos o el establecimiento de comunicaciones seguras entre máquinas.
- Certificado de empleado público: son los certificados que cada Administración pública puede proveer a su personal y que identifican tanto al titular del puesto de trabajo como a la Administración u órgano donde presta sus servicios.

Una sede electrónica es un sitio web del que es titular una Administración pública encargada de gestionarlo y administrarlo, que permite a los ciudadanos y las empresas acceder a la información y a los servicios y trámites electrónicos de la Administración en cualquier momento.

2.5 Certificados cualificados y no cualificados

Un certificado electrónico reconocido o cualificado sería aquel certificado electrónico que se ha expedido cumpliendo los requisitos cualificados en lo que se refiere a su contenido, a los procedimientos de comprobación de la identidad del firmante y a la fiabilidad y garantías de la actividad de certificación electrónica. El no cualificado sería el que no cumple estos requisitos.

DEFINICIÓN

Un prestador de servicios de certificación (PSC) es la persona física o jurídica que expide certificados electrónicos.

El certificado electrónico cualificado es un certificado expedido por un prestador se servicios de certificación que cumple los requisitos establecidos por la ley en cuanto a comprobación de identidad y demás servicios para usuarios.

Un certificado electrónico reconocido, deberá incluir los siguientes datos:

- La indicación de que se expide como reconocido.
- El código único identificativo del certificado.
- La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.
- La firma electrónica avanzada del prestador de servicios que expide el certificado.
- La identificación del firmante. En el caso de persona física, nombre y DNI y, en el caso de persona jurídica, denominación y código de identificación social.
- Los datos de verificación de firma que corresponden a los datos de creación de la misma.
- El período de validez del certificado.
- Los límites de uso del certificado y del valor de las transacciones para las que se puede utilizar.

3. FIRMA ELECTRÓNICA

La base legal de la firma electrónica se recoge por primera vez en la Ley 59/2003 de Firma Electrónica y se desarrolla en la sección Base Legal de Firmas.

La firma electrónica es un conjunto de datos electrónicos que están asociados a otros datos del documento electrónico que se va a firmar y que pueden utilizarse como medio de autenticación del firmante y de la integridad del documento firmado.

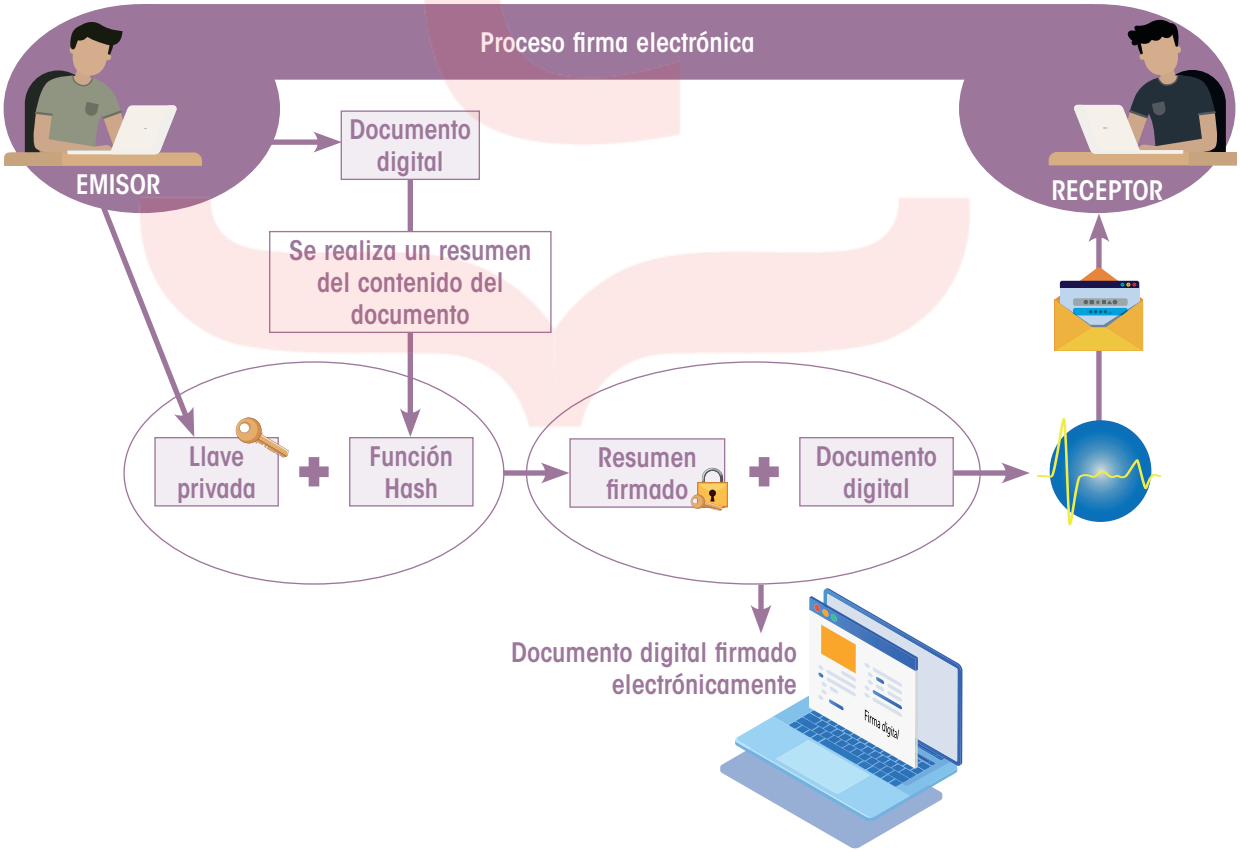
3.1 Funciones de la firma electrónica

Las funciones básicas de la firma electrónica son:

- Identificar al firmante de manera inequívoca.
- Asegurar la integridad del documento firmado, es decir, que sea el mismo que el original y no haya sufrido ninguna modificación o manipulación.
- Asegurar el no repudio del documento firmado. Puesto que los datos que utiliza el firmante son únicos, no puede decir que no ha firmado el documento.

Su naturaleza jurídica hace que asegure la identidad de una persona y constituye una prueba del consentimiento, vinculación y aprobación de la información contenida en un documento, al igual que una firma manuscrita, pero usando diversos soportes electrónicos distintos, como un lápiz electrónico o una firma digital.

3.2 Funcionamiento de la firma electrónica



DEFINICIÓN

El eIDAS (Elecronic Identification and Signature) es un nuevo reglamento europeo que regula la identificación electrónica y establece las pautas que regulan la firma electrónica.

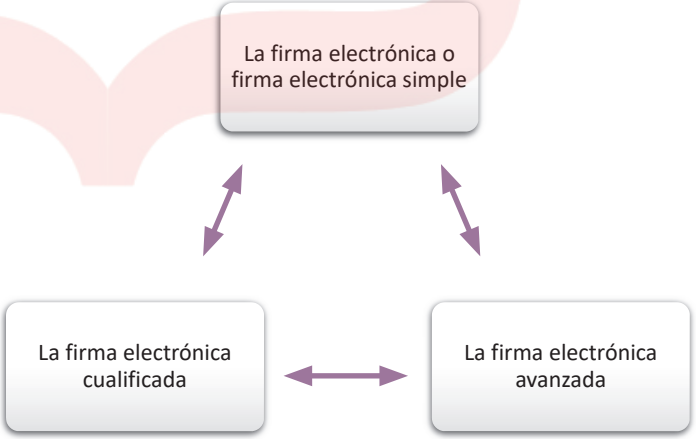
La firma electrónica sigue el proceso que explicamos a continuación:

- El usuario dispone de un documento electrónico, como un pdf o una imagen, y un certificado electrónico que le pertenece y lo identifica.
- La aplicación utilizada para la firma realiza un resumen del documento. Se trata de un resumen de unas líneas que es único, cuya modificación implica también una modificación del resumen.
- La aplicación utiliza la clave privada para codificar el resumen.
- La aplicación crea otro documento electrónico que contiene ese resumen codificado. Este documento es la firma electrónica.

3.3 Tipos de firma electrónica

Según el Reglamento n.º 910/2014, conocido como el reglamento eIDAS, que recoge la base legal sobre firmas electrónicas, hay tres tipos diferentes de firmas:

Estos tres tipos de firma electrónica se diferencian principalmente por sus distintos niveles de seguridad, por su capacidad de garantizar la integridad de los documentos que se firman y por su capacidad de identificar al firmante.



A. Firma electrónica simple

Una firma electrónica simple equivale a la firma manuscrita y se define como un conjunto de datos en formato electrónico que se adjunta o se asocia lógicamente con otros datos en formato electrónico y que el signatario utiliza para firmar. Su función es tan simple como firmar un documento y enviarlo escaneado, pero como no existe una prueba de que ha sido realmente el firmante, es la que tiene un nivel más bajo de seguridad.

Existen tres modelos de firma electrónica simple:

- **Firma electrónica indirecta.** Se trata de la identificación y verificación de identidad de una persona mediante un nombre de usuario y contraseña.
- **Firma electrónica en e-mails.** Consiste en el envío de un e-mail firmado en el que se adjuntan uno o más documentos. Existe la posibilidad de que vaya cifrado y, al existir una comunicación bidireccional entre emisor y receptor, es necesaria la existencia de dos claves, una privada y una pública.
- **Firma electrónica en documento.** Consiste en el envío de documentos electrónicos que tienen la firma dentro de su estructura. Es una firma utilizada en los documentos de pdf, por ejemplo.

Ejemplo

La dirección origen de un correo electrónico podría considerarse un mecanismo de firma electrónica suficiente para comunicar una decisión simple. Pero la suplantación en un correo es algo bastante sencillo.

B. Firma electrónica avanzada

Es un tipo de firma que, al contrario que la simple, nos permite saber si el contenido ha sufrido algún tipo de alteración. Según el artículo 26 del Reglamento europeo 910/2014 debe cumplir los siguientes requisitos:

- Estar vinculada al firmante de manera única. Se utiliza una autoridad de sellado de tiempo para garantizar la integridad de la misma.

La biometría desarrolla las técnicas que permiten medir y analizar una serie de parámetros físicos, que son únicos en cada persona, para poder comprobar su identidad. Los datos biométricos serían, por ejemplo, la huella dactilar o el iris del ojo.

- Permitir la identificación del firmante. Para ello normalmente se realizan procesos como la geolocalización del lugar de la firma, el registro de las direcciones de origen y destino y la captura de los datos biométricos del grafo.
- Haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo.
- Estar vinculada con los datos firmados por la misma, de tal modo que cualquier modificación ulterior de los mismos sea detectable.

C. Firma electrónica cualificada

La firma electrónica reconocida o cualificada es una firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. Para que sea reconocida, debe cumplir con los siguientes requisitos:

- Que sea una firma electrónica avanzada.
- Que esté basada en un certificado reconocido, que es aquel que cumple los requisitos establecidos por la ley que define la firma electrónica para la comprobación de identidad y otras circunstancias de los solicitantes.
- Que se genere mediante un dispositivo seguro de creación de firma.