TEMARIO

IFCM026PO

Seguridad informática y firma digital

TEMA 1. FIRMA ELECTRÓNICA, FIRMA DIGITAL

TEMA 2. TIPOS DE CERTIFICADOS

TEMA 3. SISTEMAS DE SEGURIDAD EN LA EMPRESA

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.

Tema 1
Firma electrónica, firma digital

- **Firma electrónica, firma digital**
- **Firma electrónica**
- **Firma digital**
- **Firma digitalizada**
- **Certificado electrónico**

OBJETIVOS:

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

INTRODUCCIÓN

La firma electrónica se ha convertido en un instrumento indispensable para hacer frente a cualquier tipo de trámite administrativo, que 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.
- Una menor disminución del almacenamiento de datos en papel y, por tanto, 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 electrónica y veremos las diferencias con la firma digital, que aunque suelen usarse como sinónimos, engloban conceptos diferentes.

1. FIRMA ELECTRÓNICA, FIRMA DIGITAL

RECUERDA

Todas las firmas digitales son electrónicas, pero no todas las firmas electrónicas son digitales.

Antes de profundizar en cada uno de los dos conceptos, debe dejarse claro que, aunque suelen usarse como sinónimos, no son exactamente lo mismo. De forma básica, podemos decir que:

- La firma digital es un conjunto de métodos criptográficos y técnicos.
- La firma electrónica abarca un concepto mucho más amplio, pues hace referencia a cuestiones legales, organizativas, técnicas, etc.

Todo esto nos lleva a afirmar que la firma digital es la firma electrónica certificada.

2. FIRMA ELECTRÓNICA

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

Sus funciones básicas son:

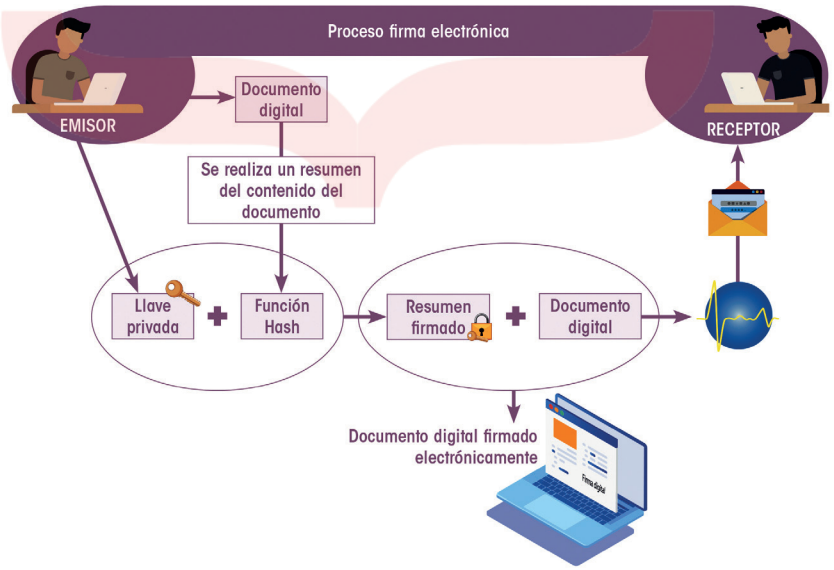
- Identificar al firmante de manera inequívoca.
- Asegurar la integridad del documento firmado, es decir, que sea el mismo que el original y no haya sufrido ninguna modificación o manipulación.

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.

2.1 Funcionamiento de la firma electrónica

La firma electrónica sigue el siguiente proceso:



Proceso de firma electrónica

- 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 y 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.

2.2 Tipos de firma electrónica

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

- La firma electrónica o firma electrónica simple.
- La firma electrónica avanzada.
- La firma electrónica cualificada.

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.

VOCABULARIO

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.

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,

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

pero como no existe ninguna prueba de quién 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 adjuntos. Existe la posibilidad de que vaya cifrado y, al existir una comunicación bidireccional entre emisor y receptor, es necesario 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.

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.
- Permitir la identificación del firmante. Para ello normalmente se realizan procesos como la geolocalicación 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 empleando 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.

VOCABULARIO

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.

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 sea generada mediante un dispositivo seguro de creación de firma.

Un dispositivo seguro de creación de firma es el DNIe, la tarjeta de FNMT, tarjetas de Camerfirma, etc.

Suele limitarse a trámites que se realizan con las administraciones públicas, como Hacienda o Seguridad

Social, debido a que su complejidad operativa no la hace una buena opción para personas o empresas que solicitan firmas a distancia.

3. FIRMA DIGITAL

Es el conjunto de caracteres que se añaden al final de un documento o cuerpo del mensaje para informar o mostrar validez y seguridad. Sirve para identificar a la persona emisora de dicho mensaje y para certificar la veracidad de que el documento no se ha modificado con respecto al original. Además, implica la existencia de un certificado electrónico emitido por un organismo o institución que valida esa firma.

Su función es aplicar mecanismos criptográficos al contenido de un mensaje o documento para demostrar al receptor del mensaje lo siguiente:

- Autentificación. El emisor del mensaje es real.
- No repudio. El emisor no puede negar que envió el mensaje.
- Integridad. El mensaje no ha sido alterado desde su emisión.

Se trata de una parte fundamental de la firma electrónica avanzada y de la cualificada o reconocida, pero no de la simple.

RECUERDA

A diferencia de la firma tradicional, la digital no es un nombre, sino un conjunto de dos claves.

3.1 Funcionamiento de la firma digital

La firma digital se basa en la criptografía de clave pública (PKI, Public Key Infrastructure), conocida como criptografía asimétrica. Hemos de aclarar que 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, y una privada, que no puede ser revelada.

La firma necesita para su funcionamiento que se generen tres algoritmos diferentes:

- Generación de dos claves que están matemáticamente vinculadas. Un algoritmo proporciona una clave privada y su clave pública correspondiente.
- Verificación. El algoritmo comprueba la autenticidad del mensaje al verificarlo junto con la firma y la clave pública.
- Firma. El algoritmo produce una firma al recibir una clave privada y el mensaje que se están formando.

3.2 Definiciones

Para aclarar conceptos, pasamos a especificar qué es un algoritmo y qué es un "hash".

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, a 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.

TOMA NOTA

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.

4. FIRMA DIGITALIZADA

La firma digitalizada es la conversión del trazo de una firma en una imagen, es decir, es la representación gráfica de la firma manuscrita obtenida o bien tras escanear la firma realizada en un papel, o a través de algún tipo de hardware como los pads (o tabletas) de firma, que te permiten guardar la imagen de tu firma en el ordenador.

La firma digitalizada se considera una firma electrónica simple, por lo tanto, es una firma legal, pero no ofrece garantía con respecto a la identidad del firmante y puede falsificarse fácilmente.

5. CERTIFICADO ELECTRÓNICO

El certificado electrónico es un documento electrónico expedido por una autoridad de certificación; 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.

El certificado electrónico puede usarse en:

- **Administración central**. Agencia Tributaria, Banco de España, Boletín Oficial del Estado, Dirección

VOCABULARIO

Las **autoridades de certificación** son una entidad de confianza, responsable de emitir y revocar los certificados electrónicos, utilizados en la firma electrónica.