



**REVISTA**  
**FIRMA**  
**DIGITAL**

Colabora:

**UNE**

Patrocinado por:

*Signaturit*  
Sign anywhere, anytime

Una iniciativa de:

**MUYPYMES**

# ÍNDICE

Prólogo: «Apoyo de los estándares a la identidad digital», por UNE .....	4
Nos adentramos en las «entrañas» tecnológicas de la firma digital .....	6
Noticias destacadas .....	8
Entrevista a Cátia Reis, de PwC.....	10
Normas técnicas para pymes.....	11
Píldoras de Firma Digital.....	12
Qué es el reglamento eIDAS y por qué es tan importante en la identificación digital.....	14



SIGN HERE





# Apoyo de los estándares a la identidad digital

Durante el periodo de crisis mundial en el que estamos inmersos, el proceso de digitalización está permitiendo que las empresas y administraciones públicas puedan establecer **relaciones contractuales** sin la necesidad de que proveedores, clientes o ciudadanos se personen físicamente en una oficina o sucursal. La **identidad digital**, que suple a la identidad física, se convierte cada vez más en un elemento clave para esta nueva forma de relacionarse.

De la misma forma que cuidamos nuestra apariencia física, debemos aplicarnos en nuestra presencia digital, puesto que todas nuestras actuaciones dentro del espacio digital (imágenes, comentarios, enlaces visitados, lugares donde publicamos nuestros datos, etc.) conforman nuestra identidad o perfil digital. Se hace cada vez más necesario, convirtiéndose en una de las competencias personales necesarias en la sociedad digital actual, el saber gestionar nuestra propia identidad digital, actuando de una manera ética, legal y segura dentro de la cultura de la participación y la interacción, lo que implica el conocimiento de las herramientas que nos **identifican** en un entorno digital.

Necesitamos contar con ella cuando queramos identificarnos en las conexiones o las transacciones a través de ordenadores, teléfonos móviles u otros dispositivos personales. Para conseguir una identificación de forma digital, deben utilizarse una serie de elementos como pueden ser: **la firma digital**, el correo electrónico o claves electrónicas que ayudan a reforzar la seguridad. De igual forma, existe el DNI Electrónico que permite acreditar electrónicamente la identidad de un individuo.

En la evolución de este contexto, las normas elaboradas en organismos europeos, como **CEN** (Comité Europeo de Normalización) y **ETSI** (Instituto Europeo de Normas de Telecomunicaciones) e internacionales de normalización, **ISO** (Organización Internacional de Normalización), han sido herramientas de apoyo al desarrollo y despliegue de la industria de la identificación digital y la seguridad.

Para llevar a cabo la mayoría de las transacciones electrónicas, apertura de cuentas bancarias, contratación de hipotecas, planes de pensiones, domiciliación, o realizar trámites en el sector de la movilidad y el turismo (check-in en hoteles, trámites fronterizos, etc.), o llevar a cabo procesos de la administración electrónica o de participación ciudadana, se hace necesario contar **con un contexto seguro y confiable de actuación**. El Reglamento Europeo 910/2014, conocido como eIDAS, delimita un nuevo marco jurídico en los siguientes aspectos: **firma electrónica**, establecimiento de sellos y marcas de tiempo, documentos electrónicos y servicios de entrega electrónica registrada o correo electrónico certificado, así como servicios de certificado para autenticación de sitios web. En este sentido, regula las transacciones electrónicas y su gestión.

## Europa, a la cabeza de la firma electrónica

Europa lidera los estándares regulatorios para firma electrónica en el mundo, y son replicados en los distintos países. En el ámbito de la identificación personal, son destacables los trabajos que se desarrollan en el marco del



**Comité Europeo de Normalización, CEN**, con el objetivo de establecer un sistema de confianza en la firma electrónica. Estas normas establecen los requisitos mínimos de seguridad que deben cumplir los diferentes dispositivos de creación de firmas electrónicas para que sean seguros frente a amenazas, como la falsificación de la firma, la suplantación de datos o el mal uso de la función de creación de firma, entre otras. Estos trabajos cobran especial relevancia por ser normas de referencia en apoyo a la entrada en vigor del Reglamento **eIDAS**.

Como derivada de la transposición del Reglamento europeo 910/2014 (eIDAS), el pasado 13 de noviembre de 2020, entró en vigor la Ley 6/2020 reguladora de determinados aspectos de los servicios electrónicos de confianza. Esta ley está, es de obligado cumplimiento para **aquellas entidades** que ofrezcan servicios electrónicos de confianza en nuestro país, y por tanto, también afecta a los certificados que expiden dichas entidades y a las empresas que los usan.

Los estándares que reconoce el Reglamento eIDAS, se elaboran en el seno del comité europeo de normalización (CEN), concretamente en el comité **CEN/TC 224** "Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment". Son destacables también los trabajos desarrollados en los comités internacionales **ISO/IEC JTC 1/SC17** "Information technology. Cards and personal identification" e **ISO/IEC JTC 1/SC 37** "Biometrics" y el ETSI/TC "Electronic Signatures and Infrastructures (ESI)"

A través de la **Asociación Española de Normalización, UNE**, se puede participar e influir en el contenido de las normas técnicas o estándares europeos e internacionales. El responsable del ámbito de la identidad digital es el **Subcomité SC17-37** "Identificación digital", que forma parte del comité nacional CTN71 "Tecnologías Habilitadoras Digitales (THD)".

El SC17-37 tiene como objeto la normalización de los sistemas digitales de identificación y documentos relacionados, tarjetas, dispositivos y tokens de seguridad y sus interfaces asociadas y tecnologías biométricas genéricas relacionadas con el ser humano, que permitan la interoperabilidad y el intercambio de datos entre aplicaciones y sistemas.

**Hay más de 15 estándares publicados**, entre los que se encuentra la UNE-CEN/TR 419030:2018 que proporciona mejores prácticas para su aplicación por las PYME. Para conocer las áreas de normalización clave para el Mercado Digital, y los estándares de apoyo a la Transformación digital, UNE ha elaborado el Informe descargable en el siguiente [enlace](#).




**Paloma García**, Directora de Normalización y Grupos de Interés de la Asociación Española de Normalización, UNE

A close-up photograph of a person's hands holding a smartphone. The person is using a black stylus to sign a document on the phone's screen. The screen displays a signature and some text, including a legal disclaimer: "This is the electronic representation of my signature. For all purposes when used in a legal context, this electronic signature is equivalent to a handwritten signature on paper." The background is blurred, showing what appears to be a desk with a laptop and other office equipment. The entire image has a warm, reddish-orange color cast.

*Nos adentramos  
en las «entrañas»  
tecnológicas de la  
firma digital*





Mucho se ha escrito últimamente sobre la [firma digital](#) y su popularización, especialmente en los últimos meses. Pero lo que no está muy extendido es el conocimiento sobre la tecnología que hay detrás para implementarla.

En realidad, para firmar un documento, **el ordenador lee el texto y le aplica una función hash**, un algoritmo matemático que calcula un resumen del contenido y lo expresa con un número. Con el **algoritmo de firma** y la clave privada, se transforma ese número en otro, y ese resultado es la firma, que se coloca en el documento.

Para verificar su autenticidad, se aplica la clave pública a la firma, y se comprueba que el número resultante es el mismo que el obtenido al aplicar al documento la función hash, asegura Ángel del Río, profesor de Teoría de Números y Criptografía de la Universidad de Murcia, en declaraciones a [El País](#).

**SEGUIR LEYENDO >**



### ***Tipos de firma digital que existen, según su nivel de seguridad***

La normativa **eIDAS** (Identificación electrónica y los Servicios de Confianza para las Transacciones Electrónicas), entre otras cosas, determina el nivel de seguridad y los diferentes tipos de **firmas electrónicas** que existen en el mercado, en relación a esta característica. Así, existen tres tipos.

**SEGUIR LEYENDO >**

### ***Qué trámites laborales puedo hacer usando la firma digital***

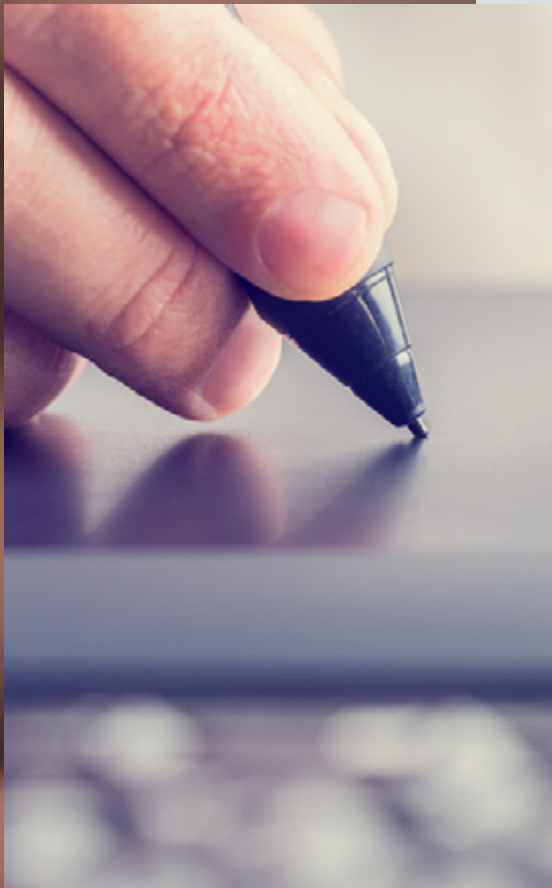
Este tipo de **firma** es legal en los contratos de compraventa de productos o servicios, pero también en las autorizaciones para la prestación de servicios y en los formularios para confirmar la prestación de un servicio técnico.

Pero es que además, la firma digital es un pasaporte para acceder a la realización de la declaración de la renta a través de internet, a las solicitudes en los registros electrónicos administrativos, a la petición de la vida laboral o a la recepción de notificaciones electrónicas. También sirve para firmar tanto correos electrónicos como facturas electrónicas.

**SEGUIR LEYENDO >**







## ***Firma digital, ¿por qué hay que recurrir a los expertos?***

Al aplicar una **firma digital** a un documento, el cifrado vincula un certificado digital (obtenido después de verificar la identidad del usuario) con los datos que se están firmando en una «huella dactilar única». Al igual que una huella dactilar física, los componentes criptográficos que conforman el documento firmado digitalmente no pueden replicarse ni alterarse, tal y como explica [Global Sign](#).

Esta característica garantiza la seguridad y el cumplimiento normativo de las firmas digitales y, por ello, son más fiables a efectos jurídicos. Las firmas digitales pueden aplicarse para transformar digitalmente, «empaquetar» digitalmente o sellar digitalmente documentos.

***SEGUIR LEYENDO >***



## ***Los cinco principales usos de la firma electrónica en las pymes***

La **firma electrónica** está experimentando una fuerte adopción. Los resultados de un reciente **estudio** realizado por MarketsandMarkets estiman que *“el mercado mundial de firmas digitales crecerá de 1.200 millones de dólares, en 2018, a 5.500 millones para 2023”*.

Esto no es sorprendente. Los procesos de firma electrónica son más rápidos y fáciles que las firmas tradicionales, lo que brinda numerosos beneficios comerciales muy atractivos y las empresas son, cada vez más, conscientes de la importancia de adaptarse a estas nuevas tecnologías.

***SEGUIR LEYENDO >***



*Cátia Reis, de PwC:*  
**«La firma digital,  
en especial la  
cualificada,  
aporta seguridad  
jurídica a la  
empresa»**

El concepto de **firma digital** fue introducido por primera vez por **Diffie y Hellman, en el año 1976**, aunque se está popularizando ahora, con el *boom* de la digitalización en las empresas. Esta herramienta ha ido evolucionando con el pasar de los años, ofreciendo cada vez más seguridad a los firmantes y siendo aceptadas por todo tipo de organismos, a nivel nacional e internacional.

La legislación que está detrás de esta solución tecnológica puede resultar un poco compleja. Para ahondar en sus raíces, lo que le da la capacidad de seguridad jurídica y fiabilidad, hemos hablado con **Cátia Reis, experta en Regulación Digital del equipo de NewLaw de PwC Tax & Legal.**

**SEGUIR LEYENDO >**



# Algunas de las normas técnicas más relevantes para pymes, publicadas hasta el momento:

<b>Serie UNE-EN 419211</b>	Perfiles de protección para los dispositivos seguros de creación de firma.
<b>UNE-CEN/TR 419030:2018</b>	Estructura racionalizada para la normalización de firmas electrónicas. Mejores prácticas para las PYME.
<b>UNE-CEN/TR 419040:2018.</b>	Estructura racionalizada para la normalización de firmas electrónicas. Directrices para los ciudadanos
<b>UNE-CEN/TS 17261:2018</b>	Autenticación biométrica para el control de accesos a infraestructuras críticas. Requisitos y evaluación.
<b>UNE-CEN/TS 17262:2018</b>	Identificación personal. Robustez frente a los ataques de presentación biométrica. Aplicación al control automático de fronteras europeo
<b>UNE-CEN/TS 419261:2015</b>	Requisitos de seguridad para sistemas de confiabilidad en la gestión de certificados y de sellos de tiempo ( <i>time-stamps</i> ).
<b>UNE-EN 15320:2007</b>	Sistemas de tarjetas de identificación. Aplicaciones para el transporte terrestre. Aplicaciones del transporte público interoperables.
<b>UNE-EN 1545-1:2015</b>	Sistemas de tarjeta de identificación. Aplicaciones de transporte en superficie. Parte 1: Tipos de datos elementales, listas generales de códigos y elementos generales de datos.
<b>UNE-EN 1545-2:2015</b>	Sistemas de tarjeta de identificación. Aplicaciones de transporte en superficie. Parte 2: Elementos de datos relacionados con el transporte y el pago del viaje y listas de códigos.
<b>Serie UNE-EN 419212</b>	Interfaz de aplicación de elementos seguros para la identificación electrónica, servicios de autenticación y de confianza.
<b>UNE-EN 419221-5:2018</b>	Perfiles de protección para los módulos criptográficos de proveedores de servicios de confianza. Parte 5: Módulo criptográfico para servicios de confianza.
<b>Serie UNE-EN 419241</b>	Sistemas confiables que permiten firma de servidor.
<b>Serie UNE-EN 419251</b>	Requisitos de seguridad para dispositivos de autenticación.
<b>UNE-CEN/TS 17489-1:2020</b>	Identificación personal. Documentos de origen europeo seguros e interoperables. Parte 1: Estructura general.
<b>UNE-EN 419231:2019</b>	Perfil de protección para sistemas confiables que soportan el mercado de tiempo.
<b>UNE-EN 17054:2020</b>	Vocabulario multilingüe de biometría basado en la versión inglesa de la norma ISO/IEC 2382-37:2012.
<b>Serie ETSI EN 319 411</b>	Firma Digital e infraestructura (ESI). Política y requisitos de seguridad para certificados emitidos por proveedores de servicio de confianza
<b>Serie ETSI EN 319 412</b>	Firma Digital e infraestructura (ESI). Perfiles de certificado.

Fuente: UNE



***El mercado inmobiliario  
adopta la firma digital  
para agilizar el cierre  
del contrato***



***Preocupación por SARA,  
plataforma de validación  
de firma digital, tras los  
últimos ataques a la AAPP***



***Una startup española se  
encargará de digitalizar  
a la Seguridad Social  
francesa***





## ***Razones por las que las pymes latinoamericanas deberían adoptar la firma digital***




## ***El futuro del mercado de la firma digital y los principales 'players' internacionales***



## ***La crisis del COVID acelera y populariza el uso de la firma electrónica***

***Más información sobre Firma Digital, pinchando aquí >***



*Qué es el reglamento  
eIDAS y por qué es  
tan importante en la  
identificación digital*





El reglamento europeo **eIDAS (electronic IDentification, Authentication and trust Services)**, recogido en el parlamento europeo con el número nº 910/2014 de 23 de julio de 2014, regula la identificación y firma digital. Se trata de una normativa muy a tener en cuenta en el sector, ya que se contrapone a los proyectos de administración electrónica basados en la ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos.

La necesidad de **garantías y seguridad** es una condición indispensable para el desarrollo y la aplicación de ciertas herramientas digitales, como la firma y los certificados electrónicos. Así, el eIDAS no solo regula las transacciones y gestiones digitales sino que es la encargada de **definir las normas y los estándares** de los tres tipos de firmas electrónicas que existen y la emisión de los certificados cualificados en toda Europa. Los servicios de confianza online que ofrecen las empresas también están bajo su paraguas.

**SEGUIR LEYENDO >**



REVISTA  
**FIRMA  
DIGITAL**

Colabora:

**UNE**

Patrocinado por:

*Signaturit*  
Sign anywhere, anytime

Una iniciativa de:

**MUYPYMES**