Universidad Internacional de La Rioja

Facultad de Derecho

Máster Universitario en Protección de Datos

Validez y Seguridad de la Firma Electrónica Digital

Trabajo fin de estudio presentado por:	Katia Vanesa Araya Ramírez
Tipo de trabajo:	Trabajo Fin de Máster
Director/a:	Nicomedes Rodríguez Gutiérrez
Fecha:	18 de abril del 2022

Resumen

Hoy en día, la transformación digital ha impulsado cada vez más, el desarrollo de las operaciones electrónicas remotas, requiriendo de un medio para firmar documentos electrónicos en forma segura. Con la llegada de la crisis por Covid – 19, se aceleraron los procesos digitales entre las organizaciones (públicas y privadas) y las personas, promoviendo la firma digital en los documentos para la gestión de una actividad comercial o de servicios. Por ello, el objetivo general de esta investigación se enfocó en analizar la validez y seguridad de la firma electrónica digital en España, concluyéndose que la firma electrónica digital es reconocida como una herramienta que proviene de la tecnología y facilita la veracidad, integridad e identidad del emisor en el documento electrónico, utilizando un componente criptográfico que le permite al receptor reconocer al firmante del mismo, confirmando que ese documento firmado se encuentra intacto y con la seguridad de la supervisión distintiva del firmante. Las firmas simples utilizan los algoritmos criptográficos correspondientes a una tecnología de cifrado, que puede cambiar los datos proporcionados en los documentos para volverlos perceptibles al ciudadano que recibe. Por su parte, la firma electrónica cualificada y avanzada revela una alta seguridad cimentada en la autenticación, integridad y no repudio.

Palabras clave: Firma electrónica, firma digital, transacciones electrónicas, regulaciones legales.

Abstract

Today, digital transformation has increasingly driven the development of remote electronic operations, requiring a means to sign electronic documents securely. With the arrival of the Covid-19 crisis, digital processes between organizations (public and private) and people were accelerated, promoting the digital signature in documents for the management of a commercial or service activity. Therefore, the general objective of this research focused on analyzing the validity and security of the digital electronic signature in Spain, concluding that the digital electronic signature is recognized as a tool that comes from technology and facilitates the veracity, integrity and identity of the sender in the electronic document, using a cryptographic component that allows the receiver to recognize the signer of the same, confirming that the signed document is intact and with the security of the signer's distinctive supervision. Simple signatures use cryptographic algorithms corresponding to an encryption technology, which can change the data provided in the documents to make them perceptible to the receiving citizen. For its part, the qualified and advanced electronic signature reveals high security based on authentication, integrity and non-repudiation.

Keywords: Electronic signature, digital signature, electronic transactions, legal regulations.

Índice de Contenidos

Índice de Figuras

Índice de Gráficos

1. Introducción

Hoy en día, el acceso a internet es global y sin fronteras, es decir no hay distancias, y navegar en la red brinda disponibilidad, flexibilidad e interactividad virtual a bajo costo, porque se encuentra disponible las 24 horas del día por los 365 días del año, en donde su actualización es automática y permanente (Rodríguez 2018). Por lo tanto, la digitalización de documentos es una tendencia mundial en la adopción de las TIC, representando un elemento favorecedor de las dinámicas de trámites y operaciones empresariales y de servicios significando un mecanismo de innovación sin precedentes. Por esta razón, el uso del internet ha requerido constantemente de herramientas de seguridad para el soporte de su validez y veracidad de información (SALVADOR 2001).

Por lo tanto, la transformación digital ha impulsado cada vez más, el desarrollo de las operaciones electrónicas remotas, requiriendo de un medio para firmar documentos electrónicos en forma segura. Con la llegada de la crisis por Covid – 19, se aceleraron los procesos digitales entre las organizaciones (públicas y privadas) y las personas, promoviendo la firma digital en los documentos para la gestión de una actividad comercial o de servicios (FERNÁNDEZ, GUTIÉRREZ, DELGADO y LÓPEZ 2020).

Desde esta perspectiva, son muchas las organizaciones que utilizan como herramienta clave la firma electrónica digital distinguiéndose como un medio formal y legal de identificación de la persona, siendo efectiva su garantía de veracidad y seguridad en el documento digitalizado. Con esta alternativa, una gran cantidad de personas ahorra tiempo, disminuye el costo operativos y de uso de papel, y prescinden de movilizaciones. La firma puede ser guardada en la nube, facilitando la información desde cualquier dispositivo en el momento que lo requiera la persona (SALVADOR 2001).

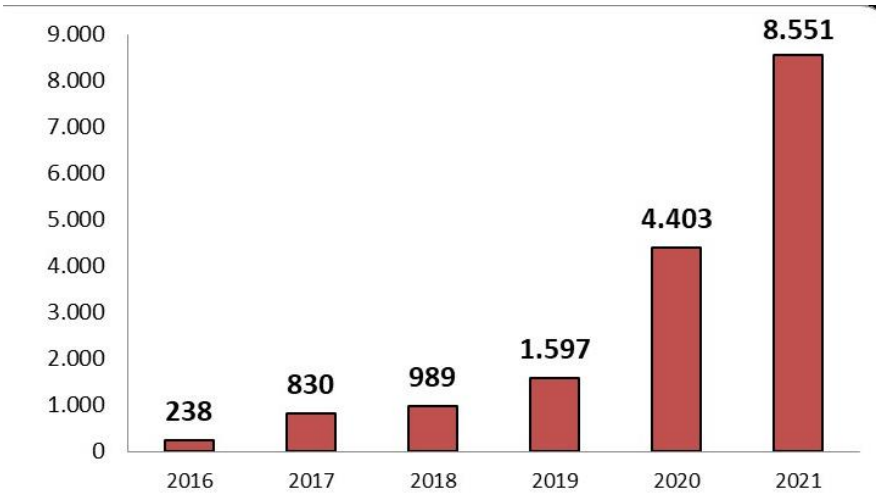

Gráfico 1. Incremento exponencial de las notificaciones electrónicas. Fuente: SEDE, 2022

Es por ello, que la firma electrónica digital debe ser utilizada en sistemas digitales confiables, seguros y válidos apegados a las normativas vigentes. Lamentablemente, la tecnología mal empleada sigue siendo vulnerable a: virus, hackers, fraudes y otros problemas por uso de medios digitales (MONGE 2009). A pesar de que la firma electrónica digital representa una solución tecnológica válida, segura y confiable en los documentos electrónicos (ver gráfico 1), por eso su incremento exponencial, y se debe cuidar las situaciones en las cuales es utilizada, sobre todo si tiene carácter probatorio y de valor legal. Por tales apreciaciones, el propósito de la investigación se centra en el análisis de la validez y seguridad que posee la firma electrónica digital en la gestión de los documentos y su efectividad antes la suplantación de personas (SARMIENTO y VILCHES 2016).

1.1. Justificación del Tema Elegido

La firma manuscrita es empleada para aceptar y aprobar un contenido firmado, y tiene validez jurídica porque el firmante prueba tal consentimiento. Por medio de la tecnología, se viene utilizando la firma electrónica digital garantizando la autenticación y seguridad en un formato electrónico. El uso de la firma electrónica en España ha sido un elemento de importancia en

el proceso de transformación digital, multiplicándose su utilización en diversos ámbitos comerciales y de servicios (RODRÍGUEZ 2016).

Actualmente, constituye una alternativa para responder a las necesidades de identificación electrónica del firmante a través de internet. Por lo tanto, la relevancia de la seguridad de la firma electrónica se compone de confidencialidad, integridad y alto nivel de confianza. En España, la firma electrónica se encuentra regulada en la Ley 6/2020, de 11 de noviembre, en donde se especifica las particularidades de los servicios electrónicos de confianza, y en el Reglamento del Parlamento Europeo y del Consejo UE Nº 910/2014, de 23 de julio de 2014 (eIDAS), que detalla las situaciones para la identificación electrónica y los servicios de confianza en las transacciones electrónicas dentro del mercado interno, derogándose la Ley 59/2003, de 19 de diciembre correspondiente a la firma electrónica y la Directiva 1999/93/CE.

Bajo estos argumentos, la investigación se considera de gran importancia académica, legal y social por el impacto significativo de la seguridad en el uso de la firma electrónica en la digitalización de documentos, contratos, transacciones, entre otros, para la gestión de las transacciones empresariales, profesionales y de servicios, bien sea del sector público o privado, permitiendo identificar al firmante, asegurando la integridad del documento y su no repudio. Por lo tanto, desde el punto de vista académico la firma electrónica digital es una ventaja tecnológica, con validez legal y de interés social (RODRÍGUEZ 2018).

1.2. Problema y finalidad del trabajo

El manejo de la información en forma electrónica constituye uno de los aspectos más comunes en la conexión de las TIC y la tramitación de documentos, por ello, la firma electrónica digital también refiere a la digitalización de los procesos, reducción de costes, incremento de la transparencia en las operaciones y garantía de seguridad (RODRÍGUEZ 2018). No obstante todavía existe en muchos firmantes, dificultades por la veracidad y fiabilidad de esta herramienta tecnológica, causando rechazo y resistencia al cambio en su utilización. Esto suele

pasar, por la ausencia de información en el firmante referente a la validez y seguridad de la firma electrónica digital y desconocimiento del ámbito jurídico que lo regula (SEDE 2022).

De lo anterior, se desprenden el problema y finalidad de este trabajo fin de máster, fundamentados en el análisis de la validez y seguridad que dicha firma electrónica tiene, permitiendo identificar, asegurar o autenticar la identidad de una persona en el envío de documentos firmados a un destinatario. Ciertamente, la firma electrónica digital es una herramienta tecnológica que respalda la autoría y consentimiento de los documentos digitales y posee tanta seguridad como la firma en los documentos en papel (SARMIENTO y VILCHES 2016).

En España, es incuestionable la cantidad de trámites y operaciones realizados a través de internet y la alternativa de la firma electrónica digital es una de las herramientas más valoradas y empleadas por los usuarios. Las transacciones jurídicas y comerciales constituyen modalidades de obligaciones expresadas en la transmisión electrónica de mensajes de datos, en donde la firma electrónica expresa la voluntad del firmante y no representa un problema inexistencia del soporte en papel y de la firma manuscrita que confirma la autenticidad y concede validez al documento (RODRÍGUEZ 2018). Según datos del INE (2022), en este país existen 11.500.000 ciudadanos que poseen algún tipo de certificado de firma electrónica (DNI) y las transacciones comerciales con firma electrónica digital alcanzaron en el 2018 más del 76.7% respecto al año anterior y en el año 2021 77, 1%.

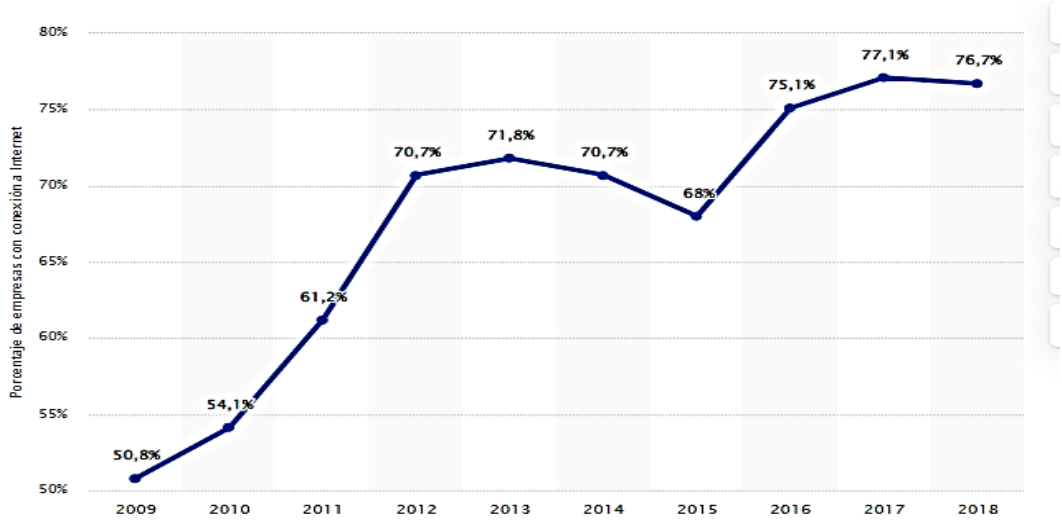

Gráfico 2. Porcentaje de compañías que utilizó firma digital en alguna comunicación enviada desde su empresa en España entre 2009 y 2018. Fuente: Statista, 2022

Esta herramienta de firma digital en 2020, se ha incrementado anualmente con 158.686 firmas totales en 2021, frente a las 89.795 de 2020, representando un 133.434 con la particularidad de firma local, 16.291 con firma en la nube y 8.961 con firma débil. También, el 84% de firmas electrónicas han sido ejecutadas con el Portafirmas en el año 2021, utilizándose la alternativa de firma con un certificado en local a través de Autofirma (SEDE 2022 y Statista, 2022). Existe un 10% de firmas ejecutadas por medio de Cl@ve Firma certificando en la nube. El 6% restante son firmas constituidas con el sistema de firma débil fundamentado en el usuario/clave UMH.

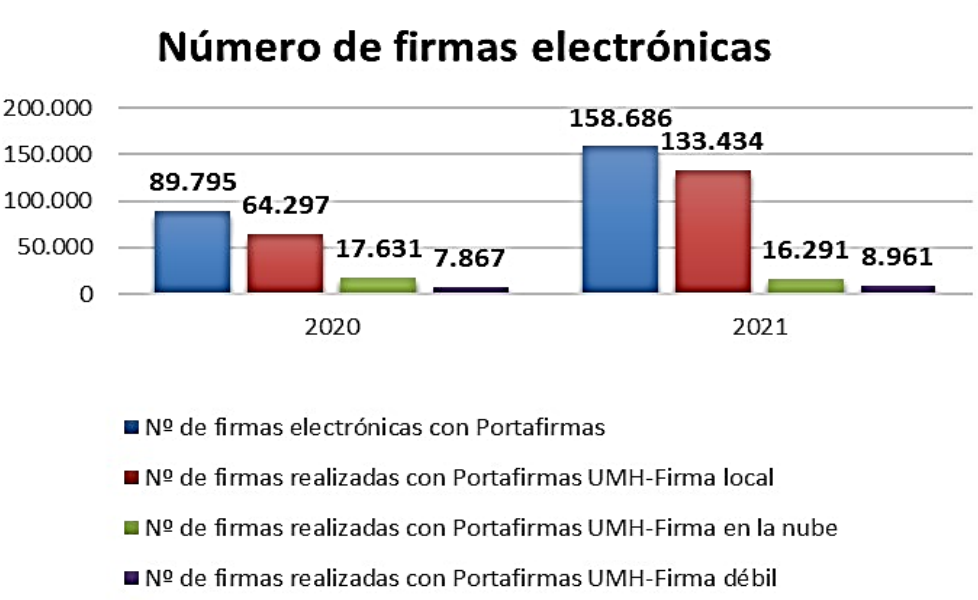

Gráfico 3. Números de firmas Electrónicas emitidas en España. Fuente: SEDE 2022

No obstante, es un aspecto polémico porque puede sufrir riesgos de ciberataque si no se utiliza adecuadamente y emplean estrategias de seguridad, por ello, firma electrónica digital requiere de controles de autenticación para mayor garantía, seguridad y confianza (RODRÍGUEZ 2018). Ciertamente, existen diversos métodos de robos de claves privadas para realizar firmas de documentos y luego validarlos como legales, infiltrándose en la identidad digital en la web hasta obtener certificaciones digitales falsas, información digital y cifrado de datos (FAJARDO 2016).

También, existen los ataques de phishing desde las aplicaciones especializadas, donde es enviado a usuario archivos o documentos de dudosa procedencia, que al ser descargados se introduce un malware que roba la información de la firma electrónica digital. Otro elemento de vulnerabilidad en firma electrónica digital es el ataque en la sombra, basado en un despliegue externo del documento en PDF, que muestra información que requiere de la firma de la persona, modificándose con datos fraudulentos luego que esta es adquirida (MONGE 2009). Todo lo expuesto, ha hecho que las instituciones públicas y privada conjuntamente con las regulaciones legales sumen esfuerzos cada vez más por fortalecer y garantizar la validez y seguridad de la firma electrónica digital, implicando un asunto de interés en el entorno académico, legal y social (SARMIENTO y VILCHES 2016).

1.3. Objetivos

1.3.1. General

Analizar la validez y seguridad de la firma electrónica digital en España

1.3.2. Específicos

- Identificar las nociones fundamentales de la firma electrónica digital.

- Determinar la fundamentación legal de la incorporación de la firma electrónica digital.

- Diferenciar las excepciones, validez, riesgos e inconvenientes en la firma electrónica digital.

- Establecer los elementos de seguridad de la firma electrónica digital.

2. Marco Teórico y Desarrollo

Este apartado, refiere a los diferentes fundamentos teóricos o aspectos conceptuales relacionados al tema de investigación, representando el soporte concreto de la temática y de los objetivos planteados referente a la validez y seguridad de la firma electrónica digital.

2.1. Nociones Fundamentales de la Firma Electrónica Digital

La firma electrónica vinculada a documentos digitalizados representa un conjunto de datos electrónicos que permiten reconocer al firmante asegurando la honestidad en el documento firmado. Esto significa, que la firma electrónica debe ser garantía de que el documento firmado en forma digital corresponde al documento original, sin alteración ni manipulación de la información (RODRÍGUEZ 2018). Por ello, los datos que emplea el firmante son confidenciales y exclusivos, lo que valida la firma en el documento. De igual forma, la firma electrónica corresponde a un grupo de datos dentro de un formato electrónico, que permite

formalizar y autorizar un documento digitalizado dando la aprobación de la voluntad de la persona (ROS 2009).

Bajo esta percepción, la firma electrónica digital no es más que una herramienta que emerge de la tecnología que facilita la veracidad, integridad e identidad del firmante del documento electrónico, utilizando un componente criptográfico que le facilita al receptor reconocer al firmante del mismo, ratificando que dicho documento se encuentra intacto al firmado en físico, con la seguridad de la supervisión distintiva del firmante referente al empleo de los datos de producción de firma electrónica (FERNÁNDEZ, GUTIÉRREZ, DELGADO y LÓPEZ 2020).

Dentro de la ejecución técnica, algunas firmas simples utilizan los algoritmos criptográficos refiriendo a una tecnología de cifrado, capaz de cambiar los datos que proporcionan los documentos para volverlos perceptibles al ciudadano que recibe, siendo no autorizado. Por su parte, la firma electrónica cualificada y avanzada revela una seguridad fundamentada en tres características básicas: autenticación, integridad y no repudio (ROS 2009).

De tal forma que, el funcionamiento de la firma electrónica (ver figura 1) se cimenta en los procedimientos y sistemas de clave pública, empleando diversas claves para el envío del documento firmado. Estas claves, constituyen realmente las llaves que restringen el acceso a otras personas, por ello, existe una clave privada que la conoce y maneja el emisor del mensaje (propietario) y una clave pública, que es asignada a los destinatarios para que puedan acceder al documento firmado (GARCÍA, ARREDONDO y BARREIROS 2015).

Bajo esta mirada, la firma electrónica digital posee estándares de seguridad en su funcionamiento (ver figura 1) capaces de ofrecer la validez, brindando una gestión confiable de los documentos desde cualquier lugar en que se encuentre el firmante, accediendo desde un dispositivo sin necesidad de desplazamientos y largas filas (FERNÁNDEZ, GUTIÉRREZ, DELGADO y LÓPEZ 2020).

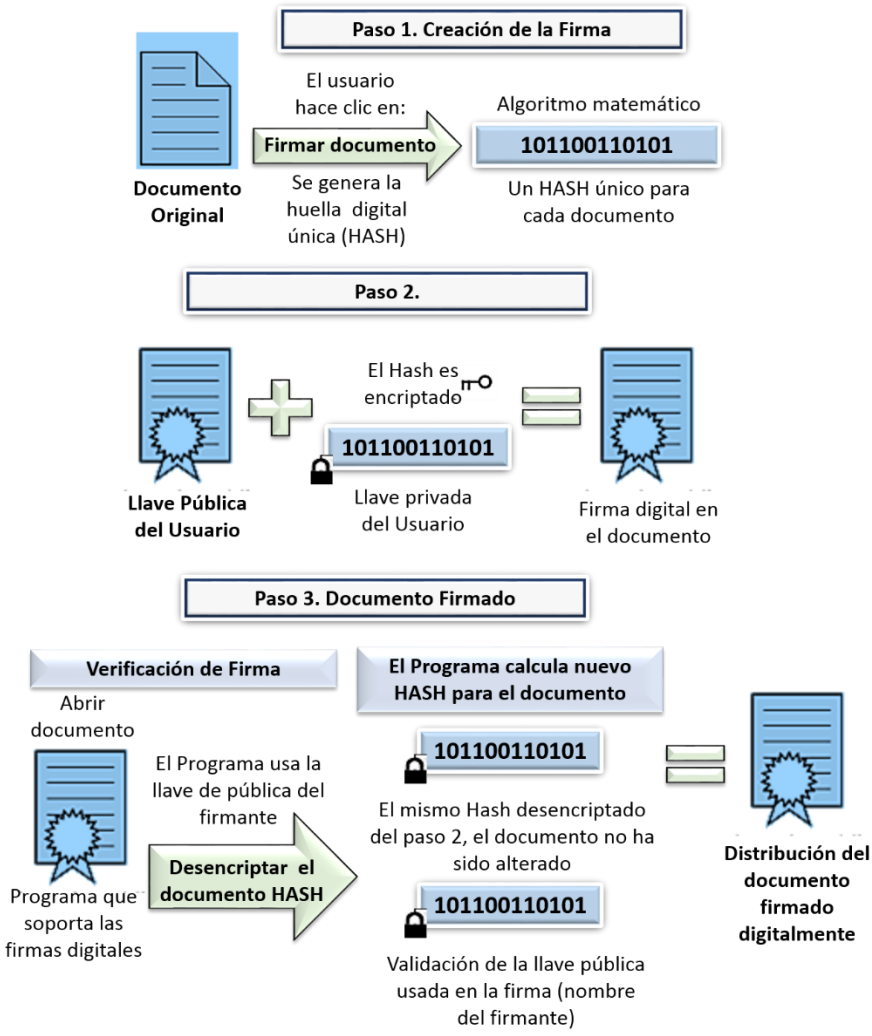

Figura 1. Funcionamiento de la firma electrónica. Fuente: *Elaboración propia*

Esta herramienta electrónica, procura versatilidad, ahorro de coste y trámites, implicando la disminución del almacenamiento de información en un espacio físico y la baja de gastos en los procedimientos administrativos de archivo de documentos (LÓPEZ 2016). También, la firma electrónica garantiza la confidencialidad porque la información contenida en el mensaje solo puede ser conocida por las personas autorizadas, conllevando a un incremento de la productividad en las operaciones empresariales y de servicios.

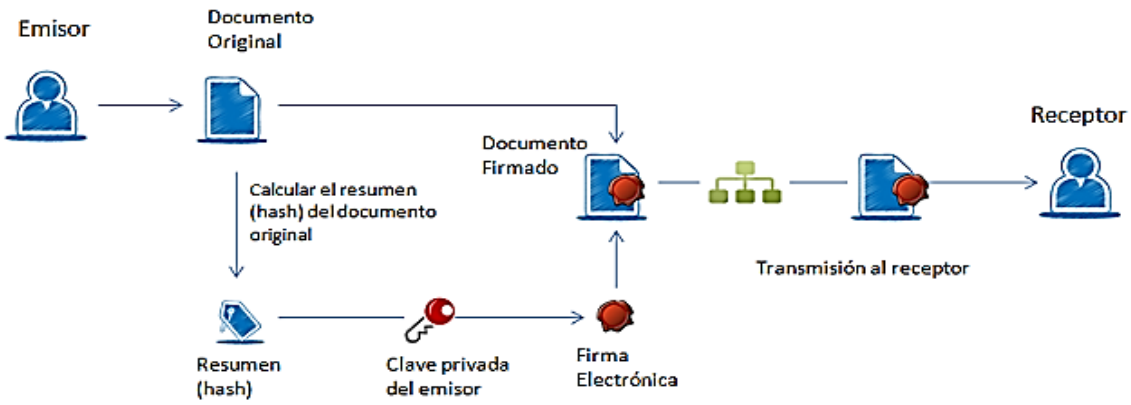

Figura 2. Utilidad y Modo de Uso de la Firma Electrónica. Fuente: PAE, 2022

2.1.1. Distinciones entre la Firma Digital y la Firma Electrónica

El uso de los términos: firma digital y firma electrónica, tiende a manejarse conjuntamente confundiéndose con un sinónimo y realmente no es así. A pesar de que existen elementos comunes en su interés de identificar al firmante y comprobar su consentimiento, existen distinciones entre ellos, porque cada uno tiene sus características de validez y riesgos en relación a la seguridad, privacidad de la información, cumplimiento de la ley, entre otros (RODRÍGUEZ 2018).

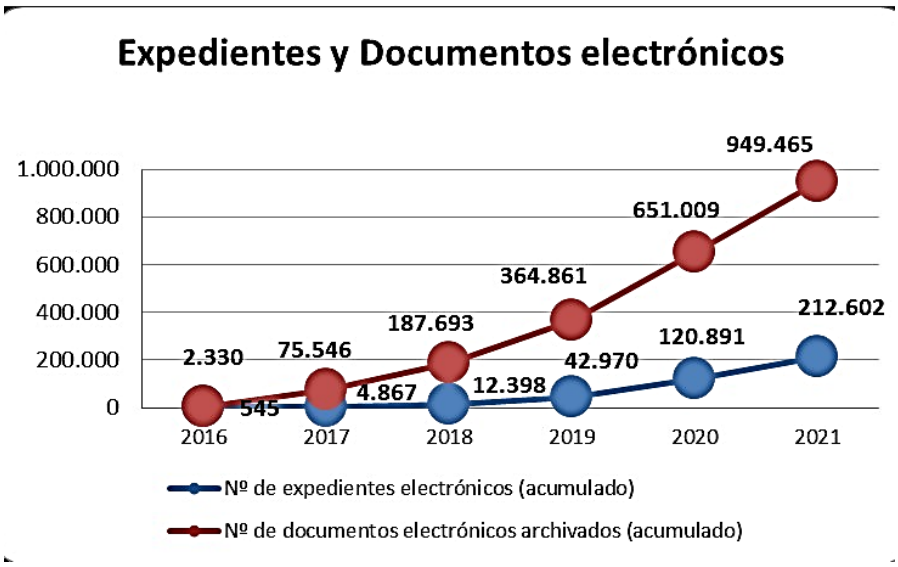

Gráfico 4. Incremento de los Expedientes y Documentos Electrónicos. Fuente: SEDE, 2022

Ciertamente, la firma digital y electrónica constituyen herramientas tecnológicas que sustituyen la firma manuscrita utilizando una autenticación y luego una firma electrónica o digital en un formato electrónico (FERNÁNDEZ, GUTIÉRREZ, DELGADO y LÓPEZ 2020). No obstante, las diferencias están relacionadas con el tipo de tecnología empleada y el grado de seguridad que ofrecen, porque la firma digital refiere a un conjunto de métodos criptográficos que asignan una valoración alfanumérica inserta a un mensaje de datos. Al utilizar un algoritmo matemático, el emisor puede establecer dicho valor alfanumérico, teniendo legalmente un no repudio de la información y la veracidad del mismo (LÓPEZ 2016).

En el caso de la firma electrónica, se puede revelar el consentimiento del firmante en un formato electrónico, representando una prueba legal totalmente válida. Lo anterior, refiere a que la firma digital puede ser considerada una firma electrónica, pero no todas las firmas electrónicas son calificadas como firma digital (LÓPEZ 2016).

2.1.2. La Firma Electrónica Cualificada

En cuanto a la firma cualificada o también llamada QES (Qualified Electronic Signature), se puede afirmar que concede un alto nivel de seguridad y veracidad. Ciertamente, esta firma posee un sistema de seguridad complejo pero ofrece una validez legal significativa por su legitimidad, que puede llegar a ser mucho más confiable que la firma manuscrita. Por esta razón, la firma cualificada se encuentra amparada en el reglamento europeo de firma (Reglamento eIDAS), porque posee la mayor garantía jurídica y de seguridad inequívoca.

Para su obtención, es necesario la emisión de un certificado cualificado (documento electrónico) que identifica al firmante, verifica los datos y valida la firma a la identidad de la persona. Este certificado, es emitido por las autoridades de certificación cualificada, porque en caso de alguna situación conflictiva, este documento puede ser utilizado como evidencia válida y legal ante un tribunal, sin requerir una prueba pericial (RODRÍGUEZ 2018).

2.1.3. Elementos de la Firma Electrónica Digital

Es importante señalar, que el Reglamento de la UE No. 910/2014, de 23 de julio, correspondiente a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior, establece en su artículo 3, tres tipos de firmas a considerar:

1. La firma electrónica, donde los datos se encuentran en un formato electrónico y no están agregados o adjuntos a otros datos electrónicos utilizados por el firmante.

2. La firma electrónica avanzada, compuesta por las exigencias establecidas en el artículo 26 de dicho reglamento (vinculación exclusiva al firmante, acceso a la identificación de la persona, creación de la firma electrónica con datos confiables del firmante y controlado únicamente por el mismo, y vinculación con datos confiables del firmante que permita la detección de cualquier modificación).

3. La firma electrónica cualificada, que representa un sistema complejo y altamente seguro por su dispositivo cualificado aplicado en la generación de la firma, emitiendo un certificado cualificado de esta firma.

Es evidente que la firma electrónica puede brindar al firmante y el destinatario de los documentos o del contenido de la información la certeza de la identidad en esta interacción y la garantía de que es una firma intacta, es decir que no ha sido alterada en el contenido de la información y por lo tanto, no se puede repudiar (SUÁREZ 2011).

Bajo estos argumentos, la firma electrónica digital está compuesta por tres elementos principales: 1. El firmante o emisor, que está representada bajo la figura de persona física, el

cual posee un dispositivo para generar la firma, por medio de la función matemática, sistema de criptografía y huella digital del mensaje, los cuales se cifra con una contraseña privada del emisor. El resultado de este proceso es la firma electrónica digital, que será adjuntado al mensaje inicial. 2. El receptor, que es la figura que comprueba en el dispositivo la veracidad de la firma electrónica digital y decifra la información contentiva en el documento electrónico, y 3. Las autoridades de Certificación, compuesta por las instituciones que emiten la certificación o por los proveedores de servicios de certificación.

2.2. Fundamentación Legal de la Incorporación de la Firma Electrónica Digital

Realizando una retrospección, se puede afirmar que en España se crearon las primeras Autoridades de Certificación en 1995, vinculando gradualmente las necesidades de firma electrónica digital con el crecimiento tecnológico, emitiéndose la primera normativa de regulación en la Directiva 1999/93CE, 13 de diciembre, de firma electrónica. Ciertamente, en Europa emergieron transformaciones e innovaciones tecnológicas significativas y cambios en la dinámica empresarial y de servicios asociadas a las TIC, lo que requirió en la Unión Europea de un marco comunitario regulador para la firma electrónica, con el propósito de suministrar garantías en su utilización adecuada y favorecer su validez jurídica (FERNÁNDEZ, GUTIÉRREZ, DELGADO y LÓPEZ 2020).

Considerando lo anterior, España impulsa la primera Ley 59/2003, referida a la regulación de la firma electrónica, determinando la veracidad y eficacia jurídica y estableciendo las especificaciones para la prestación de servicios de certificación, creándose posteriormente en el 2006, el DNI electrónico para brindar a las personas la alternativa de efectuar consultas y operaciones de manera digital.

Al incrementarse el uso de la TIC, nacieron otras oportunidades de comercialización y servicios, lo que requirió de mayor seguridad en el uso de las firmas electrónicas digitales, emergiendo las primeras firmas en la nube, promulgándose la Ley 11/2007, de 22 de junio,

correspondientes al Acceso Electrónico de los Ciudadanos a los Servicios Públicos, en donde se reconoce el derecho a las personas para vincularse por medios electrónicos con las administraciones del sector público (Cordova, Vega, Rodríguez y Escobedo 2020).

Luego, se promulga el Reglamento UE No. 910/2014 (también llamado Reglamento eIDAS) de Identificación Electrónica, con el propósito de consolidar uniformemente las normativas vigentes en todos los países pertenecientes a la unión europea, dando reconocimiento jurídico a las firmas electrónicas digitales y entrando en vigor en España el 1 de julio de 2016 como parte de la consolidación de la transformación digital (sustituye la Ley 59/2003 de firma electrónica). El Reglamento eIDAS, simboliza un marco seguro y común en los países miembros de la UE y regula legalmente las firmas electrónicas.

En esa dinámica de adaptación jurídica y de trasformación tecnológica, España promulga la Ley 6/2020, de 11 de noviembre, regulando las especificaciones de los servicios electrónicos de confianza, aplicable a los prestadores públicos y privados derogando completamente la Ley 59/2003 de firma electrónica, que presentaba incompatibilidades con el Reglamento de la UE.

2.2.1. Emisión y Creación de la Firma Electrónica Digital

En España, la Fábrica Nacional de Moneda y Timbre (FNMT) es la institución que le permite a la administración pública certificar y autenticar los trámites digitales, tanto a las a empresas como a los ciudadanos, posibilitando realizar las operaciones con total seguridad. La FNMT-RCM, es el Proveedor de Servicios de Certificación realizado en CERES, que a través de sus aplicaciones admiten el acceso a la administración pública, las personas y las empresas a efectuar sus trámites y operaciones vía on line en forma confiable, proporcionando a los usuarios validez y seguridad a las transacciones electrónicas (SEDE 2022).

Este certificado digital emitido por la FNMT en España es válido para gestionar vía internet trámites con la administración pública y es de fácil uso porque el usuario lo puede tramitar

directamente. Para lograr que una firma avanzada sea reconocida en el certificado digital emitido por la FNMT se debe contar 4 características primordiales: 1. Identificar al emisor, 2. Comprobar la integridad del documento, 3. Atestiguar el no repudio y 4. Disponer de la participación de un receptor (SEDE 2022).

Gráfico 5. Número de visitas evoluciona desde las 21.741 en el año 2016, hasta las 222.098 en el año 2021. Fuente: SEDE, 2022

También, debe fundamentarse en un certificado reconocido, es decir, que la firma electrónica digital requiere de un certificado electrónico válido, expedido por la Autoridad de Certificación o un DNI electrónico, compuesto de unas claves criptográficas necesarios para firmar. Por ello, el certificado que se emite usualmente es el Certificado de Persona Física o Jurídica que despacha en la Fábrica Nacional de Moneda y Timbre (FNMT) (ver gráfico 2), aunque también se pueden aplicar otros procedimientos (ESPINOZA 2018). Por esta razón, las autoridades de certificación consideradas en España, para la obtención de un certificado digital, para el uso a la SEDE electrónica son:

- DNI electrónico (Dirección General de la Policía).
- Fábrica Nacional de Moneda y Timbre (FNMT).
- Generalitat Valenciana (ACCV)

- Agencia Catalana de Certificación (CATCert).
- ANF Autoridad de Certificación (ANF AC).
- AC Camerfirma.
- Ziurtapen eta zerbitzu empresa, IZENPE.
- Autoridad de Certificación de la Abogacía (ACA).
- Firma profesional.

2.2.2. Tipología de Firmas Electrónicas Digitales

El Reglamento UE No. 910/2014 (Reglamento eIDAS) establece la firma electrónica simple, como una firma de carácter fácil y rápida, porque no se trata de un trazo sino que se basa en marcar una casilla o en incorporar un código PIN, también se puede hacer aceptando los términos y condiciones en conformidad con el documento. Se considera una firma fácil y rápida de configurar, pero puede presentar problemas al no identificar al usuario de forma segura (UANATACA 2020).

También, existe la firma electrónica avanzada, que fue definida como una firma de seguridad superior y que contiene los siguientes requisitos: 1. Datos de la creación de la firma bajo el control propio del firmante en el momento de realizarla, 2. Documento electrónico y los datos de la firma inalterables y 3. Acceso a la identificación del emisor (CARDENAS 2013).

Otra firma electrónica es la cualificada, que bridan un nivel de seguridad superior a las anteriores, por lo que requiere de un certificado cualificado de firma electrónica. El propósito de los certificados electrónicos es validar y certificar que una firma electrónica referente a una persona o entidad específica, y puede realizarlo porque tiene los datos del individuo y de la entidad involucrada, por ejemplo: el nombre, NIF, algoritmo y claves de la firma, fecha de vencimiento y organismo que lo expide, entre otros, mediante un dispositivo cualificado que garantiza que las firmas electrónicas sean seguras y están protegidas ante situaciones de falsificaciones, empleando algoritmos criptográficos.

	Firma electrónica simple	Firma electrónica avanzada	Firma electrónica cualificada
Facilidad de uso	✓	✓	✓
Autenticidad		✓	✓
Identidad		✓	✓
Autenticación		✓	✓
Integridad		✓	✓
Hardware o sistemas certificados			✓
Inversion de la carga de prueba			✓
Máximas garantías legales			✓

Figura 3. Diferencias entre la firma electrónica cualificada, simple o avanzada. Fuente: Prestador de Servicios de Certificación Uanataca, 2020

Desde esta perspectiva, la ejecución de la firma electrónica cualificada se suele tener muchas exigencias en los trámites y documentos de las administraciones públicas, como Hacienda o la Seguridad Social. Cabe destacar, que los requerimientos de esta herramienta tecnológica se fundamentan en el Reglamento (UE) Nº 910/2014, nexo II que señala: Los dispositivos cualificados para la generación de la firma electrónica avalarán, a través de medios técnicos y procedimiento apropiados, que:

a) Se garantiza razonablemente la confidencialidad de los datos de creación de firma electrónica empleados en la creación de firmas electrónicas

b) los datos de creación de firma electrónica utilizados sólo pueden estar presente una vez en la práctica

c) Existe una seguridad razonable de que los datos creados de firma electrónica no son hallados por deducción y de que la firma está protegida con seguridad contra la falsificación mediante la TIC accesible al momento.

d) Los datos de creación de la firma electrónica empleado puede ser resguardados por el emisor legítimo de forma confiable ante su utilización por otros.

Es evidente que los dispositivos cualificados de creación de firmas electrónicas no modifican los datos que se utilizan las firmas y la generación de dicha firma en nombre del emisor sólo podrán gestionarse a cargo de un prestador cualificado de servicios.

Sin perjudicar el literal d, los prestadores cualificados de servicios de confianza que tramiten los datos de creación de firma electrónica en nombre del emisor lograrán reproducir los datos de creación de firma solamente con propósito de formalizar una copia de seguridad cumpliendo los siguientes aspectos:

a) La seguridad del grupo de datos duplicados es aplicable a los conjuntos de datos originales

b) El número de conjuntos de datos duplicados no puede ser mayor al mínimo necesario, garantizando la continuidad del servicio.

La firma electrónica posee su nivel de seguridad, autenticidad, integridad y no repudio y por eso es clasificada en la firma electrónica simple, avanzada y cualificada (SÁNCHEZ 2007).

2.3. Excepciones, Validez, Riesgos e Inconvenientes en la Firma Electrónica Digital

2.3.1. Excepciones en la Firma Electrónica Digital

Existen en España algunas excepciones (aplicables a hipotecas, donaciones, entre otros) en las que una disposición legal determinada necesita de formalidades especiales, como el otorgamiento o la inscripción de un acuerdo en una escritura notarial o su inscripción en registros públicos (Registro de la Propiedad o el Registro Mercantil). Para ello, puede ser exigido la firma física y la comparecencia de los involucrados (PEÑARANDA 2011).

En este sentido, algunos contratos notariados no admiten firmas electrónicas, como los documentos vinculados con el derecho de familia o herencias; ejemplo de ello: los contratos de herencia, contratos matrimoniales, entre otros. Los contratos de compra, arrendamiento o transferencia de bienes raíces también se encuentran en las excepciones porque necesitan la intervención de un notario.

Otros documentos que no admiten firma electrónica digital son los estatutos de una sociedad con responsabilidad limitada y las asignaciones de acciones. Asimismo, se excluyen algunos documentos de talento humano que deben ser completados a través de agencias gubernamentales y requieren de formalidades específicas.

2.3.2. Validez, Riesgos e Inconvenientes

La firma electrónica permite suscribir documentos y contratos desde trayectos remotos y de forma eficaz, reduce costes y minimiza el tiempo utilizado en desplazamientos y envíos. Al revisar los argumentos de la validez de contratos, el Código Civil español en su artículo 1.261, indica tres elementos esenciales: consentimiento, objeto y causa. El elemento revelador en

este argumento es el consentimiento, definido en el Código Civil, artículo 1262, como la expresión por el oposición de la oferta y la aceptación sobre el objeto y la procedencia que han de formalizar el acuerdo.

El artículo 1258 también establece que los contratos se perfeccionan por la conformidad de los involucrados, y su validez no es exclusivamente la firma manuscrita, sino que se puede manifestar a través la aceptación de las partes contratantes. Se registran tres tipos de firmas: simple, avanzada y cualificada desarrolladas anteriormente.

La firma electrónica simple posee una presunción de veracidad y si hay quien considera que está falsificada y refuta ese contrato, se actuará según lo expuesto en el artículo 326 de la Ley 1/2000, de enero, de Enjuiciamiento Civil, requiriendo peritar o cotejar la firma para evidenciar si efectivamente fue falsificada o no. La firma electrónica cualificada es calificada como altamente segura, pero las otras dos también poseen resultados jurídicos y son legítimas.

El Reglamento eIDAs indica en su artículo 25 que no se refutarán implicaciones jurídicas ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el solo hecho de ser una firma electrónica o porque no cumple las exigencias de la firma electrónica cualificada. De igual forma, los Estados miembros de la UE garantizan la aceptación de las firmas electrónicas cualificadas, en el contexto de la prestación de servicios, sin la necesidad de requisitos adicionales que obstaculicen la utilización de tales firmas. En España, la Ley derogada 59/2003 de Firma Electrónica había otorgado plena validez legal a la firma electrónica cualificada, representando simultáneamente las condiciones del Reglamento eIDAS.

Ahora bien, dentro de los riesgos de firmar digitalmente un documento se puede inferir que la firma electrónica avanzada es fiable y altamente fehaciente por su cifrado asimétrico. Las firmas electrónicas digitales, son muy seguras, pero son asequibles de ser hackeadas como el resto de la tecnología. Estos sucesos se mitigan al mínimo a través de los certificados, claves,

entre otros. Cuando dicho certificado ha sido otorgado por un organismo confiable, las claves están vigiladas y no están disponibles al público. Desde esta mirada, el riesgo se encuentra en cada usuario y en el uso de la misma.

Dentro de esta visión, el mayor riesgo en el instante de firmar digitalmente un documento se localiza en tener al descubierto la contraseña, y de no cuidar la privacidad de la misma, permitiendo la visibilidad para terceros. El conocimiento de la misma en otras personas puede generar la suplantación de identidad. Para evitar dichos riesgos al firmar digitalmente un documento (FERNÁNDEZ Y GÓMEZ 2005), es imperioso considerar los siguientes aspectos:

1. Los certificados son emanados por un prestador de servicios de certificación fiable y que para su creación utiliza un hardware criptográfico.

2. Contar una política de control y protección de contraseñas, que establezca claramente un sistema seguro y centralizado para la gestión dicha clave. Este sistema debe permitir el acceso solamente a los beneficiarios autorizados, permitiendo saber quién firmó, hora, entre otros.

2.4. Seguridad de la Firma Electrónica Digital

La seguridad de la firma electrónica digital es apreciada desde una perspectiva técnica que viene dada por la criptografía. La noción de cifrada se genera en un mensaje en claro, es decir, reconocible, al que se le realiza un algoritmo de cifrado, se generando un mensaje cifrado que sólo puede ser descifrado por aquellos usuarios que conozcan el algoritmo empleado y la clave que se ha colocado. Dentro del cifrado digital se encuentra 2 opciones básicas: el cifrado de clave simétrica y el de clave asimétrica.

Figura 4. Nivel de seguridad de la firma digital. Fuente: Prestador de Servicios de Certificación Uanataca, 2020

La firma digital es un sello de autenticación electrónico cifrado en una información digital, como mensajes de correo electrónico, macros o documentos electrónicos. Esta herramienta, consiente que los datos derivan del emisor y no se ha rectificado (PAe 2022). En este aspecto las funciones para las firmas digitales al igual que las manuscritas son para identificar al autor del documento y demostrar que el autor aprueba el contenido del documento que se suscribe. De allí la electrónica es segura si sirve para cumplir adecuadamente estas funciones básicas y cumple con los parámetros legales y así verificar esto, frente a cualquier tipo de firma electrónica que se encuentre en el mercado es pertinente revisar, romando en cuenta los siguientes aspectos:

La Autenticidad: permite los métodos para validar la identidad al usar la firma electrónica

La Integridad: Revise si luego de que se firma el documento electrónico es fácil alterarlo o modificarlo.

Método apropiado: de acuerdo a la ley que indica de forma fácil este requisito significa que la tecnología de firma electrónica debe guardar correspondencia con la naturaleza y complejidad

del acto. Los criterios mencionados permiten evaluar de manera preliminar la seguridad de la firma electrónica, sin embargo se aconseja que siempre se cuente con una asesoría técnica o jurídica, precisando que la firma electrónica se suscriben documentos como contratos o títulos valores.

2.4.1. Criptografía Simétrica

Se emplea una única contraseña para cifrar y comprender el mensaje. El beneficio más significativo de la criptografía de clave simétrica es su velocidad haciendo de éste tipo de algoritmos los más idóneos para el cifrado de grandes cantidades de datos. El problema que se presenta en la criptografía de clave simétrica es la necesidad de intercambiar la clave empleada y si alguien logra entrar en el mensaje puede conseguir la clave utilizada y descifrar el mensaje. Por esta razón, se plantea el uso de un sistema criptográfico basado en claves asimétricas para tener mayor seguridad.

En el Cifrado Simétrico, se implementa la criptografía simétrica con un hardware que puede ser muy eficaz porque no experimenta ningún retraso de tiempo significativo como resultado del cifrado y descifrado. También, la criptografía simétrica suministra un grado de autenticación porque los datos cifrados con una clave simétrica no se pueden descifrar con ninguna otra. Consecuentemente, siempre que las dos partes que la utilicen para cifrar las comunicaciones conserven en secreto la clave simétrica, cada una de las partes puede estar segura de que se está comunicando con la otra siempre que los mensajes descifrados sigan teniendo coherencia.

2.4.2. Criptografía asimétrica

En este caso del sistema criptográfico asimétrico, cada usuario pose una pareja de claves: 1. Clave pública, que será utilizada por todos los usuarios y 2. Clave privada: que es resguardada por su propietario y no se da a conocer en alguien más. Esta pareja de claves es

complementaria, por esta razón, lo que cifra una persona también lo puede descifrar la otra. Estas contraseñas, se obtienen mediante métodos matemáticos complejos y es imposible conocer una clave a partir de la otra. De esta forma, el beneficio de este sistema consiste en la supresión de la necesidad del envío de la clave, representando un sistema seguro, aunque agrega lentitud en la operación. Para solventar dicha situación, el procedimiento que se aplica para realizar el cifrado de un mensaje es emplear un algoritmo de clave pública conjuntamente a uno de clave simétrica.

Por lo tanto, la criptografía (MARTÍNEZ 2021) se fundamenta en la matemática aplicada de diferentes ramas: teoría de números, álgebra, combinatoria, probabilidad, geometría algebraica, entre otros, cuyo propósito es codificar mensajes por medio de algoritmos de cifrado, de forma tal que solo los que conozcan la clave puedan conocer su significado.

Uno de estos métodos es la firma digital, que se desarrolla por medio de un tipo de criptografía conocida como asimétrica o de clave pública. En esta modalidad, hay una clave privada, que es conocida por el firmante y se guarda en el DNI electrónico o en otra tarjeta, y una pública que es la utilizada por todos.

La computadora corrobora el texto y aplica una función hash, un algoritmo matemático que calcula un resumen del contenido y lo formula con un número. El algoritmo de firma conjuntamente con la clave privada, se realiza la transformación de ese número en otro, y ese resultado sería la firma digital electrónica, que se plasma en el documento.

Para verificar su verdad, se emplea la contraseña pública a la firma, y se demuestra que el número proveniente es el mismo que el derivado en el documento en la función hash. Estas operaciones no son realizadas por el usuario, sino que, después del algoritmo matemático, viene la implementación de los profesionales en TIC que generan las herramientas técnicas online y aplicaciones para demostrar lo correcto del proceso y evitar que alguna persona falsifique una firma resolviendo un problema matemático muy difícil. En otras palabras:

1) para la Generación de hash: inicialmente, se emplea el algoritmo de generación de hash sobre el documento que se quiere firmar y enviar. Desde este proceso, se va a producir un código hash único partiendo de un algoritmo establecido, que identifica inequívocamente a dicho documento.

2) Firma y encriptación: en el proceso de firma, se procede a encriptar ese código empleando la clave privada del emisor.

3) Envío: El acuerdo firmado se envía a su receptor destino, conjuntamente con el hash encriptado y la contraseña pública del emisor.

4) Recepción y comprobación: Una vez se efectúa la recepción del documento por parte del receptor, se ejecutan tres operaciones:

- Producir un nuevo código hash partiendo del documento enviado, empleando el mismo algoritmo.

- Manejar la clave pública del emisor para desencriptar el hash enviado.

- Cotejar ambos hash. Si concuerdan fielmente, se considera que la firma es válida y que el documento no se modificó con posterioridad a su firma.

- El Cifrado Asimétrico: es la criptografía asimétrica, también llamado como criptografía de clave pública, refiere a un proceso que usa un par de claves relacionadas, una clave pública y una segunda particular, para cifrar y descifrar una información, y resguardarlo de entradas o usos no facultados. Para la utilización de una clave pública es una clave criptográfica que puede ser usar por cualquier persona para cifrar un

mensaje de manera que sólo pueda ser descifrado por el destinatario con su clave privada.

Además con una clave privada también llamada clave secreta sólo se comparte con el iniciador de la clave. Es por ello que, se infiere que el beneficio de la criptografía asimétrica es el aumento de la seguridad de los datos. Partiendo que este proceso de cifrado es seguro ya que los usuarios no deben compartir su clave privada.

- Las criptografía simétrica y asimétrica tienen diferencias en donde el cifrado simétrico utiliza una clave única que debe compartirse entre las personas que necesitan recibir el mensaje, mientras que el cifrado asimétrico maneja dos contraseñas públicas y una contraseña personal para cifrar y descifrar las informaciones al comunicarse. También el cifrado simétrico es una técnica antigua ya que mientras que el cifrado asimétrico es relativamente nuevo.

Es importante conocer que el cifrado asimétrico lleva comparativamente más tiempo que el cifrado simétrico. En cuanto al cifrado, los esquemas de seguridad más recientes pueden ser necesariamente los que mejor se adapten, destacando que siempre se debe utilizar el algoritmo de cifrado propicio para la tarea en cuestión. Es por ello que, a medida que la criptografía toma un nuevo cambio, se están perfeccionando nuevos algoritmos en un intento por contrarrestar a los espías y resguardar la información para mejorar la confidencialidad. Para ello, los piratas informáticos generaran dificultades a los expertos para crear confiabilidad en los usuarios.

2.4.3. Autoridad de Certificación y el Prestador de Servicios de Confianza Cualificado

El certificado digital identifica al usuario como persona o empresa y confirma ante los diversos organismos públicos en cualquier transacción telemática. Este certificado digital, es emitido por una institución de confianza. Ese rol lo tiene la Autoridad de Certificación (en inglés CA *Certification Authority* o RA *Registration Authority*) (UANATACA 2020 y SEDE 2022).

Una Autoridad de Certificación se encarga de emitir y anular los certificados digitales manejados en las transacciones, operaciones y firmas electrónicas. Esta confianza interviniente entre las empresas o instituciones y personas físicas. Cuando se efectúa cualquier transacción entre las partes involucradas, la Autoridad de Certificación concede la validez y confianza a los documentos tramitados y firmados (UANATACA 2020 y PAe 2022).

La infraestructura de contraseñas criptográficas ha permitido que la Autoridad de Certificación, cuente con PKCS o Public-Key Cryptography Standards, que representan la garantía de la identidad del emisor, el registro de la fecha y hora exactas en las que se ejecutó la firma electrónicamente (sellado de tiempo) así como el contenido de las transacciones ejecutadas.

Ahora bien, desde hace un buen tiempo la UE vela por la construcción de un mercado único digital que permita excluir las paredes del comercio electrónico y todo tipo de transacciones electrónicas entre los distintos países miembros. De esta realdiad, nace el Reglamento eIDAS *(Electronic Identification and Authentication Services)* para establecer un estándar de identificación electrónica, garantizando la validez de cualquier certificado digital en la UE, con independencia del Estado de origen. Este Reglamento se apoya en los Servicios electrónicos de Confianza, con el propósito de establecer en Europa dos aspectos:

1. El de los servicios electrónicos de confianza, constituyendo éstos la creación, verificación y validación de firmas electrónicas, sellos electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, para la autenticación de sitios web y la preservación de firmas, sellos o certificados electrónicos.

2. El del prestador de servicios de confianza: Representa una persona física o jurídica que facilita uno o más servicios electrónicos de confianza, bajo el rol de prestador cualificado o como prestador no cualificado (UANATACA 2020).

3. Conclusiones

Al realizar el análisis de la validez y seguridad de la firma electrónica digital en España, se pudo concluir que la firma electrónica es garantía de que el documento firmado en forma digital corresponde al documento original, sin alteración ni manipulación de la información. De igual forma, la firma electrónica conlleva a un conjunto de datos dentro de un formato electrónico, para formalizar y autorizar un documento digitalizado.

Bajo esta consideración, en la identificación de las nociones fundamentales de la firma electrónica digital se puede inferir que es reconocida como una herramienta que proviene de la tecnología y facilita la veracidad, integridad e identidad del emisor en el documento electrónico, utilizando un componente criptográfico que le permite al receptor reconocer al firmante del mismo, confirmando que ese documento firmado se encuentra intacto y con la seguridad de la supervisión distintiva del firmante.

Las firmas simples utilizan los algoritmos criptográficos correspondientes a una tecnología de cifrado, que puede cambiar los datos proporcionados en los documentos para volverlos perceptibles al ciudadano que recibe. Por su parte, la firma electrónica cualificada y avanzada revela una alta seguridad cimentada en la autenticación, integridad y no repudio.

Ahora bien, dentro del funcionamiento de la firma electrónica existen los procedimientos y sistemas de clave pública, empleando diversas claves para el envío del documento firmado. Estas claves, constituyen realmente las llaves que restringen el acceso a otras personas, por ello, existe una clave privada que la conoce y maneja el emisor del mensaje (propietario) y una clave pública, que es asignada a los destinatarios para que puedan acceder al documento firmado.

Es entendible, que la firma electrónica digital contenga estándares de seguridad en su funcionamiento para poder ofrecer la validez y brindar confianza en los documentos desde cualquier lugar en que se encuentre el emisor, con acceso a la información desde un dispositivo evitando desplazamientos. La firma electrónica, se caracteriza por tener versatilidad, ahorro de coste y trámites, promoviendo la eliminación del almacenamiento de información en un área física y la disminución de gastos en los procedimientos administrativos de archivo de documentos.

También, la firma electrónica digital garantiza la confidencialidad y su uso tiende a manejarse conjuntamente con los elementos firma electrónica y firma digital en su interés de identificar al firmante y comprobar su consentimiento. Cada uno de ellos tiene sus características de validez y riesgos en relación a la seguridad, privacidad de la información, cumplimiento de la ley, entre otros. En este sentido, la firma digital y electrónica constituye herramientas tecnológicas que reemplaza la firma manuscrita aplicando la autenticación de los datos en un formato electrónico.

En cuanto a la fundamentación legal de la incorporación de la firma electrónica digital se puede señalar que los diversos tipos de firmas están relacionadas con tecnología utilizada y el nivel de seguridad década una de ellas, porque cada firma digital refiere a un conjunto de métodos criptográficos que asignan una valoración alfanumérica inserta a un mensaje de datos. Por lo tanto, legalmente al utilizar la firma cualificada se concede un alto nivel de seguridad y veracidad, porque posee un sistema de seguridad que ofrece la validez legal significativa por su legitimidad, que puede ser mucho más confiable que la misma firma manuscrita, y se encuentra amparada en el reglamento europeo de firma (Reglamento eIDAS), siendo merecedora de la mayor garantía jurídica y de seguridad inequívoca.

Para obtenerla, es necesario la emisión de un certificado cualificado que identifica al firmante, verifica los datos y valida la firma a la identidad de la persona. Este certificado, es emitido por las autoridades de certificación cualificada, y puede ser utilizado como evidencia ante un tribunal, sin requerir una prueba pericial. Desde estos argumentos, la firma electrónica puede

ofrecer al firmante y el destinatario de los documentos la certeza de la identidad y la garantía de una firma intacta.

Vale la pena destacar, que en Europa ha habido cambios significativos en las innovaciones tecnológicas y en la dinámica empresarial y de servicios, lo que representó en la Unión Europea la necesidad de un marco comunitario regulador para la firma electrónica, permitiendo las garantías en su utilización favoreciendo su validez jurídica. En la dinámica de adaptación jurídica y de trasformación tecnológica, España promulgó la Ley 6/2020, de 11 de noviembre, donde le da carácter jurídico a las especificaciones de los servicios electrónicos de confianza, aplicable a los prestadores públicos y privados engranando las compatibilidades con el Reglamento de la UE.

En España se presentan algunas excepciones en las disposiciones legales necesarias en las formalidades especiales, como el otorgamiento o la inscripción de un acuerdo en una escritura notarial o su inscripción en registros públicos. Esto se debe a que exigen la firma física y la comparecencia de los involucrados. Sin embargo, la seguridad de la firma electrónica digital es conocida desde una perspectiva técnica aportada por la criptografía. El elemento cifrado produce en un mensaje reconocible solo por el que se le realiza un algoritmo de cifrado, generando un mensaje cifrado que sólo puede ser descifrado por aquellos usuarios que conozcan el algoritmo.

Para cerrar, se puede visualizar que existen diversos medios para avalar la seguridad de la firma electrónica digital y la información de su contenido. El empleo de las TIC sobre todo en tiempos de crisis sanitarias por Covid – 19 permitió que muchas organizaciones pudieran realizar operaciones y gestiones de forma dinámica, validad y segura, considerando la firma electrónica digital como un elemento de su ejecución. Indiscutiblemente, el contexto empresarial asumió esta firma certificando la seguridad de los datos, implementándose aplicaciones con protocolos de autentificación.

Referencias Bibliográficas

Bibliografía Básica

CÁRDENAS LESMES, R. Nueva Reglamentación de la Firma Electrónica, Portafolio. Bogotá: Grupo de Diarios América, 2013.

CORDOVA RAMIREZ J; VEGA HUERTA H; RODRIGUEZ RODRIGUEZ C; ESCOBEDO BAILÓN F. Firma Digital Basada en Criptografía Asimétrica para Generación de Historial Clínico. Tomo 9, número 4. España: Alcoy 3 Ciencias, 2020.

ESPINOZA CÉSPEDES, J. Entre la Firma Electrónica y la Firma digital. *Revista del Instituto de Ciencias Jurídicas de Puebla* [en línea] 2018**.** México: Editorial Nueva Época, Vol. 12, No. 41, pp 241 - 266 [consulta: 02 de junio de 2022] ISSN 1870-2147. Disponible en: https://revistaius.com/index.php/ius/article/view/315/601

FAJARDO LÓPEZ L. La firma electrónica en el derecho privado. *RJUAM Revista Jurídica de la universidad Autónoma de Madrid* [en línea] 2016. España: Vol. 1 No. 5, pp. 41 – 67. [consulta: 02 de julio de 2022] . Disponible en: https://revistas.uam.es/revistajuridica/article/view/6249

FERNÁNDEZ GARCÍA, I y GÓMEZ CALLEJA, I. Aplicaciones de la firma Electrónica en el Ámbito Empresarial. *Revista Estrategia Financiera* [en línea] 2005. Estados Unidos: Vol. 2, núm. 213, pp. 18 – 23. [consulta: 16 de junio de 2022] Disponible en: http://jggomez.eu/z%20Privado/b%20usuarios/n-revista/caja/1ef/2005/213.pdf

FERNANDEZ, E; GUTIERREZ, J; DELGADO, R y LOPEZ, R. Aplicación Web para la Gestión de Diplomas Digitales en Centros de Capacitación Mediante Firma Electrónica y Blockchain. *Revista Ibérica de Sistemas e Tecnologías de Información* [en línea] 2020. Portugal: Associação Ibérica de Sistemas e Tecnologias de Informacao Vol. 4, No. E28, pp 498-509 [consulta: 04 de junio de 2022] Disponible en: https://www.proquest.com/docview/2388305220

GARCÍA F. J., ARREDONDO GALVÁN X. y BARREIROS FERNÁNDEZ J., El Documento Electrónico un Reto a la Seguridad Jurídica, Madrid: Editorial Dykinson, 2015

LÓPEZ, M. Usan Firma Electrónica, Reforma México: Editora El Sol, S.A. de C.V.

MONGE DOBLES, I. El Nuevo Consentimiento Electrónico: la firma digitales en el ámbito de la Administración. *El Foro Colegio de Abogados*, [en línea] 2009. Costa Rica: Vol. 2 No. 2, pp 21 - 24. [Consulta: 09 de junio de 2022] ISSN 5 5-659-1496.

PEÑARANDA QUINTERO, H. La firma electrónica digital en Venezuela. *Revista Crítica de Ciencias Sociales y Jurídicas* [en línea] 2011. Venezuela: Red Nómadas, Vol 29, No 1, pp 29 – 35. [Consulta: 07 de junio de 2022] ISSN 1889-7231. Disponible en: https://www.redalyc.org/pdf/181/18118941022.pdf

RODRÍGUEZ AYUSO J, Ámbito Contractual de la firma electrónica, Barcelona: Bosch Editor, 2018.

ROS CORAZÓN M. Actos procesales y firma electrónica. *Revista de derecho UNED* [en línea] 2009. España: Vol. 1 No.5, pp. 287 – 317. [Consulta: 07 de junio de 2022]. Disponible en: http://e-spacio.uned.es/fez/eserv/bibliuned:RDUNED-2009-5-5090/Documento.pdf

SALVADOR AYESTARÁN I. La firma digital: Una tecnología para la intercomunicación en la sociedad. *Revista Española de Documentación Científica* [en línea] 2001. España: Vol. 24, No. 1, pp. 51-69. [Consulta: 22 de junio de 2022]. Disponible en: https://redc.revistas.csic.es/index.php/redc/article/view/33

SANCHEZ, A. La Administración Electrónica en España. *Revista do direito* [en línea] 2007. Santa Cruz do Sul: núm. 28, pp. 83-111. [Consulta: 22 de junio de 2022]**.** Disponible en: https://idus.us.es/bitstream/handle/11441/65753/La%20administracion%20electronica%20en%20Espa%c3%b1a.pdf?sequence=1&isAllowed=y

SARMIENTO GONZÁLEZ, R. y VILCHES VIVANCOS, F. Lenguaje jurídico-administrativo. Una lengua de especialidad. 2ª ed. Madrid: Dyckinson, 2016.

SUÁREZ LORENZO, F. *Construyendo la identidad digital, Situación Actual de la Firma Electrónica y de las Entidades de Certificación* [consulta: 04 de junio de 2022]. Santiago de Compostela: Colexio Profesional de Enxeñaría e Informática de Galicia, 2011. Disponible en: https://libros.metabiblioteca.org/bitstream/001/497/1/construyendo_la_identidad_digital.pdf

Bibliografía complementaria

MARTINEZ GUTIERRÉZ, R. Elementos para la Configuración de la Administración Digital. *Revista de Derecho* Administrativo [en línea] 2021. España: núm 20, pp. 212-233. ISSN 2074-0956. [Consulta: 09 de junio de 2022]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8510533

PAe, 2022. La firma Electrónica. *Portal de la Administración Electrónica* [Consulta: 10 de junio de 2022]. Disponible en: https://firmaelectronica.gob.es/Home/Ciudadanos/Firma-Electronica.html

SARMIENTO GONZÁLEZ, R. y VILCHES VIVANCOS, F. Lenguaje jurídico-administrativo. Una lengua de especialidad. 2ª ed. Madrid: Dyckinson, 2016.

SEDE, 8 de febrero de 2022. *Administración Electrónica.* Servicio de Modernización y Coordinación Administrativa [Consulta: 23 de julio de 2022] Disponible: https://smca.umh.es/administracion-electronica/

STATISTA, 2022. *Porcentaje de compañías que utilizó firma digital en alguna comunicación enviada desde su empresa en España entre 2009 y 2018, 2022*. [Consulta: 22 de junio de 2022]. Disponible en: https://es.statista.com/estadisticas/476509/empresas-con-firma-digital-espana/

UANATACA. Firma electrónica cualificada, simple o avanzada. Tipos de firmas y sus diferencias. 25 de febrero de 2020. Disponible en: https://web.uanataca.com/es/blog/firma-electronica/cualificada-simple-avanzada [Consulta: 14 de junio de 2022].

Legislación citada

Código Civil, de julio de 1889. Boletín Oficial del Estado, 24 de julio de 1889, núm. 206, p. 4763. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1889-4763

Constitución Española, de diciembre de 1978. Boletín Oficial del Estado, 29 de diciembre de 1978, núm. 311, p. 31229. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

Ley 1/2000, de enero, de Enjuiciamiento Civil. Boletín Oficial del Estado, 08 de enero de 2000, núm. 7, p. 323. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2000-323

Ley 59/2003, de 19 de diciembre, de Firma Electrónica. Boletín Oficial del Estado, 20 de diciembre de 2003, núm. 304, p. 23399 (Disposición Derogada). Disponible en: https://boe.es/buscar/act.php?id=BOE-A-2003-23399

Ley 6/2020, de 11 de noviembre, Reguladora de Determinados Aspectos de los Servicios Electrónicos de Confianza. Boletín Oficial del Estado, 11 de noviembre de 2020, núm. 298, p. 14046. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2020-14046

DIRECTIVA 1999/93/CE del Parlamento Europeo y el Consejo de la Unión Europea de diciembre de 1999, del Marco Comunitario para la Firma Electrónica. Núm. 13, p. 80059. (Disposición Derogada) Disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:ES:PDF

REGLAMENTO (UE) Nº 910/2014 del Parlamento Europeo y el Consejo de la Unión Europea de julio de 2014, relativo a la Identificación Electrónica y los Servicios de Confianza para las Transacciones Electrónicas en el Mercado Interior. Diario Oficial de la Unión Europea de 28 de agosto de 2014, núm, I. 257/73. Disponible: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32014R0910&from=ES

Listado de Abreviaturas

Certificado electrónico o el DNI electrónico: es un documento que contiene unas contraseñas criptográficas que son los aspectos requeridos para firmar.

Firma digital: tiene carácter legal de no repudio. Se fija en un mensaje de datos y el emisor acredita ese mensaje en correspondencia con el contenido del mismo. Implica que no ha sido modificado desde su producción, envío, aceptación y almacenamiento. De la firma

digital se desprende la firma electrónica avanzada y de cualificada, pero no de la firma electrónica simple.

Firma electrónica avanzada: Ofrece excelente seguridad, porque permite la identificación del emisor y ha sido creada usando datos de creación de la firma electrónica que el emisor.

Firma electrónica cualificada: Se *crea mediante un dispositivo cualificado de creación de firmas electrónicas y se emite por medio de un certificado cualificado.* Es la firma más robusta en términos de seguridad, posee el mismo valor jurídico de una firma manuscrita. La misma posee los requerimientos de seguridad estipulados en el artículo 26 del Reglamento elDAS tales como: 1. Se encuentra vinculada al emisor únicamente, 2. Identifica al emisor, 3. Se crea utilizando datos para generar firmas electrónicas y 4. Es detectable cualquier intento de cambio. Por lo tanto, la garantía de seguridad referente a la firma del emisor se encuentra en la creación de la misma, por sus dispositivos electrónicos cualificados para tal fin, de allí, que su validez tiene las mismas implicaciones que una firma manuscrita, por ello, es reconocido en todos los países miembros.

Firma electrónica: conjunto de datos electrónicos asociados a un documento electrónico. Presentan diferentes niveles de seguridad y puede ser empleado como un elemento probatorio ante una situación legal. Puede tener elementos adicionales para garantizar su autenticidad.

Persona física: El Certificado digital FNMT de Persona Física es la certificación electrónica despachada por la FNMT-RCM que relaciona a su emisor con unos Datos de verificación de Firma y confirma su identidad. Este certificado de Ciudadano o de Usuario, es un documento digital que posee datos identificativos, logrando identificarse en Internet e intercambiar información con otros usuarios y organismos con la garantía de solo el emisor puede acceder.

Valor alfanumérico: Esta valoración se encuentra incluida un mensaje de datos. Se produce por medio de la tecnología fundamentada en criptografía. Un algoritmo matemático puede determinar un valor generado de manera específica por el usuario vinculado con el contenido del documento.

Firma electrónica básica: constituye la información registrada en un formato electrónico adicionados a otros, utilizados por el emisor para firmar.