

UNIVERSIDAD DE EL SALVADOR
FACULTAD MULTIDISCIPLINARIA ORIENTAL
DEPARTAMENTO DE JURISPRUDENCIA Y CIENCIAS SOCIALES
SECCIÓN DE CIENCIAS JURÍDICAS



INFORME FINAL DEL CURSO DE ESPECIALIZACIÓN:
EN DERECHO CIVIL

TÍTULO DEL INFORME FINAL:
RÉGIMEN JURÍDICO DE LA FIRMA ELECTRÓNICA Y SU APLICABILIDAD EN LAS
RELACIONES CONTRACTUALES EN EL SALVADOR

PARA OPTAR AL GRADO ACADÉMICO DE:
LICENCIATURA EN CIENCIAS JURÍDICAS

PRESENTADO POR:
GERARDO ANTONIO HERNÁNDEZ TURCIOS. N°CARNET: HT20001

DOCENTE ASESOR:
LICENCIADO JUAN ANTONIO BURUCA GARCÍA

OCTUBRE DE 2025
SAN MIGUEL, EL SALVADOR, CENTROAMÉRICA

UNIVERSIDAD DE EL SALVADOR
AUTORIDADES



M.SC. JUAN ROSA QUINTANILLA
RECTOR

DRA. EVELYN BEATRIZ FARFÁN
VICERRECTORA ACADÉMICA

M.SC. ROGER ARMANDO ARIAS ALVARADO
VICERRECTOR ADMINISTRATIVO

LIC. PEDRO ROSALÍO ESCOBAR CASTANEDA
SECRETARIO GENERAL

LIC. CARLOS AMÍLCAR SERRANO RIVERA
FISCAL GENERAL

UNIVERSIDAD DE EL SALVADOR
FACULTAD MULTIDISCIPLINARIA ORIENTAL
AUTORIDADES



M.SC. CARLOS IVÁN HERNÁNDEZ FRANCO
DECANO

DRA. NORMA AZUCENA FLORES RETANA
VICEDECANA

LIC. CARLOS DE JESÚS SÁNCHEZ
SECRETARIO

LIC. CARLOS ARMANDO SARAVIA SEGOVIA

JEFE DEL DEPARTAMENTO DE JURISPRUDENCIA Y CIENCIAS SOCIALES

LIC. JUAN ANTONIO BURUCA GARCÍA
COORDINADOR DEL PROCESO DE GRADO DEL DEPARTAMENTO DE
JURISPRUDENCIA Y CIENCIAS SOCIALES

AGRADECIMIENTOS

A Dios: Por ser mi guía constante en mi camino, por darme fortaleza en mis momentos de incertidumbre y por iluminar cada paso de mi desarrollo personal y profesional.

A mi madre: Claudia Inés Hernández Turcios, por su apoyo y amor incondicional hacia mí, por enseñarme con su ejemplo el valor del esfuerzo y la perseverancia; por siempre estar en cuerpo y alma en cada etapa de mi vida.

A mi abuela: Rosario del Carmen Turcios de Hernández, por su ternura, apoyo y oraciones silenciosas que me han acompañado desde el inicio, por su amor y calidez en los buenos y malos momentos.

A la memoria de mi abuelo: Mercedes Antonio Hernández, cuyo legado de integridad, trabajo honesto y valores sigue inspirándome y dirigiendo mis pasos en mi camino; a su amor y cariño que desde el cielo deseo enorgullecer día a día con mis acciones.

A mis tíos y tías: por su apoyo constante, por creer en mí y brindarme siempre el espacio de afecto y confianza; por brindarme palabras de ánimo cuando más las he necesitado.

A mi novia: Daniela Victoria Escobar Cruz, por su amor, paciencia, compañía en mi desarrollo profesional y personal, por ser constante en sus palabras de aliento y motivación, por motivarme a ser una mejor persona cada día, por ser la persona con quien quiero compartir mis días, mi esfuerzo y mi vida entera.

A todos y cada uno de ustedes, quienes han sido parte en este camino, por ser un engranaje e impulso para mi progreso, por ser parte de mi vida. Este trabajo final no solo representa el esfuerzo académico, sino también es el reflejo del acompañamiento que he recibido de cada uno ¡Muchas gracias!

- Gerardo Antonio Hernández Turcios

ÍNDICE

RESUMEN.....	1
ABSTRACT.....	2
INTRODUCCIÓN.....	3
PLANTEAMIENTO DEL PROBLEMA.....	5
JUSTIFICACIÓN.....	6
OBJETIVOS.....	7
a) General.....	7
b) Específicos.....	7
1. CONTEXTO HISTÓRICO DE LA FIRMA.....	8
1.1. Origen etimológico de la firma autógrafa.....	8
1.2. La firma en la Prehistoria.....	8
1.3. La firma en la Antigua Roma.....	9
1.4. Edad Media: Signos, sellos y rúbricas.....	10
1.5. Renacimiento y consolidación de la firma autógrafa.....	11
1.6. Limitaciones y desafíos contemporáneos.....	12
1.7. Transición hacia la firma digital o electrónica en El Salvador.....	13
2. GENERALIDADES DE LOS CONTRATOS.....	14
2.1. Requisitos generales de los contratos.....	14
2.2. Clasificación de los contratos.....	15
2.3. Documentos públicos y documentos privados.....	19
3. GENERALIDADES DE LA FIRMA ELECTRÓNICA.....	21
3.1. Sujetos intervinientes.....	21
a) Unidad de Firma Electrónica.....	22
b) Proveedores de servicios de certificación.....	22
c) Firmantes o signatarios.....	23
3.2. Conceptos fundamentales y puntualizaciones prácticas sobre la Ley de Firma Electrónica (LFE).....	23
a) Certificado electrónico.....	24
b) Formas de generación de un certificado electrónico.....	24
c) Tipos de certificados electrónicos.....	25
d) Contenido del certificado electrónico.....	27
e) Documento electrónico.....	27
f) Dispositivo seguro de creación.....	29
g) Firma electrónica simple.....	30
h) Firma electrónica certificada.....	31
i) Concepto provisional de firma electrónica certificada.....	32
j) Sello electrónico y sello de tiempo.....	33
k) Clasificación de los sellos electrónicos.....	34
4. PARTICULARIDADES DE LA FIRMA ELECTRÓNICA CERTIFICADA.....	35

4.1. Contenido de la firma electrónica certificada.....	35
4.2. Funcionamiento de la firma electrónica certificada.....	36
4.3. Forma de validación de la firma electrónica certificada.....	37
5. RÉGIMEN JURÍDICO DE LA FIRMA ELECTRÓNICA.....	38
5.1. Principios rectores de la LFE.....	38
a) Autenticidad.....	39
b) Integridad.....	39
c) Confidencialidad.....	40
d) Equivalencia funcional.....	40
e) No repudio.....	41
f) Neutralidad tecnológica.....	41
g) Seguridad.....	42
h) Inalterabilidad del Derecho preexistente.....	42
5.2. Requisitos de validez para la firma electrónica certificada.....	42
5.3. Valor probatorio de la firma electrónica simple y certificada.....	45
5.4. Causales de revocatoria de un certificado electrónico.....	49
6. USO DE LA FIRMA ELECTRÓNICA POR ENTIDADES DE ESTADO.....	52
6.1. Tipos de uso institucional.....	54
7. APLICABILIDAD DE LA FIRMA ELECTRÓNICA POR EL CNR.....	55
7.1. Servicios del Centro Nacional de Registros.....	55
8. APLICABILIDAD DE LA FIRMA ELECTRÓNICA EN LAS RELACIONES CONTRACTUALES.....	57
8.1. Respecto a los contratos constituidos mediante documentos privados.....	57
8.2. Respecto a los contratos constituidos mediante Instrumento Público.....	63
8.3. De los contratos digitales.....	64
9. LA FIRMA ELECTRÓNICA EN MATERIA NOTARIAL.....	67
CONCLUSIONES.....	74
RECOMENDACIONES.....	77
BIBLIOGRAFÍA.....	78
ANEXOS.....	82
GLOSARIO.....	90

RESUMEN

Este trabajo analiza el régimen jurídico de la firma electrónica en El Salvador y su aplicabilidad en las relaciones contractuales, partiendo de una reconstrucción histórica de la firma como expresión de voluntad jurídica, desde sus formas primitivas hasta su consolidación como firma autógrafa.

Se examina la Ley de Firma Electrónica, sus principios rectores, requisitos de validez, efectos probatorios y compatibilidad con el ordenamiento jurídico salvadoreño. Se detallan los elementos técnicos que configuran la firma electrónica certificada, como el certificado electrónico, el dispositivo seguro de creación y los sujetos intervinientes en el proceso de certificación, incluyendo la Unidad de Firma Electrónica y los Proveedores de Servicios de Certificación acreditados. Se distingue entre firma electrónica simple y certificada.

Asimismo, se aborda la aplicabilidad de la firma electrónica en contratos celebrados mediante documentos privados, así como su uso por entidades estatales como el Centro Nacional de Registro, en trámites administrativos y notariales, conforme a las reformas a la Ley del Notariado.

Se concluye la importancia de la firma electrónica certificada como una herramienta idónea para la contratación en entornos digitales, siempre que se garantice su autenticidad, integridad y verificabilidad. Su implementación no modifica el Derecho preexistente, sino que lo complementa, otorgando plena validez y equivalencia funcional respecto a la firma autógrafa.

Palabras clave: Firma electrónica; contratos; documentos privados; valor probatorio.

ABSTRACT

This paper analyzes the legal framework for electronic signatures in El Salvador and their applicability in contractual relationships, beginning with a historical reconstruction of the signature as an expression of legal intent, from its primitive forms to its consolidation as a handwritten signature.

It examines the Electronic Signature Law, its guiding principles, validity requirements, evidentiary effects, and compatibility with the Salvadoran legal system. The technical components of certified electronic signatures are detailed, including the electronic certificate, the secure creation device, and the actors involved in the certification process, such as the Electronic Signature Unit and duly accredited Certification Service Providers. A distinction is made between simple and certified electronic signatures.

The study also addresses the applicability of electronic signatures in contracts executed through private documents, as well as their use by State Entities such as the National Registry Center, in administrative and notarial procedures, in light of reforms to the Notarial Law.

It concludes that the certified electronic signature is an ideal tool for contracting in digital environments, provided its authenticity, integrity, and verifiability are ensured. Its implementation does not alter preexisting law but complements it, granting full validity and functional equivalence to the handwritten signature in contractual relationships.

Keywords: Electronic signature; contracts; private documents; evidentiary value.

INTRODUCCIÓN

La firma, como expresión gráfica de la voluntad jurídica, ha acompañado al ser humano desde sus primeras manifestaciones de identidad, evolucionando desde signos rudimentarios en tablillas de arcilla hasta convertirse en trazos autógrafos que consolidan actos jurídicos con fuerza vinculante. Esta evolución histórica, que se remonta a la *manufiratio* romana y se consolida en el Renacimiento con la firma autógrafa como símbolo de individualidad y consentimiento, ha sido objeto de profundas transformaciones en el contexto contemporáneo, donde la digitalización de los procesos jurídicos exige nuevas formas de validación documental que garanticen autenticidad, integridad y seguridad jurídica.

En este escenario, la firma electrónica certificada se rige como una herramienta tecnológica-jurídica que permite replicar las funciones de la firma autógrafa en entornos digitales, dotando de eficacia probatoria y valor jurídico a los documentos electrónicos suscritos por medio de la firma electrónica. Su regulación en El Salvador, mediante la Ley de Firma Electrónica (Decreto Legislativo N.º 133 de 2015), establece un marco normativo que reconoce la equivalencia funcional entre la firma electrónica certificada y la firma autógrafa, siempre que se cumplan los requisitos técnicos y legales exigidos por la ley. No obstante, su aplicabilidad en las relaciones contractuales plantea interrogantes sustanciales sobre su compatibilidad con los elementos esenciales del contrato, su valor probatorio en juicio, y su capacidad para sustituir la función fedataria en documentos privados.

El presente trabajo tiene como propósito analizar el régimen jurídico de la firma electrónica en El Salvador, con especial énfasis en su aplicabilidad en las relaciones contractuales, tanto civiles como mercantiles. Para ello, se abordará el contexto histórico de la firma como manifestación de voluntad, se examinarán los principios rectores de la Ley de Firma Electrónica, y se estudiarán los requisitos de validez, funcionamiento técnico y efectos jurídicos

de la firma electrónica certificada. Asimismo, se evaluará su uso por parte de entidades del Estado, como el Centro Nacional de Registro (CNR), y su implementación en trámites administrativos y notariales, en atención a las reformas recientes a la Ley del Notariado (LN).

El presente trabajo se justifica en la necesidad de fortalecer la seguridad jurídica de los actos celebrados por medios electrónicos, especialmente en un contexto de creciente digitalización de los servicios públicos y privados, donde la firma electrónica certificada se convierte en un instrumento de garantía, trazabilidad y eficiencia jurídica. Además, se busca contribuir al desarrollo doctrinal del derecho digital salvadoreño, proponiendo líneas de interpretación que armonicen la tecnología con los principios fundamentales del derecho civil y mercantil, sin alterar el contenido sustancial del ordenamiento jurídico preexistente.

En suma, esta investigación pretende ofrecer una visión integral del régimen jurídico de la firma electrónica en El Salvador, articulando sus fundamentos técnicos con sus efectos jurídicos, y proponiendo criterios de aplicabilidad que permitan consolidar su uso en las relaciones contractuales, en armonía con los principios de legalidad, autonomía de la voluntad, equivalencia funcional y seguridad jurídica.

PLANTEAMIENTO DEL PROBLEMA

La firma, como manifestación de autoría y voluntad jurídica, ha experimentado transformaciones significativas a lo largo de la historia, desde su consolidación como trazo autógrafo hasta su actual versión digital. En El Salvador, la incorporación de la firma electrónica certificada mediante la Ley de Firma Electrónica ha planteado retos y oportunidades en el ámbito jurídico, particularmente en las relaciones contractuales en el ámbito civil, mercantil y notarial.

Sin embargo, persisten interrogantes sobre su compatibilidad con los principios fundamentales del derecho civil, su eficacia probatoria frente a la firma autógrafa y su aceptación plena en la práctica notarial. La ausencia de una cultura digital consolidada y las limitaciones en infraestructura tecnológica generan un escenario en el que resulta necesario un análisis doctrinal y práctico que aporte claridad sobre la aplicabilidad de la firma electrónica en el marco jurídico salvadoreño.

JUSTIFICACIÓN

Este trabajo se fundamenta en la necesidad de fortalecer la seguridad jurídica de los actos celebrados por medios electrónicos en un contexto de creciente digitalización. La firma electrónica certificada se presenta como un mecanismo de garantía de autenticidad e integridad documental, pero su implementación requiere un estudio crítico que evidencie sus alcances y limitaciones. Analizar su régimen jurídico permite aportar a la construcción doctrinal del derecho digital en El Salvador, armonizando los avances tecnológicos con los principios del derecho civil, mercantil y notarial. Asimismo, se busca ofrecer a la comunidad académica y profesional una herramienta de referencia que oriente la aplicabilidad práctica de la firma electrónica en los diferentes contratos que le son aplicables, contribuyendo al desarrollo de un marco jurídico coherente y funcional.

OBJETIVOS

a) General

1. Analizar el régimen jurídico de la firma electrónica en El Salvador, identificando su fundamentación legal, alcance normativo y principios rectores en relación a su aplicación en las relaciones contractuales.

b) Específicos

1. Determinar la compatibilidad entre la firma electrónica y los elementos fundamentales de los contratos en el derecho civil salvadoreño.

2. Evaluar el valor probatorio de la firma electrónica respecto a los documentos electrónicos consignados por ésta y su equivalencia con la firma autógrafa.

1. CONTEXTO HISTÓRICO DE LA FIRMA

Para analizar el impacto de la firma electrónica en las relaciones contractuales es necesario realizar previamente una breve reseña histórica sobre el origen, evolución y necesidad de la firma electrónica, ahondando respecto a su forma manuscrita: la firma autógrafa o firma a mano.

1.1. Origen etimológico de la firma autógrafa

El término “*firma*” proviene del latín *firmare*, que significa “*afirmar*” o “*dar fuerza*”. Esta raíz etimológica ya nos da una idea de su función: confirmar o validar el contenido de un documento. La Real Academia Española la define como el “*nombre y apellido, o título, que una persona escribe de su propia mano en un documento, para darle autenticidad o para expresar que aprueba su contenido*”.

Desde el punto de vista jurídico, autores como Eduardo Couture la describen como el “*trazado gráfico, conteniendo habitualmente el nombre, los apellidos y la rúbrica, con el cual se suscriben los documentos para darles autoría y virtualidad, y obligarse en lo que en ellos se dice*”.

1.2. La firma en la Prehistoria

Antes de la existencia de la escritura, los seres humanos ya buscaban formas de dejar constancia de su identidad, tal es el caso como el de las huellas dactilares en cavernas, los símbolos personales y los sellos en tablillas de arcilla los cuales fueron los primeros intentos de autenticar la autoría de un mensaje o acto.¹

¹ Los símbolos utilizados por los habitantes de las cavernas, o “*cavernícolas*”, principalmente se encuentran en las pinturas rupestres. Estas representaciones artísticas, encontradas en cuevas de todo el mundo, muestran principalmente animales, figuras humanas, líneas, y símbolos abstractos como espirales o puntos. Los investigadores creen que estos símbolos no eran solo expresiones artísticas, sino que también tenían significados simbólicos y prácticos, posiblemente relacionados con la caza, rituales, o la representación de eventos importantes.

En civilizaciones como la egipcia y la mesopotámica, se utilizaban sellos cilíndricos con inscripciones únicas que representaban a su portador, pudiendo individualizar y dar cierta certeza sobre su autoría. Estos sellos eran presionados sobre arcilla húmeda para dejar una marca distintiva, funcionando como una firma primitiva.

1.3. La firma en la Antigua Roma

En los primeros siglos de la Antigua Roma, la noción de firma como trazo gráfico personal aún no se había consolidado. En su lugar, existía una práctica ceremonial conocida como *manufirmitio*², que cumplía la función de autenticar documentos y expresar la voluntad del autor. Esta ceremonia consistía en que el autor del documento, o en su defecto un funcionario autorizado, leía en voz alta el contenido del manuscrito ante testigos. Luego, el pergamino era extendido sobre la mesa del escribano, y el autor pasaba su mano abierta sobre el documento como gesto simbólico de aceptación, compromiso o juramento, aunque sin pronunciar fórmula alguna de juramento formal.

Este acto no era meramente funcional, sino que formaba parte de un ritual solemne que confería autenticidad al documento. Tras el gesto de la mano, el autor estampaba su nombre, un signo personal o incluso una o varias cruces, dependiendo del grado de alfabetización y del protocolo seguido. Los testigos presentes repetían el gesto, reforzando así la validez del acto. Más que una simple formalidad, la *manufirmitio* era una expresión pública de consentimiento y una forma de solemnizar el acto jurídico, dotándolo de fuerza probatoria y legitimidad social.

Con el paso del tiempo, y a medida que la escritura se fue generalizando entre ciertos sectores de la población romana, esta práctica evolucionó hacia formas más gráficas de identificación. Se comenzó a utilizar la inscripción manuscrita del nombre del autor como señal

² Etimológicamente, *manufirmitio* proviene del latín y está compuesta por dos elementos: "*manus*", que significa mano; y "*firmitio*", derivado de *firmare*, que significa afirmar, asegurar o dar validez. Por tanto, *manufirmitio* puede traducirse literalmente como "afirmación con la mano" o "confirmación mediante la mano".

de autoría, lo que sentó las bases para el desarrollo posterior de la firma autógrafa. Esta transición se consolidó más adelante en la Edad Media, cuando los signos personales, las cruces y los sellos comenzaron a adquirir un valor identificativo más definido, especialmente entre quienes no sabían leer ni escribir.

Así, la *manufirmatio* representa un eslabón clave en la evolución histórica de la firma al ser una de las primeras manifestaciones institucionalizadas de aceptación documental en el Derecho Romano. Su carácter ceremonial y su función probatoria anticipan muchas de las funciones que más tarde asumiría la firma autógrafa en los sistemas jurídicos modernos y, primordialmente, sienta las bases sobre el rol de la firma en materia de contratos.

1.4. Edad Media: Signos, sellos y rúbricas

Durante la Edad Media, una gran parte de la población no podía leer ni escribir, por lo que se recurría a signos gráficos, cruces o marcas personales para autenticar documentos, es decir, no se alejaba mucho respecto con las anteriores épocas. Los escribanos³ y notarios de aquella época utilizaban signos compuestos por letras entrelazadas, mientras que la nobleza empleaba sellos de cera con escudos heráldicos⁴.

Un punto clave fue la diferenciación entre firmas y signos, hizo que se empezase a entender que aquellas eran más que simples “signos”, la inscripción manuscrita del nombre o de los apellidos. Como se acaba de mencionar, en ese tiempo pocas eran las personas que sabían leer y escribir, por lo que generalmente los particulares estampaban en los documentos que suscribían diversos signos o sellos, la extensión de la instrucción y el desenvolvimiento de

³ El escribano era el encargado de redactar los documentos legales por encargo de las partes, aunque su intervención no siempre confería autenticidad legal, por lo general podían dar fe de la autenticidad del documento.

⁴ Los escudos heráldicos son representaciones simbólicas que surgieron en la Edad Media para identificar a personas, familias, linajes, ciudades o instituciones, especialmente en contextos militares y nobiliarios. Funcionaban como una especie de “firma visual” que permitía distinguir a los caballeros en el campo de batalla, ya que cada escudo era único y cargado de significado.

las transacciones comerciales, hicieron que la firma fuera adquiriendo la importancia y uso que con el transcurso del tiempo se fue consagrando como un símbolo de identificación y de enlace entre el autor de lo escrito o estampado y su persona.

Por lo tanto, se fue consolidando la costumbre de firmar con el nombre propio, acompañado de una rúbrica. Esta rúbrica, que proviene del latín *rubrum* (rojo), consistía en trazos decorativos debajo o al lado de la firma o signo al que originalmente le acompañaban frases latinas escritas en tinta roja, como *scripsit*, *firmavit*, *recognovit* (“Escribió”, “firmó”, “reconoció”), que daban fe de autenticidad.

Haciendo un pequeño paréntesis en este punto, es de recalcar la gran importancia de los fedatarios a lo largo de la historia, denotando la necesidad de validar de forma certera, aunque presunta por su forma de validación no tan segura para las formas disponibles de la época, las manifestaciones de voluntad de las personas, principalmente cuando se consolidaban acuerdos o contratos.

1.5. Renacimiento y consolidación de la firma autógrafa

Durante el Renacimiento⁵ (época de profundas transformaciones culturales, filosóficas y jurídicas) la firma autógrafa dejó de ser un privilegio reservado a unos pocos para convertirse en un instrumento clave de la vida jurídica y social. Este cambio estuvo estrechamente vinculado al auge del humanismo, que colocó al individuo en el centro del pensamiento, reconociéndose como sujeto autónomo, racional y responsable de sus actos; es decir, la conversión a un pensamiento antropocéntrico.

⁵ El Renacimiento fue un movimiento cultural, artístico y científico que surgió en Europa entre los siglos XV y XVI, marcando la transición entre la Edad Media y la Edad Moderna. Su nombre proviene del concepto de “*renacer*” o “*volver a nacer*”, en referencia al redescubrimiento de los valores, conocimientos y formas estéticas de la Antigüedad clásica grecorromana.

Con el incremento de la alfabetización, especialmente entre las clases burguesas y profesionales, la firma autógrafa pasó a ser una expresión de identidad personal y de voluntad jurídica. Ya no bastaba con sellos o signos gráficos heredados, para ese entonces ya se requería que el firmante dejara constancia de su consentimiento de forma directa, mediante su propia escritura. Esto otorgaba a la firma un doble valor, siendo un valor declarativo al expresar la voluntad de obligarse; y un valor probatorio para servir como medio de prueba ante cualquier controversia ulterior.

En este contexto, comenzaron a consolidarse prácticas notariales más rigurosas. Los escribanos y notarios exigían la firma autógrafa en documentos como contratos, testamentos, poderes, escrituras públicas y cartas de obligación, lo que fortalecía la seguridad jurídica y la valoración de los actos.

Además, la firma empezó a adquirir un carácter individualizador, al punto que su forma, estilo y rúbrica se convirtieron en elementos distintivos del firmante, es decir, cada individuo tenía una firma asociada a su persona. En algunos casos, incluso se consideraba que la firma reflejaba aspectos del carácter o la posición social del sujeto, anticipando lo que más tarde sería objeto de estudio por la grafología.

Este proceso de consolidación también sentó las bases para el desarrollo posterior de la firma como requisito legal, que hoy en día sigue siendo esencial en la mayoría de los sistemas jurídicos contemporáneos.

1.6. Limitaciones y desafíos contemporáneos

A pesar de su importancia, la firma autógrafa presenta ciertas limitaciones en el contexto actual, las cuales son las siguientes:

- **Falsificación:** Puede ser imitada con relativa facilidad.

- **Dificultad de verificación a distancia:** Requiere presencia física o envío del documento original.
- **Pérdida de trazabilidad:** No siempre es posible determinar cuándo y dónde fue firmada.

Estas limitaciones han impulsado la búsqueda de mecanismos alternativos que ofrezcan mayor seguridad y adaptabilidad al entorno digital; tal es el caso de la firma electrónica certificada, el cual si bien brinda una mayor seguridad y certeza jurídica en cuanto al factor de autenticidad y trazabilidad mediante el uso de los medios electrónicos existentes. No obstante, sigue siendo una herramienta novedosa que es necesaria de afianzar respecto al conocimiento general de la población en cuanto a la utilización de esta herramienta, como en la protección que gira en torno de la misma. En otras palabras, aún es necesario avanzar en la ciberseguridad para prevenir y protegerse de futuras formas de falsificación.

1.7. Transición hacia la firma digital o electrónica en El Salvador

La necesidad de afrontar los desafíos contemporáneos antes mencionados, especialmente en el ámbito comercial y administrativo, ha llevado al desarrollo de la firma electrónica. Esta busca replicar las funciones de la firma autógrafa en entornos digitales, garantizando autenticidad e integridad.

Sin embargo, la firma electrónica no elimina la relevancia de la firma autógrafa. Ambas coexisten y se complementan, cada una con sus propias características, ventajas y ámbitos de aplicación.

En El Salvador, la firma autógrafa sigue siendo plenamente válida y reconocida por el ordenamiento jurídico. No obstante, con la entrada en vigor de la **Ley de Firma Electrónica (Decreto Legislativo N.º 133 de 2015) y sus posteriores reformas**, se ha establecido un

marco normativo que permite equiparar la firma electrónica certificada con la firma autógrafa, siempre que se cumplan ciertos requisitos técnicos y legales que se desarrollarán más adelante en su respectivo apartado dentro de este trabajo.

Así que, como preámbulo, es importante remarcar que esta ley reconoce la equivalencia funcional entre ambas formas de firma, siempre que se garantice la identidad del firmante, la integridad del documento y la posibilidad de verificación; siendo una alternativa novedosa y segura respecto a la firma autógrafa.

2. GENERALIDADES DE LOS CONTRATOS

Para establecer el impacto de la firma electrónica en las relaciones contractuales, es preciso definir qué es un contrato y sus características; por lo tanto un contrato es, a *grosso modo*, una fuente de obligaciones que implica un acuerdo de voluntades entre dos o más personas, mediante el cual se obligan a dar, hacer o no hacer alguna cosa. También se considera contrato a aquellas manifestaciones de voluntad unilaterales en las que solo una de las partes se obliga sin que la otra contraiga obligación alguna, como ejemplo típico de este tipo de contratos están los testamentos.

2.1. Requisitos generales de los contratos

El Código Civil (C.C.) hace una distinción y denominación de los diferentes tipos de contratos atendiendo a sus elementos esenciales, no obstante también establecen parámetros generales que todo contrato debe cumplir para su validez, siendo esas las características generales las cuales son, en base al artículo 1316 del mismo cuerpo legal, las siguientes.

- **Capacidad legal:** La persona debe tener aptitud jurídica para obligarse, es decir, debe ser mayor de dieciocho años y no acarrear ninguna de las incapacidades mencionadas en el

artículo 1317 C.C. (por ejemplo, por interdicción judicial, estado de demencia o minoría de edad). Esto garantiza que quien se obliga comprenda las consecuencias legales de su acto.

- **Consentimiento libre de vicios:** Debe haber consentimiento real y voluntario, es decir, que la persona haya aceptado sin coacción o fuerza, error o dolo (artículo 1322 C.C.). Si hay alguno de estos vicios del consentimiento como coacción o engaño para que al menos una de las partes firme o consienta el acto, puede ser declarado nulo.

El consentimiento es un punto muy importante ya que éste se manifiesta mediante la firma del contratante en el documento público o privado en el que se consigna, contrayendo de esta manera los derechos y obligaciones que en el contenido del documento se establecen.

- **Objeto lícito:** La obligación debe recaer sobre algo permitido por la ley. No se puede contratar, por ejemplo, para vender órganos humanos o realizar actos contrarios a la moral, la ley o el orden público.

- **Causa lícita:** La causa es el motivo que lleva a una parte a obligarse (por ejemplo, recibir un pago, obtener un servicio, etc.). Esa motivación debe ser legal y no puede basarse en fines prohibidos (como el pago para la ejecución de un ilícito).

- **Solemnidades:** Según el tipo de contrato, existen disposiciones legales que regulan también la forma en la que se perfecciona y en virtud del cual tendrá validez legal, tal es el caso como en los contratos de compraventa de inmuebles, debiendo realizarse ante notario y constituirse en escritura pública, también denominado como instrumento público.

2.2. Clasificación de los contratos

En cuanto a los contratos, el Código Civil del artículo 1310 al 1315 realiza una clasificación de cada uno atendiendo a diferentes criterios respecto a sus características, dentro de los cuales cabe hacer mención de las más importantes en atención los efectos

jurídicos que se producen por las relaciones contractuales entre las partes dentro de la misma ya que, como se señaló anteriormente, estas relaciones jurídicas generan derechos y obligaciones entre las partes que pueden variar en base a las características del propio contrato.

Primeramente, atendiendo a las partes que adquieren obligaciones, los contratos pueden ser unilaterales o bilaterales; son unilaterales cuando sólo una de las partes contrae la obligación de dar, hacer o no hacer a beneficio de otra persona que no contrae obligación alguna como, por ejemplo, en el caso de los testamentos que es el causante o testador quien se obliga a repartir su patrimonio para con sus herederos o legatarios. Por otro lado, serán bilaterales aquellos contratos en donde las partes se obligan recíprocamente, contrayendo más de una de las partes las obligaciones y derechos que nacen en virtud del contrato.

Un segundo criterio se basa en el beneficio generado por el contrato, clasificándose como contratos gratuitos u onerosos. Serán gratuitos aquellos que es una de las partes la que acarrea una pérdida o gravamen en favor de otra que, *contrario sensu*, se beneficia; mientras que será oneroso aquel contrato en donde ambas partes generan un beneficio y adquieren pérdidas o gravamen en favor del otro. Para entenderlo de otra forma, se puede poner el ejemplo de una persona que dona su vehículo a otra sin recibir nada a cambio; en este caso, el contrato es gratuito ya que únicamente una de las partes, el donante, sufre una pérdida patrimonial (la entrega del vehículo), mientras que la otra parte obtiene un beneficio directo (el dominio o propiedad del vehículo) sin asumir ninguna obligación ni gravamen en favor del donante. Por otro lado, de una compraventa de ese mismo vehículo, el comprador entrega una suma de dinero y el vendedor transfiere la propiedad del automóvil, siendo en este caso un contrato oneroso, porque ambas partes reciben un beneficio y al mismo tiempo asumen una carga: el vendedor gana dinero pero pierde el vehículo, y el comprador obtiene el vehículo pero paga por él.

El tercer criterio se tiene en base a la existencia del contrato, por lo que este puede ser principal o accesorio. Será principal cuando tiene una existencia independiente de otra convención, acto o contrato, teniendo validez por sí mismo. Mientras que será accesorio aquel contrato cuya existencia dependa de otro, es decir, que dicho contrato se cree para garantizar o asegurar el cumplimiento de una obligación que nace de otro contrato, haciendo su subsistencia dependiente del otro; para este caso se encuentra, por ejemplo, el contrato de hipoteca o cualquier otro contrato denominados como “garantía”.

Como cuarto criterio, se basa en la forma en que se “perfecciona” un contrato, pudiendo ser real, consensual o solemne. Será un contrato considerado real (no en relación a su existencia) cuando se da la “tradición” del bien o cosa, es decir, cuando existe una entrega material del bien o cosa y a partir de ese momento el contrato se considera perfecto y, por consiguiente, válido. Será considerado consensual cuando se perfecciona por el mero consentimiento de las partes sin que sea necesaria alguna solemnidad especial o una entrega material, tal como lo son aquellos contratos de prestación de servicios. Un contrato será solemne cuando la ley exige una forma específica y preestablecida para que el contrato adquiera validez jurídica, sin la cual el acuerdo de voluntades no produce efectos vinculantes. En otras palabras, aunque exista consentimiento entre las partes, el contrato no se considera perfeccionado si no se cumple con la forma exigida por el ordenamiento jurídico, pudiendo esta formalidad consistir en la redacción del contrato mediante escritura pública ante notario, el uso de documento protocolizado, o incluso el otorgamiento del acto en presencia de una autoridad determinada, como ocurre en los casos de testamentos, matrimonios, o compraventas de bienes inmuebles.

Como último criterio, se hace una clasificación respecto a los elementos de los contratos, pudiendo ser esenciales, naturales o accidentales.

Son de la esencia de un contrato aquellos requisitos o elementos indispensables para que el contrato exista válidamente como tal, sin los cuales se produciría una alteración sustancial que lo convertiría en otro tipo de contrato o, sencillamente, lo dejaría sin efectos jurídicos; es decir, la esencia constituye el núcleo vital del acto jurídico. Por ejemplo, en un contrato de compraventa, es de su esencia la existencia del precio (valor económico que se paga a cambio de un bien o servicio), si no hay precio determinado o determinable, entonces no es una compraventa sino otro tipo de contrato, como una donación.

Son de la naturaleza del contrato aquellos elementos que no son esenciales, pero que se entienden incorporados al contrato por disposición general del ordenamiento jurídico, sin que las partes tengan que estipularlos expresamente por las partes. Dichos elementos surgen de la presunción legal de aplicabilidad, y se integran al contrato por virtud de su especie, costumbre jurídica o por inferencia normativa. Por ejemplo, en un arrendamiento, aunque no se haya establecido expresamente la obligación de mantener el bien arrendado en condiciones de uso, el arrendador tiene esa responsabilidad por disposición legal. No es esencial para la existencia del contrato, pero naturalmente forma parte de las obligaciones contraídas. En otras palabras, estos elementos son implícitos y se configuran en virtud del marco jurídico que rige un contrato determinado mientras no se pacte lo contrario.

Por último, son accidentales al contrato aquellas cláusulas, condiciones o estipulaciones que no pertenecen ni a la esencia ni a la naturaleza del contrato, pero que las partes deciden agregar de forma voluntaria y expresa mediante cláusulas especiales. Estos elementos son facultativos, y su inclusión responde al ejercicio de la autonomía de la voluntad contractual en cuanto "lo estipulado en el contrato es ley entre las partes", permitiendo a las partes regular aspectos específicos que el derecho no impone ni presume. Por ejemplo, añadir una cláusula penal en caso de incumplimiento, establecer una prórroga automática del contrato, definir condiciones suspensivas o resolutorias, o fijar un lugar específico de cumplimiento. Son figuras

que modifican, amplían o delimitan el marco general del contrato, pero que no deben afectar su existencia jurídica fundamental, es decir, no deben de contrariar a los elementos esenciales ni requisitos de validez generales de los contratos, so pena de degenerar en otro contrato o producir su nulidad.

2.3. Documentos públicos y documentos privados

Para que un contrato llegue a la “vida jurídica”, además de cumplir con los requisitos antes relacionados en el anterior apartado, debe tener una existencia material o, con el avance de la tecnología, de carácter digital, por lo que es correcto aseverar y necesario aclarar que éstos se ven representados y plasmados ya sea en un papel común, papel especial como el papel para protocolo o de forma electrónica a fin de demostrar una existencia real del “pacto”; y atendiendo a los criterios fijados por el Código Civil y por la Constitución, se categorizan en documentos públicos y documento privados.

El artículo 331 del Código Procesal Civil y Mercantil (CPCM) establece que los **documentos públicos son aquellos expedidos por notario en el ejercicio de su función pública notarial o por cualquier autoridad o funcionario público y que gozan de presunción de veracidad (fe pública)**. A efectos aclaratorios, se entenderá por funcionario público a toda persona natural que presta temporal o permanentemente servicios dentro de la administración pública, con facultad para tomar decisiones dentro de las atribuciones de su cargo (Artículo 3 literal b de la Ley de Ética Gubernamental).

En cuanto a la Función Pública Notarial, en lo relativo a documentos públicos se encuentran los instrumentos notariales como las escrituras públicas de compraventas, testamentos, mandatos judiciales, entre otros; contratos que se autorizan ante notario. Estas se originan en la escritura matriz, asentada en el libro protocolo del notario, y de la cual se derivan los testimonios públicos entregados a los interesados. Las actas notariales, por su parte,

documentan hechos o declaraciones de ante el notario, como inventarios, inspecciones o manifestaciones de voluntad.

Además de las anteriores, las instituciones también extienden certificaciones registrales, como por ejemplo las que emite el Centro Nacional de Registro o el Registro Nacional de las Personas Naturales, entre otras, ya que estos verifican datos como inscripciones de bienes, nacimientos, matrimonios o defunciones. Asimismo, existen constancias oficiales de estudios, cargos públicos, solvencias municipales o tributarias, emitidas por alcaldías, ministerios y otras entidades estatales.

Por otro lado, en base al artículo 332 CPCM, **serán documentos privados instrumentos a aquellos cuya autoría es atribuida a los particulares o cuando el documento no ha cumplido las formalidades que la ley prevé para los instrumentos públicos.**

Dicho de otro modo, se considera documento privado a aquellos que no son otorgados por un funcionario, autoridad pública de los antes mencionados o algún fedatario como delegado del Estado, sino que son elaborados por personas particulares y que, por lo tanto, no gozan de fe pública.

Entre los ejemplos más comunes de documentos privados tenemos a las compraventa de bienes muebles, contratos de prestación de servicios, compraventa de bienes consumibles, documentos bancarios con firma autenticada, cualquier tipo de factura o documento que acredite o conste la compra de productos, bienes y servicios en el sector comercio tales como los anteriormente mencionados; e incluso cualquier contrato cuyos requisitos establecen que no es necesario que se haga mediante instrumento público notarial, como es el caso de los contratos de arrendamiento de bienes muebles o de inmuebles en el caso de, por ejemplo, locales para vivienda en base al artículo 4 de la Ley de Inquilinato.

También se encuentra el caso en el ámbito mercantil de la Constitución de las Sociedades de Acciones Simplificadas (SAS), el cuál se realiza mediante formulario electrónico que debe consignarse mediante firma electrónica certificada en base a lo establecido por el artículo 305-B del Código de Comercio (C.Com.).

“Art. 305-B C.Com.- Las sociedades por acciones simplificadas se constituirán exclusivamente por los formularios proporcionados por el Registro de Comercio para tal efecto, debiendo cumplir dicho formulario con los siguientes requisitos:

(...) IX. Firma de los accionistas de la Sociedad que se constituye, o bien, de sus representantes legales, ejecutores especiales o apoderados. En caso de firmar de manera electrónica, deberá utilizar Firma Electrónica Certificada.” (el resaltado es propio)

3. GENERALIDADES DE LA FIRMA ELECTRÓNICA

Si bien la Firma Electrónica es lo equivalente, en medios digitales, a lo que conocemos como firma autógrafa, llamada coloquialmente como “firma a mano”, hay que aclarar ciertos aspectos no solo sobre su procedencia, tal como se agotó en su contexto histórico, sino también sus características, funcionamiento y algunos conceptos básicos para entender sus efectos en la vida jurídica.

3.1. Sujetos intervinientes

Dentro de los sujetos que se encuentran relacionados en este tema, encontramos una jerarquización entre los mismos, resumidos en un ente regulador, un prestador de servicios y los usuarios; los cuales se definen de la siguiente manera.

a) Unidad de Firma Electrónica

La Unidad de Firma Electrónica (UFE)⁶ es una entidad establecida por la Ley de Firma Electrónica (LFE) como dependencia del Ministerio de Economía según lo dispuesto en el artículo 35 de dicha ley. Su función se divide en dos ámbitos principales: el técnico y el regulatorio, conforme al artículo 36 LFE.

Desde la perspectiva técnica, la UFE actúa como la autoridad registradora y acreditadora en El Salvador. En su función regulatoria o legal, gestiona el certificado electrónico primario o raíz, el cual permite la emisión y administración de los certificados electrónicos de los proveedores de servicios de certificación (PSC). Estos proveedores, a su vez, emiten certificados electrónicos para los usuarios finales. Existe una relación de dependencia entre estos certificados: los de los usuarios finales están subordinados a los emitidos por los PSC, y estos últimos dependen del certificado electrónico raíz administrado por la UFE, consolidando una cadena que permite la gestión y supervisión de los mismos.

b) Proveedores de servicios de certificación

Los PSC son las Personas jurídicas acreditada por la (UFE) para prestar los servicios de certificación en la modalidad de firma electrónica certificada, sello electrónico, sello de tiempo o autenticación de web⁷.

Actualmente las entidades jurídicas legalmente acreditadas para la prestación de este servicio de certificación son tres: UANATACA El Salvador S.A. de C.V., PBS El Salvador S.A. de C.V., y el Banco Central de Reserva de El Salvador. Para conocer cuales son los proveedores autorizados por la UFE, se puede consultar en la página oficial de la firma

⁶ Ministerio de Economía (s.f.). Conoce a la Unidad de Firma Electrónica. *Definición de UFE*. Firmaelectronica.economia.edu.sv.

⁷ D.L. 133 (2015). Ley de Firma Electrónica. Artículo 3, letra q. *Definición de Proveedor de servicios de certificación*. D.O. 196, Tomo 409, 26 de Octubre de 2015.

electrónica⁸ a efectos de que la población se cerciore sobre con quién o quiénes pueden obtener su firma electrónica certificada y evitar posibles fraudes por parte de terceros que no se encuentren debidamente acreditados.⁹

c) Firmantes o signatarios

Es el usuario o persona natural que contrata los servicios de un proveedor de servicios de certificación debidamente acreditado por la Unidad de Firma Electrónica para la obtención de un certificado electrónico (el cual se definirá más adelante) y consecuentemente de una firma electrónica certificada, siendo esta persona natural su titular.

Haciendo un pequeño paréntesis, cabe recalcar que se denominará como firmante a aquella *persona natural*, dejando de lado a las personas jurídicas ya que para que estas “puedan firmar” se debe de hacer mediante su representante legal, el cual lógicamente debe de ser una persona natural y cuya calidad de representante se verá plasmada en el certificado electrónico otorgado por el proveedor y, por ende, en su firma electrónica certificada.

3.2. Conceptos fundamentales y puntualizaciones prácticas sobre la Ley de Firma Electrónica (LFE)

Una vez definidos los sujetos intervinientes, es necesario mencionar tanto el concepto técnico como los aspectos prácticos de los objetos del presente tema en materia de firma electrónica regulados por la LFE, lo cual es muy importante para entender qué es exactamente esta herramienta tecnológica cuyo impacto es y será significativo en la vida práctica- jurídica de nuestro país.

⁸ <https://firmaelectronica.economia.gob.sv/proveedores/>

⁹ Ver “anexo 1” sobre los Proveedores de Servicios de Certificación acreditados en El Salvador.

a) Certificado electrónico

Es aquella declaración electrónica expedida por un proveedor de servicios de certificación debidamente acreditado, el cual vincula los datos de una persona natural o jurídica con una firma electrónica certificada, sello electrónico, sello de tiempo o un sitio web que le pertenecen.

En otras palabras, un certificado electrónico es aquello que **acredita a una persona natural o jurídica como titular o dueña de una firma electrónica**, entre las demás mencionadas; relacionando los datos de dicha persona con los datos de validación que se encuentran dentro del código de la firma electrónica certificada, tal como se explicará más adelante.

Usando la analogía, a efectos prácticos el certificado electrónico cumple la misma función que un Documento Único de Identidad o credencial en esta materia, ya que si bien no son lo mismo, contiene la información de su titular y acredita que dicho titular es dueño de determinada firma electrónica certificada (caso similar como en el Documento Único de Identidad en el cual se relacionan los datos personales y se encuentra plasmada la firma autógrafa, dando a entender que esa firma es de su titular de generales determinadas y descritas en el mismo Documento).

b) Formas de generación de un certificado electrónico

En cuanto al trámite a seguir para la obtención del certificado electrónico, dependerá del PSC con quien se quiera contratar dichos servicios, no obstante se debe comenzar con el reconocimiento del usuario, donde en relación al artículo 33 del Reglamento de la Ley de Firma Electrónica (RLFE) es deber del PSC comprobar fehacientemente la identidad del solicitantes antes de la emisión de cualquier certificado electrónico, es decir, el punto clave es la verificación de la existencia de la persona natural y su concordancia con el DUI y demás

documentos personales presentados y requeridos por el proveedor para la extensión del certificado, sea dicho reconocimiento de forma física o electrónica, tal como lo establece el artículo 58-A de la LFE.

Una vez otorgados los datos personales se remite, por parte del PSC, un correo electrónico o *email* al usuario donde se presenta el contrato de prestación de servicios con los términos y condiciones para que, una vez aceptados, se requerirá generar un número de usuario, una contraseña y el PIN¹⁰ con el cual se validará la creación y consignación de la firma electrónica certificada cada vez que se quiera utilizar en un documento electrónico. Una vez generados, el proveedor remitirá otro email donde especifica el número de usuario y contraseña generados, pero no el PIN, por lo que es necesario anotarlo y guardarlo en un lugar seguro para evitar problemas a futuro.

c) Tipos de certificados electrónicos

En relación a la calidad de firma que se quiere consignar en un documento será el tipo de certificado electrónico que se deba adquirir. Estos se dividen en perfiles y se clasifican de la siguiente forma:

1. Para Personas Naturales: perfil personal, profesional y de funcionario público.
2. Para Representantes Legales: perfil de persona natural y de persona jurídica.
3. Para Personas Jurídicas (Sello electrónico): perfil para Instituciones Públicas y privadas como, por ejemplo, comerciantes sociales o sociedades.

En cuanto al certificado para personas naturales, puede ser de perfil personal cuando es aquel adquirido por cualquier persona particular que quiera contratar servicios o adquirir

¹⁰ PIN es el acrónimo de “*Personal Identification Number*” (número de identificación personal en español) y se refiere a un número de seguridad que se utiliza para autenticar a una persona en un sistema.

bienes de forma electrónica como individuo; es decir, que hará un uso de la firma electrónica para sí misma.

Cuando se menciona un perfil profesional, se refiere a aquel que puede ser adquirido por cualquier persona natural que ejerce una profesión regulada por un ente, como es el caso de los abogados y notarios regulados por la Corte Suprema de Justicia del Órgano Judicial; las profesiones del sector Salud como los médicos, doctores y enfermeros; entre otros.

Sobre el perfil de funcionario público, es aquel que puede ser adquirido por cualquier persona natural que ostenta un cargo en el sector público y que cuya firma electrónica se consigna en el ejercicio de sus funciones atendiendo a las funciones inherentes al cargo.

En cuanto al certificado para representantes, puede ser un perfil para personas naturales o para personas jurídicas, siempre y cuando se actúe como representante legal de otra persona natural o jurídica, conllevando la aptitud para firmar todo lo relacionado con el cargo que está desempeñando y dentro de sus alcances preestablecidos. Dicho de otro modo, con este tipo de certificado se puede firmar en nombre de la persona natural o jurídica que se está representando.

El perfil para Instituciones Públicas sólo puede brindarse a una entidad o persona jurídica, acreditando certeza y seguridad de que un documento extendido con este sello es proveniente de dicha entidad o institución.

El perfil de Sello electrónico para instituciones privadas va relacionada con la emisión de factura electrónica, el cual es extendido únicamente por el Ministerio de Hacienda a aquellos comerciantes que emitan o deban emitir facturas sobre los bienes y servicios que otorgan.

El tiempo de vigencia de este tipo de certificados puede ser de uno a cinco años, pudiendo ser renovados de tracto sucesivo año con año dependiendo de los términos y condiciones del proveedor de servicios de certificación en cuestión.

d) Contenido del certificado electrónico

Dentro del contenido del certificado electrónico se encuentra, en base al artículo 58 de la LFE, los siguientes aspectos:

- Identificación del titular de la firma electrónica, tales como el nombre y apellidos de la persona, así como su Documento Único de Identidad.
- Clave Pública del certificado, el cual es el número de serie del certificado expedido por el proveedor.
- Identificación del proveedor de servicios de certificación que extiende el certificado, así como su domicilio, correo electrónico y número de registro.
- Fecha de emisión y expiración del certificado.
- La firma electrónica certificada o sello electrónico del proveedor que emite el certificado.
- Datos de verificación de la firma electrónica certificada, los cuales son las generales de su titular, destacar la inalterabilidad del documento electrónico desde la hora y fecha en que fue firmado y que la vigencia del certificado.
- Atributos o tipo de perfiles del titular. Por ejemplo, si se actúa como representante legal de una persona jurídica se debe definir y relacionar con el documento o poder en virtud del cual se acredita actuar en tal calidad.

e) Documento electrónico

El artículo 3 letra j. de la LFE lo define como “*Información de cualquier naturaleza contenida en soporte electrónico, según un formato determinado.*”

Haciendo énfasis en este concepto, se puede sustraer dos elementos esenciales: soporte electrónico y formato determinado.

En cuanto al soporte electrónico, puede ser cualquier dispositivo que pueda almacenar información electrónica, ejemplos de ellos son el diskette, disco compacto o CD, memoria USB o tarjetas SD, discos duros, entre otros.

Respecto al formato determinado, se refiere a que la información almacenada en un soporte electrónico debe ser manifestada de forma determinada, ya sea texto, audio o imagen; para mayor comprensión se detalla el siguiente listado de los formatos más comunes:

- PDF (Portable Document Format): Un formato ampliamente utilizado para documentos que necesitan conservar su formato original y ser visualizados de manera consistente en diferentes dispositivos y sistemas operativos.
- DOCX/DOC (Microsoft Word): Formatos estándar para documentos de texto creados con Microsoft Word.
- XLSX/XLS (Microsoft Excel): Formatos para hojas de cálculo creadas con Microsoft Excel.
- HTML/HTM: Lenguaje de marcado utilizado para crear páginas web.
- TXT (Texto Plano): Formato de texto simple sin formato, compatible con cualquier editor de texto.
- PNG/JPG: Formatos de imagen comunes.
- MP3/WAV: Formatos de audio comunes.

Dentro de estos tipos de formatos, el más óptimo en base a sus características es el formato PDF, ya que permite que el texto y su contenido en general solo pueda ser visualizado sin modificación, a menos que se utilicen herramientas de edición especiales pero comúnmente

mantiene su contenido “estático”, dando mayor confiabilidad en comparación a los demás formatos.

Este documento electrónico, en base a su contenido, puede actuar en calidad de, a efectos que conciernen al presente trabajo, un contrato o documento privado o público, para los cuales se considerarán ciertas reglas de validez que se desarrollarán de forma más precisa en los posteriores apartados.

f) Dispositivo seguro de creación

Un dispositivo seguro de creación es un *“equipo o programa informático configurado, que se utiliza para crear una firma electrónica certificada o sello electrónico.”* (art. 3 letra i. LFE)

En términos sencillos, este dispositivo o programa es una “llave” para poder consignar una firma electrónica certificada, siendo dicha llave un dispositivo físico o “token¹¹” o un programa informático, también denominado “certificado cloud¹²”; la modalidad depende del proveedor y la elección del usuario en cuanto al lugar establecido para contener el certificado electrónico, sea desde un dispositivo físico como una USB o desde los servidores del proveedor, respectivamente.

En cuanto a la utilización de un certificado cloud, se realiza mediante un programa informático cuya descarga es proporcionada por el proveedor; se debe ingresar el usuario y contraseña generados al momento de obtención del certificado electrónico y además, al iniciar sesión, se debe ingresar el PIN para “firmar” o, dicho de forma más técnica, validar la consignación de la firma electrónica certificada en un documento electrónico.

¹¹ Un certificado en token es un certificado digital que se almacena de forma segura en un dispositivo físico llamado token, generalmente un dispositivo USB.

¹² Un certificado cloud es un tipo de certificado electrónico que no se almacena en un dispositivo físico, sino que reside de forma segura en la nube, es decir, en los servidores del proveedor de servicios de certificación. Este modelo permite al usuario acceder a su firma electrónica certificada desde cualquier dispositivo con conexión a internet, mediante credenciales seguras como usuario, contraseña y un PIN personal.

g) Firma electrónica simple

Esta es definida como cualquier dato electrónico consignado en un mensaje de datos o documento electrónico que se utiliza para relacionar al firmante por cualquier medio tecnológico, indicando el consentimiento y autoría del firmante con el contenido del mensaje de datos o documento electrónico.

Para la utilización del mismo se prescinde de un PSC o cuando este proveedor no se encuentra debidamente autorizado por la Unidad de Firma Electrónica y queda a criterio de cada firmante la forma y riesgo que quieran asumir a la hora de dar su firma electrónica simple en cualquier medio electrónico.

Ahondando en el concepto, al no ser certificado y establecer que se configura mediante “*cualquier medio tecnológico*”, la simple validación o clic en cualquier casilla, recuadro u opción aportada por un sitio web puede ser considerado como una firma electrónica simple, siempre y cuando implique consentimiento del firmante. Ejemplo de ello se encuentra la aceptación de los términos y condiciones al momento de crear un usuario de cualquier red social como Facebook, en donde para tales efectos es necesario marcar una casilla para confirmar que se ha leído y se está de acuerdo con los términos y condiciones; por lo tanto, a este dato electrónico, al relacionar autoría y consentimiento por parte del usuario, entra en la categoría de firma electrónica simple.

No obstante, no hay forma de verificar fehacientemente el libre consentimiento del firmante de esta forma, por lo que es materia de debate y, por su puesto, de valoración al momento de cualquier inconveniente con el contenido que se firme de forma simple, ejemplo de ello son los términos y condiciones que se aceptan al crear cualquier usuario de las redes sociales, comprometiéndose el usuario a cumplir con una serie de lineamientos ya que, como

se mencionó anteriormente, basta cualquier medio tecnológico que exprese el consentimiento del firmante en un medio digital para ser considerada como tal.

h) Firma electrónica certificada

Existe una ambigüedad sobre lo que realmente es una firma electrónica, ya que el concepto establecido en el artículo 3 letra m. de la Ley de Firma Electrónica establece que son aquellos “*datos en forma electrónica*” plasmados en un documento electrónico mediante un dispositivo seguro de creación proporcionado por el proveedor de servicios de certificación acreditado por la Unidad de Firma Electrónica y que **vinculan a la firma con su titular**. Si bien es cierto que existe esta relación y su vinculación es fundamental para la existencia de una firma electrónica, “firmar” implica otorgar un consentimiento por parte del titular de la firma y no es meramente una representación de sus datos personales pese a su vinculación a ellos, siendo por lo tanto necesario matizar esta circunstancia.

Tomando el mismo caso análogo utilizado para definir lo que es un certificado electrónico, si este se asemeja a lo que es un Documento de Identidad o una credencial; la firma electrónica es análoga y funcionalmente hablando una firma contenida en ese mismo documento de identidad, por lo que al ser plasmada en algún documento expresa consentimiento y pertenencia de esa persona con esa firma determinada.

Entonces, cuando se quiere firmar un documento electrónico, después de iniciar sesión o ingresar al usuario dentro del dispositivo seguro de creación, se abrirá una ventana emergente¹³ dentro del cual se ingresará el código PIN (creado al momento de obtener el certificado electrónico con el proveedor) e *ipso facto* el Sistema Seguro de Creación encriptará el código hash del documento electrónico dentro del mismo código del documento, siendo este

¹³ Una ventana emergente es una ventana pequeña y temporal que aparece en una página web o aplicación, generalmente para mostrar información adicional o solicitar al usuario que realice una acción. (GetResponse, 2025)

momento de que **al ser ingresado el PIN, implica consintiendo por parte del firmante sobre el contenido del documento electrónico**, consentimiento que se verá representado gráficamente como una imagen, el cual al darle clic podremos visualizar el certificado electrónico o credencial del firmante, el cual contiene sus datos generales (Nombre, domicilio, DUI, oficio, etc.), la fecha y hora en que fue firmado, si presenta alguna modificación a *posteriori* de ser firmado y quién es el proveedor que certifica dicha información.

Asimismo, puede concluir que una firma electrónica certificada, no obstante de ser definido dentro del artículo 3 letra m. de la Ley de Firma Electrónica como aquel o aquellos datos electrónicos que relacionan la identidad del firmante con la imagen codificada que se plasma en un documento electrónico y no esa representación gráfica *per se*, cabe realizar una serie de matices al respecto.

i) Concepto provisional de firma electrónica certificada

Como se mencionó, existe una encriptación del código hash del cual se hablará detalladamente en su respectivo apartado, pero como premisa cabe hacer mención este aspecto a efectos aclaratorios sobre la definición de lo que es una firma electrónica certificada. Entonces, es “esa” encriptación parte de la firma electrónica ya que es mediante el cual se brinda la seguridad en cuanto a la veracidad e integridad de la firma y el documento. Por lo tanto, es recomendable hacer una modificación provisional del concepto.

Por lo tanto, una definición de firma electrónica certificada que podría ser más precisa es la siguiente:

“Conjunto de datos en formato electrónico consignados en un mensaje de datos o documento electrónico, a través de cualquier tecnología de protección de datos producido por el dispositivo seguro de creación proporcionado por un proveedor de servicios de certificación de firma electrónica autorizado por la Unidad de Firma Electrónica del Ministerio de Economía,

el cual permite vincular de manera exclusiva, inequívoca y verificable la firma con su titular y la integridad del documento al momento de ser firmado".

Con este concepto se añaden los elementos de la tecnología utilizada por el PSC para la protección de los datos electrónicos y la capacidad de que la veracidad e integridad de la firma y del documento electrónico en el cual ha sido consignada pueda ser verificable de forma fehaciente, recalcando a su vez que la firma electrónica certificada no es su representación gráfica, sino el conjunto de datos dentro de dicha representación gráfica los cuales deberán ser seguros y verificables; plasmados en el momento que se introduce el PIN para consignar la firma, acción a la cual se le denomina como "*firmar electrónicamente*".

j) Sello electrónico y sello de tiempo

Comenzando con el concepto general, un sello es una marca, usualmente física o digital, que se utiliza para autenticar, autorizar o validar un documento. Puede ser un sello físico con tinta, un sello digital incrustado en un archivo, o incluso un sello de tiempo para validar la fecha y hora de creación o modificación de un documento. Los sellos sirven para varios propósitos, como verificar la autenticidad de un documento, indicar su origen o propietario, y garantizar la integridad del contenido.

En cuanto al sello de tiempo, partiendo de la base de que al consignarse una firma electrónica certificada se muestra dentro de su contenido diferentes datos relativos al firmante, así como lo son la fecha y la hora en que ésta fue puesta en el documento electrónico según la fecha y hora del dispositivo (como una computadora, por ejemplo) del firmante; pero al poseer un sello de tiempo, estos datos se tendrán por fehacientes atendiendo a que es el proveedor de servicios quién los acredita desde un sistema ajeno al equipo del firmante, brindando certeza sobre determinado dato, garantizando la integridad temporal del documento electrónico firmado.

En cuanto al sello electrónico, es aquel o aquellos datos en formato electrónico adjuntos a otros datos en formato electrónico, o asociados de manera lógica con ellos, que garantizan el origen y la integridad de estos últimos. Dicho de otra manera, el sello electrónico es el homólogo digital del tradicional sello estampado sobre papel. Sirve para identificar una empresa o entidad, por lo que solo está disponible para personas jurídicas.

Por lo tanto, el sello electrónico es un mecanismo criptográfico que permite a una persona jurídica (empresa, institución pública, organización, etc.) autenticar el origen y garantizar la integridad de un documento electrónico. A diferencia de la firma electrónica, que está vinculada a una persona natural y expresa consentimiento como se ha establecido reiteradamente, el sello electrónico no implica voluntad, sino *autoría institucional*.

k) Clasificación de los sellos electrónicos

Los sellos electrónicos, atendiendo si la persona jurídica que los quiera adquirir es una entidad pública o privada, se clasifican de la siguiente manera.

Sello de órgano AAPP (Administración Pública)

Es un certificado electrónico cualificado que acredita el origen e integridad de los datos de un Organismo Público. Permite a una Administración Pública autenticarse y realizar firmas electrónicas en procesos administrativos automatizados.

Sello de empresa (Persona jurídica)

Si bien es llamado “sello de empresa”, se utiliza un concepto común erróneo ya que es una persona jurídica (como por ejemplo una sociedad mercantil) quien se considera como sujeto de derecho y propietaria del sello en cuestión, ya que lo que se denomina como “empresa” es una cosa mercantil que si bien forma parte del ente, no son lo mismo.

Obviando lo anterior, será sello electrónico de empresa un certificado electrónico cualificado que acredite el origen e integridad de los datos de una persona jurídica. Permite a una persona jurídica autenticarse y realizar firmas electrónicas en procesos automatizados, por ejemplo: generación de recibos, facturas, sellar acuerdos contraídos por la entidad, entre otros.

4. PARTICULARIDADES DE LA FIRMA ELECTRÓNICA CERTIFICADA

4.1. Contenido de la firma electrónica certificada

Cuando se consigna la firma electrónica certificada, se puede dar clic sobre su representación gráfica para acceder a la información encriptada el cual contiene los siguientes datos que le relacionan con el firmante y la integridad de la firma.

Estado de validación de la firma: En un primer momento se abre una ventana donde se muestra la información resumida de la firma, conteniendo el nombre del firmante y su correo electrónico, la verificación de que la firma es válida y si el documento ha sufrido alteraciones luego de haber sido firmada. También sobresale la opción “propiedades de la firma” que lleva a la siguiente información.

Resumen de validez: arroja de forma más detallada la información extractada anteriormente, agregando la hora y fecha en que fue firmado, a la vez que habilitando la opción para verificar el certificado electrónico, también llamado a efectos prácticos como “credencial” en atención a lo desarrollado en su respectivo apartado.

Certificado del firmante: Al ingresar en esta ventana, se repliegan muchas opciones de las cuales la más importante se encuentra en la pestaña “detalles” y en la sección “asunto”, donde se muestran más datos del firmante tales como, según el caso, su nombre, Documento Único de Identidad, domicilio, la función o cargo en cuya calidad y ejercicio está firmando, la

institución que representa, la nacionalidad, el proveedor de su servicio de certificación e incluso el inicio y fin de la validez de su firma electrónica según su contrato con el proveedor.

Recalcando la idea, es este contenido de datos a lo que se le denomina “*firma electrónica*”, por lo que para su validez es necesaria la verificación de la misma (punto el cual se explicará más adelante).

4.2. Funcionamiento de la firma electrónica certificada

Uno de los aspectos más relevantes de la firma electrónica es el sistema seguridad que impide la falsificación o alteración inobservada de la firma dentro del documento electrónico firmado en relación a su contenido, pero esta seguridad se logra mediante una serie de datos encriptados dentro del código del documento.

Teniendo como base que los documentos electrónicos deben contener un formato determinado, tomando de ejemplo el formato .PDF, la firma electrónica certificada, como mecanismo de validación digital, opera mediante procesos criptográficos que garantizan la autenticidad, integridad y no repudio de los documentos electrónicos como se establece en el presente. Técnicamente, su funcionamiento se basa en la generación, cifrado y verificación de un código denominado “*hash*”¹⁴, el cual constituye un tipo de “*huella digital única*” del contenido del documento.

Este hash convierte el contenido del documento electrónico en una cadena alfanumérica única e irrepetible. Si dicho contenido sufre cualquier alteración, incluso mínima, el hash generado será completamente diferente, lo cual permite detectar modificaciones no autorizadas.

¹⁴ El *código hash* es una sucesión alfanumérica (letras y números) de longitud fija, que identifica o representa a un conjunto de datos determinados. Se trata, simplemente, de un algoritmo matemático que transforma el conjunto de datos de entrada en una expresión alfanumérica que tiene una longitud predeterminada e identifican de manera inequívoca el documento o conjunto de datos que representan (Signaturit Group, 2025)

Una vez generado el hash, éste es cifrado con la clave privada del firmante. Este proceso de cifrado se realiza dentro del sistema seguro de creación proporcionado por el PSC, siendo mediante un dispositivo físico (token USB) o de una plataforma en la nube (aplicación cloud). El resultado de este cifrado es la firma digital propiamente dicha, que se incorpora al documento electrónico junto con el certificado digital del firmante y, en su caso, el sello de tiempo que registra la hora exacta de su emisión¹⁵.

4.3. Forma de validación de la firma electrónica certificada

Para validar o verificar la validez de una firma electrónica certificada, se debe subir el documento firmado a la plataforma o página electrónica del proveedor de servicios o de la Unidad de Firma Electrónica en la sección correspondiente, el cual funciona generando nuevamente el hash del contenido actual del documento. Posteriormente, utiliza la clave pública contenida en el certificado digital del firmante para descifrar el hash original. Si el hash recién generado y el hash descifrado coinciden, se confirma que el documento no ha sido alterado desde su firma y que ésta es auténtica y válida, manteniéndose su integridad.

Este proceso técnico es fundamental para dotar a la firma electrónica certificada de efectos jurídicos equivalentes a los de la firma autógrafa, cumpliendo con los principios de autenticidad, integridad y no repudio regulados en la LFE. Además, permite la trazabilidad exacta de la firma, ya que cada documento firmado almacena la fecha, hora, identidad del firmante, entidad certificadora, y estado de validez del certificado. Tales elementos refuerzan la seguridad jurídica en entornos digitales, especialmente en actos contractuales, administrativos y notariales que requieren certeza documental.

Entonces, se podría decir *a grosso modo* que el sistema seguro de creación pone “bajo candado” el código hash del documento que se firma (código que representa exactamente cada

¹⁵ Ver “Anexo 2” sobre los pasos para la consignación de una firma electrónica certificada.

punto y coma contenido en el documento), por lo que y al consultar la veracidad e integridad de un determinado documento electrónico con firma electrónica certificada mediante la opción proporcionada por el PSC o la página oficial de la UFE (los cuales tienen bases de datos relacionados para tales efectos), se realiza un “cotejo” entre el cálculo que se hace del contenido del documento que se quiere verificar generando un nuevo código hash o huella única de ese contenido en concreto que se quiere verificar y lo compara con el código hash descifrado que se encuentra encriptado en el mismo documento electrónico el cual, si coinciden, implica que no ha sido modificado desde que fue firmada¹⁶.

5. RÉGIMEN JURÍDICO DE LA FIRMA ELECTRÓNICA

A manera de síntesis, se puede afirmar que todo contrato es una convención o manifestación de voluntades entre dos o más personas (con excepción de las obligaciones unilaterales) que se expresa mediante su consentimiento representado gráficamente por una firma, sea autógrafa o electrónica, la cual se plasma en un documento público, privado o digital, adquiriendo de esta forma los derechos y obligaciones de dar, hacer o no hacer una cosa, según lo estipulado por el contenido del documento en que se consigna la firma.

Una vez fijadas estas bases y ubicando a la firma electrónica certificada como manifestación de voluntad y requisito de validez de los contratos, es procedente entrar a detalle sobre sus efectos jurídicos en base a la Ley de Firma Electrónica.

5.1. Principios rectores de la LFE

El artículo 4 de la LFE, como todo cuerpo normativo, establece los principios generales o principios rectores que lo configuran; estos son una especie de “guía” sobre el contenido a desarrollar en el mismo cuerpo legal; es decir, son parámetros de los cuales las disposiciones contenidas en la ley no deben de salirse y que cuyo encuadre se percibe al momento de su

¹⁶ Ver “Anexo 3” sobre la forma de validación de una firma electrónica certificada.

análisis, interpretación y alcance, sirviendo como base para comprender la ley y poder examinar su fin y concordancia con el ordenamiento jurídico y, principalmente, con la Constitución. Dentro de estos principios tenemos los siguientes.

a) Autenticidad

Este principio afirma que un mensaje de datos o documento electrónico es confiable cuando está suscrito con firma electrónica certificada, sello electrónico y sello de tiempo. Su objetivo es garantizar la identidad del emisor, asegurando que el documento proviene efectivamente de quien lo firma y que dicha firma no ha sido falsificada. Se trata de una traslación digital del tradicional valor probatorio de la firma autógrafa, pero con herramientas criptográficas como se ha explicado en los anteriores apartados. La autenticidad es clave en relaciones contractuales donde la certeza sobre el origen de la voluntad expresada es fundamental para generar efectos jurídicos válidos.

b) Integridad

Este principio se centra en garantizar que la información contenida en un documento electrónico no haya sido alterada desde el momento en que se colocó la firma electrónica certificada, sello electrónico o sello de tiempo. Aplica también desde la desmaterialización de documentos (que no es más que escanear o convertir a digital un documento físico). Es decir, preserva la invariabilidad del contenido del documento físico en relación a su versión electrónica una vez desmaterializado. Esto cobra relevancia en ámbitos donde la alteración de un documento puede tener graves consecuencias jurídicas, como en procesos judiciales o registros notariales digitales como la entrega digital del libro de protocolo y demás instrumentos notariales. La integridad permite confiar en que los documentos almacenados reflejan fielmente el contenido original autorizado por el firmante.

c) Confidencialidad

Consiste en la protección de la información proporcionada por los usuarios a los proveedores de servicios. Se prohíbe que dicha información, como el domicilio, nombre y demás generales, sea compartida sin autorización expresa del titular de una firma electrónica. Este principio introduce una dimensión ética y de protección de datos personales en el ecosistema de la firma electrónica. Es especialmente relevante frente al creciente uso de la tecnología en la administración pública y el comercio electrónico, donde la protección de la información sensible garantiza la confianza de los usuarios ante cualquier tipo de hurto de datos personales o cualquier otro tipo de delitos cibernéticos a los que actualmente la población se encuentra vulnerable.

d) Equivalencia funcional

Es uno de los pilares de esta ley y que establece un criterio base sobre el funcionamiento de la firma electrónica certificada, sello electrónico, sello de tiempo y documento electrónico. Este principio determina que los documentos electrónicos cumplen con los mismos efectos y finalidades que los documentos en papel, siempre que satisfagan los requisitos legales establecidos para los efectos jurídicos deseados, teniendo la misma validez legal que el tipo de documento al que en calidad equivalga un documento electrónico.

Así, un contrato firmado electrónicamente tendrá el mismo valor que uno firmado a mano, salvo que la ley exija una solemnidad específica no reproducible electrónicamente en base a lo dispuesto en el artículo 7 LFE, como por ejemplo aquellos contratos que legalmente deben de ser otorgados ante notario mediante Escritura Pública, ya que el papel sellado especial para protocolo o también llamado “papel protocolo” no puede ser reemplazado electrónicamente, siendo únicamente su entrega ante la Corte Suprema de Justicia la que se debe desmaterializar y firmar electrónicamente, no extensión de contratos *per se*. Además, la

razón de ser de este principio es armonizar la ley con la evolución tecnológica, garantizando la continuidad jurídica en nuevos formatos, especialmente los digitales.

e) No repudio

Este principio garantiza que el firmante no puede negar la autoría de un mensaje de datos o documento electrónico cuando ha sido suscrito conforme a los requisitos de la LFE. Opera como una presunción *iuris tantum*¹⁷ de que la firma electrónica certificada fue colocada voluntaria y legítimamente por su titular. Esto fortalece la seguridad jurídica, especialmente en transacciones contractuales y procedimientos judiciales donde se cuestiona la autenticidad de los documentos, no obstante cabe la posibilidad de poder redargüirse de falso y poderse demostrar en cuanto la firma electrónica no reúna los requisitos de validez exigidos por la LFE en su artículo 23 o acarree algún vicio del consentimiento como el error, fuerza o dolo.

f) Neutralidad tecnológica

En virtud de este principio se prohíbe la discriminación entre tecnologías, siempre que sean seguras y aptas para cumplir con las funciones que la ley exige; es decir, cada proveedor es libre de optar por sus propios medios de seguridad electrónica con tal de que cumplan con ciertos parámetros exigidos por la Unidad de Firma Electrónica, abriendo el marco jurídico a la innovación constante, evitando que la normativa quede obsoleta frente al avance tecnológico. Además, implica que la ley no se ata a un dispositivo o proveedor específico, sino a los criterios funcionales y de seguridad. Por ende, es una cláusula de flexibilidad legal que permite incorporar nuevas herramientas digitales sin necesidad de modificar el texto legal de la LFE.

¹⁷ *iuris tantum* proviene del latín y se traduce como “en tanto que derecho” o “por disposición del derecho”.

g) Seguridad

Establece la obligación de garantizar la certeza jurídica de que el titular de un certificado ha sido debidamente identificado, y que se protege la información digital asegurando su disponibilidad, integridad, autenticación, no repudio, confidencialidad y uso correcto. Es un principio transversal que sustenta y recopila todos los anteriores. El énfasis en la “certeza y legalidad” refuerza la visión de la firma electrónica como un mecanismo tan confiable como los tradicionales, especialmente relevante en entornos gubernamentales o judiciales. Si bien se puede entender como un principio redundante, refuerza la idea y fin de seguridad jurídica que se quiere brindar e instaurar con la implementación de la firma electrónica y demás figuras digitales reguladas en la LFE.

h) Inalterabilidad del Derecho preexistente

Este principio tiene un valor interpretativo decisivo, pues aclara que la firma electrónica no modifica el derecho sustantivo aplicable a cada materia jurídica; es decir, su uso no altera los requisitos, efectos o procedimientos establecidos por otras ramas del derecho, principalmente el derecho civil, mercantil, laboral y penal; sino que sólo introduce un mecanismo distinto de manifestación de voluntad, pero **las relaciones jurídicas seguirán rigiéndose por las reglas del fondo o derecho preexistente.**

Esto resume, junto al principio de equivalencia funcional, la aplicación de la firma electrónica y demás figuras digitales en las relaciones contractuales en una mera opción adicional de carácter digital que no implica alteración alguna.

5.2. Requisitos de validez para la firma electrónica certificada

La firma electrónica certificada, según lo establecido en los artículos 23 y 32-A de la LFE, constituye un mecanismo digital dotado de efectos jurídicos equivalentes a los de la firma

autógrafo o manuscrita, siempre y cuando cumpla con determinados requisitos técnico-normativos que garantizan su funcionalidad, autenticidad y seguridad so pena de ser considerada como una firma electrónica simple en virtud de lo establecido por el artículo 8 inciso 2° numeral 3 LFE.

“Art. 32-A LFE.- CUANDO LA LEY REQUIERA UNA FIRMA AUTÓGRAFA, ESA EXIGENCIA TAMBIÉN QUEDA SATISFECHA POR UNA FIRMA ELECTRÓNICA. ESTE PRINCIPIO ES APLICABLE A LOS CASOS EN QUE LA LEY ESTABLECE LA OBLIGACIÓN DE FIRMAR O PRESCRIBE CONSECUENCIAS PARA SU AUSENCIA.”

Además, la ley delimita seis criterios esenciales que deben observarse para que la firma electrónica pueda ser reconocida como certificada y, por consiguiente, válida; los cuales se explican a continuación:

En primer lugar, **la firma debe vincular al firmante de manera única**, lo que implica que la estructura digital que conforma dicha firma ha de estar asociada exclusivamente a una persona natural, de forma inequívoca e irrepetible. Este vínculo se logra mediante la implementación de algoritmos criptográficos que generan claves privadas personalizadas y que, al operar en conjunto con sistemas de verificación y dispositivos seguros de creación, impiden que otra persona pueda replicar la firma sin ser titular legítimo o sin alterar el código hash propiciando su detección. Así, se establece una correspondencia directa entre el firmante y su expresión de voluntad en el documento digital consignado por su firma electrónica certificada.

En segundo lugar, la firma electrónica certificada debe estar basada en un **certificado electrónico emitido por un proveedor de servicios de certificación debidamente acreditado por la Unidad de Firma Electrónica del Ministerio de Economía**. Este certificado

actúa como el respaldo legal y técnico de la identidad del firmante, pues contiene datos como su nombre, Documento Único de Identidad, domicilio y demás atributos que confirman su titularidad. La existencia de este certificado garantiza que el firmante ha pasado por un proceso de verificación conforme al artículo 58 de la ley, y que su identidad ha sido validada de manera fehaciente.

En tercer lugar, se exige **que la firma permita la verificación inequívoca de la autoría e identidad del signatario**, lo que supone que cualquier tercero receptor del documento debe poder corroborar, sin ambigüedad o lugar a dudas de forma significativa, quién lo firmó, cuándo lo hizo y mediante qué certificado digital proporcionado por cuál proveedor de servicios. Esta verificación se realiza mediante el uso de la clave pública contenida en el certificado, que permite descifrar el código hash cifrado del documento y compararlo con uno recién generado. Si ambas huellas digitales coinciden, se comprueba la autoría e integridad del documento por parte de la plataforma de la Unidad de Firma Electrónica o del proveedor acreditado, según el caso.

El cuarto requisito establece que **la firma debe haber sido creada utilizando medios de creación y verificación confiables y seguros, bajo el control exclusivo del signatario**. Esto significa que el proceso de generación de la firma debe realizarse en un entorno protegido contra intervenciones externas, como puede ser un token USB o plataforma en la nube. Además, el PIN personal requerido para activar la firma debe estar en posesión exclusiva del usuario firmante, lo que asegura que nadie más pueda ejecutar el acto de firma en su nombre.

Como quinto punto, **la firma electrónica certificada debe estar vinculada con la información de modo tal que cualquier modificación posterior sea detectable**. Este principio garantiza la integridad documental, ya que, si el contenido del documento electrónico se altera después de haber sido firmado, el sistema generará un nuevo hash que no coincidirá

con el original cifrado. Este mecanismo opera como una alerta digital de manipulación, protegiendo tanto al firmante como a los terceros involucrados en el acto jurídico.

Finalmente, el artículo establece que ***“los certificados electrónicos emitidos para firma electrónica certificada cumplirán los requisitos del artículo 58 de la presente ley”***, lo cual remite a un conjunto de especificaciones adicionales relativas a la identificación del titular, vigencia del certificado, entidad emisora (proveedor de servicios de certificación), datos técnicos y atributos legales; o dicho de otro modo, es el contenido mínimo que debe poseer un certificado electrónico. Este vínculo normativo fortalece la exigencia de seguridad jurídica, transparencia y trazabilidad que debe observar todo proceso de certificación, especialmente para garantizar la identidad del firmante y validez del certificado.

En conjunto, estos requisitos conforman el estándar jurídico-técnico que delimita la validez de la firma electrónica certificada. Su cumplimiento garantiza que dicha herramienta no sea un simple instrumento tecnológico, sino un “vehículo” legítimo de voluntad jurídica, capaz de sostener la validez probatoria, la equivalencia funcional y la exigibilidad propia de los actos jurídicos suscritos con firma autógrafa.

5.3. Valor probatorio de la firma electrónica simple y certificada

Al momento de encontrarse en un proceso judicial, los contratos sirven como medio de prueba para demostrar la existencia, veracidad o contenido de un hecho o acto jurídico; es el caso de que en un documento electrónico, atendiendo a si fue consignado con firma electrónica certificada o simple, tiene un valor diferente según el caso, partiendo del principio de equivalencia funcional antes desarrollado en el presente trabajo.

Respecto a la firma electrónica certificada, el artículo 8 LFE establece que, atendiendo a si el documento electrónico consignado con ésta se encuentra en calidad de documento público, constituye prueba plena conforme a las reglas del Código Procesal Civil y Mercantil

(CPCM); es decir, se presume cierto el contenido del documento electrónico y el consentimiento dado por parte del firmante.

En cuanto el documento electrónico se encuentre en calidad de un documento privado, tendrá el mismo valor que el anterior o, dicho de otro modo, también gozarán de presunción de veracidad con tal de ser suscrito con firma electrónica certificada o sello electrónico.

“Valor probatorio de los instrumentos

Art. 341 CPCM.- Los instrumentos públicos constituirán prueba fehaciente de los hechos, actos o estado de cosas que documenten; de la fecha y personas que intervienen en el mismo, así como del fedatario o funcionario que lo expide.

Los instrumentos privados hacen prueba plena de su contenido y otorgantes, si no ha sido impugnada su autenticidad o ésta ha quedado demostrada. Si no quedó demostrada tras la impugnación, los instrumentos se valorarán conforme a las reglas de la sana crítica.”

En otras palabras, al emplear una firma electrónica certificada en un documento electrónico, lo dota de veracidad respecto a su contenido e identidad del firmante, así como el consentimiento suscrito por el mismo. En este mismo orden de ideas, el artículo 25 LFE recalca que el empleo de una firma electrónica certificada convierte al documento electrónico consignado por ello en un medio de prueba dotado de presunciones de veracidad e integridad, salvo que se demuestre lo contrario mediante prueba suficiente. Dichas presunciones operan bajo el principio jurídico denominado *iuris tantum* (presunción de derecho), el cual establece que determinados hechos se consideran verdaderos por disposición legal, mientras no se pruebe lo contrario.

La primera presunción contenida en el literal a) del artículo 25 LFE establece que, cuando se utiliza una firma electrónica certificada que cumple los requisitos exigidos por la ley, se entiende que dicha firma pertenece al titular del certificado electrónico; es decir, que existe correspondencia entre la persona que figura como firmante y el propietario legítimo del certificado utilizado para cifrar el documento. Esto implica que el sistema legal reconoce que, mientras no se acredite falsedad, la firma debe considerarse jurídicamente vinculada al firmante, como manifestación legítima de su voluntad. La presunción aquí tiene efectos directos en la determinación de la autoría del documento, exonerando al firmante de tener que demostrar repetidamente que fue él quien suscribió el acto, trasladando la carga de la prueba a quien niegue esa autoría.

La segunda presunción, contenida en el literal b) del mismo cuerpo legal, refiere al principio de integridad documental y establece que el documento electrónico firmado electrónicamente no ha sido modificado desde el momento de su firma, siempre que el procedimiento técnico de verificación arroje dicho resultado. Esta verificación se realiza mediante el cotejo de códigos hash (tal como se ha explicado previamente en su respectivo apartado) que permite confirmar si el contenido del documento actual coincide plenamente con la versión firmada. Si el procedimiento técnico determina que no hay alteraciones, se presume legalmente que el documento permanece íntegro, lo que implica que las condiciones bajo las cuales se suscribió el acto jurídico siguen intactas. Esta presunción garantiza que el contenido del documento no fue objeto de manipulación posterior, protegiendo así la seguridad jurídica de las partes y la validez del acuerdo plasmado en estos medios electrónicos, equiparando a la firma electrónica certificada con la firma autógrafa autenticada por un fedatario.

Por otro lado, respecto a la firma electrónica simple el artículo 6 LFE establece que existe una equivalencia entre la ésta y la firma autógrafa, recalcando que no tendrá la misma validez que una firma electrónica certificada; es decir, la firma electrónica simple no goza de

presunción de veracidad ni integridad, pero puede ser utilizado como medio de prueba atendiendo a las reglas de la sana crítica¹⁸ por el juzgador o autoridad en su ejercicio valorativo dentro de un procedimiento judicial o administrativo.

Un dato a tener en cuenta es que las firmas electrónicas, tanto la simple como la certificada, gozan de un cierto valor jurídico en cuanto a la forma que se tenga de poder verificar su veracidad; *ergo* su valor jurídico, independientemente de si figura como prueba fehaciente o debiéndose valorar conforme a las reglas de la sana crítica, radica en la certeza con la que se pueda identificar su autoría y la integridad del documento electrónico en que se consigne. Como ejemplo de ésto se encuentra el caso de una copia impresa de un documento electrónico con firma certificada, en donde al imprimirse pierde su capacidad de ser verificada de forma electrónica y, por lo tanto, también pierde su validez legal; no obstante, para superar esta barrera se puede insertar un Código Qr¹⁹ en calidad de firma electrónica simple, el cuál al ser detectado por un lector de Qr podrá redirigirse al documento electrónico correctamente almacenado por un Proveedor de Servicios de Almacenamiento de Documentos Electrónicos (PSADE) o por una Institución Estatal, ya que de esta forma se gozará de presunción de integridad del documento respecto a su contenido en virtud de lo establecido en el Art. 8 Inciso 3ro LFE.

“Art. 8 LFE.- (...) LOS MENSAJES DE DATOS Y DOCUMENTOS ELECTRÓNICOS, ALMACENADOS EN PROVEEDORES DE SERVICIOS DE ALMACENAMIENTO DE DOCUMENTOS ELECTRÓNICOS, DEBIDAMENTE ACREDITADOS POR LA UNIDAD DE FIRMA ELECTRÓNICA, GOZARÁN DE LAS PRESUNCIONES DE

¹⁸ Las reglas de la sana crítica se refieren a un sistema de valoración de pruebas en los procesos judiciales. Implica que el juez debe analizar las pruebas de manera lógica, utilizando las máximas de su experiencia, lógica y conocimientos o psicología, para llegar a una conclusión razonada sobre los hechos, sin estar sujeto a reglas preestablecidas que determinen el valor de cada prueba de forma rígida.

¹⁹ QR significa «respuesta rápida». Un código QR es un tipo de código de barras que puede leerse fácilmente mediante un dispositivo digital y que almacena información como una serie de píxeles en una cuadrícula de forma cuadrada. (Kaspersky, s.f.)

*CONSERVACIÓN E INTEGRIDAD DE LA INFORMACIÓN CONTENIDA EN ELLOS
(...)”*

5.4. Causales de revocatoria de un certificado electrónico

Los artículos 60 de la Ley de Firma Electrónica (LFE) y 35-A del Reglamento de la Ley de Firma electrónica (RLFE) establecen el régimen aplicable a la revocatoria de cualquier tipo de certificado electrónico (entendidos a grosso modo como los instrumentos jurídicos o “credenciales” que vinculan la identidad del titular de la firma electrónica certificada).

Estas disposiciones legales constituyen son de carácter sustancial, toda vez que regula los supuestos bajo los cuales el certificado (que en sí mismo da vida jurídica a la firma electrónica certificada) pierde su validez, eficacia y fuerza jurídica, ya sea por **voluntad del usuario o titular del certificado, por resolución judicial o por disposición administrativa** debidamente fundada en las causales establecidas por la misma disposición.

Comenzando con estas causales de revocatoria, **se permite la revocación del certificado electrónico por resolución judicial**, lo que implica que cualquier órgano jurisdiccional competente, en el marco del ordenamiento legal salvadoreño, podrá declarar la pérdida de vigencia o validez del certificado electrónico. Esta resolución puede originarse, por ejemplo, en casos de suplantación de identidad, falsedad, uso indebido del certificado (artículos 196, 283 y 284 del Código Penal respectivamente) o por nulidad por vicios del consentimiento que dio lugar u origen en el entendido de que al constituirse un certificado electrónico se debe celebrar un contrato entre usuario y proveedor (artículos 1316, 1322 y 1551 C.C.), los cuales se deberán de dirimir en el proceso penal o civil correspondiente. La intervención judicial garantiza, en este caso, una decisión revestida de autoridad y con plena fuerza vinculante, que puede incluso tener efectos retroactivos en cuanto a los documentos suscritos mediante la firma electrónica vinculada a dicho certificado.

Por otro lado, la norma establece que el certificado electrónico puede ser revocado por resolución razonada emitida por el Ministerio de Economía, a través de la Unidad de Firma Electrónica (UFE). Esta **modalidad o vía administrativa** no requiere una sentencia judicial, pero debe cumplir con los principios de legalidad, debido proceso y motivación, en virtud de ser una resolución que afecta derechos y produce efectos directos sobre los documentos electrónicos suscritos bajo ese certificado. La UFE, en calidad de ente regulador, actúa como garante de la integridad y confiabilidad de los servicios de certificación, por lo que su facultad de revocación responde a la necesidad de preservar el ecosistema digital frente a irregularidades o fallos de seguridad acorde a las causales taxativamente establecidas.

Los supuestos que habilitan la revocación administrativa se encuentran enumerados expresamente en el mismo artículo. El primero corresponde al caso en el que se compruebe que alguno de los datos contenidos en el certificado electrónico es falso, lo que pone en entredicho la autenticidad y validez del documento firmado. Este supuesto afecta el principio de confianza pública en los medios digitales y justifica plenamente la cancelación del certificado a fin de evitar perjuicios mayores.

El segundo supuesto contempla la vulneración del sistema de seguridad del proveedor de servicios de certificación o de la autoridad certificadora raíz (UFE), en términos que afecten la integridad y confiabilidad del certificado. Esta causal responde a situaciones de intrusión informática, hackeos²⁰, brechas de ciberseguridad o fallos estructurales que comprometan la legitimidad de los certificados emitidos.

El tercer supuesto establece la posibilidad de revocación cuando el signatario da aviso de la destrucción, extravío o compromiso de su clave privada, evento que genera una vulnerabilidad directa en el proceso de firma electrónica. En este caso, el proveedor debe

²⁰ El hacking se define, en términos generales, como la explotación de vulnerabilidades en las redes y sistemas informáticos de una organización para obtener acceso no autorizado u obtener el control de los archivos digitales. (Proofpoint, s.f.)

proceder de forma inmediata a la revocación del certificado, como medida precautoria ante el posible uso fraudulento del mismo. Además, el proveedor está obligado a informar a la Unidad de Firma Electrónica para que esta también proceda a la revocación. Esta doble cadena de notificación y actuación refleja la importancia de la trazabilidad y reacción oportuna frente a cualquier compromiso de seguridad.

Por último, el artículo contempla como causal de revocación el fallecimiento o muerte presunta del titular del certificado, previa resolución judicial en los términos establecidos por el ordenamiento civil, esto es en los casos de muerte natural o muerte presunta regulados en los artículos 77 al 93 comprendidos en los Capítulos II y III del Título II, Libro I del Código Civil para el caso de las personas naturales.

“Art. 77 C.C.- La persona termina en la muerte natural.”

“Art. 79 C.C.- Se presume muerto el individuo que ha desaparecido, ignorándose si vive y verificándose las condiciones que van a expresarse.”

En caso de la “muerte” de las personas jurídicas, el certificado deja de tener validez por extinción de la personalidad jurídica del titular. Además, se prevé la revocación del certificado electrónico ante el cese de actividades o disolución y liquidación de la entidad, evento que también pone fin a su capacidad para actuar jurídicamente y suscribir documentos electrónicos con efectos vinculantes, tal como lo establecen los artículos 63 y 65 del Código de Comercio.

“Art. 63 C.Com.- La disolución no es automática. En consecuencia, las causales de disolución contempladas en este código no ponen fin por sí solas a la existencia de la sociedad, hasta que no se acuerde o reconozca la disolución por los socios, en junta general, o se pronuncie sentencia declarando la disolución (...)”

“Art. 65 C.Com.- La disolución de una sociedad incapacita a ésta para continuar la explotación de sus negocios y llevar a cabo nuevas operaciones. En consecuencia, los administradores deben suspender las actividades sociales, so pena de incurrir en responsabilidad personal, solidaria e ilimitada por la violación de este precepto.”

Este conjunto de causales configura un sistema de salvaguarda jurídica que garantiza que únicamente los certificados válidos, seguros y legalmente atribuibles se mantengan activos en el entorno digital. El artículo 60 LFE, por tanto, opera como una cláusula de “depuración” jurídica, necesaria para preservar la confianza pública en los documentos electrónicos, y asegurar la autenticidad e integridad de las firmas que se amparan en estos certificados.

En cuanto a la revocatoria del certificado electrónico por voluntad o solicitud expresa del titular del certificado electrónico, el artículo 35-A RLFE, se hará por cualquier medio establecido previamente por el Proveedor de Servicios de Certificación, donde una vez informados por el titular sobre el cese o revocatoria de su certificado electrónica, dicho proveedor tiene 24 horas para dar trámite a la solicitud y notificar la conclusión del mismo.

6. USO DE LA FIRMA ELECTRÓNICA POR ENTIDADES DE ESTADO

En El Salvador se han implementado diferentes políticas de modernización de sus Instituciones Públicas, específicamente en materia administrativa en cuanto a los trámites a realizar por los administrados, pasando de ventanillas de atención físicas a ventanillas electrónicas para requerir cierta información o documentación.

En este sentido, la LFE brinda las facilidades para la utilización de firma electrónica certificada para la agilidad de estos trámites administrativos, en atención a lo establecido en los artículos 36 y 37 RLFE.

“Art. 36 RLFE.- Incentivos de los mecanismos de gobierno electrónico.

Con excepción de aquellos trámites que necesariamente requieran la presencia del ciudadano o que este opte por realizarlos de ese modo, todos los órganos del Estado deberán incentivar el uso de documentos electrónicos, firma electrónica, sello electrónico y sello de tiempo, para la prestación directa de servicios a los administrados, así como para facilitar la recepción, tramitación y resolución electrónica de sus gestiones y la comunicación del resultado correspondiente.

Todos los órganos del Estado y demás instituciones públicas, deberán ajustar sus disposiciones a los principios de neutralidad tecnológica e interoperabilidad.

Los documentos electrónicos generados por cualquier actuación, bajo la competencia de cualquier institución del Estado, podrán ser almacenados por medio de la figura del almacenamiento por cuenta propia (...).”

“Art. 37 RLFE. Actos de las Entidades del Estado

Las autoridades, funcionarios y empleados del Estado podrán ejecutar o realizar actos y expedir cualquier documento, dentro de su ámbito de competencia, suscribiéndolos por medio de firma electrónica, con excepción de lo regulado en el inciso segundo del artículo 30 de la Ley.

Para tal efecto, los actos administrativos formalizados por medio de documentos electrónicos y que consten en decretos o resoluciones, en acuerdos de órganos colegiados y la emisión de cualquier otro documento que exprese la voluntad de un órgano o servicio público de las entidades del Estado, en ejercicio de sus potestades legales, y los documentos que revistan la naturaleza de instrumento público o aquellos

que deban producir los efectos jurídicos de estos, deberán suscribirse mediante firma electrónica certificada.

No obstante, lo anterior, las instituciones públicas podrán celebrar acuerdos o convenios interinstitucionales, dentro de los cuales podrán determinar, entre otros aspectos, el tipo de firma electrónica que habrá de utilizarse en el intercambio de información entre las instituciones involucradas.”

6.1. Tipos de uso institucional

Haciendo una diferenciación, existe una utilización por parte de las Instituciones Públicas en cuanto a los documentos electrónicos que pueden expedir, siendo que, cuando su utilización sea para uso interno de la institución, bastará la firma electrónica simple; pero para el caso de que se destine su uso hacia fuera de la institución, como es el caso de expedir algún documento a algún solicitante, deberá consignarse con firma electrónica certificada. Lo anterior en base a los artículos 29 y 30 inciso primero de la LFE.

“Uso de Firma Electrónica Certificada

Art. 30 LFE.- EN AQUELLOS CASOS EN QUE LOS FUNCIONARIOS O EMPLEADOS DEL ESTADO EXPIDAN CUALQUIER DOCUMENTO O REALICEN ACTOS ADMINISTRATIVOS EN QUE SE OTORGUEN DERECHOS, SANCIONEN, O CONSTITUYAN INFORMACIÓN CONFIDENCIAL, SEGÚN LO DISPUESTO EN EL ARTÍCULO 24 DE LA LEY DE ACCESO A LA INFORMACIÓN PÚBLICA A LOS ADMINISTRADOS, SERÁ NECESARIO UTILIZAR FIRMA ELECTRÓNICA CERTIFICADA (...)

En cuanto a la aplicación práctica de estos preceptos por parte de la Administración Pública tenemos como ejemplo el caso de “SIMPLE S.V.”, el cual es una ventanilla electrónica mediante el cuál se pueden solicitar documentos tales como constancia de antecedentes penales, de antecedentes policiales, certificación de partidas de nacimiento, entre otros. Si bien

los documentos extendidos por esta ventanilla electrónica se categorizan como firmados por firma electrónica simple al no ser creado por un Sistema Seguro de Creación respaldado por un Proveedor de Servicios de Certificación autorizado, en su lugar utilizan un código Qr el cual nos lleva a la plataforma oficial de SIMPLE S.V. en donde se puede visualizar el documento almacenado electrónicamente para poder contrastar su contenido y cumplir con el requisito de autenticidad e integridad al ser objeto de verificación, pero que para efectos legales entra en la categoría de firma electrónica simple por lo antes expuesto.

7. APLICABILIDAD DE LA FIRMA ELECTRÓNICA POR EL CNR

Otro de los ejemplos más importantes del uso de firma electrónica por parte de Instituciones Públicas es el que utiliza el Centro Nacional de Registro o CNR, Institución la cual es un ente perteneciente al gobierno de El Salvador, que garantiza los principios de publicidad, legalidad y seguridad jurídica de los registros de propiedad raíz e hipotecas, de comercio, propiedad intelectual, garantías mobiliarias, cartográficas y catastrales.

7.1. Servicios del Centro Nacional de Registros

El CNR es una de las primeras Instituciones en brindar trámites en línea, por lo que en el ejercicio de sus funciones se ha creado un sitio web oficial o ventanilla electrónica²¹ donde brinda sus servicios de manera completamente electrónica.

Dentro de estos servicios se encuentra la consulta de aranceles, inscripción de documentos de manera electrónica en los institutos de Propiedad Intelectual, Bienes raíces e hipotecas, Instituto Geográfico y del Catastro Nacional, Registro de Comercio y Registro de garantías inmobiliarias; además de servicios de consulta de información como estado de inscripción, de mapas catastrales y la expedición de certificaciones literales y extractadas de los asientos registrales, carencia de bienes, entre otros.

²¹ Plataforma oficial del Centro Nacional de Registro: <https://www.e.cnr.gob.sv/ServiciosOL/index.htm>

Sobre este punto, al ser trámites a realizar en línea, el uso de documentos electrónicos es imprescindible y, por consiguiente, también figura la utilización de la firma electrónica certificada, tanto para la presentación de documentos al realizar los trámites respectivos en la plataforma del CNR, así como en la extensión por parte de la Institución de los respectivos documentos como por ejemplo las certificaciones literales o extractadas, tal como lo establece el artículo 30 LFE antes desglosado y en el artículo 32 LFE sobre la presentación de estos documentos electrónicos por parte de los administrados.

“Interacción Electrónica entre Administrados y Funcionarios Públicos

Art. 32 LFE.- EN LAS ACTUACIONES DE LOS ADMINISTRADOS, ÉSTOS PODRÁN PRESENTAR LA INFORMACIÓN SOLICITADA POR LA ADMINISTRACIÓN PÚBLICA EN FORMULARIOS ELECTRÓNICOS OFICIALES, SISTEMAS ELECTRÓNICOS EN LÍNEA O MEDIANTE DOCUMENTOS ELECTRÓNICOS SUSCRITOS CON FIRMA ELECTRÓNICA SIMPLE O CERTIFICADA, SELLO ELECTRÓNICO O SELLO DE TIEMPO.”

Por lo tanto, los certificados electrónicos acreditados que extiende el CNR de forma electrónica tienen plena validez jurídica sin necesidad de tener dicho documento en formato físico, sino que el mero documento electrónico consignado con firma electrónica certificada goza de presunción de veracidad, así como se presume veraz la procedencia de dicho documento acorde a los establecido por el artículo 32-B LFE.

“PRESUNCIÓN DE REMITENTE

Art. 32-B LFE.- CUANDO UN DOCUMENTO ELECTRÓNICO SEA FIRMADO POR UN CERTIFICADO DE APLICACIÓN, SE PRESUMIRÁ, SALVO PRUEBA EN CONTRARIO, QUE EL DOCUMENTO FIRMADO PROVIENE DE LA PERSONA TITULAR DEL CERTIFICADO.”

8. APLICABILIDAD DE LA FIRMA ELECTRÓNICA EN LAS RELACIONES CONTRACTUALES

Atendiendo a todo lo desarrollado en el presente trabajo, una firma electrónica siempre será consignada en un documento electrónico el cual puede hacer las veces de un documento público o privado, teniendo la misma equivalencia funcional e implicando una inalterabilidad del derecho preexistente. Por lo tanto, se concluye que **la implementación de la firma electrónica es meramente una nueva opción o medio de contraer estos derechos y obligaciones al manifestar consentimiento de manera electrónica, sin implicar una modificación a lo ya establecido**. Es decir, a partir de los principios establecidos en la LFE se fijan las bases para entender la influencia de la firma electrónica certificada en las relaciones contractuales.

No obstante, es necesario precisar algunos puntos respecto a la aplicación de esta nueva modalidad de firma en relación a la forma de contraer derechos y obligaciones; y es aquí donde radica el principal uso de la firma electrónica: en el ámbito privado o comercial.

8.1. Respecto a los contratos constituidos mediante documentos privados

Los documentos privados, en base al artículo 332 CPCM, son aquellos aquellos cuya autoría es atribuida a los particulares o cuando el documento no ha cumplido las formalidades que la ley prevé para los instrumentos públicos.

Atendiendo a los artículos 3 y 4 del Código de Comercio, estos documentos, atendiendo a los sujetos y objeto del contrato en que se manifieste, pueden ser de carácter civil o de carácter mercantil. Una relación contractual será civil cuando se trate de un acto eventual y realizado entre particulares no comerciantes y cuando el objeto del contrato no es una cosa mercantil; *contrario sensu*, será mercantil cuando al menos una de las partes de la relación

contractual es comerciante o cuando ésta recaiga sobre una cosa mercantil como los títulos valores.

“Art. 3 C.Com.- *Son actos de comercio:*

I.- Los que tengan por objeto la organización, transformación o disolución de empresas comerciales o industriales y los actos realizados en masa por estas mismas empresas.

II.- Los actos que recaigan sobre cosas mercantiles.

Además de los indicados, se consideran actos de comercio los que sean análogos a los anteriores.”

“Art. 4 C.Com.- *Los actos que sean mercantiles para una de las partes, lo serán para todas las personas que intervengan en ellos.”*

En cuanto al ámbito civil, la mayoría de contratos se consignan en documentos públicos, mediante escritura matriz, requiriendo por lo general esta solemnidad. Por otro lado, en cuanto al ámbito mercantil, por regla general la mayoría de contratos se consignan en documentos privados con firma autenticada y es en este último donde se puede ver la mayor influencia de la firma electrónica certificada, ya que cualquier documento electrónico en calidad de documento privado consignado con una firma electrónica certificada, goza de presunción de veracidad, por lo que no requieren la autenticación de la firma ni del contenido por parte de un fedatario. En otras palabras, con la implementación de la firma electrónica certificada, la función pública notarial en cuanto a los documentos privados pasarían a estar en un segundo plano por la practicidad que generaría para los particulares, especialmente para los comerciantes, el celebrar este tipo de contratos vía electrónica.

Bajo este contexto, con el avance de las tecnologías surgieron diferentes medios en los cuales las personas, en virtud del Derecho Constitucional de libre comercio (artículos 22 y 102

de la Constitución), ofrecen bienes o servicios con el fin de conseguir un lucro y, por el otro lado, personas buscan determinados bienes y servicios que de forma personal o presencial no pueden o se les dificulta conseguir; es decir, hoy en día los medios electrónicos como las redes sociales son el lugar en donde las personas realizan un comercio electrónico los cuales deben de gozar de seguridad jurídica para cumplir con las medidas adoptadas por los artículos 13-C y 21-B de la Ley de Protección al Consumidor (LPC); además de evitar posibles estafas o incumplimientos por parte de cualquiera de los involucrados, quienes al ser por lo general personas cuya existencia y fiabilidad no va más allá de lo que quieren reflejar ante el público a través de sus perfiles o usuarios.

“Art. 13-C LPC.- PARA EFECTOS DE ESTA LEY, SE ENTENDERÁ COMERCIO ELECTRÓNICO, COMO EL PROCESO DE CONTRATACIÓN O INTERCAMBIO DE BIENES, SERVICIOS E INFORMACIÓN COMERCIAL A TRAVÉS DE REDES DE COMUNICACIÓN DE DATOS.

Art. 21-B LPC.- SON OBLIGACIONES ESPECIALES PARA PROVEEDORES DE BIENES Y SERVICIOS MEDIANTE COMERCIO ELECTRÓNICO DURANTE LA FASE DE CONTRATACIÓN Y POSTERIOR A ELLA, LOS SIGUIENTES:

*(...) **C) MANTENER EN MEDIOS DE ALMACENAMIENTO DE INFORMACIÓN, DURANTE UN PLAZO DE 10 AÑOS, CONTADOS A PARTIR DE LA FECHA DE LA FINALIZACIÓN DE LA TRANSACCIÓN, LA DOCUMENTACIÓN QUE CONTENGA LA PRUEBA DE LA RELACIÓN COMERCIAL, EN ESPECIAL LA IDENTIDAD PROPORCIONADA POR EL CONSUMIDOR, LAS ETAPAS CONSIGNADAS EN EL SITIO, MEDIANTE LAS CUALES SE CONSTATA LA VOLUNTAD DE CONTRATAR, DE LA FORMA EN QUE SE REALIZÓ EL PAGO Y LA ENTREGA REAL Y EFECTIVA DE LOS BIENES O SERVICIOS ADQUIRIDOS, DE TAL FORMA QUE GARANTICE***

LA INTEGRIDAD Y AUTENTICIDAD DE LA INFORMACIÓN, DE CONFORMIDAD CON LO REGULADO EN LA LEY DE FIRMA ELECTRÓNICA (...)” (El resaltado es propio)

Dentro de los contratos mediante documentos electrónicos en calidad de documentos privados que pueden celebrarse entre particulares se encuentran una amplia gama de relaciones jurídicas que se configuran voluntariamente entre sujetos de derecho, sin la intervención directa de un fedatario público, y que se plasman por escrito utilizando medios digitales conforme a los requisitos establecidos por la legislación salvadoreña según el tipo de contrato.

Entre los contratos que pueden ejecutarse por esta vía figuran, de manera ejemplificativa y no restrictiva, los contratos de compraventa de bienes muebles, especialmente en el comercio electrónico, donde el adquirente consiente la operación mediante plataformas virtuales como las redes sociales, pudiendo incluso consignarse condiciones generales del contrato que el usuario debe aceptar explícitamente mediante su firma electrónica.

También se encuentran los contratos de prestación de servicios, donde una persona natural o jurídica acuerda realizar una actividad determinada (como asesoría, diseño gráfico, programación, contabilidad, entre otros) sin que medie un documento protocolizado, pero sí respaldado por un archivo electrónico en formato PDF u otros similares, siempre y cuando se haya suscrito con firma electrónica certificada que permita verificar la autoría y fecha de la obligación asumida.

Asimismo, puede celebrarse contratos de arrendamiento de bienes muebles o inmuebles, en aquellos casos donde el objeto del contrato no requiera solemnidad, como sucede en los contratos de vivienda bajo la Ley de Inquilinato, en los cuales se exige únicamente que consten por escrito, sin que sea indispensable la autorización notarial. En tales

casos, el documento digital firmado electrónicamente por ambas partes representa un título válido que genera derechos y obligaciones exigibles, y cuya eficacia probatoria dependerá del tipo de firma empleada, sea simple o certificada, tal como se ha explicado en el respectivo apartado.

Otro ejemplo corresponde a los contratos de mutuo (préstamo de consumo) donde se estipulan montos, plazos, intereses y condiciones de devolución en un documento electrónico que puede ser validado mediante firma electrónica certificada, brindando mayor fuerza jurídica a la pretensión de pago. Igualmente, pueden celebrarse contratos de compraventa de productos digitales, licencias de uso, entre otros.

La incorporación de la firma electrónica certificada en el ámbito de los contratos mercantiles ha permitido que relaciones jurídicas tradicionalmente formalizadas de manera presencial se trasladen legítimamente al entorno digital, sin que ello implique merma alguna en cuanto a su validez, exigibilidad o fuerza vinculante. Tal adecuación opera conforme al principio de equivalencia funcional recogido en el artículo 4 literal d) de la LFE, el cual reconoce que los documentos electrónicos, debidamente suscritos mediante firma electrónica certificada, pueden generar efectos jurídicos equiparables a los documentos físicos firmados autógrafamente.

Haciendo un análisis específico, existen contratos que resultan plenamente compatibles con el uso de la firma electrónica en el marco normativo de El Salvador.

La **compraventa de bienes muebles o consumibles** son aquellas como transacciones de insumos, productos elaborados, herramientas o mercancías de rotación rápida. En estos contratos, las partes acuerdan el precio, las condiciones de entrega y los plazos de pago, elementos que pueden ser consignados en documentos electrónicos, usualmente generados en formatos estandarizados como PDF, los cuales permiten que dicha compraventa se perfeccione desde el momento en que las voluntades coinciden de forma digital. La firma

electrónica certificada, al incorporarse en estos documentos, permite identificar inequívocamente al vendedor y al comprador, dejando constancia verificable del consentimiento y la integridad del documento electrónico suscrito.

En cuanto a los **contratos de prestación de servicios** en línea, se trata de una categoría que encuentra plena operatividad en entornos digitales y cuya formalización mediante firma electrónica resulta particularmente idónea dada la naturaleza del servicio pactado. Estos servicios pueden ser de diseño gráfico, consultoría jurídica, desarrollo de software, asesoría empresarial, marketing digital, entre otros; pueden ser objeto de contratos celebrados entre partes distantes geográficamente. La utilización de firma electrónica certificada en estos documentos garantiza que las condiciones, derechos y obligaciones contraídos (honorarios, cronogramas, propiedad intelectual, cláusulas de confidencialidad, etc.) hayan sido aceptadas por ambas partes, pudiendo dicho contrato ser invocado como medio probatorio legítimo ante cualquier controversia futura.

Finalmente, los **contratos de transporte**, tanto de mercancías como de personas, presentan igualmente una estructura compatible con la firma electrónica certificada. En el transporte terrestre de carga, por ejemplo, el contrato puede establecerse entre el remitente y el transportista por medio de órdenes electrónicas de despacho, guías de carga y documentos de recepción, todos los cuales pueden ser firmados electrónicamente. La firma electrónica permite acreditar quién instruyó el traslado, bajo qué condiciones, y quién recibió la mercancía en destino, generando un sistema confiable y auditable que reemplaza la necesidad del papel físico y facilita el control logístico.

Es así como el uso de documentos electrónicos privados en las relaciones contractuales entre particulares representa una evolución natural del ejercicio de la voluntad jurídica en entornos digitales, facilitando la contratación a distancia, la simplificación de trámites, y la

reducción de costos operativos al operar de forma directa entre las partes contratantes, sin que ello implique la pérdida de seguridad jurídica, siempre que se respeten los parámetros establecidos por el Ordenamiento Jurídico salvadoreño aplicable al contrato en cuestión. Su aplicación es especialmente relevante en el comercio electrónico, en el teletrabajo, en la contratación de servicios digitales, y en cualquier tipo de acuerdo que, por su naturaleza, pueda perfeccionarse por escrito sin exigencia de forma solemne.

Por lo tanto, en estos contratos, acorde a los efectos jurídicos relacionados en los artículos 6, 8 y 25 de la LFE, mientras estén consignados con firma electrónica certificada, gozarán de presunción de veracidad siempre y cuando puedan ser verificables y presentados en modo y forma mediante soporte electrónico (CD, USB u otro Dispositivo de almacenamiento de datos que pueda soportar el documento electrónico) para tales efectos.

8.2. Respecto a los contratos constituidos mediante Instrumento Público

Los instrumentos públicos son aquellos realizados ante y por notarios quienes son delegados del Estado y su función es dar fe de los actos, contratos y declaraciones de voluntad que ante su presencia se manifiesten. El artículo 2 de la Ley de Notariado establece que dichos instrumentos públicos o instrumentos notariales son los siguientes:

- **Escritura matriz.** Es el documento original asentado en el libro de protocolo del notario.
- **Testimonio o escritura pública.** Es una copia fiel de la escritura matriz, la cual se entrega a los interesados o contratantes.
- **Actas notariales.** Documentos que recogen hechos o declaraciones, sin asentarse en el protocolo.

Respecto a la aplicación en la firma electrónica sobre estos instrumentos notariales, debe precisarse los efectos mediatos e inmediatos del mismo con el fin de esclarecer su influencia en la constitución de los contratos vía notarial de forma breve.

8.3. De los contratos digitales

Si bien es cierto que se ha mencionado la utilización de la firma electrónica en cuanto a su equivalencia funcional con los contratos plasmados en documentos privados o públicos, en la actualidad existen otro tipo de contratos (eminentemente de carácter mercantil) los cuales surgen directamente desde los medios digitales, teniendo un gran auge e impacto en el sector mercantil: el comercio electrónico.

Por tanto, en el contexto jurídico salvadoreño, la noción de *contratos digitales*²² debe entenderse como aquella categoría de actos jurídicos que, si bien conservan los elementos esenciales del contrato tradicional (consentimiento, objeto lícito y causa lícita), se configuran y perfeccionan mediante medios electrónicos, en entornos digitales, y bajo dinámicas de consumo global que trascienden las fronteras físicas del Estado. Estos contratos, celebrados a través de plataformas tecnológicas, aplicaciones móviles y sistemas automatizados, representan una evolución de las fuentes de obligaciones en donde la firma electrónica se convierte en el instrumento técnico-jurídico que permite plasmar la voluntad de las partes, garantizar la integridad del contenido contractual y dotar de validez jurídica al vínculo suscrito en el contrato.

En el plano internacional, aplicaciones como TEMU, SHEIN, Pedidos YA, Amazon, Uber Eats y otras plataformas de comercio electrónico y servicios digitales han transformado la forma en que los consumidores interactúan con proveedores de bienes y servicios. En estas

²² El contrato electrónico es un convenio entre ambas partes que se formaliza por medios electrónicos. Mediante este acuerdo legal, las partes firmantes expresan su voluntad, adquiriendo obligaciones legítimas cuyo cumplimiento puede ser exigido por ambas partes (Uanataka, s.f.).

plataformas, el contrato se perfecciona mediante la aceptación de términos y condiciones, la selección de productos o servicios, y la confirmación de pago, todo ello realizado en tiempo real y por medios electrónicos. Aunque en muchos casos no se suscribe un documento formal, el sistema genera un registro digital que contiene los elementos del contrato, y que puede ser respaldado mediante firma electrónica, especialmente en operaciones que requieren mayor trazabilidad o que involucran compromisos recurrentes, como suscripciones, garantías extendidas o servicios personalizados y cuyo precio se hace efectivo mediante valores físicos o electrónicos, es decir, mediante el pago en metálico al recibir el producto o servicio; o mediante transacción electrónica a través de tarjetas de débito o crédito.

En cuanto a la aceptación de los términos y condiciones, a la vez que la confirmación de la solicitud por parte del consumidor respecto a los productos o servicios solicitados al proveedor, se realiza mediante las plataformas proporcionados por las mismas, por lo general no se consigna firma electrónica certificada, sino firma electrónica simple, ya que la consignación de cada compra de consumo en estas plataforma se hace a través de opciones arrojados por dichas plataformas a las cuales al solo dar un clic o tap en “enviar”, “aceptar”, “confirmar pedido”, etc., se está consignando la firma electrónica simple y configurándose en ese momento el vínculo jurídico, la relación contractual.

En este mismo orden de ideas, el artículo 21-B de la LPC establece un conjunto de obligaciones específicas que deben cumplir los proveedores de bienes y servicios constituidos legalmente en El Salvador cuando operan mediante comercio electrónico, antes de que se perfeccione cualquier transacción con el consumidor, siendo los más importantes y en síntesis los siguientes:

Primeramente, los proveedores de bienes y servicios deben presentar al consumidor, antes de finalizar la transacción, un resumen detallado del pedido que incluya la descripción

completa de los productos, sus precios individuales, el total a pagar, los costos adicionales como envío, y la suma final, permitiendo al consumidor aceptarlo, corregirlo o cancelarlo, además de ofrecer la opción de imprimir o descargar dicho resumen.

Además, deben confirmar la recepción de la orden a más tardar el día siguiente, indicando el tiempo de entrega, el desglose de productos y servicios, los impuestos aplicables, los gastos de envío y el monto total.

Asimismo, están obligados a conservar durante diez años la documentación que pruebe la relación comercial, incluyendo la identidad del consumidor, las etapas del proceso de contratación, el método de pago y la entrega efectiva, garantizando la integridad y autenticidad de la información conforme a la LFE.

Finalmente, el proveedor debe entregar el pedido en un plazo máximo de treinta días calendario desde la compra; si este plazo se excede sin acuerdo previo o disponibilidad del producto, el consumidor podrá terminar el contrato unilateralmente y recibir la reversión de pago según lo dispuesto en el artículo 13-D LPC.

“Art. 13-D LPC.- CUANDO LAS VENTAS DE BIENES O SERVICIOS SE REALICEN CON PROVEEDORES LEGALMENTE ESTABLECIDOS EN EL SALVADOR MEDIANTE COMERCIO ELECTRÓNICO O CUALQUIER OTRA MODALIDAD DE CONTRATACIÓN, LOS PROVEEDORES DE BIENES O SERVICIOS DEBERÁN REVERSAR LOS PAGOS QUE SOLICITE EL CONSUMIDOR, CUANDO:

- a) EJERZA SU DERECHO DE RETRACTO;*
- b) EL PRODUCTO ADQUIRIDO NO HAYA SIDO RECIBIDO, O EL SERVICIO CONTRATADO NO HAYA SIDO PRESTADO;*
- c) EL OBJETO DEL CONTRATO NO CORRESPONDA CON LO SOLICITADO, O RESULTE DEFECTUOSO; y,*

d) *EXISTAN ERRORES EN EL COBRO DE LAS TRANSACCIONES POR FALLAS EN LOS SISTEMAS DE PAGO DE TERCEROS (...)*”

Todo lo anterior es con el objetivo de transparentar, brindar seguridad y legitimidad a las obligaciones y derechos surgidos de estos contratos digitales, haciendo contraste con establecer detalladamente qué producto o servicio se está ofreciendo (objeto lícito), con qué fin se está ofreciendo (causa lícita) y que el consentimiento plasmado con la firma electrónica simple, tal como se explicó anteriormente, sea con total certeza de qué producto o servicio se está contratando (consentimiento libre de vicios).

En cuanto al valor jurídico de la firma electrónica simple o certificada (según el caso) consignados en estos contratos digitales, ésta permite fortalecer la seguridad jurídica del consumidor, garantizar la trazabilidad de la operación y facilitar la resolución de controversias. En el caso de reclamaciones, devoluciones o disputas sobre el cumplimiento del contrato, el documento electrónico suscrito con firma certificada puede ser presentado como prueba válida ante autoridades administrativas o judiciales, gozando de presunción de autoría e integridad conforme a los artículos 6, 7 y 25 LFE. Esta presunción *iuris tantum* traslada la carga de la prueba a quien niegue la autenticidad del documento, lo que representa una ventaja significativa en contextos donde la prueba documental es determinante y en la relación de inferioridad adquisitiva del consumidor frente al proveedor o comerciante.

9. LA FIRMA ELECTRÓNICA EN MATERIA NOTARIAL

Es el caso de que en virtud del Decreto Legislativo No. 555, publicado en el Diario Oficial No. 85, Tomo 443 de fecha 07 de mayo de 2024, se promulgaron las Reformas a la Ley del Notariado (RLN) con el objetivo de, tal como consta en sus considerando, cumplir con lo establecido por el art. 36 del RLFE, configurando el deber de las entidades del Estado de incentivar el uso de documentos electrónicos, certificados y firmas electrónicas para la

prestación directa de servicios a los administrados, con el propósito de facilitar la recepción, tramitación y resolución electrónica de sus gestiones y la comunicación del resultado correspondiente; y reforzar de este modo el deber de la Sección del Notariado de la Corte Suprema de Justicia el archivo, almacenamiento y conservación de los libros de protocolo, utilizando para este fin el avance de la tecnología.

En este mismo orden de ideas, dichas reformas a **la Ley de Notariado no van destinados a la modificación de la Función Pública Notarial en principio, sino de la gestión notarial** o gestión administrativa entre los Notarios y la Sección de Notariado de la Corte Suprema de Justicia en cuanto a su control y conservación de los libros de protocolo como se mencionó en el párrafo anterior. En otras palabras y en relación con el tema del presente trabajo, estas reformas no implican un cambio en el otorgamiento de escrituras públicas o celebración de contratos vía notarial, sino sobre la entrega de los libros de Protocolo de forma digital, por lo que *a priori* se seguirán otorgando estos instrumentos de la forma tradicional en concordancia con los principios de inalterabilidad del derecho preexistente y su inequivalencia funcional, en base a los artículos 4 letra h), 7 inciso segundo y principalmente el artículo 30 LFE.

“Uso de Firma Electrónica Certificada

Art. 30 LFE.- (...) SE EXCEPTÚAN DEL USO DE LA FIRMA ELECTRÓNICA CERTIFICADA, EN AQUELLAS ACTUACIONES PARA LAS CUALES LA CONSTITUCIÓN DE LA REPÚBLICA O LAS LEYES EXIJAN ALGUNA SOLEMNIDAD QUE NO SEA SUSCEPTIBLE DE CUMPLIRSE MEDIANTE DOCUMENTOS ELECTRÓNICOS (...)”

No obstante lo anterior, la firma electrónica certificada se podrá usar en algunas circunstancias por parte de la Sección del Notariado de la Corte Suprema de Justicia en cuanto

a la extensión de testimonios públicos de forma digital, por lo que es necesario puntualizar en qué consisten algunas de estas reformas en en materia de firma electrónica.

Primeramente, el artículo 3 de los Lineamientos Técnicos para la Presentación y Resguardo de los Libros de Protocolo e Instrumentos Notariales y Arancel por los Servicios Prestados por la Sección del Notariado (en adelante llamado Lineamientos Técnicos o LT) impera como requisito la adquisición obligatoria por parte de los Notarios de adquirir un certificado electrónico de carácter profesional (si se firma como Notario, debe hacerse constar que lo es) a posteriori de conseguir el certificado de Notario activo o rehabilitado.

El Fedatario deberá presentar la siguiente documentación al PSC: Documento Único de Identidad, Tarjeta de de Identificación de la Abogacía vigente, Acuerdo de autorización para el ejercicio de la función notarial publicado en el Diario Oficial (o, en su caso, constancia de rehabilitación del ejercicio de dicha función), Constancia de notario activo o rehabilitado según sea el caso y cualquier otro requisito que se estime conveniente conforme a la ley (art. 4 LT).

En cuanto al certificado de Notario activo o rehabilitado, se podrá adquirir previa solicitud electrónica en la plataforma del Expediente Único de Abogados y Notarios, estableciendo con qué PSC se quiera adquirir la firma electrónica (artículo 5 y 6 LT).

Como segundo punto, la entrega de instrumentos notariales de forma digital: Los Notarios deberán desmaterializar (escanear a una resolución estándar de 200 DPI²³ de resolución y convertirlos en documento digital) sus libros de protocolo y anexos en dos documentos electrónicos por separado y firmarlo electrónicamente, para posteriormente ser enviados junto al índice que se realizará de forma preliminar (primero el índice y luego se

²³ En español, DPI significa puntos por pulgada (Dots Per Inch). Es una medida de la resolución de una imagen, tanto impresa como digital. Se refiere a la cantidad de puntos individuales que se pueden imprimir o mostrar en un espacio de una pulgada. Un valor de DPI más alto indica una mayor densidad de puntos, lo que se traduce en una imagen más nítida y detallada, pero ocupará mayor espacio de almacenamiento.

habilitará la opción para subir ambos archivos) en la misma plataforma creada por la Corte Suprema de Justicia para la entrega digital del libro del protocolo.

“Art. 1 RLN.- Refórmase el Art. 23 de la manera siguiente:

Art. 23 LN.- Los notarios están obligados a entregar a la Sección de Notariado, dentro de los quince días siguientes a su agotamiento o a la fecha en que termina el año de su vigencia, documento electrónico debidamente suscrito utilizando firma electrónica certificada tanto de los libros de protocolo agotados o vencidos que hubieren llevado, así como sus respectivos anexos; ambos documentos electrónicos deberán garantizar su legibilidad e integridad. El jefe de la Sección de Notariado indicará electrónicamente si son conformes o no las circunstancias expresadas en la nota de cierre a que se refiere el Art. 21. (...)”

“Art. 2 RLN.- Refórmase el Art. 24 de la manera siguiente:

Art. 24 LN.- Con los documentos anexos que hubieren de formar parte del protocolo físico, se formará un documento electrónico por separado, siguiendo el orden de los instrumentos a que corresponden. Cada uno de los documentos físicos de que consta el legajo será sellado al dorso y expresará el número del instrumento al que se refiere. El documento electrónico así formado se remitirá al mismo tiempo que el libro de protocolo respectivo. Los poderes especiales con que hubieren actuado los otorgantes que no contuvieren autorización para otros actos aun no ejecutados y los demás documentos que solo puedan servir para la celebración del acto o contrato de que se trate, se agregarán necesariamente a este legajo.”

El libro de protocolo que será entregado digitalmente deberá contener: Razón de cierre, Escrituras autorizadas y suspendidas de forma correlativa junto con sus sacas, razón de cierre y la firma electrónica consignada abajo de la razón de cierre.

Adicionalmente, el artículo 10 de los LT establece que la Oficina Regional o Sección del Notariado de la Corte Suprema de Justicia informará cuando el libro de Protocolo y Anexos están debidamente entregados y resguardados electrónicamente, por lo que dentro de los 10 días hábiles siguientes dicha notificación se deberá acudir presencialmente ante dicha sección o la oficina regional correspondiente para el embalaje del libro de protocolo y anexos en físico e impedir la suplantación o alteración de los mismos.

Un tercer punto refiere sobre la conservación física del libro del Protocolo a partir de su entrega digital, produciendo la obligación por parte del notario de conservar el libro de protocolo físico durante 15 años y la imposibilidad de extender testimonio público de estos libros una vez entregado.

“Art. 1 RLN.- Refórmase el Art. 23 de la manera siguiente:

Art. 23 LN.- (...) El notario deberá conservar los libros físicos de protocolo y demás documentos que tiene en su poder por un periodo de quince años, posterior a la entrega del documento electrónico. En todo caso, deberá presentar el libro de protocolo físico cuando la Sección de Notariado o la autoridad competente lo requiera.”

“Art. 5 RLN.- Refórmase el inciso 2° del Art. 43 LN de la siguiente manera:

Sin embargo, el notario no podrá extender ningún testimonio una vez presentado el documento electrónico del libro de protocolo. El contenido del libro y sus anexos no podrán variar de forma alguna respecto al documento electrónico entregado a la Sección de Notariado; caso contrario, dará lugar a las responsabilidades correspondientes.”

Como cuarto punto, no obstante el notario no podrá otorgar testimonio público una vez entregado digitalmente su libro de protocolo, se destaca la posibilidad por parte de la Sección

del Notariado de poderlos extender mediante documento electrónico consignado con firma electrónica certificada.

Art. 6 RLN.- Refórmase el Art. 45 de la siguiente manera:

"Art. 45 LN.- Devueltos los libros de protocolo por los notarios los testimonios serán extendidos en documento electrónico con firma electrónica certificada por el jefe o subjefe de la Sección de Notariado según el caso. Para expedir un segundo o ulterior testimonio, se deberá citar a la parte contraria en los casos en que esta formalidad sea necesaria (...)"

Como último punto, en lo relativo a las actas notariales y los testamentos nuncupativos²⁴, se deberá entregar digitalmente, en la misma plataforma que en el caso del libro de protocolo y sus anexos, una copia o testimonio respectivamente con firma electrónica certificada dentro de los 5 días siguientes a su otorgamiento.

"Art. 8 RLN.- Refórmase el Art. 47 de la siguiente manera:

Art. 47 LN.- El notario extenderá un testimonio de todo testamento nuncupativo que se otorgue ante sus oficios, el cual remitirá a la Sección de Notariado en documento electrónico con firma electrónica certificada, a más tardar, dentro de los cinco días siguientes a la fecha de su otorgamiento (...)"

"Art. 10 RLN.- Refórmase el Art. 53 de la siguiente manera:

Art. 53 LN.- De toda acta notarial que autorice, el notario estará obligado a entregar a la Sección de Notariado, dentro de los cinco días siguientes a la fecha de su

²⁴ Testamento abierto, nuncupativo o público es aquel en que el testador hace sabedoras de sus disposiciones a las personas que según la ley deben presenciarlo.

otorgamiento, copia en documento electrónico debidamente suscrito, utilizando firma electrónica certificada."

No obstante el artículo anterior, el artículo 13 LT establece que inicialmente solo serán entregados electrónicamente, en la misma plataforma del Expediente Único de Abogados y Notarios, aquellas actas que se refieran a cualquier operación o transacción de las establecidas en el artículo 9 de la Ley contra el Lavado de Dinero y Activos y el artículo 77 del Instructivo de la Unidad de Investigación Financiera para la Prevención del Lavado de Dinero y de Activos, y toda aquella que como Notario esté obligado a reportar a la Unidad de Investigación Financiera de la Fiscalía General de la República; y de las salidas del país de niñas, niños y adolescentes previa validación electrónica que efectúa la Dirección General de Migración y Extranjería.

Así es que, por todo lo desarrollado en el presente trabajo, la implementación de la firma electrónica en materia notarial no representa ninguna alteración a la Función Pública Notarial de momento, únicamente afecta en la forma en que se entregan y resguardan los Instrumentos Públicos Notariales; no obstante, tampoco se descarta la posibilidad de que más adelante se implemente, creando algún tipo de protocolo completamente electrónico, aunque para ello se debe romper la barrera puesta por el principio de inalterabilidad del derecho preexistente y del de equivalencia funcional equiparando una hoja de protocolo con un documento digital.

CONCLUSIONES

La evolución histórica de la firma como manifestación de voluntad jurídica ha sido objeto de profundas transformaciones, desde la *manufirmatio* romana hasta la consolidación de la firma autógrafa en el Renacimiento. En ese recorrido, se evidencia cómo la necesidad de validar actos jurídicos ha sido constante, y cómo la tecnología ha permitido desarrollar mecanismos más seguros y eficientes para garantizar autenticidad, integridad y trazabilidad documental. En este contexto, la firma electrónica certificada se configura como una herramienta idónea para replicar las funciones de la firma manuscrita en entornos digitales, sin alterar el contenido sustancial del Ordenamiento Jurídico preexistente.

La Ley de Firma Electrónica, en su articulado y principios rectores, establece un marco normativo que reconoce la equivalencia funcional entre la firma electrónica certificada y la firma autógrafa, siempre que se cumplan los requisitos técnicos y legales exigidos y mientras no se requieran solemnidades que únicamente puedan ser cumplidos en formato físico. Esta equivalencia no implica una sustitución absoluta, sino una coexistencia que permite ampliar las formas de manifestación de voluntad jurídica, especialmente en el ámbito contractual. La firma electrónica certificada, al estar respaldada por un certificado electrónico emitido por un Proveedor de Servicios de Certificación debidamente acreditado, permite vincular de manera exclusiva, inequívoca y verificable la identidad y consentimiento del firmante con el contenido del documento, dotándolo de presunción de veracidad e integridad conforme a los artículos 7, 8 y 25 de la LFE.

En el ámbito contractual, la firma electrónica certificada demuestra plena compatibilidad con los elementos esenciales del contrato, tales como el consentimiento libre de vicios, el objeto lícito y la causa lícita. Su uso en documentos privados permite perfeccionar contratos sin necesidad de intervención notarial, lo cual representa una evolución natural en la forma de

celebrar acuerdos jurídicos entre particulares, especialmente en el comercio electrónico, la prestación de servicios digitales, el arrendamiento de bienes muebles y otras figuras contractuales que no requieren solemnidad. Esta modalidad de contratación electrónica, además de facilitar la operatividad jurídica, reduce costos, agiliza trámites y fortalece la seguridad jurídica mediante mecanismos de verificación técnica como el código hash y el sello de tiempo.

En cuanto al valor probatorio, la firma electrónica certificada goza de presunciones legales de autoría e integridad, lo que la convierte en un medio de prueba eficaz en procesos judiciales y administrativos. Esta presunción *iuris tantum* o presunción de veracidad permite trasladar la carga de la prueba a quien niegue la autenticidad del documento, fortaleciendo la posición jurídica del firmante y del contenido suscrito. Por otro lado, la firma electrónica simple, aunque válida como medio de prueba, no goza de las mismas presunciones, lo que limita su eficacia probatoria y genera mayor incertidumbre en caso de controversia, debiéndose valorar conforme a las reglas de la Sana Crítica.

La implementación de la firma electrónica certificada por parte de entidades del Estado, como el Centro Nacional de Registro, demuestra que su uso no se limita al ámbito privado, sino que también puede fortalecer la gestión pública, la transparencia administrativa y la interacción electrónica entre ciudadanos y autoridades. Asimismo, las reformas recientes a la Ley del Notariado evidencian una tendencia hacia la digitalización de la función notarial, aunque aún limitada a la entrega y conservación de instrumentos públicos, sin alterar la solemnidad exigida para ciertos actos jurídicos.

Finalmente, se concluye que la firma electrónica certificada representa una herramienta jurídica legítima, segura y funcional para la celebración de contratos en entornos digitales, siempre que se respeten los requisitos de validez establecidos por la LFE.. No obstante, es

necesaria la capacitación de toda la sociedad y principalmente de la comunidad jurídica sobre el uso de esta nueva herramienta que aporta seguridad jurídica a los vínculos formados entre particulares y/o comerciantes al momento de adquirir y vender bienes o servicios vía contractual mediante medios electrónicos; además, la utilización de la firma electrónica opera en pro de la eficiencia y eficacia administrativa. En definitiva, al acortar distancias, trámites y relaciones interpersonales de cada individuo mediante las nuevas tecnologías de la comunicación, ante una realidad cambiante, debe haber un Derecho que se adapte a favor de los derechos individuales y de la seguridad jurídica, un Derecho *pro homine*.

RECOMENDACIONES

En atención a los resultados del presente estudio, se recomienda fomentar programas de capacitación dirigidos a notarios, jueces, abogados y operadores jurídicos sobre el uso y validez de la firma electrónica certificada, a fin de garantizar su adecuada implementación.

Asimismo, se sugiere a las instituciones públicas y privadas fortalecer la infraestructura tecnológica que permita el uso seguro y accesible de este mecanismo, garantizando la trazabilidad y verificación de los documentos electrónicos.

Finalmente, resulta necesario promover reformas complementarias que armonicen la Ley de Firma Electrónica con otras normativas civiles y notariales, asegurando un marco jurídico integral que otorgue certeza y confianza en la utilización de herramientas digitales dentro del tráfico jurídico, así como su implementación en aquellos documentos digitales en calidad de contratos en cuanto a las disposiciones que les regulen.

BIBLIOGRAFÍA

Normativa jurídica:

ASAMBLEA LEGISLATIVA, *Código de Comercio*, D. No. 671, 26 de mayo de 1970, [en línea].

San Salvador, El Salvador, D.O. No. 140, T. 228, 31 de julio de 1970. [Consulta: 04 de agosto 2025] disponible en:

https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_072920482_archivo_documento_legislativo.pdf

ASAMBLEA LEGISLATIVA, *Código Penal*, D.No. 1030, 30 de abril de 1997, [en línea]. San

Salvador, El Salvador, D.O. No. 105, T. 335, 10 de junio de 1997. [Consulta: 03 de agosto 2025] disponible en:

<https://www.uif.gob.sv/wp-content/uploads/leyes/Codigo-Penal.pdf>

ASAMBLEA LEGISLATIVA, *Ley de Firma Electrónica*, D. No. 133, 21 de octubre de 2015, [en línea]. San Salvador, El Salvador, D.O. No. 196, T. 409, 26 de octubre de 2015.

[Consulta: 04 de agosto 2025] disponible en:

<https://www.bcr.gob.sv/documental/public/docs/852c034b0b0360c624e7dd216a588d7d.pdf>

ASAMBLEA LEGISLATIVA, *Ley de Protección al Consumidor*, D. No. 776, 31 de agosto de

2005, [en línea]. San Salvador, El Salvador, D.O. No. 166, T. 368, 08 de septiembre de 2005. [Consulta: 04 de agosto 2025] disponible en:

<https://www.defensoria.gob.sv/wp-content/uploads/2021/09/Ley-de-Proteccion-al-Consumidor-AL.pdf>

ASAMBLEA LEGISLATIVA, *Reformas a la Ley de Notariado*, D.No. 555, 03 de mayo de 2024,

[en línea]. San Salvador, El Salvador, D.O. No. 85, T. 443, 07 de mayo de 2024.

[Consulta: 04 de agosto 2025] disponible en:

<https://www.asamblea.gob.sv/sites/default/files/documents/decretos/A7BBAFBA-18AD-4257-B2B4-3B14F413B276.pdf>

CORTE SUPREMA DE JUSTICIA, *Lineamientos Técnicos para la Presentación y Resguardo de los Libros de Protocolo e Instrumentos Notariales y Arancel por los Servicios Prestados por la Sección del Notariado*, Acuerdo No. 7-P, 10 de abril de 2025, [en línea]. San Salvador, El Salvador, D.O. No. 79, T. 447, 30 de abril de 2025. [Consulta: 04 de agosto 2025] disponible en:
<https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/2/2020-2029/2025/04/10A054.PDF>

ÓRGANO EJECUTIVO, Presidencia de la República de El Salvador, *Reglamento de la Ley de Firma Electrónica*, D. No. 60, 24 de octubre de 2016, [en línea]. San Salvador, El Salvador, D.O. No. 201, T. 413, 28 de octubre de 2016. [Consulta: 04 de agosto 2025] disponible en:
<https://firmaelectronica.economia.gob.sv/wp-content/uploads/2023/11/Reglamento-de-la-Ley-de-Firma-Electronica-Consolidado.pdf>

ÓRGANO LEGISLATIVO, Asamblea Constituyente, *Constitución*, D. No. 38, 15 de diciembre de 1983, [en línea]. San Salvador, El Salvador, D.O. No. 234, T. 281, 16 de diciembre de 1983. [Consulta: 29 de julio 2025] disponible en:
https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_072857074_archivo_documento_legislativo.pdf

TRIBUNAL DE ÉTICA GUBERNAMENTAL, *Ley de Ética Gubernamental*, Acuerdo No. 48, 13 de febrero de 2013, [en línea]. San Salvador, El Salvador, D.O. No. 58, T. 399, 02 de

abril de 2013. [Consulta: 02 de agosto 2025] disponible en:

<https://www.teg.gob.sv/phocadownload/Legislaciones/RELEG.pdf>

Sitios Web:

Alvarenga, F. A. (febrero. 2022). *Aplicación de la Ley de Firma electrónica a los contratos de arrendamientos en El Salvador*. Repositorio UES. [Consulta: 04 de agosto 2025]

Disponible en:

<https://repositorio.ues.edu.sv/server/api/core/bitstreams/b18abba0-f1a7-4d88-9a36-c0dbacebcca6/content>

BBC News. (julio. 2024) *Los símbolos prehistóricos que no murieron con la escritura*. BBC.

[Consulta: 09 de junio 2025] Disponible en:

https://www.bbc.com/mundo/noticias/2014/07/140714_ciencia_simbolos_arcilla_asirios_np

Consortium Legal. (2025). *Aspectos legales y tendencias del uso de la firma electrónica en Centroamérica*. Consortium Legal. [Consulta: 17 de junio 2025] Disponible en:

<https://consortiumlegal.com/2023/07/12/aspectos-legales-y-tendencias-del-uso-de-la-firma-electronica-en-centroamerica/>

EAD Trust. (enero, 2017). *Aspectos históricos de la firma – Firmadigitalizada.net*. Firma Digitalizada. [Consulta: 22 de junio 2025] Disponible en:

<http://firmadigitalizada.net/aspectos-historicos-de-la-firma/>

Economía Gobierno de El Salvador (Canal). (2025). *122 Generalidades sobre Firma Electrónica* [Video]. YouTube. Disponible en: <https://youtu.be/B7f--tnjZII?si=SfKl8BV-QNVXXJ4N>

Economía Gobierno de El Salvador (Canal). (2025). *Implementación y uso de Firma Electrónica* [Video]. YouTube. Disponible en: <https://www.youtube.com/watch?v=3diulQt1Oxg>

Firma Electrónica El Salvador (Canal). (2025). *¿Cómo se firma un documento de manera electrónica? Firma Electrónica.El Salvador* [Video]. YouTube. Disponible en:

<https://youtu.be/Peio28FlxF8?si=dU6eIN6BwHHmwyIK>

GetResponse. (2025). *Ventana emergente - qué es? | Glosario*. GetResponse. [Consulta: 10 de junio 2025] Disponible en: <https://www.getresponse.com/es/ayuda/pop-up.html>

GuruSoft. (noviembre, 2024). *Esto es lo que tienes que conocer sobre la firma electrónica en El Salvador*. linkedin. [Consulta: 12 de junio 2025] Disponible en:
<https://www.linkedin.com/pulse/esto-es-lo-que-tienes-conocer-sobre-la-firma-electr%C3%B3nica-en-wn5se/>

Kaspersky. (s.f.). *¿Qué es un código QR y cómo puedo leerlo?* Kaspersky. [Consulta: 29 de julio 2025] Disponible en:
<https://www.kaspersky.es/resource-center/definitions/what-is-a-qr-code-how-to-scan>

Ministerio de Economía de la República de El Salvador. (s.f.). *Firma Electrónica*. Firma Electrónica: Inicio. [Consulta: 17 de junio 2025] Disponible en:
<https://firmaelectronica.economia.gob.sv/>

Proofpoint. (s.f.). *¿Qué es hacking o hackear?* Proofpoint. [Consulta: 08 de julio 2025] Disponible en:
<https://www.proofpoint.com/es/threat-reference/hacking>

Signaturit Group. (marzo, 2025). *¿Qué es un hash y cómo funciona?* Signaturit. [Consulta: 02 de julio 2025] Disponible en: <https://www.signaturit.com/es/blog/que-es-un-hash/>

STRATEGIST. (2024). *Ley de Firma Electrónica en El Salvador: Digitalización Segura y Legal*. Blog Strategist. [Consulta: 17 de junio 2025] Disponible en:
<https://strategistconsult.com/la-ley-de-firma-electronica-en-el-salvador-modernizacion-y-seguridad-juridica-en-la-era-digital/>

Uanataca. (noviembre, 2021). *¿Qué es un sello electrónico (eSeal) y para qué sirve?* Uanataca. [Consulta: 02 de julio 2025] Disponible en:
<https://web.uanataca.com/es/blog/transformacion-digital/sello-electronico>

Videoteca CNJ (Canal). (2025). *Reformas a la Ley de Notariado y Lineamientos Técnicos para la presentación y resguardo de libros* [Video]. YouTube. Disponible en:
https://youtu.be/LLiPWWfY6eg?si=LVxdbn_0PU3WRhbq

ANEXOS

- Anexo 1: Proveedores de Servicios de Certificación acreditados por la Unidad de Firma Electrónica hasta la fecha (septiembre 2025).

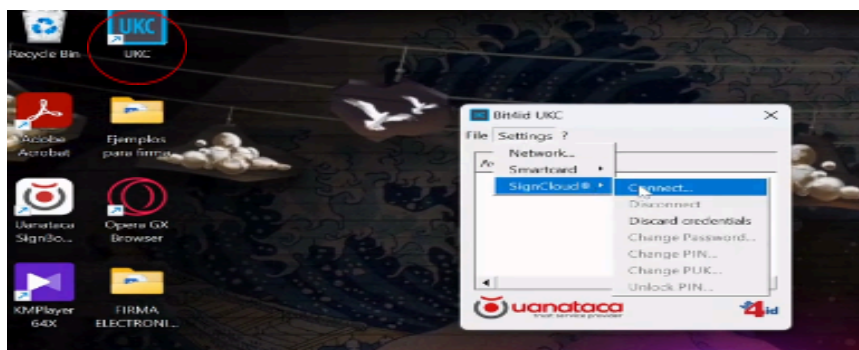
Fuente: <https://firmaelectronica.economia.gob.sv/proveedores/>

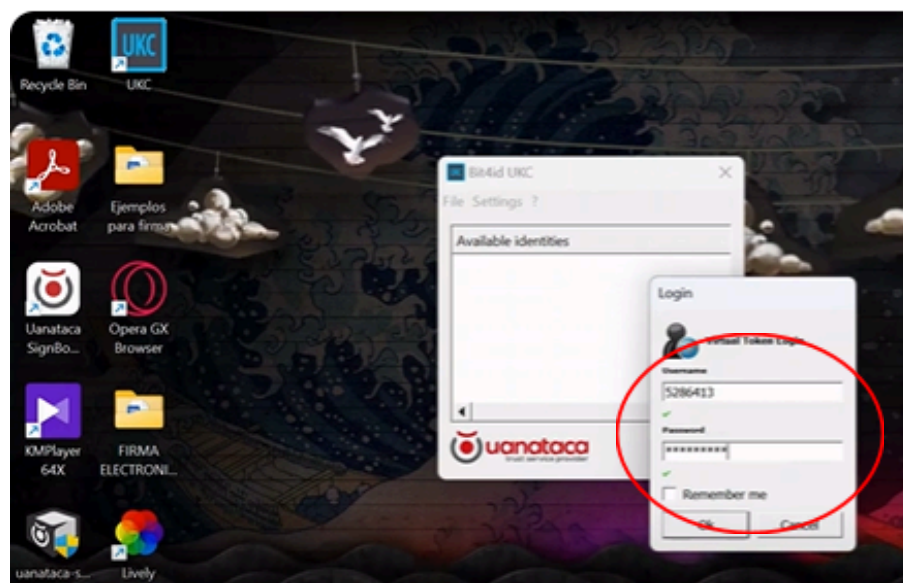
Proveedor	Servicio(s) Acreditado(s)	*Resolución de acreditación	**Identificación a distancia
UANATACA El Salvador S.A. de C.V.	Firma Electrónica Certificada y Sello Electrónico de Tiempo	UFE-001-PSC-2021 y UFE-002-TSA-2021	Autorización mediante resolución UFE-USV-CV (001/2023)
PBS El Salvador S.A. de C.V.	Firma Electrónica Certificada, Sello Electrónico y Sello de Tiempo	UFE-003-PSC-2022	Autorización mediante resolución UFE-PBS-CV (003/2022)
Banco Central de Reserva de El Salvador	Firma Electrónica Certificada, Sello Electrónico y Sello de Tiempo	UFE-004-PSC-2023	Autorización mediante resolución UFE-004-PSC-2023

Anexo 2: Pasos para consignar una firma electrónica certificada utilizando certificado cloud.

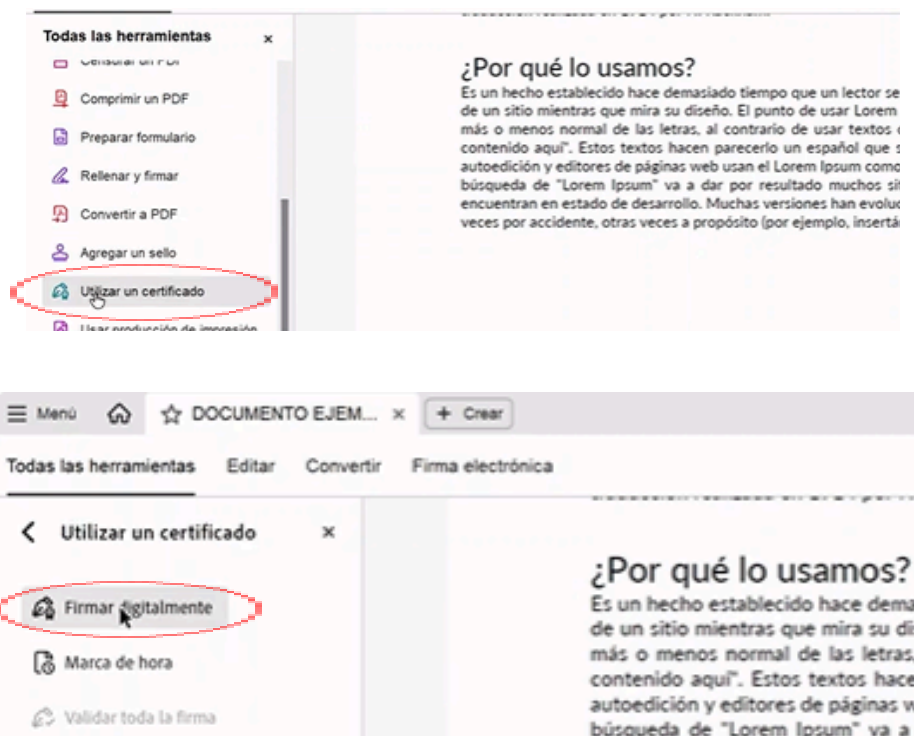
Fuente: Video de YouTube: “¿Cómo se firma un documento de manera electrónica? Firma Electrónica.El Salvador” (Canal: Firma Electrónica El Salvador). Obtenido de: <https://www.youtube.com/watch?v=Peio28FlxF8&t=2s>

- **Paso 1**: Ingresar sesión desde el Dispositivo Seguro de Creación en modalidad de certificado cloud (aplicación llamada “UKC”)

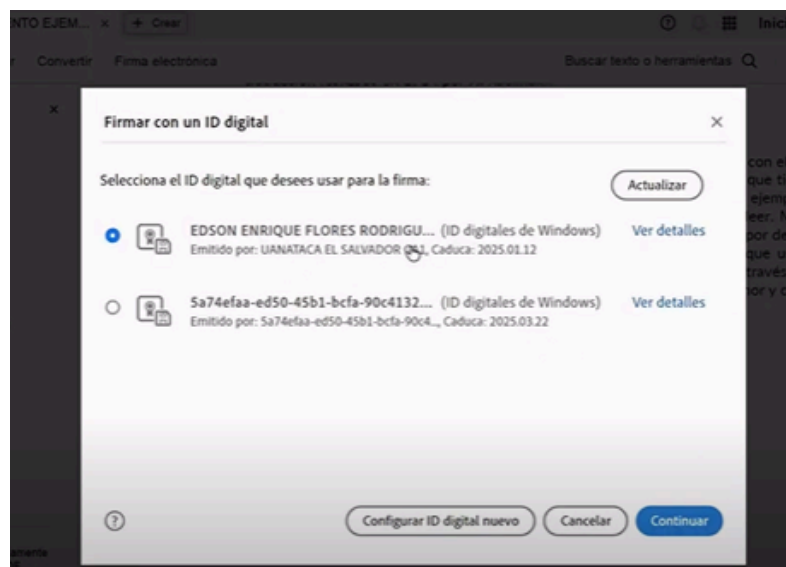




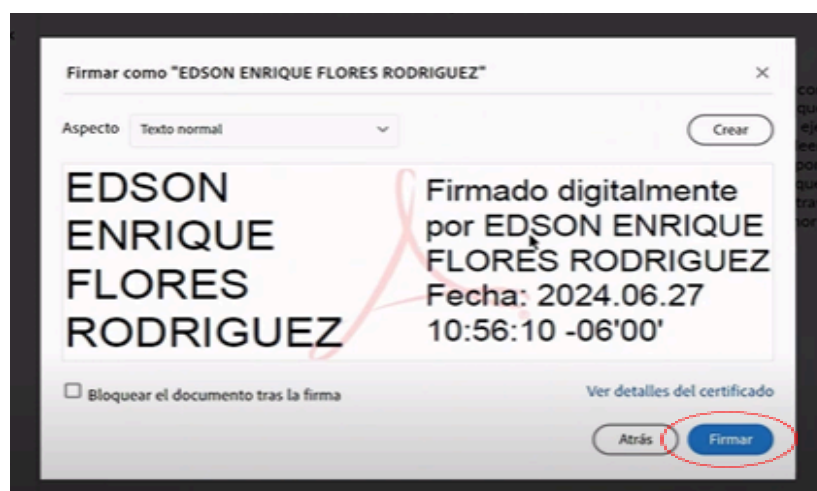
- **Paso 2:** Una vez iniciada la sesión, se debe abrir el documento electrónico que se desee consignar, preferiblemente en formato .PDF y dentro del cuál, se debe seleccionar la opción “Utilizar un certificado” y luego “firmar digitalmente”, delimitando el área en donde quiera ubicarse la firma dentro del documento.



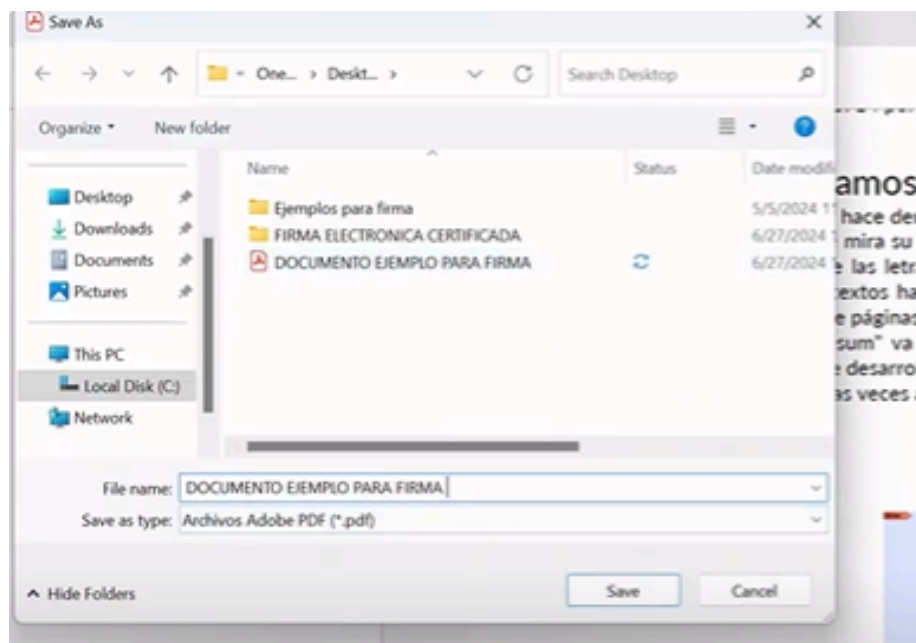
- **Paso 3:** Seleccionar el certificado que se quiera utilizar (Esto puede ocurrir, por ejemplo, cuando al adquirir el certificado electrónico se obtiene uno con perfil de persona natural y otro de representante legal de una persona jurídica; es decir, se puede firmar en a título personal o como representante legal)



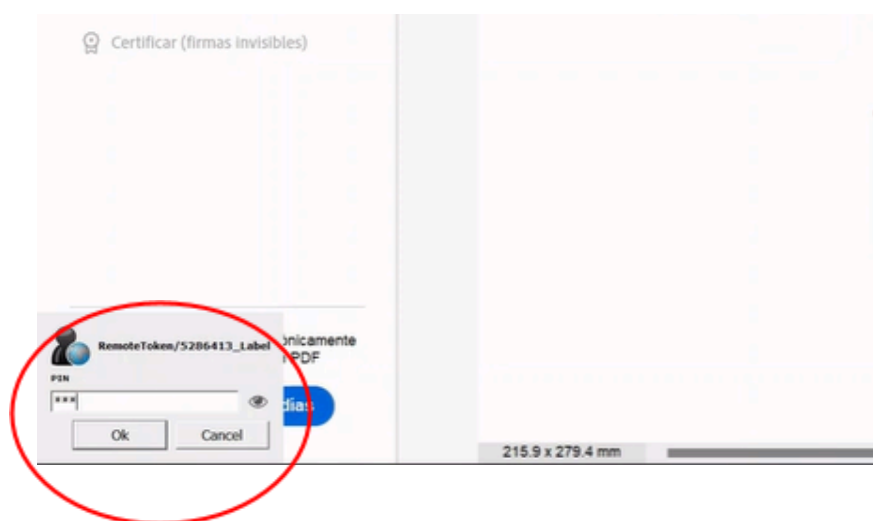
- **Paso 4:** Seleccionar la representación gráfica que tendrá la firma electrónica y seleccionar "firmar".



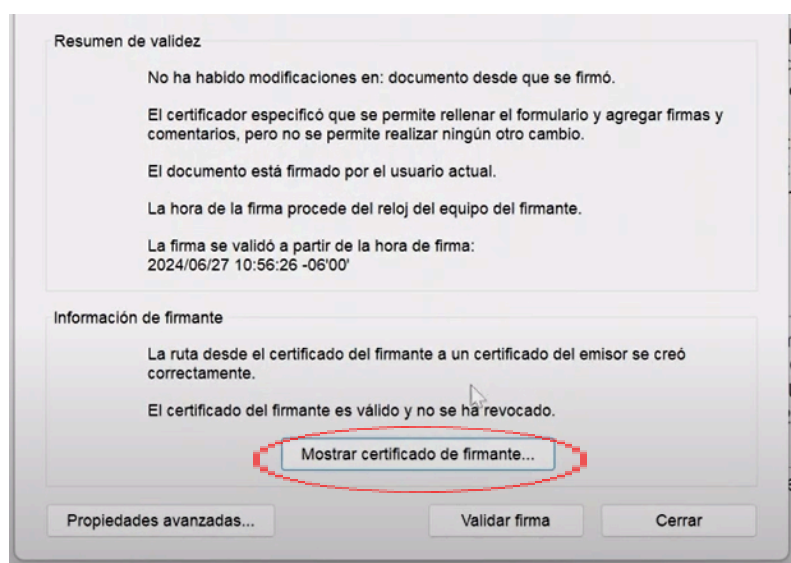
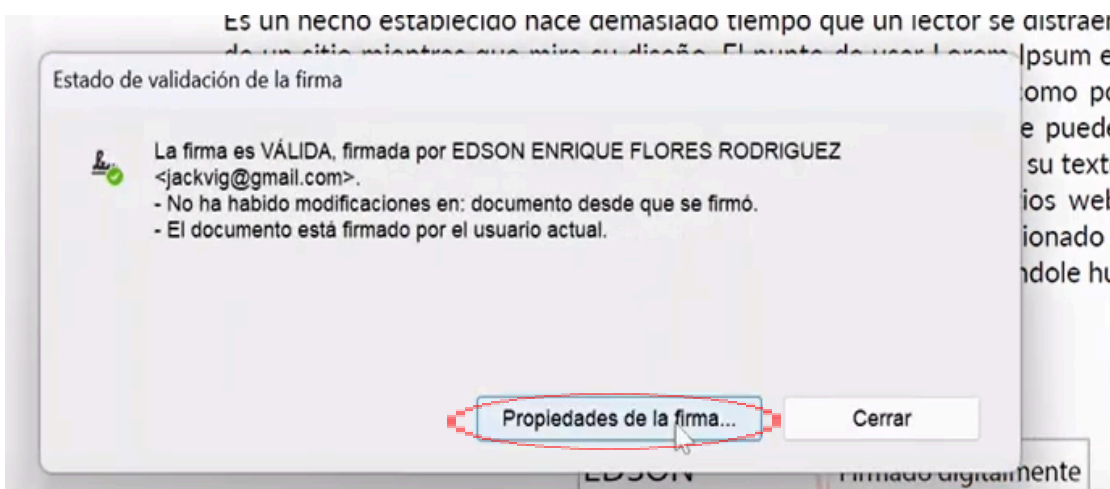
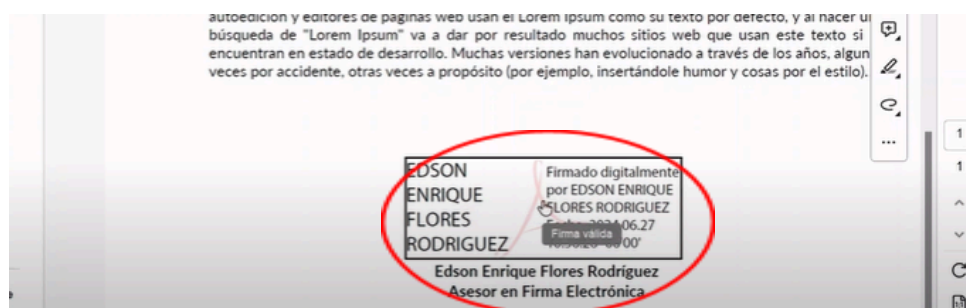
- **Paso 5:** Renombrar y guardar en el dispositivo el nuevo documento .PDF que se generará con la firma electrónica certificada ya consignada en el documento.

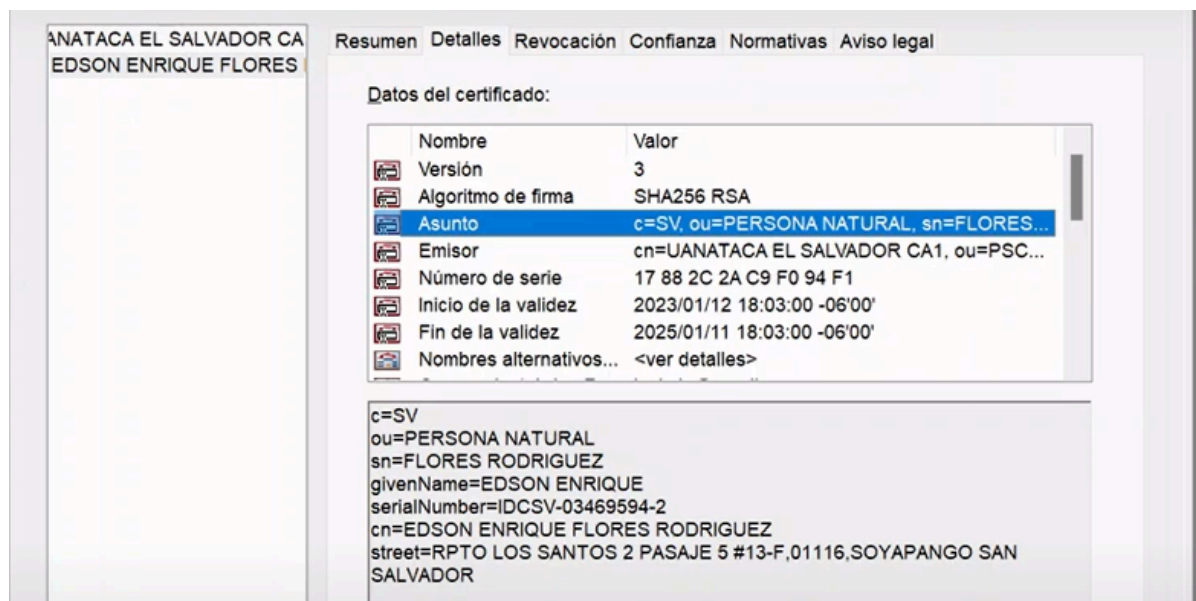


- **Paso 6:** Por último, aparecerá una ventana emergente en la esquina inferior izquierda en donde se debe ingresar el código PIN para consignar la firma en el documento.



- **Paso 7:** Para corroborar la consignación de la firma, se debe dar clic dentro de la representación gráfica de la misma, la cuál relacionará la autoría de la firma y su validez por parte del proveedor.





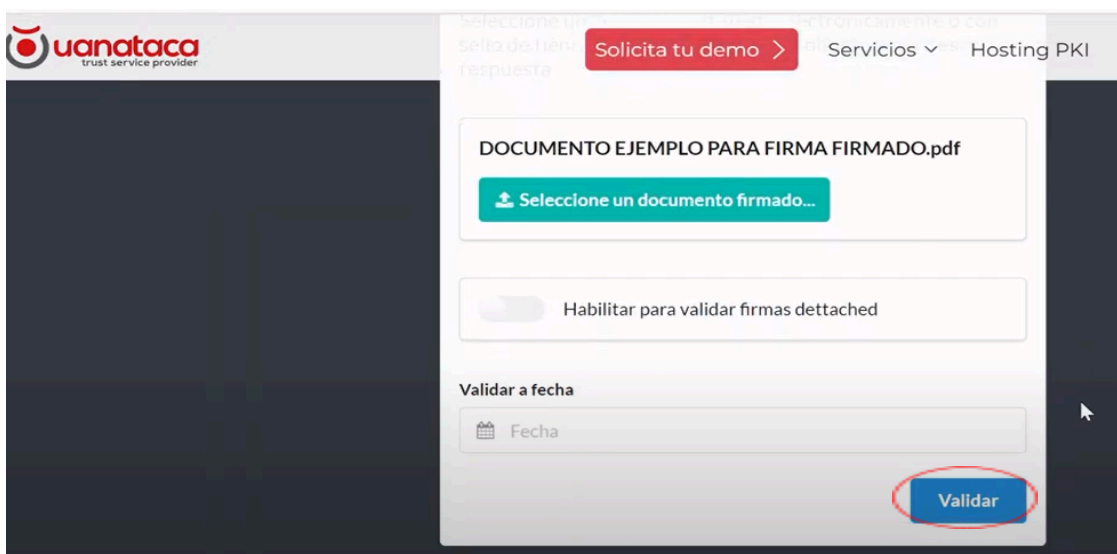
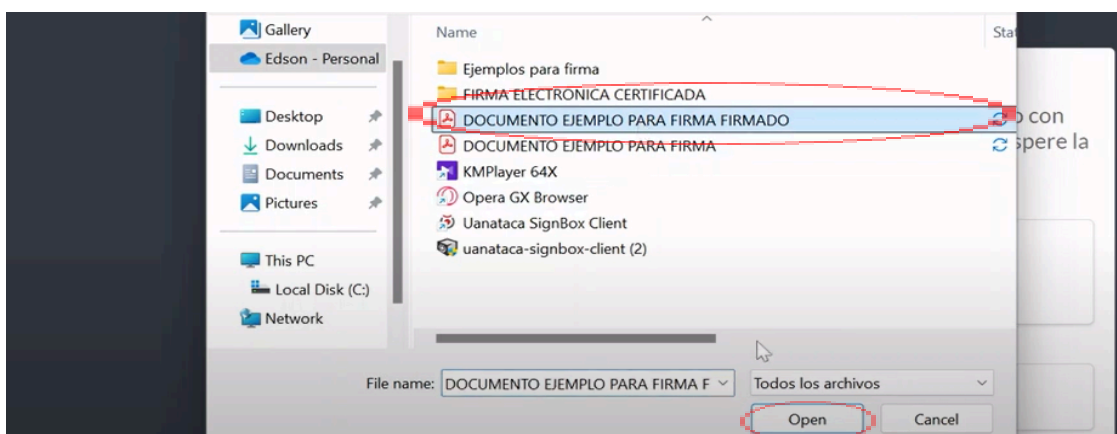
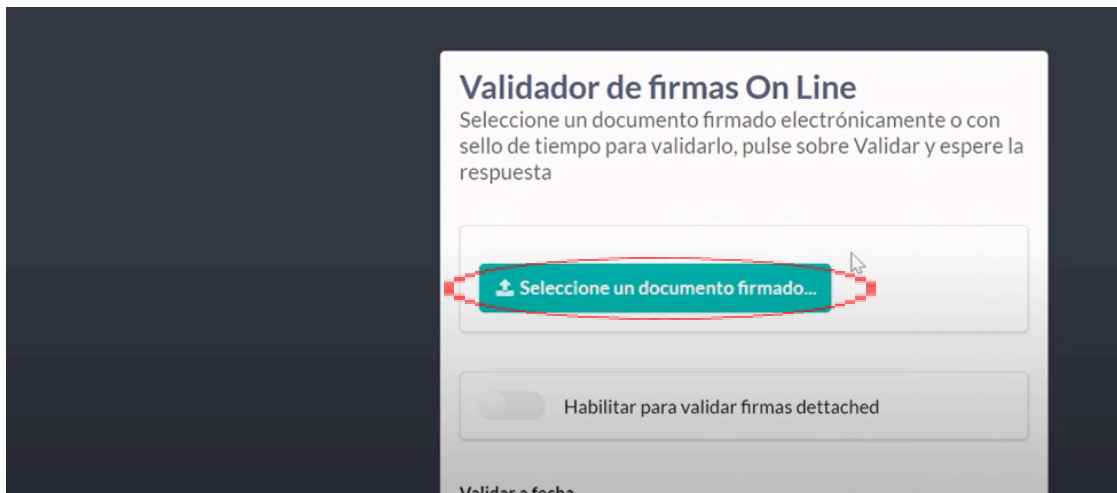
Anexo 3: Pasos para verificar la validez de una firma electrónica certificada.

Fuente: Video de YouTube: “¿Cómo se firma un documento de manera electrónica? Firma Electrónica.El Salvador” (Canal: Firma Electrónica El Salvador). Obtenido de: <https://www.youtube.com/watch?v=Peio28F1xF8&t=2s>

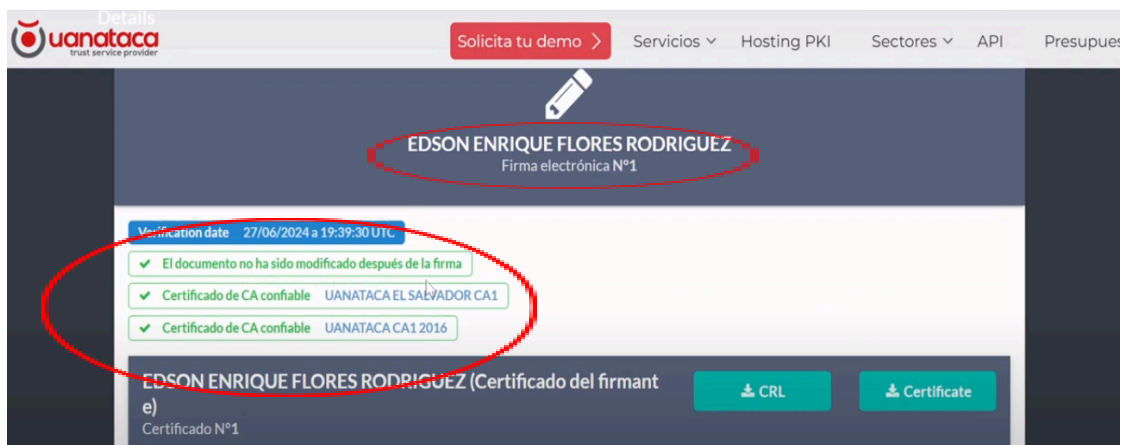
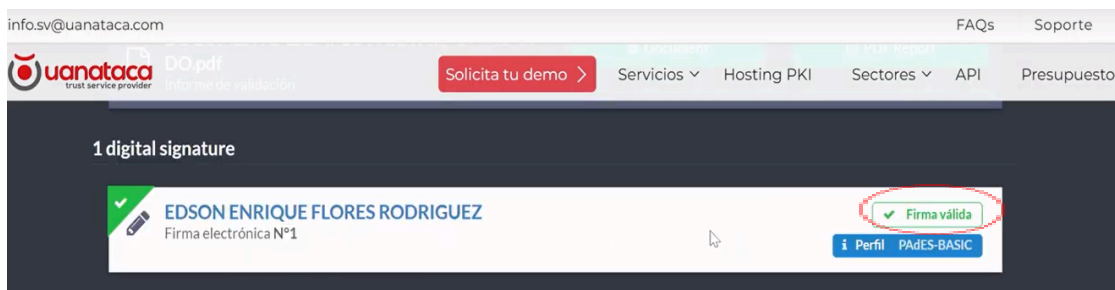
- **Paso 1:** Ingresar al sitio web oficial de la Unidad de Firma Electrónica (<https://firmaelectronica.economia.gob.sv/>) o en el del Proveedor de Servicios de Certificación, en la sección “validador de firmas electrónicas” (para este ejemplo se utilizará el del Proveedor “UANATACA S.A. de S.V.”)



- **Paso 2:** Subir el documento electrónico firmado para comprobar la validez de su firma.



- **Paso 3:** Por último, observar los datos que se mostrarán en pantalla para verificar la validez, integridad y autoría de la firma electrónica certificada, así como los demás datos del firmante contenido en su certificado.



GLOSARIO

Acta notarial: Documento público autorizado por notario que recoge hechos, declaraciones o manifestaciones de voluntad, sin asentarse en el protocolo, y que puede ser entregado digitalmente con firma electrónica certificada.

Autenticidad: Principio rector de la Ley de Firma Electrónica que garantiza que un documento electrónico proviene efectivamente del firmante, asegurando su identidad mediante mecanismos criptográficos.

Certificado electrónico: Declaración electrónica expedida por un proveedor acreditado que vincula los datos de una persona natural o jurídica con su firma electrónica certificada, sello electrónico o sello de tiempo.

Clave pública: Elemento técnico contenido en el certificado electrónico que permite verificar la autenticidad de la firma electrónica mediante el descifrado del código hash.

Código hash: Cadena alfanumérica única generada a partir del contenido de un documento electrónico, utilizada para garantizar su integridad y detectar cualquier modificación posterior.

Confidencialidad: Principio que protege los datos personales del titular de la firma electrónica, prohibiendo su divulgación sin autorización expresa.

Contrato consensual: Aquel que se perfecciona por el mero consentimiento de las partes, sin necesidad de entrega material ni solemnidad específica.

Contrato digital: El contrato electrónico es un convenio entre ambas partes que se formaliza por medios electrónicos. Mediante este acuerdo legal, las partes firmantes expresan

su voluntad, adquiriendo obligaciones legítimas cuyo cumplimiento puede ser exigido por ambas partes.

Contrato real: Contrato que se perfecciona con la entrega material del objeto, siendo esta tradición indispensable para su validez jurídica.

Contrato solemne: Contrato que requiere una forma específica exigida por la ley, como escritura pública o intervención notarial, para producir efectos jurídicos.

Documento electrónico: Información de cualquier naturaleza contenida en soporte digital y manifestada en un formato determinado, como PDF, DOCX o XML.

Documento privado: Instrumento elaborado por particulares sin intervención de autoridad pública, que no goza de fe pública pero puede adquirir valor probatorio si se suscribe con firma electrónica certificada.

Documento público: Instrumento expedido por autoridad o funcionario público en el ejercicio de sus funciones, que goza de presunción de veracidad conforme al Código Procesal Civil y Mercantil.

Dispositivo seguro de creación: Equipo o programa informático configurado para generar firmas electrónicas certificadas, ya sea mediante token físico o certificado cloud.

Equivalencia funcional: Principio que reconoce que los documentos electrónicos tienen los mismos efectos jurídicos que los documentos físicos, siempre que cumplan los requisitos legales.

Firma electrónica certificada: Conjunto de datos electrónicos generados mediante un dispositivo seguro de creación, que vinculan de forma exclusiva, inequívoca y verificable la firma con su titular y el documento suscrito.

Firma electrónica simple: Dato electrónico que relaciona al firmante con el contenido de un documento digital, sin respaldo de certificación oficial, y cuyo valor probatorio depende de la sana crítica.

Firmante o signatario: Persona natural que suscribe un documento electrónico mediante firma electrónica certificada, siendo titular del certificado correspondiente.

Función pública notarial: Actividad ejercida por notarios como delegados del Estado, consistente en dar fe de actos, contratos y declaraciones de voluntad mediante instrumentos públicos.

Integridad: Principio que garantiza que el contenido de un documento electrónico no ha sido alterado desde el momento de su firma, preservando su invariabilidad.

Neutralidad tecnológica: Principio que prohíbe la discriminación entre tecnologías, permitiendo que cualquier medio seguro y funcional pueda ser utilizado para generar firmas electrónicas válidas.

No repudio: Principio en virtud del cual el firmante no puede negar la autoría de un documento electrónico firmado conforme a los requisitos de la Ley de Firma Electrónica.


Proveedor de servicios de certificación (PSC): Entidad jurídica acreditada por la Unidad de Firma Electrónica para emitir certificados electrónicos y prestar servicios relacionados con la firma electrónica certificada.

Revocatoria del certificado electrónico: Procedimiento mediante el cual se anula la validez de un certificado electrónico por causas judiciales, administrativas o por solicitud del titular.

Sello electrónico: Dato electrónico que permite a una persona jurídica autenticar el origen y garantizar la integridad de un documento electrónico, sin implicar voluntad personal.

Sello de tiempo: Dato electrónico que acredita la fecha y hora exacta en que un documento electrónico fue firmado, emitido por el PSC para garantizar su integridad temporal del documento.

AUTOR: GERARDO ANTONIO HERNÁNDEZ TURCIOS
TODOS LOS DERECHOS RESERVADOS

A handwritten signature in blue ink, appearing to read "Gerardo", is written over a solid horizontal black line. The signature is stylized and somewhat cursive.