REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 12 (2023) • e68567 • DOI 10.5354/0719-2584.2023.68567
RECIBIDO: 16/10/2022 • APROBADO: 21/4/2023 • PUBLICADO: 28/8/2023

DOCTRINA

La prueba documental de fuentes informáticas basadas en documentos digitales con firma electrónica certificada: Un análisis desde la perspectiva de las tecnologías de la información y el principio de libertad de prueba en el proceso penal venezolano

The documentary evidence of computer sources based on digital documents with certified electronic signature: An analysis from the perspective of information technologies and the principle of freedom of proof in the Venezuelan criminal procedure

Carlos Alfonso Acosta-León
Universidad Central de Venezuela y Universidad Católica Andrés Bello, Venezuela

RESUMEN Los mensajes de datos que fluyen masivamente a través de internet se han constituido en documentos que prueban conductas, actos consensuales y negocios jurídicos, o la comisión de delitos informáticos. Este artículo presenta los fundamentos tecnológicos y jurídicos del documento digital firmado electrónicamente y su incorporación al proceso penal venezolano usando el medio de prueba documental, con base en la libertad de prueba. Además, muestra cómo el marco jurídico venezolano le otorga los efectos jurídicos, la integridad y autenticidad que el medio de prueba documental requiere para ser valorada por el juez o jueza. Se concluye que una vez incorporado como prueba documental electrónica al proceso penal, si esta es desconocida o tachada de falsa por la parte contraria entonces debe ser evacuada mediante una experticia informática para determinar su valor probatorio.

PALABRAS CLAVE Documento digital, firma electrónica, prueba documental, libertad de prueba, proceso penal de Venezuela.

ABSTRACT The data messages that flow massively through the Internet have become documents that prove behaviors, consensual acts and legal business, or the commission of computer crimes. This article presents the technological and legal foundations of the electronically signed digital document and its incorporation into the Venezuelan criminal procedure using the means of documentary evidence, based on the freedom of proof. In addition, it shows how the Venezuelan legislation gives them the legal effects,

integrity and authenticity that the means of documentary evidence requires to be valued by the judge. It is concluded that once incorporated as electronic documentary evidence to the criminal procedure, it must be examined by means of a computer expertise to determine its probative value.

KEYWORDS Digital document, electronic signature, documentary evidence, freedom of proof, Venezuelan criminal procedure.

Introducción

En la actual sociedad digital y del conocimiento existe un creciente auge de las tecnologías de la información (TI) producto de diversos paradigmas emergentes, como, por ejemplo, las criptomonedas, el *blockchain*, el comercio electrónico, las redes sociales, los grandes volúmenes de datos, los servicios en la nube, la inteligencia artificial, etcétera (Joyanes Aguilar, 2015: 44-169). Estos paradigmas cambian la dinámica de la educación, la ciencia, la tecnología, la medicina, la industria, los servicios, la administración pública, la banca y las finanzas, las empresas, el comercio, el derecho, etcétera (Fugini y otros, 2019: 76).

Esta realidad se evidencia a diario cuando enviamos y recibimos mensajes de datos en forma de correos electrónicos, mensajes por telefonía celular, por mensajería instantánea, a través de redes sociales, cuando escuchamos música o vemos películas en transmisión digital en tiempo real. Además, cuando creamos y editamos documentos en el computador usando programas de edición o aplicaciones. De la misma manera, cuando registramos una cuenta o subimos comentarios a una página web o almacenamos datos y documentos en nuestros dispositivos como teléfonos inteligentes, tabletas, computadores o memorias *flash*; o elementos de almacenamiento pasivo, discos duros convencionales y los nuevos de estado sólido, la nube, etcétera.

Esto promueve una constante creación, flujo e intercambio de mensajes de datos, particularmente documentos digitales con y sin firmas electrónicas, producto de las diversas interacciones sociales, jurídicas, económicas, etcétera, susceptibles de efectos jurídicos que tienen lugar en internet y el ciberespacio.

Las estadísticas, hasta el 2021, muestran que un 62,5% de la población mundial tiene acceso y uso de internet y demás tecnologías de la información. Esto con base en el reporte de la Unión Internacional de Telecomunicaciones[1] y mostradas con más detalle por el Grupo Yi-Min Shum,[2] que indican un comportamiento generalizado,

1. Unión Internacional de Telecomunicaciones, «Datos y análisis. Estudio de la sociedad de la información», disponible en https://bit.ly/42P4iOa.

2. Grupo Yi-Min Shum, «Situación digital (abril 2021). Internet, social media, estadísticas». Disponible en https://bit.ly/3Ng1O5z.

particularmente, del uso del documento digital. De igual forma, la Comisión Económica para América Latina y el Caribe (Cepal)[3] en sus indicadores refleja un aumento sostenido del uso de las TI, tanto por el sector público gubernamental como el sector privado latinoamericano.

Pero un reconocimiento mayor a esta realidad es cuando la Asamblea General de la Organización de las Naciones Unidas en junio de 2016 declara, aunque no de forma vinculante, el acceso a internet y al ciberespacio, así como de otros derechos inherentes al uso de esta tecnología como el derecho a la protección de los datos personales en formato digital, a la propiedad intelectual de las obras en formato digital, etcétera.[4]

En este escenario, el derecho ha ido asimilando las TI como un medio para automatizar y mejorar la eficiencia y eficacia de la administración de justicia. Es así como los documentos digitales, en especial aquellos firmados electrónicamente, se han constituido en instrumentos de prueba de conductas y actos consensuales con valor y eficacia jurídica. En particular, son útiles como fuentes digitales o informáticas para trasladar al proceso judicial la demostración de hechos alegados por las partes a través del medio de prueba documental.

En Venezuela, el documento digital, los certificados electrónicos y la firma electrónica están regulados para hacerlos trascendentes a la administración privada y pública, especialmente de justicia. Esto con el fin de que puedan apreciarse y valorarse para garantizar los negocios jurídicos y sus respectivas obligaciones, así como evidencias de comisión de delitos tanto tradicionales como informáticos.

En este sentido, el propósito del artículo es examinar de forma integral la relación entre: a) los fundamentos informáticos del funcionamiento del documento digital y la firma electrónica generada con un certificado digital o electrónico válido; b) los principios de neutralidad tecnológica y de equivalencia funcional usados para adoptar el documento digital y la firma electrónica en la legislación venezolana, así como la fuente normativa que regula sus efectos jurídicos, y c) el valor probatorio del documento digital con firma electrónica certificada como medio de prueba documental en el proceso penal venezolano y su proceso de validación mediante una experticia informática.

Además, esta investigación constituye una fuente útil para que el abogado litigante conozca los aspectos tecnológicos y jurídicos del documento digital y la firma electrónica certificada. También, para que comprenda el procedimiento de experticia técnica informática como método para verificar la integridad y autenticación del documento digital con firma electrónica certificada y así determinar su valor probatorio

3. Cepal, «Una mirada regional al acceso y tenencia de tecnologías de la información y comunicaciones - TIC, a partir de los censos», disponible en https://bit.ly/3Nea9XD.

4. Organización de las Naciones Unidas, «Promoción, protección y disfrute de los derechos humanos en internet», 27 de junio de 2016, disponible en https://bit.ly/3qXKeM5.

como medio de prueba documental. Por último, para que entienda las ventajas del uso de la criptografía de clave pública con respecto a la integridad, autenticidad, no repudio y confidencialidad, como aspectos esenciales para que el documento digital firmado electrónicamente pueda ser valorado por el órgano jurisdiccional.

Es oportuno aclarar que el objeto de estudio se delimita a los documentos digitales, los certificados y las firmas electrónicas como mensajes de datos. De estos mensajes, unos son producto del intercambio automático entre los sistemas informáticos como parte de su interoperabilidad y protocolos de comunicación. Otros, los que se abordan acá, son producto de la interacción humana en forma de documentos digitales o electrónicos en términos jurídicos, útiles y pertinentes como fuente de prueba. De igual manera, la firma electrónica bajo estudio es la generada con un certificado electrónico emitido por un proveedor de servicios de certificación electrónica acreditado por la Superintendencia de Servicios de Certificación Electrónica.

Por último, el estudio tiene como premisa el principio de libertad probatoria, establecido en los artículos 395 del Código de Procedimiento Civil (CPC) de 1990 y 182 del Código Orgánico Procesal Penal (COPP) de 2021. En fin, el documento digital y la firma electrónica se analizan en el contexto de la libertad probatoria y el medio de prueba documental en el proceso penal de Venezuela.

Antecedentes de investigación

En Venezuela, un trabajo reciente relacionado es el artículo de Chacón y Proaño (2021), en el que las autoras estudian la prueba electrónica como medio para probar obligaciones mercantiles desde que son contraídas hasta que son extinguidas, haciendo énfasis en el valor del documento con firma electrónica. También, hacen una revisión del principio de equivalencia funcional y su significación en la prueba electrónica de obligaciones mercantiles.

Otro artículo es de González Torres (2020) en el que se revisa la incorporación del documento electrónico en la actividad probatoria del proceso civil ordinario venezolano, tratándolo como mensajes de datos, como refiere el Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas (2001).

Más trabajo es el artículo de Marín Meilán (2018) en el que el autor hace un análisis general del valor probatorio del documento electrónico en la legislación venezolana y aborda las pruebas basadas en medios electrónicos en las etapas de la actividad probatoria del sistema procesal de Venezuela, excepto del penal. Para ello, hace una revisión de la doctrina, triangula la opinión de varios autores, explica los procedimientos establecidos en el Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas (2001) y el Código de Procedimiento Civil (1990) y cita jurisprudencia del Tribunal Supremo de Justicia con respecto a la validez jurídica de los

medios electrónicos y su valor probatorio. Al final, hace un breve estudio comparado con legislaciones de otros países.

En Hispanoamérica, autores como Jiménez y Caballero (2019) investigan los efectos de la firma electrónica avanzada sobre el mensaje de datos y su valor probatorio en el proceso judicial de México. Para ello, describen el proceso de confianza del sistema de certificación electrónica donde los proveedores de servicios de certificación participan como terceros de confianza y proveen las propiedades de seguridad asociadas a esta tecnología. También, hacen un análisis de los elementos de existencia y requisitos de validez del consentimiento, voluntad y reconocimiento legal de la firma cuando se emite de forma digital o electrónica, óptica o con cualquier otra tecnología. Estos resaltan la importancia de la aplicación del principio de equivalencia funcional y de neutralidad tecnológica en el área jurídica.

Otro trabajo es el artículo de Ortiz y Jacome (2019) donde hacen un análisis crítico del ordenamiento jurídico de Colombia, el cual consideran desfasado con respecto a los avances de las nuevas tecnologías. Ellas opinan que la regulación de la prueba electrónica es vaga, simple e inconsistente, lo que incide negativamente en la actividad probatoria. Las autoras hacen una revisión del marco legal colombiano asociado al concepto de prueba electrónica, documento electrónico y mensaje de datos para determinar la pertinencia de la valoración de este tipo de pruebas y resaltan sus diferencias mutuas; con base en los requisitos legales de la prueba electrónica en Colombia.

Un trabajo interesante sobre la aplicación de las tecnologías de la información en el proceso judicial se expone en el artículo en línea del doctor Claudio Meneses Pacheco (2014),[5] profesor de Derecho Procesal de la Universidad de Valparaíso de Chile. En este artículo el autor analiza el uso del documento digital y la firma electrónica en la sustanciación de procesos judiciales penal y civil. En ese momento, las principales regulaciones estaban consagradas en el Acta 91-2007 del 7 de junio de 2007, que fija el texto refundido sobre procedimientos en los tribunales que tramitan con carpeta electrónica, y en el Acta 25-2009 del 30 de enero de 2009 (modificada por medio del Acta 40-2014 del 14 de marzo de 2014), que establece disposiciones sobre el uso de documento y firma electrónica en el Poder Judicial. Asimismo, el estudio resalta los actos de la Corte Suprema de Chile, como máximo tribunal de la República, que implementa, a partir del marco jurídico chileno, los procedimientos de los tribunales para la tramitación judicial de la carpeta o expediente electrónico. De estas, una regulación relevante es la Ley 19.799 de 2002, referida a los documentos electrónicos, la firma electrónica y los servicios de certificación de dicha firma. Sin embargo, fuera del alcance de este artículo existe otra regulación posterior, la Ley 20.886, del 18 de

5. Claudio Meneses Pacheco, «El expediente electrónico en los procesos civiles», *Instituto Chileno de Derecho Procesal*, 12 de mayo de 2014, disponible en https://bit.ly/468YVfw.

diciembre de 2015, que aborda la reciente reforma sobre tramitación electrónica de las causas civiles, la cual modifica el Código de Procedimiento Civil de la República de Chile, para establecer la tramitación digital de los procedimientos judiciales, y que se complementa por los autos emitidos por la Corte Suprema contenidos en las Actas 37-2016 y 71-2016, los cuales determinan el estado actual del proceso civil chileno en esta materia.

En otro trabajo, Olmos García (2017) analiza la prueba electrónica en el contexto del proceso civil de España. El autor se concentra en su incorporación al proceso, así como en la cadena de custodia para su conservación y verificación mediante la prueba pericial para garantizar su integridad y autenticidad. En particular, revisa la incorporación al proceso civil de correos electrónicos, mensajes de texto (SMS) o de Whatsapp a través de medios de prueba similares al documento con soporte de papel. También, analiza la relación entre la obtención de la prueba digital y el respeto de ciertos derechos fundamentales como a la intimidad, la protección de datos personales y el secreto de las comunicaciones, para que se tome en cuenta por el órgano jurisdiccional competente.

Por último, en un artículo de Marianella Ledesma Narváez (2016) se aborda la prueba documental electrónica en la legislación peruana, donde hace una diferencia entre medio de prueba y fuente de prueba, y resalta la relevancia de la prueba documental cuando tiene como soporte la tecnología informática. Explica, además, que la prueba electrónica puede generar suficiente grado de certeza jurídica cuando se emplea adecuadamente la informática en la actuación pericial para producir fiabilidad.

Las tecnologías de la información como fundamento del documento digital y la firma electrónica certificada

Las tecnologías de la información como internet, el ciberespacio, las telecomunicaciones digitales, la informática y la computación se han constituido en una plataforma global de herramientas necesarias e imprescindibles para las personas y la sociedad a nivel mundial en el quehacer diario, individual y colectivo, del sector público y privado.

Según el glosario tecnológico de la Unesco, el término tecnologías de la información[6] alude a las tecnologías asociadas a internet, el ciberespacio y todas aquellas herramientas tecnológicas producto de la electrónica, la informática y la computación. En este particular, Joyanes Aguilar (2015: 2) afirma que:

> Los sistemas de información recogen o reúnen, procesan, almacenan, analizan y distribuyen la información para un propósito u objetivo específico. El conjunto

6. Unesco, «Glosario de términos: Tecnologías de la información», *Media & information literacy for teachers*, disponible en https://bit.ly/46hlWwL.

de sistemas de computación utilizados por una organización o empresa se conocen como tecnologías de la información (TI) en sentido general o también tecnologías de la información y la comunicación (TIC) cuando se desea especificar y citar expresamente los soportes de comunicación.

Una definición más detallada de las TI incluye computadores, redes de computadores, dispositivos y *software* de interconexión de red, dispositivos móviles, aplicaciones, sistemas de información, *software* y *hardware*, sistemas de telecomunicaciones, etcétera, que permiten la captura, procesamiento, almacenamiento, comunicación y resguardo de datos, información y conocimiento en formato digital o binario. Pero, además, incluyen otras herramientas como los métodos y técnicas de desarrollo de *software*, procesos y procedimientos de administración y gestión de sistemas, algoritmos, etcétera, que complementan y determinan los aspectos operativos, usos y beneficios de las TI.[7]

Naturaleza informática del documento digital o electrónico

El término mensajes de datos hace referencia a documentos, certificados y firmas (indistintamente si son electrónicos o digitales) tanto en forma inteligible (texto claro) como no inteligible (texto cifrado). En internet y el ciberespacio, este flujo continuo de mensajes de datos representa una jerarquía semántica de documentos donde los «datos, información y conocimiento (con un cuarto nivel considerado por muchas escuelas y expertos, la sabiduría) son el soporte de los sistemas de información» (Joyanes Aguilar, 2015: 2).

Al respecto, de acuerdo con el *Diccionario de las ciencias de la información*,[8] los datos representan valores o símbolos de hechos sin contexto, mientras que la información es la semántica o significado que se atribuye a dichos datos (contexto, propósito, relevancia) con utilidad para tomar decisiones y, actualmente, el conocimiento es lo que se desprende del conjunto de relaciones que se establecen entre datos, información y experiencias, lo que permite una mejor toma de decisiones.

Como antecedente, los actuales avances de las TI han sido principalmente el resultado de un proceso evolutivo desde las décadas de los cincuenta y sesenta, en *hardware* y *software*, de áreas asociadas a la electrónica, las matemáticas, la informática y las ciencias de la computación. Con respecto a esta evolución, Stallings (2006: 18-30) hace un recorrido histórico por generaciones tecnológicas, donde la tecnología del *hardware* de computadores ha evolucionado desde sistemas mecánicos y eléctricos, al principio, pasando por la electrónica de tubos de vacío, el diodo, el transistor y

7. Tal como se expone: Livia Gershon, «What is information technology (IT)?», *Universidad de Nueva Hampshire del Sur*, 11 de agosto de 2022, disponible en https://bit.ly/3JqihTC.

8. Joan M. Reitz, «Dictionary for library and information science», disponible en https://bit.ly/3JSRobl.

los circuitos integrados, hasta los sistemas electrónicos analógicos y digitales de hoy, cuya tecnología de fabricación se basa en la microelectrónica de semiconductores o de estado sólido.

Esta tecnología microelectrónica es la base del diseño e implementación de circuitos integrados, microprocesadores, dispositivos, sistemas y computadores electrónicos analógicos, donde la información se representa como un fenómeno continuo en tiempo y espacio, y los digitales, donde la información se representa como un fenómeno discreto, generalmente binario de estados «0» o «1», discontinuo en tiempo y espacio.

Las instrucciones, los datos, la información y el conocimiento que los computadores capturan, almacenan, manipulan, procesan e intercambian se representan con un sistema numérico en base 2. Este sistema usa un dígito o bit, el cual toma solo dos valores, 0 y 1, pero que, agrupados en palabras o cadenas (múltiplos de 8 bits o bytes), permiten representar cualquier carácter, número y símbolo, y es denominado código binario o digital.

Como ejemplo, en la **figura 1** se muestra un circuito eléctrico para representar un bit que puede tomar dos estados: el estado «1» (uno), cuando el circuito está cerrado (estado de conducción de corriente), y el estado «0» (cero), cuando el circuito está abierto (estado de no conducción de corriente). De esta manera, con distintas combinaciones de cadenas de bits de unos y ceros, es posible representar en un computador datos, información y conocimiento en forma de números, caracteres, símbolos, voz, imágenes, videos, etcétera, además de operaciones matemáticas, simples y complejas, que permiten al computador electrónico digital el procesamiento cuantitativo y cualitativo de datos, información y conocimiento.

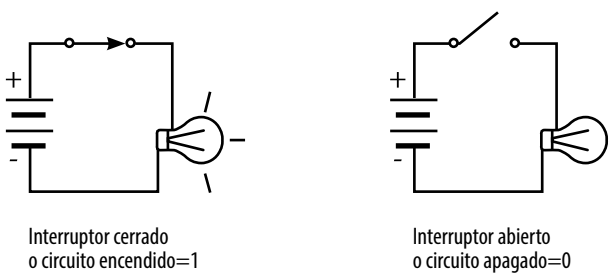

Figura 1. Circuito eléctrico que emula la lógica binaria. Fuente: Elaboración propia.

En efecto, como afirman Angulo y García (2007: 67), «las computadoras están hechas de dispositivos de conmutación que reducen toda la información a ceros y unos, representan números utilizando el sistema numérico binario, un sistema que denota todos los números con combinaciones de dos dígitos». Como consecuencia, el lenguaje usado por los sistemas informáticos es el binario, en *hardware* y en *software*, para representar números, caracteres y símbolos en forma de datos, información y conocimiento, el cual define el lenguaje nativo o de máquina del computador.

Esta representación binaria tiene al menos dos niveles de abstracción: a) un bajo nivel de abstracción asociado a la representación física de estos bits, como campos magnéticos, eléctricos, electromagnéticos, electrostáticos o electrónicos, sobre un soporte informático; y b) un alto nivel de abstracción asociado a la representación conceptual o virtual de estos bits en la forma como el humano percibe y entiende los objetos en el mundo real, en lenguaje natural.

Una forma de abstracción que busca una primera aproximación a un lenguaje natural de comunicación humana es el asociado a la representación de caracteres alfabéticos, numéricos, gráficos, especiales y demás símbolos con tablas estándar de códigos binarios. Un ejemplo es el actual estándar Unicode, otro el antiguo estándar ASCII (**tabla 1**).

Tabla 1. Tabla ASCII 8 *bits*.

Caracter	Código binario	Caracter	Código binario	Caracter	Código binario
A	0100 0001	a	0110 0001	!	0010 0001
B	0100 0010	b	0110 0010	"	0010 0010
C	0100 0011	c	0110 0011	#	0010 0011
D	0100 0100	d	0110 0100	$	0010 0100
E	0100 0101	e	0110 0101	%	0010 0101
F	0100 0110	f	0110 0110	&	0010 0110
G	0100 0111	g	0110 0111	'	0010 0111
H	0100 1000	h	0110 1000	(	0010 1000
I	0100 1001	i	0110 1001	)	0010 1001
J	0100 1010	j	0110 1010	*	0010 1010
K	0100 1011	k	0110 1011	+	0010 1011
L	0100 1100	l	0110 1100	,	0010 1100
M	0100 1101	m	0110 1101	-	0010 1101
N	0100 1110	n	0110 1110	.	0010 1110
O	0100 1111	o	0110 1111	/	0010 1111
P	0101 0000	p	0111 0000	0	0011 0000
Q	0101 0001	q	0111 0001	1	0011 0001
R	0101 0010	r	0111 0010	2	0011 0010
S	0101 0011	s	0111 0011	3	0011 0011

Caracter	Código binario	Caracter	Código binario	Caracter	Código binario
T	0101 0100	t	0111 0100	4	0011 0100
U	0101 0101	u	0111 0101	5	0011 0101
V	0101 0110	v	0111 0110	6	0011 0110
W	0101 0111	w	0111 0111	7	0011 0111
X	0101 1000	x	0111 1000	8	0011 1000
Y	0101 1001	y	0111 1001	9	0011 1001
Z	0101 1010	z	0111 1010	?	0011 1111
		_	0101 1111	@	0100 0000

Fuente: «Codificación binaria», Areatecnología.com, disponible en https://bit.ly/46SNCss.

Es así como, desde una concepción general, se puede concebir el documento como un objeto o instrumento portador de una idea, pensamiento o acto voluntario expresado de forma escrita, grabada o asentada. Pero, en un sentido análogo el documento digital, es un nivel de abstracción que también es portador de una idea, pensamiento o acto voluntario en forma de datos, información o conocimiento, expresados en patrones binarios o cadenas de bits.

Estos documentos digitales o electrónicos, en términos tecnológicos, están almacenados en un tipo de objeto digital denominado archivo o fichero que sirve de contenedor de diversos tipos de documentos binarios. Dependiendo de su contenido, son de varios tipos: archivos de audio, sonido o voz, archivos de video (simple, tridimensional de realidad virtual o de realidad aumentada o extendida), archivos de texto, archivos de imágenes, fotos o gráficos, archivos de programas fuentes y ejecutables, archivos comprimidos, archivos de mensajes de correo o chat, archivos de configuración, archivos de transacciones bancarias, archivos de imagen de disco, datos de audio y video en flujo continuo o en *streaming*, etcétera.

Es oportuno mencionar una sutil diferencia entre el documento digital y el documento digitalizado, al considerar su forma de producción, creación u origen. El documento es digital en su origen cuando se ha creado directamente dentro del entorno digital, mediante el empleo de herramientas informáticas. En cambio, un documento es digitalizado, como explica Díaz Rodríguez (2018: 498), cuando se le aplica un «proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en un fichero electrónico que contiene la imagen codificada, fiel e íntegra del documento».

Naturaleza informática de la firma digital o electrónica

Desde una noción general, la firma se puede entender como una forma de manifestación personal y voluntaria que tiene un individuo de establecer su vinculación jurídica con una idea, pensamiento o acto. Por ejemplo, la firma autógrafa o manuscrita está basada en el trazo con puño y letra de rasgos individuales sobre un soporte físico. Pero, en el mundo de las TI la firma digital o electrónica es un nivel de abstracción que permite tal vinculación voluntaria de una persona con una idea, pensamiento o acto, pero representada en patrones de bits.

Al respecto, Gómez Vieites (2011: 407) define la firma electrónica o digital como:

> Los datos añadidos a un conjunto de datos que permiten al receptor probar el origen y la integridad de los datos, así como protegerlos contra falsificaciones [...] la firma electrónica de un mensaje permite garantizar la integridad, la autenticación y la no repudiación en un sistema informático.

Esta definición solo alude a aquella firma generada usando tecnologías criptográficas y excluye aquellas firmas tipo facsímil, como las firmas manuscritas digitalizadas o capturadas mediante un escáner, cámaras o dispositivo electrónico como un lápiz óptico sobre pantalla táctil, por ejemplo.

Al respecto, Tanenbaum y Wetherall (2012: 686) destacan que:

> La autenticidad de muchos documentos legales, financieros y de otros tipos se determina mediante la presencia o ausencia de una firma manuscrita autorizada. Para que los sistemas de mensajes computarizados reemplacen el transporte físico de papel y tinta, hay que encontrar un método que permita firmar documentos de una manera imposible de falsificar.

Además, agregan (2012: 686):

> El problema de idear un reemplazo para las firmas manuscritas es difícil. En esencia, lo que se requiere es un sistema mediante el cual una parte pueda enviar un mensaje firmado a otra parte de modo que se cumplan las siguientes condiciones: 1. Que el receptor pueda verificar la identidad del transmisor. 2. Que el emisor no pueda repudiar más tarde el contenido del mensaje. 3. Que el receptor no haya podido elaborar el mensaje él mismo.

La criptografía moderna es una solución a lo anterior y es la base tecnológica de la firma digital o electrónica actual. Es un área de las matemáticas, la informática y la computación donde se buscan algoritmos matemáticos lo suficientemente robustos o complejos para proveer una mayor y mejor seguridad, y protección. Este método busca, mediante códigos secretos y contraseñas, proteger la confidencialidad de los datos e información. Permite cifrar, codificar o convertir mensajes legibles o inteligi-

bles a un formato de representación que sea ilegible, ininteligible y difícil de descifrar sin la clave apropiada.

Tanenbaum y Wetherall (2012: 747) definen la criptografía como «una herramienta que se puede utilizar para mantener confidencial la información y para asegurar tanto su integridad como su autenticidad». En consecuencia, la criptografía se presenta como una herramienta de seguridad que permite, mediante cifrado y descifrado, ocultar (confidencialidad) y proteger (autoría e integridad) una idea, pensamiento o acto, cuyo contenido está incorporado en un documento o comunicación digital que se intercambia entre personas, procesos o entes.

Una forma simple de mostrar cómo funciona el cifrado y descifrado de mensajes en criptografía es usando un operador lógico binario como XOR sobre cadenas de caracteres, cuya representación binaria se observa en la tabla ASCII 8-*bit* de la **tabla 1**. Aquí, una cadena de texto puede ser cifrada aplicando el operador binario XOR (algoritmo criptográfico) sobre cada uno de los caracteres del mensaje utilizando una clave (clave privada).

Por ejemplo, una cadena arbitraria de caracteres como el mensaje de texto «HOLA» (en mayúsculas), cuya representación binaria es «01001000 01001111 01001100 01000001», puede ser cifrada con una clave también arbitraria, por ejemplo «#», y cuya representación binaria es «1100010». Lo anterior produce el mensaje cifrado «klob» (en minúsculas) donde su representación binaria es «01101011 01101100 01101111 01100010». Para obtener este resultado es necesario aplicar la tabla de verdad del operador XOR entre cada *bit* respectivo de cada carácter del mensaje de texto plano con cada *bit* del carácter de la clave, donde las operaciones lógicas asociadas son: 0 xor 0 = 0, 0 xor 1 = 1, 1 xor 0 = 1 y 1 xor 1 = 0. Esto se puede observar en la **tabla 2**.

Tabla 2. Ejemplo de funcionamiento del cifrado y descifrado de mensajes en criptografía usando el operador lógico OR-Exclusivo (XOR). Fuente: Elaboración propia.

Texto plano (binario)	H (01001000)	O (01001111)	L (01001100)	A (01000001)
Clave (binario)	# (00100011)	# (00100011)	# (00100011)	# (00100011)
Texto cifrado (binario)	k (01101011)	l (01101100)	o (01101111)	b (01100010)

Fuente: Elaboración propia.

Como se observa, el texto claro «HOLA» es transformado o codificado en el texto cifrado (no entendible) «klob». Ahora, para descifrar este texto cifrado solo hay que volver a aplicar la misma clave a cada *bit* usando el operador XOR.

Criptografía de clave pública como base de la firma digital o electrónica

En criptografía existen dos técnicas de cifrado: una basada en una sola clave única y privada y otra con dos claves, una privada y otra pública. Sin embargo, la técnica de cifrado de clave pública es la que se trata en este artículo por ser la base de la firma electrónica certificada actual.

La criptografía de clave pública es una técnica que usa dos tipos de claves que, mediante un algoritmo criptográfico, permiten cifrar y autenticar un mensaje de datos. Esto lo explican Kurose y Ross (2017: 500):

> Consiste de un par de llaves o claves, donde una clave privada solo la debe conocer y usar el propietario o signatario (persona que la usa para cifrar o firmar documentos digitales), y otra llave pública que se puede exponer sin riesgo de seguridad con el fin de permitir a otros (personas, entes o sistemas) la validación de la identidad del firmante del mensaje de datos o documento digital.

Por lo tanto, la criptografía de clave pública permite la protección del documento digital y la firma electrónica mediante propiedades de seguridad como la integridad, autenticación y no repudio, y confidencialidad. Estas propiedades de seguridad de las TI se definen en la Norma ISO/IEC 27000 (2018).[9]

Según esta norma, la confidencialidad es la propiedad de ocultar el contenido de la información impidiendo su acceso o divulgación a entidades, sistemas o personas no autorizadas; la integridad es la propiedad de prevenir la creación, modificación o destrucción no autorizada de la información, ya sea accidental o intencional; y la autenticidad y no repudio es la propiedad conjunta de reconocer como válido al emisor que envía un mensaje de datos y que dicho emisor no pueda negar la transmisión o autoría de dicho mensaje o que el destinatario niegue su recepción.

Entonces, el cifrado de clave pública provee lo siguiente:

a) Confidencialidad mediante cifrado y descifrado (**figura 2**). Para proveer confidencialidad a un mensaje de datos se debe convertir o codificar (cifrar) su contenido en texto claro o legible, a un texto cifrado o ilegible que oculte su significado a personas no autorizadas, usando para ello una clave. Ahora, para tener acceso al contenido del mensaje cifrado, es necesario realizar el proceso inverso, es decir, decodificar (descifrar) el mensaje cifrado a su texto original claro y legible, usando la clave apropiada (Tanenbaum y Wetherall, 2012: 683-684). El cifrado garantiza la propiedad de confidencialidad por cuanto protege el acceso no autorizado al contenido legible de los documentos digitales.

9. La norma ISO/IEC 27001 (2018) es un estándar abierto e internacional que proporciona un conjunto de recomendaciones, definiciones y términos usados en seguridad de la información. Disponible en https://bit.ly/3PpVUBz.

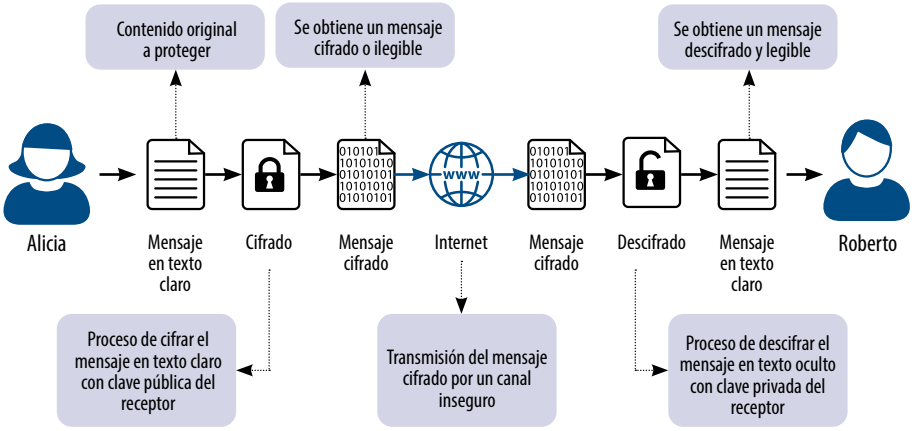

Figura 2. Proceso simplificado de cifrado/descifrado del contenido de un mensaje de datos para proveer confidencialidad. Fuente: www.suscerte.gob.ve.

b) Integridad y autenticidad mediante cifrado y descifrado (**figura 3**). Ahora, para proveer integridad a un mensaje de datos se usa un método criptográfico denominado función *hash* o resumen. Tanenbaum y Wetherall (2012: 683-684) explican que consiste en aplicar una función matemática que extrae, a nivel de *bits*, un bloque más pequeño y de tamaño fijo a partir del contenido del mensaje de datos. Este bloque es único para cada mensaje de datos y equivale a su resumen o huella digital. Esto quiere decir que cada mensaje de datos con contenido distinto tendrá un resumen o *hash* diferente. Es más, cualquier cambio en el contenido del mensaje, aunque sea leve, genera un *hash* totalmente diferente.

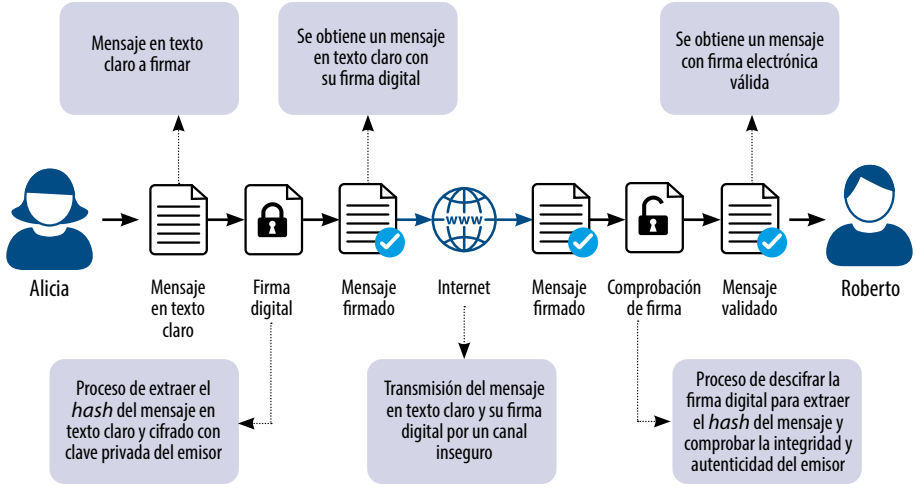

Figura 3. Proceso simplificado de firma electrónica de un documento digital para proveer integridad y autenticación. Fuente: www.suscerte.gob.ve.

Lo anterior permite proveer la propiedad conjunta de autenticación y no repudio, asociando el *hash* o huella digital del mensaje de datos con la identidad del autor de dicho mensaje. Para hacer esto, se toma la huella digital del mensaje como su identificador único y se cifra con la clave privada del autor, firmante o signatario del mensaje, dado que las claves pública y privada deben estar asociadas a su identidad digital.

De esta forma, se establece automáticamente una vinculación voluntaria entre la identidad del autor y el contenido del mensaje; a esto se le denomina firma digital o electrónica.

El certificado electrónico y la firma electrónica certificada

El proceso de proveer confidencialidad, integridad y autenticación, y no repudio a un documento digital presupone no solo conocer la identidad del firmante o signatario, sino la posibilidad de validar esta identidad a través de un órgano, persona o entidad que tenga la autoridad como tercero de confianza. Esto es necesario para dar fe pública de la identidad física asociada a la identidad digital del firmante o signatario, por cuanto la identidad se puede usurpar o falsificar. Esto implica que es necesario garantizar que las claves privada y pública usadas por un firmante o signatario sean legítimas.

Una forma de lograr esta legitimidad de las claves es usar certificados digitales o electrónicos emitidos por una autoridad de certificación autorizada, la cual funciona como un tercero de confianza con un rol de proveedor de servicios de certificación y certificados.

Un certificado digital o electrónico es un documento digital sujeto al estándar X.509, el cual define un conjunto de campos asociados a la identidad del signatario, fecha de emisión y caducidad del certificado, un número de serial único, el tipo de algoritmo de cifrado y descifrado usado para la firma, el algoritmo de resumen o *hash*, la clave pública y su tamaño, un campo que indica el uso del certificado (firma, estampado de tiempo, cifrado, SSL de servidor web, etcétera), otro campo que indica el tipo de certificados digitales o electrónicos, un enlace al servidor de autenticación del proveedor de servicio de certificación, datos de ese proveedor, etcétera.

Así, un certificado electrónico se convierte en un medio que permite al signatario lograr que otras personas o entes validen su identidad. Aquí, la clave privada del signatario, que es personal e intransferible (no se debe compartir), se emite y almacena de forma separada al certificado electrónico, en un archivo protegido con contraseña o en un *hardware* especial protegido, como tarjetas criptográficas o en llaves USB (tókenes).

El proceso de firma electrónica certificada de un documento digital se inicia con el signatario que usa su certificado electrónico a través de un *software* de firma digital o electrónica que permite generar el patrón de *bits* asociados al documento digital.

Para realizar esto, el *software* extrae del certificado digital o electrónico del signatario el tipo de algoritmo *hash* y lo usa para calcular un bloque de tamaño fijo único a partir del contenido del documento que se quiere firmar. Luego, el *software* de firma usa la clave privada del signatario y cifra dicho bloque *hash*. De esta manera, se produce un archivo cifrado que vincula el documento (el *hash* de su contenido) con la identidad del signatario (asociada a su clave privada).

La infraestructura de clave pública y el Sistema Nacional de Certificación Electrónica (SNCE)

No obstante, aunque todo lo anterior es necesario, aún no es suficiente dado que hace falta un sistema de cadena de confianza con una autoridad raíz y proveedores subordinados que soporten el ciclo de vida de los certificados a través de un servicio de certificación electrónica.

La existencia de un sistema de cadena de confianza necesita un órgano rector con atribuciones con base en un marco regulatorio asociado. Esta cadena de confianza estaría conformada por una autoridad de certificación raíz, como órgano rector; autoridades de certificación subordinadas, denominadas proveedores de servicios de certificación, y en la base estarían los usuarios de certificados como signatarios.

Este sistema es el responsable de mantener el ciclo de vida de los certificados a través de un servicio de certificación electrónica que permite la validación y legitimación de la identidad del poseedor del certificado, las claves y la firma electrónica embebida en los documentos digitales, todo soportado por una infraestructura de clave pública.

Esta infraestructura, como describe Stallings (2017: 146), consiste en una plataforma informática con «un conjunto de roles, políticas, *hardware*, *software*, procedimientos y personal necesarios para crear, gestionar, administrar, distribuir, usar, almacenar y revocar certificados digitales y administrar el cifrado de clave pública». En la **figura 4** se observan los siguientes componentes: a) una autoridad de certificación, encargada de emitir y revocar certificados y ser el tercero de confianza que otorga legitimidad al vínculo de las claves privada y pública con la identidad del usuario; b) una autoridad de registro, responsable de validar y registrar la relación entre el certificado, su clave pública y la identidad del signatario para autorizar la emisión del certificado electrónico; c) una autoridad de validación, encargada de comprobar la validez de los certificados digitales emitidos y que son consultados vía internet, y d) repositorios, encargados de almacenar la información relativa a la infraestructura de clave pública, un repositorio para certificados vigentes y otro con los certificados revocados, que son inválidos antes de la fecha caducidad.

En Venezuela, la Superintendencia de Servicios de Certificación Electrónica (Suscerte) es el órgano rector del Sistema Nacional de Certificación Electrónica y del Sistema Nacional de Protección y Seguridad Informática. Tiene su fuente de creación

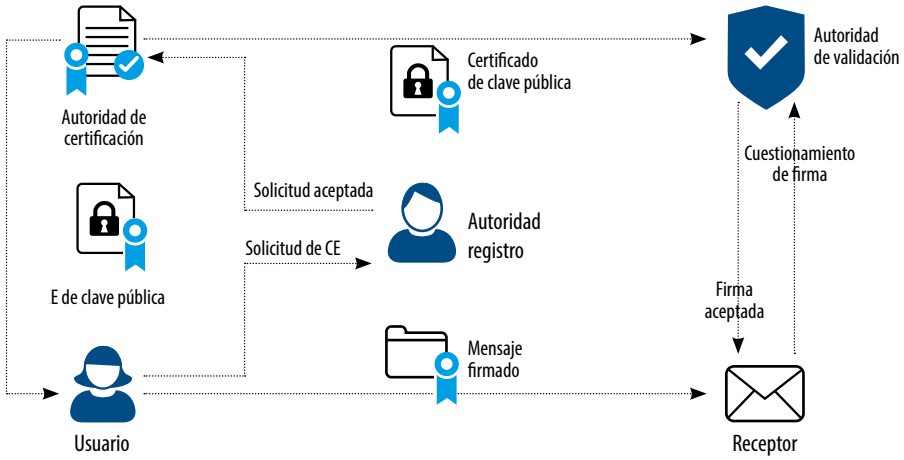

Figura 4. Diagrama de componentes de infraestructura de clave pública.
Fuente: www.suscerte.gob.ve.

y competencias en los artículos 20, 21 y 22 del Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas (2001) y una extensión de sus competencias en los artículos 54 y 55 de la Ley de Infogobierno (2013). La Suscerte junto con los proveedores de servicio de certificación electrónica soportan la infraestructura de clave pública de la cadena de confianza de certificación electrónica de Venezuela.

Principios para la adopción y regulación jurídica del documento digital y la firma electrónica certificada

En derecho se han asimilado al menos dos principios básicos que permiten adoptar las TI en el ámbito social y jurídico, el principio de neutralidad tecnológica y el principio de equivalencia funcional. Estos principios son criterios que justifican la integración al marco jurídico nacional e internacional de medios tecnológicos basados en las TI como alternativas a los medios tradicionales que usan las personas en sociedad, con los mismos o similares efectos jurídicos. A continuación, se explican brevemente.

Principio de neutralidad tecnológica

El principio de neutralidad tecnológica, como comenta Cullell March (2010: 3), «fue usado por primera vez en el año 1999, en un documento oficial de la Comisión Europea para la revisión del marco normativo de las comunicaciones electrónicas». Se empleó como un principio para su regulación jurídica, de tal manera de evitar los efectos de la discriminación de otras tecnologías y al mismo tiempo promover el desarrollo de las TI.

Por otro lado, Landáez y Landáez (2007: 24) interpretan que:

> Este principio significa que las normas del comercio electrónico puedan abarcar las tecnologías que propiciaron su reglamentación, así como las tecnologías que se están desarrollando y están por desarrollarse, teniendo en cuenta una interpretación realista que permita que se desarrolle acorde a los hechos y las situaciones en concreto, de modo que la legislación esté acorde con el constante desarrollo de las nuevas tecnologías.

La neutralidad tecnológica se refiere al hecho de no favorecer unas tecnologías existentes sobre otras a la hora de redactar un instrumento normativo. Esto significa no limitar a una tecnología existente sin prever avances tecnológicos futuros, lo que implicaría una obsolescencia adelantada de la norma legal y un esfuerzo inútil en su creación y aprobación.

La finalidad de este principio es lograr la vigencia de la legislación durante el mayor tiempo posible, dándole un tratamiento abstracto y neutral a la tecnología, como principio regulador. No obstante, es un error pretender con esto la perpetuidad de la ley dado que pueden surgir saltos tecnológicos revolucionarios que serían imposibles de prever y obligar, aun así, a adaptar la ley a la nueva realidad tecnológica.

Principio de equivalencia funcional

Otro principio importante es de equivalencia funcional tecnológica, cuya fuente y antecedente se encuentra en la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre Firmas Electrónicas (CNUDMI).[10] Según se interpreta de esta ley, el principio alude a la similitud que existe entre los medios tecnológicos modernos y los medios físicos tradicionales en cuanto a validez, efectos y consecuencias jurídicas en el mundo real, de tal manera que, aunque son diferentes materialmente, pueden usarse para realizar una función igual o similar en el mundo jurídico y social.

De esta manera, se pueden equiparar los medios tecnológicos a los medios físicos similares, aprovechando lo ya desarrollado por la legislación y hacerlos equivalentes solo en sus efectos y consecuencias jurídicas.

Por ejemplo, sobre los mensajes de datos y firmas electrónicas, Landáez y Landáez (2007: 15) expresan que «la equivalencia funcional consiste en atribuirle la eficacia probatoria o mismo valor probatorio, a los mensajes y firmas electrónicas, que los que la ley consagra para los instrumentos escritos».

10. Ley Modelo de la Comisión de la Naciones Unidas para el Derecho Mercantil Internacional sobre Comercio Electrónico (2001), disponible en https://bit.ly/3JmtEft.

Marco jurídico del documento digital y la firma electrónica según los principios de neutralidad tecnológica y equivalencia funcional

En el marco jurídico de Venezuela, la muestra más reciente del principio de equivalencia funcional se encuentra en el artículo 182 del vigente Código Orgánico Procesal Penal de 2021 (COPP), en el cual se interpreta la libertad de usar medios de pruebas basados en TI:

> Salvo previsión expresa en contrario de la ley, se podrán probar todos los hechos y circunstancias de interés para la correcta solución del caso y por cualquier medio de prueba, incorporado conforme a las disposiciones de este Código y que no esté expresamente prohibido por la ley.

Sin embargo, la primera manifestación de este principio en el ordenamiento jurídico venezolano se remonta al año 1990 cuando el Código de Procedimiento Civil (CPC) dio cabida a la incorporación al proceso judicial de otros medios de prueba innominados como, por ejemplo, las fuentes de prueba electrónicas, tecnológicas e informáticas como medios de prueba libre, al establecer en su artículo 395 que:

> Son medios de prueba admisibles en juicio aquellos que determina el Código Civil, el presente Código y otras leyes de la República. Pueden también las partes valerse de cualquier otro medio de prueba no prohibido expresamente por la ley, y que consideren conducente a la demostración de sus pretensiones. Estos medios se promoverán y evacuarán aplicando por analogía las disposiciones relativas a los medios de pruebas semejantes contemplados en el Código Civil, y en su defecto, en la forma que señale el juez.

Desde entonces, se abrió el camino para hacer valer jurídicamente las TI y nuestro ordenamiento ha ido progresivamente madurando y asimilándolas en la Constitución, en leyes especiales y ordinarias, así como en otros instrumentos jurídicos de rango sublegal. La primera manifestación de rango constitucional que declara las TI como un medio para lograr los objetivos del Estado la tenemos en el artículo 110 de la Constitución de la República Bolivariana de Venezuela (1999), donde se establece que:

> El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional.

Asimismo, la Constitución incorpora en otros artículos aspectos relativos a las TI que se manifiestan como derechos y principios de la actual sociedad digital o de la información, como el artículo 28 referido al *habeas data*, donde se declara que:

> Toda persona tiene el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley.

También, en el artículo 108, se reconoce la influencia y necesidad de las TI en los servicios públicos y en la educación, cuando dispone que:

> El Estado garantizará servicios públicos de radio, televisión y redes de bibliotecas y de informática, con el fin de permitir el acceso universal a la información. Los centros educativos deben incorporar el conocimiento y aplicación de las nuevas tecnologías, de sus innovaciones, según los requisitos que establezca la ley.

En el rango legal, las leyes de mayor interés por su contenido tecnológico y relación directa con el documento digital, la firma electrónica y la prueba documental son el Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas (2001) y su respectivo Reglamento Parcial (2004); el Decreto con Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado (Ley de Interoperabilidad, 2012); la Ley de Infogobierno (2013) y la Ley Especial contra los Delitos Informáticos (2001), entre otras. También, la reciente reforma del Código Orgánico Procesal Penal (2021) y otras de índole supletorio como el Código de Procedimiento Civil (1990).

Como complemento, dentro de las leyes ordinarias contamos con varias que abordan diferentes aspectos de las TI que muestran el alcance e interés del Estado venezolano en aprovechar sus beneficios en la actividad económica, social, en la administración pública del Estado, en los entes públicos e instituciones privadas, así para los ciudadanos y ciudadanas. De estas leyes tenemos la Ley Orgánica de Ciencia, Tecnología e Innovación (2014); Ley Orgánica de Administración Pública (2014); Ley de Tarjetas de Crédito, Débito, Prepagadas y demás Tarjetas de Financiamientos o Pago Electrónico (2008); Ley Orgánica de Telecomunicaciones (2011); Ley de Contrataciones Públicas (2014); Ley Orgánica de Seguridad de la Nación (2002); Decreto con Fuerza de Ley sobre Simplificación de Trámites Administrativos (2014); Ley de Registro Público y del Notariado (2014); Código Orgánico Tributario (2014); Ley Orgánica de Identificación (2014); Ley Orgánica Procesal del Trabajo (2002) y la Ley para la Protección de Niños, Niñas y Adolescentes en Salas de Uso de Internet, Videojuegos y otros Multimedias (2006), entre otras.

Por último, en un rango sublegal, el Decreto 825 (2000) continúa vigente en su declaración del acceso y uso de internet como una política gubernamental de interés prioritario para lograr el desarrollo cultural, económico, social y político de la República Bolivariana de Venezuela.

También, existe jurisprudencia de los tribunales ordinarios y del Tribunal Supremo de Justicia, así como normas técnicas emanadas de los órganos del poder público, en el área de las TI.

Una consideración especial merece la Ley de Infogobierno (2013), debido a su objeto y motivación con respecto a las TI, que según el artículo 1, apunta a:

> Establecer los principios, bases y lineamientos que rigen el uso de las tecnologías de información en el Poder Público y el Poder Popular, para mejorar la gestión pública y los servicios que se prestan a las personas; impulsando la transparencia del sector público; la participación y el ejercicio pleno del derecho de soberanía; así como, promover el desarrollo de las tecnologías de información libres en el Estado; garantizar la independencia tecnológica; la apropiación social del conocimiento; así como la seguridad y defensa de la nación.

La citada ley hace un adelanto importante por cuanto resalta la política del Estado a fortalecer la integración, uso y protección de las tecnologías de la información cuando crea el Sistema Nacional de Seguridad Informática.

Para ello, la Ley de Infogobierno ratifica las competencias de la Superintendencia de Servicios de Certificación Electrónica (Suscerte), ya establecidas en los artículos 20, 21 y 22 del Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas (2001) como órgano rector del Sistema Nacional de Certificación Electrónica (SNCE). Además, las extiende en los artículos 50, 51, 54, 55 y 57 cuando le atribuye también las de ente normalizador en seguridad informática en Venezuela.

Esto implica la rectoría del Sistema Nacional de Protección y Seguridad Informática, el cual comprende los subsistemas de Criptografía Nacional; Gestión de Incidentes Telemáticos; Informática Forense y Protección de Datos.

En Venezuela, el 28 de febrero de 2001 se publicó el Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas cuyo artículo 1 afirma que su objeto es «otorgar y reconocer eficacia y valor jurídico a la firma electrónica, al mensaje de datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas». Aunque, en opinión del autor, este artículo debería incluir también a los mensajes de datos no inteligibles o cifrados los cuales son de uso común y de necesaria protección tecnológica y jurídica.

Partiendo de esta ley especial, y con base en el principio de equivalencia funcional tecnológica, se tiene que el artículo 4 del Decreto con Fuerza de Ley sobre Mensajes

de Datos y Firmas Electrónicas lo consagra al establecer, con respecto a los mensajes de datos y documentos escritos, que:

> Los mensajes de datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, sin perjuicio de lo establecido en la primera parte del artículo 6 de este Decreto con Fuerza de Ley. Su promoción, control, contradicción y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil. La información contenida en un mensaje de datos, reproducida en formato impreso, tendrá la misma eficacia probatoria atribuida en la ley a las copias o reproducciones fotostáticas.

De igual manera, el artículo 6 lo hace respecto a la firma electrónica y la firma autógrafa:

> Cuando para determinados actos o negocios jurídicos la ley exija el cumplimiento de solemnidades o formalidades, estas podrán realizarse utilizando para ello los mecanismos descritos en este Decreto Ley. Cuando para determinados actos o negocios jurídicos la ley exija la firma autógrafa, ese requisito quedará satisfecho en relación con un mensaje de datos al tener asociado una firma electrónica.

Se observa entonces, que este decreto aplica el principio de equivalencia funcional cuando regula el uso de los mensajes de datos en forma de documentos digitales y firmas electrónicas para producir los efectos jurídicos iguales al documento escrito y la firma autógrafa.

En cuanto al principio de neutralidad tecnológica, se tiene también que el artículo 1 del decreto adopta tal principio al expresar que:

> El presente Decreto Ley será aplicable a los mensajes de datos y firmas electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los mensajes de datos y firmas electrónicas.

Otros cuerpos normativos posteriores al Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas hacen referencia al uso del documento digital, la firma electrónica y las TI en relación con la automatización de los procesos de la administración pública nacional, estadal y municipal, particularmente de los procesos de gestión, servicios de atención y protección de datos personales de los ciudadanos y ciudadanas.

De igual manera, en la Ley de Infogobierno (2013) el artículo 5 en su numeral 6 define el documento electrónico como «un documento digitalizado que contiene un dato, diseños o información acerca de un hecho o acto, capaz de causar efectos jurídicos»; y el artículo 8 en su ordinal 5 declara su uso dentro del ejercicio del derecho

de acceso a las TI en las relaciones que tienen las personas con el Poder Público y el Poder Popular. Lo mismo hace dicha ley con respecto al uso de los servicios de certificación y firma electrónica en su artículo 24, cuando expresa que:

> El Poder Público debe garantizar la integridad, confidencialidad, autenticidad y disponibilidad de la información, a través del uso de certificados y firmas electrónicas emitidas dentro de la cadena de confianza de certificación electrónica del Estado venezolano, de conformidad con el ordenamiento jurídico venezolano y la legislación que rige la materia.

También, la Ley de Infogobierno (2013) en su artículo 26 alude a que «los archivos y documentos electrónicos que emitan el Poder Público y el Poder Popular, que contengan certificaciones y firmas electrónicas tienen la misma validez jurídica y eficacia probatoria que los archivos y documentos que consten en físico» y en el artículo 81 se dispone que «aquellas personas en el ejercicio de una función pública, incurren en responsabilidad cuando en sus actuaciones electrónicas, omitan el uso de certificados y firmas electrónicas».

Otro ejemplo es el Decreto con Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado, conocida como Ley de Interoperabilidad (2012). Esta ley regula lo referente al intercambio de datos, información y documentos digitales capaces de causar efectos jurídicos, así como la interoperabilidad tecnológica entre órganos y entes del Estado a través de sistemas informáticos, según sus artículos 4, 22 y otros; y también sobre la firma y certificación electrónica en los artículos 44 y 64 ordinal 9.

Asimismo, la Ley de Registro Público y del Notariado (2014) adopta el documento electrónico y la firma electrónica como elementos fundamentales dentro de los servicios de gestión registral y notarial de documentos de los ciudadanos y ciudadanas. Es así, que en su artículo 2 sobre la finalidad y medios electrónicos establece que «para el cumplimiento de las funciones registrales y notariales, de las formalidades y solemnidades de los actos o negocios jurídicos, podrán aplicarse los mecanismos y la utilización de los medios electrónicos consagrados en la ley». También, en el artículo 23, sobre el manejo electrónico se determina que «todos los soportes físicos del sistema registral y notarial actual se digitalizarán y se transferirán a las bases de datos correspondientes. [...] El proceso registral y notarial podrá ser llevado a cabo íntegramente a partir de un documento electrónico». Finalmente, el artículo 24 sobre la firma electrónica declara que «la firma electrónica de los registradores o registradoras y notarios o notarias tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa».

Al respecto, cabe resaltar que el Tribunal Supremo de Justicia de Venezuela ha estado apuntando en el sentido necesario de usar las tecnologías de la información para automatizar y, por ende, mejorar el sistema de administración de justicia. Es

así como, en una reciente sentencia[11] del Tribunal Supremo de Justicia, la Sala de Casación Civil, con ponencia del magistrado Yvan Dario Bastardo Flores, estableció que la formalización del recurso extraordinario de casación puede ser presentada de forma digital, es decir, ratificó el uso del mensaje electrónico de datos como forma válida para formalizar el recurso de casación. Según el Tribunal Supremo de Justicia, la misma podrá realizarse por correo electrónico institucional dirigido a la secretaría de esa sala. Al final de la sentencia, y como determinación al margen del asunto allí planteado y resuelto, se establece que las formalizaciones e impugnaciones de recursos de casación se podrán hacer en correo electrónico, así como las citaciones y notificaciones se harán por cualquier medio tecnológico.

Libertad de prueba y valor probatorio del documento digital con firma electrónica certificada como medio de prueba documental en el proceso penal venezolano

La prueba judicial puede concebirse como la forma en que las partes apoyan y controvierten sus argumentos en juicio para intentar demostrar o probar, y por ende convencer al juez o jueza, de que un hecho alegado es cierto o falso, usando para ello los medios de prueba y demás reglas procesales legales establecidas para ello, y obtener así la declaración del derecho sustancial mediante sentencia.

Con base en lo anterior, el derecho a probar o derecho a la prueba en Venezuela está consagrado en la Constitución de la República Bolivariana de Venezuela (1999) y sustentado en el principio de acceso a la prueba judicial, previsto en su artículo 49, junto con otros principios como a la tutela judicial efectiva que son esenciales para el derecho al debido proceso, a la defensa y a la prueba.

Principio de libertad probatoria

El principio de libertad probatoria tiene como base constitucional el ordinal 1 del artículo 49, según el cual las partes en el proceso judicial disponen de los medios adecuados y lícitos para su defensa. Esto implica el derecho a promover medios de pruebas que le favorezcan, así como a contradecirlos, controlarlos, evacuarlos y que sean apreciados y valorados por el órgano jurisdiccional natural y competente, como lo establece el mismo artículo en su ordinal 4.

También, el artículo 395 del Código de Procedimiento Civil (1990) establece que:

> Son medios de prueba admisibles en juicio aquellos que determina el Código Civil, el presente Código y otras leyes de la República. Pueden también las partes

11. Sentencia 125 de la Sala de Casación Civil del Tribunal Supremo de Justicia, 27 de agosto de 2020.

> valerse de cualquier otro medio de prueba no prohibido expresamente por la ley, y que consideren conducente a la demostración de sus pretensiones. Estos medios se promoverán y evacuarán aplicando por analogía las disposiciones relativas a los medios de pruebas semejantes contemplados en el Código Civil, y en su defecto, en la forma que señale el juez.

Otro alcance está previsto en el artículo 182 de la reforma del Código Orgánico Procesal Penal (2021), heredado del anterior código (2012) derogado, que expresa:

> Salvo previsión expresa en contrario de la ley, se podrán probar todos los hechos y circunstancias de interés para la correcta solución del caso y por cualquier medio de prueba, incorporado conforme a las disposiciones de este Código y que no esté expresamente prohibido por la ley.

Ambos códigos mantienen que las partes pueden valerse de cualquier medio de prueba legal y lícito que les permita llevar al convencimiento del juez sobre sus alegatos.

Al respecto, Devis Echandía (1981: 103) sostiene que:

> La libertad de los medios de pruebas o de la prueba libre es un complemento ideal del sistema de la libre apreciación. Esto, porque si bien hay amplitud en el debate probatorio, permitiendo a las partes aportar cualesquiera medios de prueba que consideren conducentes para probar los hechos aducidos, también hay una libertad para que el juez, sin regla preestablecida, aprecie los hechos probados. Respetando sin embargo las formalidades exigidas para su producción y las que contienen la ley sustancial para la validez de ciertos actos o contratos.

Además, Devis Echandía (1993: 42) considera que este principio tiene dos aspectos:

> Libertad de medios y libertad de objeto. El primero se refiere a que no debe haber limitación legal acerca de los medios probatorios admisibles, dejando al juez la facultad para la calificación de su pertinencia probatoria; el segundo se refiere a que puede probarse todo hecho que tenga relación con el proceso y que las partes puedan intervenir en la práctica. No se debe limitar la actividad probatoria en forma absurda y ocurrente, porque de alguna manera sería atentar contra el derecho de defensa.

La Constitución de Venezuela, en su artículo 26, también establece la garantía del derecho que tenemos todas las personas a la tutela judicial efectiva sin que pueda haber alguna indefensión. Es por esto que, para garantizar el goce efectivo a obtener satisfacción de nuestros derechos e intereses legítimos, se han establecido normas de cómo utilizar cualquier medio de prueba lícito, oportuno, necesario y pertinente para ejercer el derecho a la defensa.

El medio de prueba documental como soporte de fuentes de prueba informáticas

Debido al principio de equivalencia funcional, el documento digital o electrónico conserva los mismos principios básicos de la prueba documental. Además, tomando en cuenta que las TI sirven de fuentes de prueba, es importante analizar la prueba documental en el contexto del documento digital y la firma electrónica certificada.

Por ejemplo, un concepto de prueba documental compatible con las tecnologías de la información lo propone Lluch (2010: 356) cuando expresa que:

> La prueba documental también constituye un soporte para incorporar al proceso las nuevas fuentes electrónicas, pues, en realidad, un email o una página web no dejan de ser un documento con la singularidad que aparece recogido en un soporte informático. Podemos distinguir su acceso como documento privado, público o multimedia.

En este contexto, Rivera Morales (2009: 902) opina que las TI o «los medios informáticos pueden considerase como fuente de prueba, como objeto de prueba y como medio probatorio». En este sentido, para este autor (2009: 903):

> La fuente de prueba es el órgano, instrumento o circunstancia que conduce el hecho concreto al proceso porque en él está el hecho o hechos que demuestran la existencia de un hecho aducido [...], la fuente es de donde se extrae el conocimiento de los hechos en su sentido integral, pudiendo traer por cualquier medio probatorio.

Ahora, con referencia al medio de prueba, Rivera Morales (2009: 903) expresa lo siguiente:

> Los medios de pruebas son los caminos o instrumentos que se utilizan para conducir al proceso los hechos y posibilitar la reconstrucción de los acontecidos en «la pequeña historia», que es pertinente al proceso que se ventila. Son aquellos que transportan los hechos al proceso. Son los instrumentos regulados por el derecho para la introducción en el proceso de la fuente de prueba. Visto así son instrumentos de intermediación requeridos en el proceso para dejar constancia material de los datos de hechos.

Entonces, el medio de prueba puede ser una persona o cosa que permite probar hechos pertinentes al proceso, como testigos, prueba de peritos, inspección judicial, prueba documental, entre otros.

Sin embargo, cuando se habla de medios informáticos como medio de prueba nos referimos a la forma en que serán reproducidos los hechos ya ocurridos, permitiéndole al juez o jueza elegir la forma correcta de apreciación de la prueba promovida por la parte promovente, de acuerdo con lo que establezca la ley o, en caso de ser necesario, la sana crítica del juez o jueza.

Un aspecto interesante es cuando las TI, como medios informáticos, son usados como objetos de prueba, donde un sector de la doctrina ha llamado prueba sobre prueba. Rivera Morales (2009: 906-907) se refiere a los medios informáticos como objetos de prueba cuando:

> Sobre ellos pueden practicarse otros medios probatorios, para comprobar algún hecho relativo a ellos como cosas, por ejemplo, que no hayan sido alterados, que hayan sido encriptados, etcétera. O también, puede realizarse alguna comprobación técnica, como la existencia de una firma digital encriptada, o pueden encontrarse rastros o evidencias de que existieron unos datos determinados.

Doctrina sobre el documento digital o electrónico

En la doctrina jurídica se han debatido diferentes definiciones acerca del documento digital o electrónico. Una fuente normativa importante sobre el documento digital y la firma electrónica es la Ley Modelo CNUDMI sobre Firmas Electrónicas (2001) vinculada al contexto del comercio electrónico. Esta ley puso en escena al documento y la firma digital al equiparar el documento escrito con un mensaje de datos, y la firma autógrafa manuscrita con la firma digital o electrónica. Esta ley en su artículo 2 señala por:

> Mensaje de datos como toda información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax.

Otra definición de documento digital es la expresada por Falcón (citado por Nemirovsky, 2006: 181), quién según su criterio:

> El documento electrónico estaría representado por las variaciones de los campos magnéticos u ópticos registrados en el soporte, lo cual deja por fuera el instrumento de entrada usado para registrar la grafía que representa la idea o pensamiento en el soporte, ni incluye el instrumento de salida del mismo.

Sin embargo, es necesario resaltar que en el área de la electrónica digital se usa la óptica y los campos magnéticos, eléctricos, electromagnéticos, electrostáticos y electrónicos para representar *bits* (Angulo y García, 2007).

La definición de documento digital de Delgado Salazar (2015: 172), plantea que:

> El documento electrónico es un conjunto de impulsos eléctricos que recaen en un soporte de computadora, teléfono celular u otro equipo similar, que sometidos a un proceso, permiten su traducción a lenguaje natural a través de una pantalla o una impresora, que se encuentra en la memoria de la máquina, cuyo contenido o texto

> está en el lenguaje del sistema, el que puede ser pasado a lenguaje natural o comprensible para facilitar su utilización o lectura, por ejemplo, los correos electrónicos, mensajes de texto y los expresados a través de las llamadas redes sociales.

Pero, Barriuso (1998: 367) simplifica opinando que «el documento electrónico o informático se concibe como un medio de expresión de la voluntad con efectos de creación, modificación o extinción de derechos y obligaciones por medio de la electrónica, informática y telemática».

También, se cita la definición que aporta el Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas (2001) en su artículo 2: «Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio». Asimismo, la Ley de Infogobierno (2013) en su artículo 5 define: «Documento digitalizado que contiene un dato, diseños o información acerca de un hecho o acto, capaz de causar efectos jurídicos».

En este artículo se propone como definición de documento: cualquier objeto o cosa donde se representan datos, información y conocimientos conceptualmente en forma de ideas, pensamientos, declaraciones, actos y conductas emitidos voluntariamente, mediante signos y símbolos escritos o visuales, grabaciones de audio o video, y cualquier forma de representación natural, analógica o digital que permita demostrar la ocurrencia de hechos de relevancia jurídica. Esta definición adopta los principios de neutralidad tecnológica y equivalencia funcional dado que concilia lo tecnológico y lo jurídico, y hace la definición compatible con lo físico en papel y lo virtual en digital.

Como ejemplo, tomemos el caso de dos tecnologías actuales como la realidad virtual y la realidad aumentada. Ambas pueden ser fuentes de prueba informática e incorporarse al juicio usando el medio de prueba documental. Son de interés jurídico dado que, al igual que los videos, pueden representar un pensamiento, hecho, acto, conducta o idea manifestada voluntariamente por una persona, simulada digitalmente como un *avatar* (identidad virtual que escoge el usuario para representarse en un videojuego, una aplicación o sitio web); usando tecnología CGI (*computer-generated imagery*) siempre que dicho *avatar* se pueda vincular inequívocamente a la identidad de la persona física que lo usa.

Doctrina sobre la firma electrónica o digital

De acuerdo con el *Diccionario de la lengua española*, por firma se entiende: «Nombre y apellidos escritos por una persona de su propia mano en un documento, con o sin rúbrica, para darle autenticidad o mostrar la aprobación de su contenido».

Esta firma puede ser autógrafa o manuscrita, digital o electrónica. Es autógrafa cuando es un trazo por puño y letra que representa los rasgos individuales de una persona sobre un soporte físico; y es electrónica o digital cuando es «el producto de la

aplicación de un algoritmo criptográfico y matemático realizado mediante sistemas de *software* y/o equipos de *hardware* usando un soporte físico digital o electrónico» (Gómez Vieites, 2011: 407).

Esta firma digital o electrónica se genera directamente en el mundo digital usando tecnologías informáticas como la criptografía. Pero también es digital la firma autógrafa tipo facsímil, por cuanto ha sido digitalizada su fuente manuscrita de puño y letra (generada por medios físicos como lápiz, bolígrafo, etcétera) y luego convertida a formato digital o binario usando medios electrónicos (dispositivos como pantalla táctil y lápiz óptico, cámaras, escáner, etcétera).

Para Frosini (2019: 173), «una firma electrónica es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje». Por otro lado, Delgado Salazar (2015: 173) propone una definición al decir que:

> La firma electrónica es un método o símbolo basado en medios electrónicos utilizados con la intención de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de la firma manuscrita siendo la firma digital la misma firma electrónica que utiliza una técnica segura que identifica fehacientemente al firmante del documento electrónico garantizando la autenticidad e integridad.

Adicionalmente, podemos revisar la definición que sobre la firma electrónica dispone el Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas (2001), en su artículo 2, como la «información creada o utilizada por el signatario, asociada al mensaje de datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado».

Por último, también la Ley Modelo CNUDMI sobre Firmas Electrónicas (2001), en su artículo 2, se refiere a la:

> Firma digital o electrónica como los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos.

En este artículo también se propone como definición de firma electrónica o digital «el patrón binario único e irrepetible, que se asocia a un mensaje de datos para vincular su contenido con la identidad digital o física del signatario, proporcionando integridad, autenticidad y no repudio».

En conclusión, en Venezuela las firmas válidas con efectos jurídicos son la firma autógrafa y la firma electrónica basada en certificado electrónico adquirido de un PSC acreditado por Suscerte, según lo establece el Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas (2001).

Base jurídica que sustenta la incorporación del documento digital firmado con certificado electrónico al proceso penal mediante la prueba documental

Los documentos, tanto públicos como privados, son admisibles como medios de prueba en la legislación venezolana, siempre que cumplan requisitos de existencia, validez y eficacia establecidos en la ley, como se observa en los artículos 1.356 y 1.363 del Código Civil (1982).

En el caso particular de los medios digitales o electrónicos, con base en la libertad probatoria dispuesta en el artículo 395 del Código de Procedimiento Civil (1990) y el artículo 182 del Código Orgánico Procesal Penal (2021), es posible la promoción de los mensajes de datos en forma de documentos digitales y firmas electrónicas, siempre que se cumpla con lo dispuesto en el Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas (2001), en sus artículos 1, 4, 6, 7, 16, 17 y 18. En este sentido, aquel decreto le da igual eficacia y valor probatorio a la firma electrónica y a los mensajes de datos que la ley le otorga al documento escrito y firma autógrafa, aunque para determinados actos jurídicos la ley exija la firma autógrafa.

Sin embargo, a pesar de la reciente reforma del Código Orgánico Procesal Penal, el procedimiento para la promoción, admisión, control, práctica, contradicción y valoración de la prueba documental aún se rige por lo establecido en el Código de Procedimiento Civil y el Código Civil y, en particular, el mensaje de datos como medio de prueba, se realiza según lo establecido para las pruebas libres en el artículo 395 del Código de Procedimiento Civil, tal como lo exige el artículo 4 del Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas.

Promoción y admisión de la prueba documental electrónica

Como ya se ha explicado, el Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas equipara los mensajes de datos a los documentos físicos y firmas autógrafas. En este contexto, el referido decreto ley en su artículo 6 expone que:

> Cuando para determinados actos o negocios jurídicos la ley exija el cumplimiento de solemnidades o formalidades, estas podrán realizarse utilizando para ello los mecanismos descritos en este decreto ley [...]. Cuando para determinados actos o negocios jurídicos la ley exija la firma autógrafa, ese requisito quedará satisfecho en relación con un mensaje de datos al tener asociado una firma electrónica.

Además, el artículo 8 expresa que: «Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con relación a un mensaje de datos, si la información que este contiene es accesible para su ulterior consulta».

Ahora, en cuanto a la promoción y producción de la prueba libre, es preciso citar la sentencia[12] del Tribunal Supremo de Justicia (2007), de la Sala de Casación Civil sobre la promoción y producción de la prueba libre, la cual manifiesta que el documento electrónico o mensaje de datos es un medio de prueba atípico, que requiere su tramitación mediante el procedimiento de las pruebas libres establecido en el Código de Procedimiento Civil. Además, la sala explica que la parte que promueve un medio de prueba libre tiene la responsabilidad de proporcionar al juez o jueza, durante la etapa de promoción de pruebas, los medios probatorios que demuestren la autenticidad de la prueba libre, usando cualquier medio probatorio legítimo.

Agrega la sala que el juzgador, en la oportunidad de admitir o no dicha prueba libre, debe establecer la manera en que esta se sustanciará, según lo establecido en los artículos 7 y 395 del Código; y en caso de impugnación, debe indicar la oportunidad y forma de revisar la credibilidad e idoneidad de la prueba.

Por último, la sala establece que es obligatorio para los jueces de instancia fijar la forma en que debe tramitarse la contradicción de la prueba libre distinta a los medios de prueba regulados explícitamente en la legislación. Además, una vez incorporada al proceso en forma de documento digital firmado electrónicamente, se aplica el adecuado sistema de valoración para determinar su valor probatorio.

Práctica de la prueba electrónica mediante experticia técnica informática

Luego de promovido y admitido el documento digital firmado electrónicamente como medio de prueba documental, se establece la forma de practicarla para crear en el juez o jueza la suficiente convicción y le otorgue pleno valor probatorio, pero permitiendo antes su control por la parte contraria.

Los mensajes de datos no pueden ser exhibidos directamente por estar almacenados en un soporte electrónico y por el riesgo de ser alterados intencional o accidentalmente. Esto impide presentarlos en juicio y, por ello, es necesario garantizar la cadena de custodia y realizar una experticia técnica, con el fin de proteger las fuentes de prueba informáticas y acceder de forma segura a su contenido para garantizar su autenticidad e integridad.

En este sentido, según el artículo 223 del Código Orgánico Procesal Penal (2021) la experticia se usa como un complemento que apoya al juez o jueza en su valoración de la prueba documental para determinar la autenticidad del documento digital y su firma electrónica, en los supuestos en que el documento no haya sido reconocido, o cuando se haya impugnado su autenticidad, según lo establece el artículo 429 del Código de Procedimiento Civil. Es decir, la experticia se solicita en caso de dudas, entendiendo que el juez o jueza no es una persona experta técnica en la materia.

12. Sentencia 769 sobre la promoción y producción de las pruebas libres, Sala de Casación Civil del Tribunal Supremo de Justicia, 24 de octubre de 2007.

Procedimiento de experticia técnica informática de la prueba documental que soporta un documento digital con firma electrónica certificada

La forma para que adquiera valor probatorio un mensaje de datos en forma de documento digital firmado con certificado electrónico está establecido en los artículos 16, 34 y 38 del Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas, con base en la libertad de prueba establecida en los artículos 395 del Código de Procedimiento Civil y 182 del Código Orgánico Procesal Penal, siempre que el certificado electrónico sea adquirido de un PSC de la cadena de confianza del Sistema Nacional de Certificación Electrónica.

Entonces, para otorgar valor jurídico a la prueba documental como medio de prueba para llevar al órgano jurisdiccional convicción, usando un documento digital firmado electrónicamente, es necesario verificar dos condiciones de validez, como lo exige el decreto:

a) Verificación de integridad: Se confirma que el contenido del documento digital no ha cambiado de manera no autorizada posterior a su firma, con base en los artículos 7, 16 y 38.

b) Verificación de autenticidad: Se confirma que el certificado electrónico del firmante existe en la lista de identidades del proveedor de servicio de certificación electrónica acreditado por Suscerte, ente rector y tercero de confianza, con base en los artículos 18, 34, 35 y 38 del decreto.

Las condiciones anteriores de validez se aplican tanto al documento digital como a la firma y al certificado electrónico usado para firmar. Además, presupone la existencia de un certificado electrónico adquirido de un PSC acreditado por la Suscerte, con base en lo dispuesto en los artículos 2, 22 y 32 del mencionado decreto; o de algún PSC extranjero, según los artículos 34 y 44, *ejusdem*.

Esta experticia informática busca verificar la integridad y autoría de los documentos firmados que se promueven digitalmente. Esta sigue un procedimiento realizado por un perito o experto, quien debe poseer suficientes conocimientos técnicos, científicos, metodologías y herramientas de *software* y *hardware* que permitan determinar la integridad, confidencialidad, autenticidad y eficacia jurídica de las fuentes informáticas que sirven de medio de prueba. Dicha experticia está definida en el artículo 5 ordinal 9 de la Ley de Infogobierno y puede ser realizada por un experto del Centro Nacional de Informática Forense o de la Dirección de Criptografía y Certificación Electrónica, unidades adscritas a la Suscerte.

El objetivo es demostrar que la autenticidad e integridad de la prueba digital o electrónica no se han visto comprometidas en su traslado desde su soporte informático fuente hasta su presentación en juicio para la inmediación del juez.

El procedimiento general de experticia técnica informática se muestra en la **figura 5**. Aquí, el experto usa un *software* de firma para hacer lo siguiente:

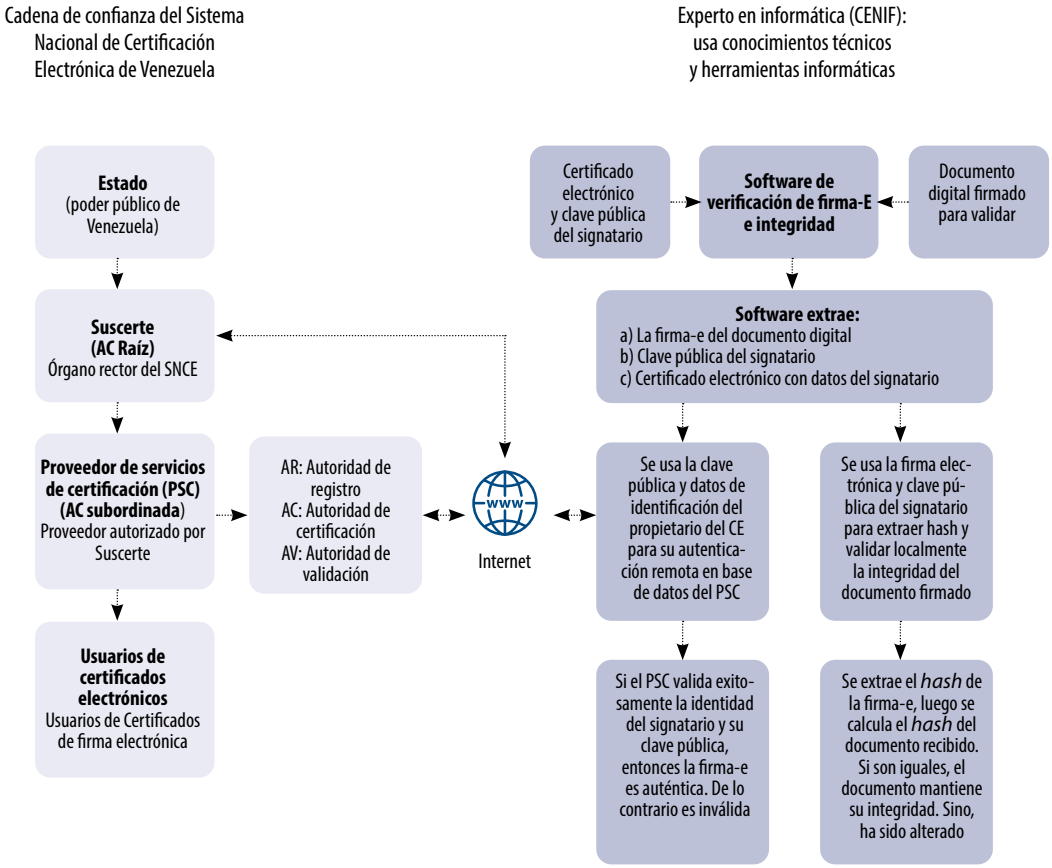

Figura 5. Modelo de validación de identidad de firma e integridad de un documento digital firmado. Fuente: Elaboración propia.

a) Verificación de integridad: Primero, extrae a partir del documento digital firmado, el certificado electrónico del signatario para recuperar su clave pública, el tipo de algoritmo de cifrado y de *hash*, la identidad digital del firmante y el enlace web que apunta al servidor de autenticación del PSC que emitió el certificado. Luego, el *software* extrae la firma digital embebida en el documento digital y la descifra con la clave pública del signatario, así obtiene del documento el *hash* que se generó al momento de su firma. Ahora, el *software* calcula nuevamente el *hash* del documento digital luego de firmado. Entonces, el *software* compara ambos *hash* y si son iguales, entonces el documento ha mantenido su integridad. En caso contrario, ha sido alterado y no es válido. Así, se verifica la integridad del documento.

b) Verificación de autenticidad: Luego, el experto procede a validar el certificado electrónico y la identidad del signatario. Para esto, el *software* usa la clave pública del signatario y, mediante el enlace al servidor del PSC extraído del certificado electróni-

co, procede a hacer una consulta cliente-servidor usando el protocolo OCSP (online certificate status protocol) a su base de datos de certificados válidos registrados. Esto implica preguntar la identidad del propietario de la clave pública enviada. El *software* recibe una respuesta positiva si el certificado está vigente en el servidor del PSC y si la identidad del emisor de la firma coincide con la del propietario del certificado. Si alguna respuesta es negativa, la firma electrónica o el certificado electrónico es inválido. Así se determina la autenticidad o no del certificado y la firma electrónica del documento digital. El resultado final es un informe técnico forense o la declaración del experto ante la jueza o juez de juicio sobre el hallazgo de la experticia técnica informática realizada.

Es oportuno citar la sentencia[13] del Tribunal Supremo de Justicia, en Sala de Casación Civil, con ponencia de la magistrada Marisela Godoy Estaba, referida a la experticia de correos electrónicos y firma con certificado electrónico adquiridos de un PSC acreditado por la Suscerte, donde se expresa:

> Como la juez de la recurrida no detectó el vicio de procedimiento, reconociendo únicamente que la prueba de experticia había sido admitida, sin percatarse que el juez del Tribunal a quo no estableció los parámetros en que la misma debía realizarse, por ejemplo, si debía ser realizada por expertos del servicio de Certificación Electrónica (Suscerte); determinar quién fue el emisor o la persona autorizada para actuar en su nombre y saber desde cuál y hacia cuál dirección o puerto electrónico fue enviado y recibido el mensaje; bajo cuál firma electrónica fue enviado, la fecha y hora de la emisión del mensaje; su contenido; y cualquier otro dato de relevancia para el proceso que las partes soliciten o el juez ordene para resolver la controversia.

Asimismo, de la motivación de la sentencia se desprende que:

> A tal efecto, como se pudo observar de la doctrina y jurisprudencia citada al momento de valorar los correos electrónicos en cuestión, el mecanismo idóneo en el presente caso, dado que los proveedores de servicio de certificación establecidos en el Decreto con Rango y Fuerza de Ley de Mensajes de Datos y Firmas Electrónicas no se encuentran en funcionamiento; era la promoción de una experticia informática, que pudiera darle el carácter de documento privado «original» a los mismos, la cual efectivamente fue promovida y admitida por el Juzgado *ad quo* en los términos de una prueba libre establecida en el artículo 395 del Código de Procedimiento Civil, por lo que queda desechado el argumento de que el mencionado juzgado no fijó las pautas necesarias para que la referida prueba adquiriera validez probatoria.

La referida sentencia evidencia los aspectos tecnológicos y jurídicos involucrados en la promoción, admisión y evacuación de pruebas libres en el proceso judicial ve-

13. Sentencia 386 sobre la experticia informática a mensajes de datos con firmas electrónicas, Sala de Casación Civil del Tribunal Supremo de Justicia, 1 de julio de 2015.

nezolano, cuya norma supletoria y reguladora aún sigue siendo el Código de Procedimiento Civil, según el artículo 395.

Valoración del documento digital con firma electrónica certificada

El valor probatorio del documento digital y la firma electrónica dependen de la integridad, así como de la autenticidad al obtener la identidad legítima de su autor firmante. Por consiguiente, las funciones principales de la firma sobre un documento consisten en suministrar autoría y veracidad al documento signado, otorgando el correspondiente valor probatorio y credibilidad jurídica según las distintas disposiciones legales.

En Venezuela, el valor probatorio y efectos jurídicos de la firma electrónica y el documento digital están establecidos en el Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas, en su artículo 1:

> El presente decreto ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la firma electrónica, al mensaje de datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los proveedores de servicios de certificación y los certificados electrónicos.

Sin embargo, el mismo artículo en su último párrafo hace la salvedad de que «la certificación a que se refiere el presente decreto ley no excluye el cumplimiento de las formalidades de registro público o autenticación que, de conformidad con la ley, requieran determinados actos o negocios jurídicos». Otro es el artículo 4 de la referida ley, que ratifica esta validez jurídica del mensaje de datos:

> Los mensajes de datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, sin perjuicio de lo establecido en la primera parte del artículo 6 de este decreto ley. Su promoción, control, contradicción y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil.

Pero el mismo artículo también advierte que un documento digital firmado al ser reproducido en papel pierde las propiedades jurídicas que había adquirido con la firma electrónica certificada y, como consecuencia, ahora adquiere la eficacia probatoria que la ley le atribuye a las copias fotostáticas o simples. En este caso, las copias fotostáticas para recuperar su valor probatorio y eficacia jurídica plena deben ser certificadas mediante firma autógrafa o manuscrita por el autor o por un órgano administrativo o judicial que tenga la potestad de dar fe pública, como el caso de los documentos públicos, artículo 1.357 del Código Civil (1982).

No obstante, el artículo 4 no exige la previa demostración de la autenticidad del mensaje para otorgarle eficacia probatoria, esto se deduce de la interpretación de los

artículos 7, 8 y 16 del Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas (2001) y de los principios que rigen la prueba escrita. Es decir, es esencial que la parte promovente del documento digital con firma electrónica certificada haya acreditado ante el órgano jurisdiccional la integridad, autenticidad y autoría del mensaje de datos para que pueda ser considerado como plena prueba de un hecho controvertido. Lo anterior implica que, en caso de ser aceptada de forma expresa o tácita por la contraparte, la autenticidad, autoría e integridad quedarían demostradas y establecidas, sin necesidad de acudir a los procedimientos procesales, como sería el caso de una experticia informática, para obtener así la convicción del órgano jurisdiccional sobre su valor probatorio.

Asimismo, el artículo 16 afianza lo anterior cuando dispone que «la firma electrónica que permita vincular al signatario con el mensaje de datos y atribuir la autoría de este, tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa».

Finalmente, los artículos 17 y 18 dictan lo referente a su valoración por el juez o jueza usando la sana crítica: «La firma electrónica que no cumpla con los requisitos señalados en el artículo anterior no tendrá los efectos jurídicos que se le atribuyen en el presente capítulo, sin embargo, podrá constituir un elemento de convicción valorable conforme a las reglas de la sana crítica».

Al respecto, el autor considera que el Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas (2001) es un instrumento legal importante que promueve la seguridad jurídica de los negocios jurídicos producto de las transacciones y actividades que tienen lugar en internet y demás medios de comunicación digital. Pero es necesario lograr la correcta y objetiva apreciación de los hechos que constituyen prueba, establecidos en los documentos digitales firmados electrónicamente. Así, los órganos encargados de impartir justicia (judiciales y administrativos) deben ampliar sus conocimientos y criterios con base en la confianza en las tecnologías de la información o informáticas, pues de nada sirve que las partes en conflicto utilicen los avances de la ciencia y de la tecnología como fuentes y medios de prueba si los responsables de la administración de justicia limitan la adecuada apreciación de todo su valor probatorio por ignorancia, desconocimiento o desconfianza.

Conclusiones

La tecnología informática es el fundamento de los mensajes de datos, particularmente de los documentos digitales y firmas electrónicas. La diferencia entre lo electrónico (género) y lo digital (especie) en las TI no es relevante por cuanto en ambos casos su representación y funcionamiento es binario o digital, dado que lo electrónico es el dispositivo o *hardware*, y lo binario es el *software* y los mensajes de datos.

Entonces, ya que las firmas, sea que se denominen electrónicas o digitales, usan la criptografía de clave pública, lo apropiado es diferenciarlas entre firma simple y firma avanzada. Para ello, se debe usar como elemento diferencial la propiedad conjunta de autenticación y no repudio. Esta propiedad solo la provee la firma avanzada mediante un órgano o entidad oficial con cualidad jurídica que, actuando como tercero de confianza, permite validar la identidad del autor o signatario y otorgar legitimidad. La firma simple lamentablemente no provee esta legitimidad a priori de la firma avanzada. Aquí la criptografía de clave pública juega un papel importante porque les provee potencialmente de medidas de seguridad como disponibilidad, confidencialidad, integridad, autenticidad y no repudio.

En este sentido, los documentos digitales y las firmas electrónicas son instrumentos operacionalmente equivalentes al documento físico y la firma autógrafa en lo jurídico. Debido a esta equivalencia funcional, el documento digital o electrónico permite representar ideas, pensamientos o actos voluntarios con efectos jurídicos. Asimismo, con la firma digital o electrónica una persona puede expresar su voluntad de vincularse como autor con el contenido de un documento digital o electrónico.

Así, los principios de equivalencia funcional y neutralidad tecnológica constituyen criterios útiles, válidos y universales que justifican la incorporación de los avances de las TI en la legislación.

En Venezuela, estos principios son el fundamento de la regulación jurídica del documento digital y la firma electrónica, referidos como mensajes de datos. Como hemos visto, estos están consagrados en el Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas (2001), la Ley de Infogobierno (2013) y otros instrumentos legales y sublegales del ordenamiento jurídico. No obstante, estas y otras leyes poseen algunos errores de redacción, además de tener pendiente su reglamentación. Esto dificulta la adopción práctica y efectiva de estas tecnologías para la implementación adecuada de políticas públicas.

Es necesario resaltar que la reciente reforma del Código Orgánico Procesal Penal de Venezuela (2021) no incluyó un procedimiento probatorio para las pruebas basadas en fuentes digitales o electrónicas. Todavía, el procedimiento a seguir en el proceso penal para incorporar fuentes de prueba de naturaleza informática, según la libertad de prueba, es el establecido en el Código de Procedimiento Civil (1990) y el Código Civil (1982), como normas supletorias, y así se ratifica en el artículo 4 del Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas (2001).

Como conclusión, para que el documento digital y la firma electrónica se constituyan en plena prueba y eficaces como un medio de prueba documental, es necesario garantizar que la firma electrónica del documento sea auténtica y que el documento digital mantenga su integridad desde el momento que se firmó. Para ello, es esencial que el documento digital firmado electrónicamente, una vez incorporado como prueba documental al proceso penal, deba ser practicado o evacuado mediante una

experticia informática para verificar su integridad y autenticidad, para que luego el órgano jurisdiccional pueda realizar la adecuada apreciación de su valor probatorio.

Además, se reafirma la importancia que tiene para abogados, jueces, fiscales, órganos de investigación penal y demás auxiliares de justicia el conocimiento y uso instrumental de las TI, en particular de los documentos digitales, la firma electrónica, del computador y demás *softwares* informáticos relacionados.

Referencias

Angulo, José, Ignacio Angulo y Javier García (2007). *Sistemas digitales y tecnología de computadores*. 2.ª ed. Madrid: Paraninfo.

Barriuso, Carlos (1998). *La contratación electrónica*. Madrid: Dykinson.

Chacón, Nayibe y Gladis Proaño (2021). «Breves anotaciones sobre los principios aplicables a la prueba electrónica de las obligaciones mercantiles: Tratamiento en Ecuador y Venezuela». *Revista Venezolana de Derecho Mercantil,* 6: 15-31. Disponible en https://bit.ly/3Dg1LCl.

Cullell March, Cristina (2010). «El principio de neutralidad tecnológica y de servicios en la UE: La liberalización del espectro radioeléctrico». *Revista de Internet, Derecho y Política,* 11: 1-10. Disponible en https://bit.ly/3Ddv48s.

Delgado Salazar, Roberto (2015). *Las pruebas en el proceso penal venezolano*. 5.ª ed. Caracas: Vadell Hermanos.

Devis Echandía, Hernando (1981). *Teoría general de la prueba judicial*. Volumen 1. Buenos Aires: Zavalía. Disponible en https://bit.ly/3JWtVWP.

—. (1993). *Compendio de la prueba judicial*. Buenos Aires: Rubinzal-Culzoni. Disponible en https://bit.ly/3JWB6OE.

Díaz Rodríguez, Alfonso (2018). «De la digitalización y los documentos conversos». *Boletín de la Federación Española de Asociaciones de Archiveros, Bibliotecarios, Arqueólogo, Museólogos y Documentalistas,* 68 (3-4): 494-506. Disponible en https://bit.ly/3pKrrUx.

Frosini, Vittorio (2019). *Cibernética, derecho, internet y sociedad*. Santiago: Ediciones Jurídicas Olejnik.

Fugini, Mariagrazia, Piercarlo Maggiolini, Daniele Pagani y Ramón Vallés (2019). *Sistemas y tecnologías de la información en las organizaciones.* 1.ª ed. Madrid: Pirámide.

González Torres, Carlos (2020). «Formas y oportunidad para la promoción del documento electrónico en el procedimiento civil ordinario». *Revista Venezolana de Legislación y Jurisprudencia,* 14: 293-312. Disponible en https://bit.ly/46QDxfE.

Gómez Vieites, Álvaro (2011). *Enciclopedia de la seguridad informática*. 2.ª ed. México: Alfaomega.

Jiménez, Jesús y Patricia Caballero (2019). *El valor probatorio de la firma electrónica en el proceso judidical*. Tesis de maestría. México: Centro de Investigación e Inno-

vación en Tecnologías de la Información y Comunicación. Disponible en https://bit.ly/3PUyxjO.

Joyanes Aguilar, Luis (2015). *Sistemas de información en la empresa: El impacto de la nube, la movilidad y los medios sociales*. 1.ª ed. México: Alfaomega.

Kurose, James y Keith Ross (2017). *Redes de computadoras: Un enfoque descendente*. 7.ª ed. Madrid: Pearson Educación.

Landáez, Leoncio y Nelly Landáez (2007). «La equivalencia funcional, la neutralidad tecnológica y la libertad informática». *Revista de la Facultad de Ciencias Jurídicas y Políticas,* 3: 11-49.

Ledesma Narváez, Marianella (2016). «La prueba documental electrónica». *Foro Jurídico,* 15: 17-25. Disponible en https://bit.ly/43vErLj.

Lluch, Xavier (2010). *La prueba documental*. Barcelona: Esade-Bosch. Disponible en https://bit.ly/3NPqhza.

Marín Meilán, Héctor (2018). «El documento electrónico en la legislación y jurisprudencia venezolana». *Magistra*, 10 (1), 71-104. Disponible en https://bit.ly/3rkNYHM.

Nemirovsky, Hugo (2006). «El valor probatorio del documento electrónico». *Revista de Derecho Probatorio*, 14: 177-193. Disponible en https://bit.ly/3DehCkO.

Olmos García, Mercedes (2017). *La prueba digital en el proceso civil: Verificación y régimen general*. Tesis de maestría. Madrid: Universidad Pontificia Comillas. Disponible en https://bit.ly/46Lmb3z.

Ortiz, Daniela y Luisa Jacome (2019). «La prueba electrónica: Una crítica a su valoración en la legislación colombiana». *Revista de Derecho* (Universidad Centroamericana), 27: 99-117. Disponible en https://bit.ly/44FKb6o.

Rivera Morales, Rodrigo (2009). *Las pruebas en el derecho venezolano: Civil, penal, oral, agrario, laboral y Lopnna*. Caracas: Librería J. Rincón G.

Stallings, William (2006). *Organización y arquitectura del computador*. 7.ª ed. Madrid: Pearson.

—. (2017). *Network security essentials: Applications and standards*. 6.ª ed. Nueva York: Pearson.

Tanenbaum, Andrews y David Wetherall (2012). *Redes de computadoras*. 5.ª ed. México: Pearson.

Sobre el autor

Carlos Alfonso Acosta-León es abogado; egresado de la Escuela de Derecho de la Universidad Central de Venezuela (UCV); especialista en derecho probatorio por la Escuela Nacional de Fiscales del Ministerio Público; licenciado en Computación de la Escuela de Computación de la UCV; magíster en Ciencias de la Computación por la Facultad de Ciencias de la UCV y doctor (PhD) en Informática por la Uni-

versidad de Edimburgo. Se desempeña como docente de la Escuela de Computación y es investigador adscrito al Centro de Computación Paralela y Distribuida de la UCV; también es docente de la Escuela de Ingeniería Informática e investigador asociado al Centro de Investigación y Desarrollo de Ingeniería de la Universidad Católica Andrés Bello. Sus correos electrónicos son cacostal@yahoo.co.uk, carlos.acosta@ucv.ve, cacostal@ucab.edu.ve y carlos.acostaleon@gmail.com. https://orcid.org/0000-0003-1895-4040.