



**AUTENTICIDAD DEL DOCUMENTO ELECTRÓNICO EN LA LEGISLACIÓN
COLOMBIANA**

SANTIAGO ARROYAVE RESTREPO

STEFANNY CANO GRISALES

MONOGRAFÍA DE INVESTIGACIÓN PARA OPTAR AL TÍTULO DE:

ABOGADO (A)

UNIVERSIDAD AUTÓNOMA LATINOAMERICANA –UNALA–

FACULTAD DE DERECHO

MEDELLÍN

2016



**AUTENTICIDAD DEL DOCUMENTO ELECTRÓNICO EN LA LEGISLACIÓN
COLOMBIANA**

SANTIAGO ARROYAVE RESTREPO

STEFANNY CANO GRISALES

MONOGRAFÍA DE INVESTIGACIÓN PARA OPTAR AL TÍTULO DE:

ABOGADO (A)

Asesor:

Dr. ARTURO TABORDA RESTREPO

UNIVERSIDAD AUTÓNOMA LATINOAMERICANA –UNALA–

FACULTAD DE DERECHO

MEDELLÍN

2016

Nota de aceptación

Presidente del jurado

Jurado

Jurado

Fecha:

Autenticidad del documento electrónico en la legislación colombiana

Contenido

Introducción	6
1. Formulación del problema de investigación	7
1.1. Pregunta de investigación	7
1.2. Descripción	7
1.3. Justificación	8
2. Formulación de objetivos.....	8
2.1. Objetivo general.....	8
2.2. Objetivos específicos	8
3. Marco metodológico	9
4. Cronograma de actividades.....	9
5. Marco teórico	10
5.1. Documento y documento electrónico	11
5.1.1. Documento como forma.....	12
5.1.2. Documento como signo	12
5.1.3. Documento como medio	13
5.2. Elementos del documento	13
5.2.1. Cosa mueble.....	13
5.2.2. El sujeto	14
5.2.3. Signos de representación (contenido)	14
5.3. Aspectos básicos del documento y el documento electrónico	15
5.3.1. Integridad	15
5.3.2. Autenticidad.....	15
5.3.3. Confidencialidad	15
5.4. Antecedentes normativos	16
5.5. Importancia del documento electrónico en Colombia	21
5.6. Utilización del documento electrónico como medio de prueba en Colombia.....	21
Características.....	22
5.7. Uso de la firma (electrónica y digital) para otorgar validez al documento electrónico	27
Requisitos para la existencia jurídica del documento electrónico.....	30

5.8. Repaso del documento electrónico en algunas legislaciones de Latinoamérica (Derecho Comparado).....	30
Argentina.....	31
Brasil.....	31
Chile.....	31
Costa Rica.....	32
Ecuador.....	32
México.....	32
Perú.....	33
Uruguay.....	33
Venezuela.....	33
6. Conclusiones.....	34
Referencias.....	34
Anexos.....	36
Anexo 1:.....	36
LEY 527 DE 1999.....	36
Anexo 2:.....	52
DECRETO 2364 DE 2012.....	52

Autenticidad del documento electrónico en la legislación colombiana

Introducción

La presente monografía, busca ilustrar el avance que ha tenido el documento electrónico en la legislación colombiana en cuanto a su autenticidad desde una perspectiva probatoria, evidenciando el avance que ha tenido la noción de documento en el derecho contemporáneo, distanciándose del soporte en papel como único medio de prueba tradicional e introduciéndonos en el documento electrónico como medio que se exige en la sociedad actual de la información.

La investigación tiene una estructura de seis capítulos que son distribuidos de la siguiente manera:

En el primer capítulo, se plantea la descripción sucinta del problema que nos ocupa y la justificación de nuestra propuesta.

En el segundo y tercer capítulo, se establecen los objetivos; general y específicos, que guían y dirigen el desarrollo de la presente investigación y se enuncia el enfoque metodológico y la técnica utilizada para la recolección de datos. Así también, el cuarto capítulo hace una descripción amplia, a través del cronograma de actividades, de las fechas y tareas en las que tuvo cabida el desarrollo de la presente investigación.

El quinto capítulo fundamenta el marco teórico de la investigación, en el que se contemplan los antecedentes normativos, la transformación social que conlleva el empleo de nuevas tecnologías en la vida cotidiana y en la Administración Pública, y formula una crítica constructiva en cuanto a la posibilidad del ahorro de tiempo y recursos de trámites dispendiosos con la implementación de este innovador y beneficioso método. A su vez, destaca el documento electrónico como estrategia de tipo cultural y social para evitar el consumo masivo de papel y generar un ahorro material y energético. La utilización de éste como medio de prueba en la legislación colombiana y la importancia de la firma, tanto electrónica como digital, ya que se constituye en el símbolo que otorga validez al mismo. Así mismo, se realiza un breve repaso a efecto de generar un ejercicio de derecho comparado del documento electrónico en algunas legislaciones de Latinoamérica.

Finalmente, el sexto y último capítulo, se compone de las conclusiones. Las cuales dejan constancia del pleno desarrollo, discusión y análisis de los objetivos fijados en esta investigación, a manera de expresar los principales hallazgos y propuestas posibles para tener en cuenta en el inicio de presentes y futuras investigaciones que versen sobre el mismo objeto y/o materia.

Autenticidad del documento electrónico en la legislación colombiana

1. Formulación del problema de investigación

1.1. Pregunta de investigación

¿Cómo se determina la autenticidad del documento electrónico en la legislación colombiana?

1.2. Descripción

La escritura surge de la imperiosa necesidad de otorgar permanencia a lo imaginado, pensado o percibido por el hombre. Él siente la necesidad de captar y perpetuar el hecho producido, a efectos de poder reproducirlo toda vez que sea necesario. Surge así la necesidad de la forma, o sea, de la búsqueda de un elemento material, sensible, que sirva para envolver y retener la realización de un acto o hecho que interesa. (Rengifo García, 2000, pág. 29).

Anteriormente, los derechos y obligaciones que se adquirían se probaban basados en lo que estuviese plasmado por escrito, en un papel, que fuese tangible. Hoy, se avizora un cambio en el panorama, estamos altamente influenciados por la tecnología que da origen a nuevos tratados jurídicos, nuevas inter-relaciones personales, nuevos retos. Es por esto que el soporte material del papel tiende a desaparecer.

Siempre ha existido desconfianza hacia lo nuevo. Con el descubrimiento de la escritura se pensó que este método iba a acabar con la capacidad de recordación y de memoria del hombre. Al surgir la fotografía, creyeron que no era viable porque solo mediante la pintura se podía reflejar la realidad. Con el apareamiento de la fotocopia, se cuestionó su aceptación en cuanto a la validez probatoria, lo mismo que pasó con las grabaciones sonoras y visuales. Actualmente, la desconfianza está dirigida al documento electrónico, pues estamos en una cultura dominada por el papel (Rengifo García, 2000), sobre todo en el campo jurídico, que parece estar llamado a empapelar el mundo.

Es por lo anterior, que, como se evidencia en el desarrollo de la monografía, se indaga sobre la autenticidad del documento electrónico, debido a que es precisamente sobre este aspecto, donde especialmente se evidencia dicha desconfianza tanto de los funcionarios judiciales como de los ciudadanos en general, creando una barrera que impide dar un paso a hacia la tendencia tecnológica, que procura, sobre todo, un ahorro económico y energético, así como complicaciones en la tramitología.

Según la Real Academia Española, autenticidad es la calidad de auténtico. Auténtico, por su parte, es un adjetivo que se define como “acreditado como cierto y verdadero por los caracteres o

requisitos que en ello concurren” es también “certificación con que se testifica la identidad y verdad de algo.” (RAE).

Concretamente y referido al documento electrónico, la autenticidad hace referencia a que pueda demostrarse que el documento es lo que afirma ser, que ha sido creado o enviado por la persona que afirma haberlo creado o enviado, y que ha sido creado o enviado en el momento que se afirma. Para garantizar la autenticidad de los documentos, las entidades deben implantar y documentar políticas y procedimientos para el control de la creación, recepción, transmisión, mantenimiento y disposición de los documentos, de manera que se asegure que los creadores de los mismos estén autorizados e identificados y que los documentos estén protegidos frente a cualquier adición, supresión, modificación, utilización u ocultación no autorizadas. (T.I.C & línea).

1.3. Justificación

Este proyecto es viable ya que se debe insistir en la propuesta de gestionar la información contenida en los documentos; de una manera competente, válida y eficaz, valiéndose con responsabilidad de las nuevas herramientas tecnológicas, jurídicas y específicas, que surgen de la normativa actualmente existente en el marco jurídico colombiano y que se adaptan al contexto inmanente de la posmodernidad.

Esto resulta útil, puesto que el tratamiento adecuado de la información es una realidad evidente y nos permite la disminución y/o supresión de trámites engorrosos, aglomeración de documentos, posibilitando el uso de técnicas de innovación a la Administración Pública y ajustarse a nuevas políticas culturales, económicas, sociales y ambientales en consonancia con las nuevas tecnologías de la información exigidas por la sociedad actual.

2. Formulación de objetivos

2.1. Objetivo general

Determinar la autenticidad del documento electrónico en la legislación colombiana.

2.2. Objetivos específicos

1. Enunciar la normatividad principal que alude a la utilización del documento electrónico en el marco de la legislación colombiana.
2. Definir la importancia del documento electrónico en Colombia.

3. Identificar como se utiliza el documento electrónico como medio de prueba en la legislación colombiana.
4. Resaltar el uso de la firma electrónica para otorgar validez al documento electrónico.

3. Marco metodológico

La investigación tiene un enfoque cualitativo, pues posee bondades de riqueza interpretativa, profundidad de ideas y además contextualiza el fenómeno investigado, teniendo como proceso el análisis de la realidad subjetiva sin tener una secuencia lineal.

Se utilizó como herramienta el método inductivo o de inducción, pues lo que es verdad en un caso particular no tiene por qué serlo del universal. (Corbetta, 2010).

Los datos fueron obtenidos utilizando como técnica la recopilación y análisis documental de las leyes y decretos más relevantes emitidos por el Congreso y el Gobierno Nacional, revistas y libros de grandes doctrinantes e investigadores del tema.

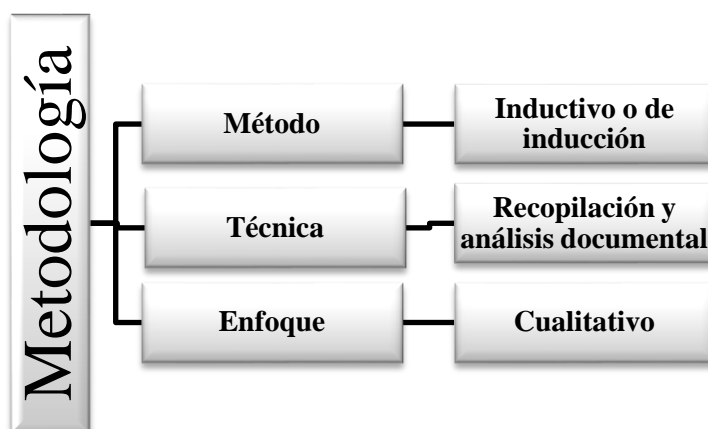


Figura 1

Fuente: elaboración propia.

4. Cronograma de actividades

TÍTULO	Autenticidad del documento electrónico en la legislación colombiana
MODALIDAD	Monografía
NOMBRE DE LOS ESTUDIANTES	Stefanny Cano Grisales
	Santiago Arroyave Restrepo

ASESOR	Arturo Taborda Restrepo		
JURADOS	Ajani Akin Cuesta Davu		
	Jhon Jairo Rodríguez		
FECHA	PROPÓSITO Y/O METODOLOGÍA	TIEMPO	TAREAS PENDIENTES
Febrero de 2016	Inscripción del trabajo de grado en el Centro de Investigaciones (Radicado asignado: 2016-044)		
22 de marzo de 2016	Primer encuentro con el asesor en el que comentamos los propósitos de la investigación, leímos el anteproyecto enviado al centro de investigación y dialogamos sobre el tema	1 hora	Ampliación del tema
23 de mayo de 2016	Entregamos avances de la investigación, resolvimos dudas, aclaramos conceptos	1 hora	-Ampliación del tema -Desarrollar un breve derecho comparado
17 de agosto de 2016	Entrega de avances	30 minutos	
30 de septiembre de 2016	Entrega trabajo final en el centro de investigaciones		
23 de noviembre de 2016	Sustentación oral ante jurados	15 minutos	
07 de diciembre de 2016	Notificación concepto de jurados (Aprobado con modificación)		Entrega de modificaciones
23 de enero de 2017	Entrega de trabajo final con modificaciones		

Figura 2

Fuente: elaboración propia.

5. Marco teórico

5.1. Documento y documento electrónico

Establecer un concepto claro y más o menos aceptado de documento fue una tarea que se comenzó a complicar a medida que aparecían nuevas formas de expresión distintas a la escrita y en otros soportes que excedían a los impresos –entre ellos el papel, que sin ser el primero, desde hace siglos es el más empleado–, donde además era ya necesario recurrir a aparatos o medios técnicos a fin de conocer su contenido. Basta pensar en el documento electrónico para hacer palpable la idea: su contenido se encuentra en soporte electrónico y para visualizarlo se requiere de una pantalla y un dispositivo adecuado, y para escucharlo, un equipo que emita el audio. Muchas veces, el problema de la necesaria intermediación tecnológica puede ser resuelto recurriendo a un ordenador. (Calvinho, 2012, págs. 43, 44).

Con el correr del tiempo, se han deslizado desde posiciones muy amplias acerca del documento –que tienen por tal a todo objeto mueble que puede presentarse ante el juez–, hasta restringidas –que lo circunscriben a aquellos que contienen pensamientos por signos escritos–. La definición que puede encontrarse en la obra de Chiovenda¹ y que ha sido una de las más influyentes en la doctrina procesal, lo considera toda representación material destinada –e idónea– para reproducir una cierta manifestación del pensamiento. Con el término representación se hace posible englobar no sólo la escritura, sino también a todo otro medio. De este modo, se alejan los problemas que puedan suscitar los avances tecnológicos: documento, en general, es una cosa que contiene la representación de un hecho sucedido. Al hacerse mención de cosa, bien puede pensarse en el soporte, que es diferente del hecho o acto jurídico que representa. (Calvinho, 2012)

Así pues, “el documento es todo objeto producido, directa o indirectamente, por la actividad del hombre y que, representa una cosa, un hecho o contiene una manifestación del pensamiento.” (Parra Quijano, I Convención Internacional de Derecho Informático, Documentación y Documento Electrónico , 2006).

Desde la noción clásica del documento, se analiza la evolución conceptual de este término, considerando las perspectivas de la forma, signo y medio, y atendiendo, en cada caso, el cambio en la noción por comparación entre documento y documento electrónico, surgido por las tecnologías de la información y la comunicación. (Marzal & Gonzales, 2010, pág. 84).

Por su parte, la definición de documento electrónico corresponde con la de mensaje de datos que trae la ley 527 de 1999 en su artículo 2do: La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.

¹ Giuseppe Chiovenda. Nacido en Premosello en 1872, fallecido en Novara en 1937. Jurista italiano. Como se citó en (Calvinho, 2012) *Principios de derecho procesal civil*. Trad. española de la 3° ed. italiana de José Casáis y Santaló. Madrid: Reus.

5.1.1. Documento como forma

La forma debe entenderse como objeto en relación con un formalismo; es decir, que este objeto o inscripción responde a las reglas que lo constituyen. Esta noción nos lleva a lo que en derecho romano se denominaba el *instrumentum* y que da lugar a las formalidades y condiciones de legalidad del escrito jurídico. Este documento se percibe de manera directa hacia su modo de lectura, y aleja, por tanto, cualquier posibilidad de interacción con el documento y su contenido. El documento electrónico, por su forma, es la concatenación de una estructura electrónica y unos datos digitales, por lo demás, tiene como aporte sumamente interesante que la forma se convierte sin dificultad en fondo, o contenido. De una manera perfectamente integrada, el documento electrónico se manifiesta y se utiliza manipulando sus códigos textuales, icónicos y auditivos. (Marzal & Gonzales, 2010, págs. 87, 88).

Es entonces que se puede definir el documento electrónico, respecto a su forma, como el conjunto de datos organizados a partir de una estructura estable, asociada a reglas formales que permiten una mutua legibilidad entre su autor intelectual y sus lectores. (Pedauque, 2003).

5.1.2. Documento como signo

El documento se concibe como un objeto significante y contenedor semántico, que podrá tener en cuenta la forma, si es portadora de sentido. La estructura, pues, puede ser significativa, o sea, ser un signo de inteligibilidad, ya que en contextos de lenguajes de especialidad, la estructura diplomática del documento, sus partes metódicas, signos de autenticación y lenguaje formal, producen una contundencia semántica indiscutible.

El cambio que se opera en el documento electrónico es muy importante y se encuentra en los signos con los que acoge el contenido. Las posibilidades tecnológicas hacen que el documento electrónico sea interactivo, de modo que su contenido no está en modo alguno cerrado cuando lo edita su autor. Es más, el documento electrónico tiene, y debe tener, por vocación, que después de cada lectura su contenido se transforme y enriquezca. Por otro lado, la propia naturaleza del documento electrónico lo convierte en dinámico. Esta noción se refiere no sólo a que integra textos de diferentes códigos semióticos, como la escritura, la imagen estática y móvil, y el sonido, sino que toda su potencialidad reposa en los enlaces e hipervínculos a los que remite y por los que es enlazado. Más aún, un documento electrónico, por su estructura tecnológica, tiene, y debe tener, la vocación de ser reutilizable, esto es, que las partes de su contenido puedan utilizarse con distintas funcionalidades según el contexto de uso. El documento electrónico, desde esta perspectiva conceptual, se concibe como un formato electrónico, capaz de soportar mediante signos bien estructurados una interactividad, dinamicidad y reutilización que facilite el camino de la información digital al conocimiento. (Marzal & Gonzales, 2010, págs. 88, 89).

5.1.3. Documento como medio

Esta noción considera y analiza el documento como un fenómeno social, un vector de la comunicación. Esta faceta del documento toma sus raíces en la pragmática, desde el punto de vista de la comunicación en una organización o colectividad. En el documento, esta perspectiva le suponía otorgarle un valor, de modo que su inscripción y símbolos le conferían una “legitimidad”, sea cual fuere la naturaleza de ésta (legal, científica, etc.). La noción de legitimidad, de forma específica, tiene un gran impacto en el derecho. La validez del documento procede de sus autores, su procedimiento normalizado, símbolos de autenticación, efectividad en la vida pública, norma a la que se atiene y a la que sirve. El documento, por tanto, se entiende como un texto conforme con un procedimiento. El valor del documento electrónico y su legitimidad, deriva de una alteración considerable de los símbolos de autenticación. Es bien cierto que hay progresos notabilísimos en la encriptación de documentos electrónicos, como también un esfuerzo normativo en el reconocimiento legal y legítimo de los signos de autenticación digitales como las firmas electrónicas. (Marzal & Gonzales, 2010, págs. 89, 90).

Ramírez Gómez (2008), afirma que el documento como medio de prueba se materializa en una cosa mueble que cumple una función representativa; coligiéndose así como elementos integrantes de su estructura: la corporalidad (cosa mueble), la subjetividad (el autor) y el contenido (signos de la representación).

5.2. Elementos del documento

5.2.1. Cosa mueble

Relacionada directamente con la función representativa, el documento se califica como cosa mueble porque puede ser transportado al proceso judicial para que allí obre como medio de prueba.

Así se refiere el inciso primero del artículo 243 del Código General del Proceso:

“Son documentos los escritos, impresos, planos, dibujos, cuadros, mensajes de datos, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, videograbaciones, radiografías, talones, contraseñas, cupones, etiquetas, sellos y, en general, todo **objeto mueble** que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares.” (Negrita fuera del texto).

Resulta criticable que las inscripciones en lápidas, monumentos, edificios o similares, tengan carácter de cosa mueble, pues para ellas poder obrar en el proceso,

ante la dificultad de su transporte, se entienden adheridas a bienes inmuebles, por lo que se requiere de otros medios de prueba, tales como el testimonio, el dictamen de peritos, la inspección judicial y la misma prueba documental (fotografías, videos o cintas que representen las inscripciones), caso en el cual no serían cosas muebles propiamente dichas.

5.2.2. El sujeto

Hace referencia al autor del documento. Elemento que está implícito en el ser mismo del documento porque éste sólo tiene entendimiento como una producción humana.

Se introduce en la definición de documento el elemento subjetivo al consagrar que éste es toda expresión de persona conocida o conocible, negándole valor probatorio al documento anónimo, precisamente por no quedar al descubierto su autoría.

El concepto de autor debe comprenderse desde el ángulo de la creación intelectual (Ramírez Gómez, 2008).

5.2.3. Signos de representación (contenido)

“El contenido del documento se refiere a su texto, a su tenor, a los signos con los cuales se hace la representación, o se expresa el hecho representado, que en todo caso deben ser inteligibles.” (Ramírez Gómez, 2008).

Carnelutti (como se citó en Ramírez Gómez, 2008) piensa que el contenido del documento, según la teoría de la representación, está definida por la representación de un hecho. Agregando, que el mecanismo de la representación estriba en la sustitución de un hecho por otro como objeto de la percepción para la determinación de la misma idea. La representación supone dos hechos: el hecho representativo, que es el hecho subrogante, y el hecho representado, que es el hecho subrogado.

Parra Quijano (2003), percibe el documento electrónico como aquel que:

1. Tiene cuerpo (consta), tiene un soporte material.
2. Contiene un mensaje en lenguaje electrónico que puede ser además de texto; voz, datos, videos, imágenes, etc.
3. Está escrito en un código determinado.
4. Tiene grafía y puede ser atribuido (autenticidad) a una persona determinada.

5.3. Aspectos básicos del documento y el documento electrónico

Cuando alguien recibe un documento, éste procede a verificar al menos los siguientes aspectos de dicho documento (Parra Quijano, Tratado de la Prueba Judicial: Los Documentos, 2003):

5.3.1. Integridad

Se verifica que el documento esté completo, que no falte ninguna hoja, que no esté mutilado, que no exista ningún signo de alteración, tachado, modificación o falsificación.

5.3.2. Autenticidad

Se verifica que la persona que lo firmó o que alega que lo firmó realmente lo haya hecho, esto se puede realizar mediante la verificación de los sellos de notaría adjuntos al documento o verificando la firma digital.

5.3.3. Confidencialidad

En algunos casos es importante que los documentos no sean de dominio público, y que la información sea solamente accesible por personas autorizadas. Este aspecto puede ser verificado analizando si el sobre en el cual fue enviado no fue alterado, cambiado o abierto.

En el siguiente cuadro, se puede ver con más claridad los aspectos básicos antes mencionados:

	Documento en papel	Documento Electrónico
--	---------------------------	------------------------------

<p>Integridad: ¿Cómo se asegura la integridad de un documento?</p>	<p>Se utiliza una empresa de correo y/o envíos confiables (tal como correo certificado o sistemas similares), igualmente se puede utilizar un sobre de correo con alguna clase de sello de seguridad.</p>	<p>Se utiliza una técnica de la criptografía² denominada firma digital que además de permitir la verificación de la integridad permite verificar simultáneamente la autenticidad del documento.</p>
<p>Autenticidad: ¿Cómo se asegura la autenticidad de un documento?</p>	<p>Se utilizan los servicios de una notaría como testigo del acto voluntario de la firma del documento.</p>	<p>Se utiliza una técnica de la criptografía denominada firma digital que permite la verificación de la autenticidad del documento.</p>
<p>Confidencialidad: ¿Cómo se asegura la confidencialidad de un documento?</p>	<p>Se puede utilizar un sobre adecuadamente sellado y con algún tipo de protección que le permita al receptor analizar el sobre y determinar si éste fue o no abierto durante el envío. De la misma forma se utiliza un medio de envío confiable.</p>	<p>Se utiliza una técnica de la criptografía denominada cifrado³. De esta forma se asegura que solo las personas que cuentan con acceso a una clave pueden leer el documento.</p>

Figura 3

Fuente: (Parra Quijano, Tratado de la Prueba Judicial: Los Documentos, 2003).

5.4. Antecedentes normativos

Es innegable y evidente la transformación que ha tenido la sociedad actual con la creciente evolución de las nuevas tecnologías en los últimos años y Colombia no podía ser ajena a esa realidad, ya que la materialización del pensamiento no se da únicamente en papel, puesto que los avances tecnológicos se han encargado de sustituir ese papel, documento tradicional, por el documento electrónico.

² Es la técnica o ciencia dirigida al estudio de la ocultación, disimulación, o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones. (Parra Quijano, Tratado de la Prueba Judicial: Los Documentos, 2003, pág. 188).

³ Es la transformación de datos a una forma que es imposible entender sin la apropiada clave. Su propósito fundamental es asegurar confidencialidad manteniendo la información protegida incluso si alguien no autorizado tiene acceso a la información. La única forma de descifrar el mensaje es por medio de una clave. (Parra Quijano, Tratado de la Prueba Judicial: Los Documentos, 2003, pág. 188).

El proceso de replicar documentos de papel en un contexto digital se llama desmaterialización, que desde el punto de vista jurídico, un documento desmaterializado debe tener el mismo significado del documento de papel sin sacrificar la eficacia legal y las ventajas del documento electrónico. Teniendo como reto, suplir la función adquirida por el papel en el ámbito consuetudinario, jurisprudencial, doctrinario y legal. (Palacio Ochoa & Rojas Jimenez, 2005).

Fue necesaria entonces, la creación de una Ley que definiera y reglamentara el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, por tal razón el 18 de agosto de 1999, se expidió la Ley 527, la cual fue fruto de la recomendación de la Asamblea General de la ONU, mediante Resolución 51/162 de 1996 que aprobó la ley modelo sobre Comercio Electrónico elaborada por la Cnudmi (Comisión de las Naciones Unidas para el Desarrollo del Derecho Mercantil Internacional) y que fue base fundamental para el proyecto que impulsó dicha ley desde el año 1998.

La Ley 527 de 1999, está conformada por 47 artículos distribuidos en cuatro partes, así:

- Parte I: Parte general.
 - Capítulo I: disposiciones generales.
 - Capítulo II: aplicación de los requisitos jurídicos de los mensajes de datos.
 - Capítulo III: comunicación de los mensajes de datos.
- Parte II: comercio electrónico en materia de transporte de mercancías.
- Parte III: firmas digitales, certificados y entidades de certificación.
 - Capítulo I: firmas digitales.
 - Capítulo II: entidades de certificación.
 - Capítulo III: certificados.
 - Capítulo IV: disposiciones varias.
- Parte IV: Reglamentación y vigencia.

Esta norma no está únicamente destinada a regir las técnicas actuales de comunicación, sino que pretende ser apta para acomodar todos los avances técnicos de información. En ese mismo sentido, la definición de mensajes de datos está formulada en términos tales que abarca todo tipo de mensajes generados, archivados o comunicados en alguna forma distinta al papel. (Palacio Ochoa & Rojas Jimenez, 2005). Este reconocimiento jurídico de los mensajes de datos, es tal vez, el principal logro de la Ley.

Así las cosas, desde el punto de vista jurídico, un mensaje de datos debe ser tratado igual que un mensaje escrito en papel. Por lo tanto, cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, siempre y cuando la información que éste contiene sea accesible para su posterior consulta (Art.6).

Se establece además la admisibilidad de los mensajes de datos como pruebas en actuaciones administrativas o judiciales. Por lo tanto, su eficacia, validez y fuerza obligatoria y probatoria no podrán desconocerse en tales actuaciones ni en las privadas. Eliminando así, obstáculos jurídicos que pueden impedir la admisión de la prueba electrónica y proporciona unos principios sobre como evaluar la fuerza probatoria de la misma. (Palacio Ochoa & Rojas Jimenez, 2005).

Sin embargo, la ley modelo, no fue el primer acercamiento que tuvo la legislación colombiana en el tema, ya desde el Decreto 1400 de 1970 (Código de Procedimiento Civil), en su artículo 251, se mencionaban las distintas clases de documentos, así: “Son documentos los escritos, impresos, planos, dibujos, cuadros, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, radiografías, talones, contraseñas, cupones, etiquetas, sellos y, en general, todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares”. (Presidencia, Decreto 1400, 1970). Así también, el artículo 175 del mismo Código, contempló los “Medios de Prueba: Sirven como pruebas, la declaración de parte, el juramento, el testimonio de terceros, el dictamen pericial, la inspección judicial, los documentos, los indicios y cualesquiera otros medios que sean útiles para la formación del convencimiento del juez”. (Presidencia, Decreto 1400, 1970). (Subraya fuera del texto).

En la Ley 98 del 20 de diciembre de 1993, por medio de la cual se dictan normas sobre democratización y fomento del libro colombiano, su artículo segundo equipara las publicaciones tradicionales con las realizadas por medios electromagnéticos: “Para los fines de la presente Ley se consideran libros, revistas, folletos, coleccionables seriados, o publicaciones de carácter científico o cultural, los editados, producidos e impresos en la República de Colombia, de autor nacional o extranjero, en base papel o publicados en medios electro-magnéticos”. (Congreso, Ley 98, 1993).

Con la ley 223 del 20 de diciembre de 1995, se eleva la factura electrónica a la categoría de factura de venta, tal y como lo contempla el artículo 37:

Adiciónase el Estatuto Tributario con el siguiente artículo:

"Artículo 616-1. Factura o documento equivalente. La factura de venta o documento equivalente se expedirá, en las operaciones que se realicen con comerciantes, importadores o prestadores de servicios o en las venta a consumidores finales.

Son documentos equivalentes a la factura de venta: El tiquete de máquina registradora, la boleta de ingreso a espectáculos públicos, la factura electrónica y los demás que señale el Gobierno Nacional.

Dentro de los seis meses siguientes a la vigencia de esta Ley el Gobierno Nacional reglamentará la utilización de la factura electrónica". (Congreso, Ley 223, 1995).

Efectivamente, mediante el Decreto 1094 del 21 de junio de 1996, el Gobierno Nacional reglamentó la utilización de la factura electrónica, tal y como lo señaló el inciso final del artículo anterior.

El 5 de diciembre de 1995, con el Decreto 2150, se estableció, en el artículo 26, la utilización de sistemas electrónicos de archivo y transmisión de datos, así:

Las entidades de la Administración Pública deberán habilitar sistemas de transmisión electrónica de datos para, que los usuarios envíen o reciban información requerida en sus actuaciones frente a la administración.

En ningún caso las entidades públicas podrán limitar el uso de tecnologías para el archivo documental por parte de los particulares, sin perjuicio de los estándares tecnológicos que las entidades públicas adopten para el cumplimiento de algunas de las obligaciones legales a cargo de los particulares. (Presidencia, Decreto 2150, 1995).

Una prueba fehaciente del reconocimiento del documento electrónico (validez y eficacia) en la legislación nacional nos la brinda la Ley Estatutaria de la Administración de Justicia cuando en su artículo 95 dispone (Rengifo García, 2000):

Tecnología al servicio de la administración de justicia. El Consejo Superior de la Judicatura debe propender por la incorporación de tecnología de avanzada al servicio de la administración de justicia. Esta acción se enfocará principalmente a mejorar la práctica de las pruebas, la formación, conservación y reproducción de los expedientes, la comunicación entre los despachos y a garantizar el funcionamiento razonable del sistema de información.

Los juzgados, tribunales y corporaciones judiciales podrán utilizar cualesquier medios técnicos, electrónicos, informáticos y telemáticos, para el cumplimiento de sus funciones.

Los documentos emitidos por los citados medios, cualquiera que sea su soporte, gozarán de la validez y eficacia de un documento original siempre que quede garantizada su autenticidad, integridad y el cumplimiento de los requisitos exigidos por las leyes procesales.

Los procesos que se tramiten con soporte informático garantizarán la identificación y el ejercicio de la función jurisdiccional por el órgano que la ejerce, así como la confidencialidad, privacidad, y seguridad de los datos de carácter personal que contengan en los términos que establezca la ley. (Congreso, Ley 270, 1996).

Derecho de petición electrónico: mediante circular del 14 de mayo de 1997, expedida por la Secretaría Jurídica de la Presidencia de la República, se determina que el derecho de petición de los ciudadanos que se realice mediante el uso de las modernas herramientas tecnológicas (internet, por ejemplo), debe ser asumido como si fuese una petición de la que trata el artículo 23 de la Carta Política. (Rengifo García, 2000).

En 1999, con el Decreto 1122, por el cual se dictan normas para suprimir trámites, facilitar la actividad de los ciudadanos, contribuir a la eficiencia y eficacia de la Administración Pública y fortalecer el principio de la buena fe, modificó el decreto 2150 en lo concerniente con los medios tecnológicos, dejando el artículo 26 de este decreto así:

“Artículo 26. Medios tecnológicos. Se autoriza a la Administración Pública el empleo de cualquier medio tecnológico o documento electrónico, que permita la realización de los principios de igualdad, economía, celeridad, imparcialidad, publicidad, moralidad y eficacia en la función administrativa, así como el establecimiento de condiciones y requisitos de seguridad que para cada caso sean procedentes, sin perjuicio de las competencias que en la materia tengan algunas entidades especializadas.

Toda persona podrá en su relación con la administración hacer uso de cualquier medio técnico o electrónico, para presentar peticiones, quejas o reclamaciones ante cualquier autoridad. Las entidades harán públicos los medios de que dispongan para permitir esta utilización.

Los mensajes electrónicos de datos serán admisibles como medios de prueba y su fuerza probatoria será la otorgada en las disposiciones del capítulo VIII del título XIII, sección III Libro Segundo del Código de Procedimiento Civil, siempre que sea posible verificar la identidad del remitente así como la fecha de recibo del documento.”

Este decreto fue declarado inexecutable por la Sentencia de la Corte Constitucional C-923 de 1999.

El actual Código General del Proceso, Ley 1564 del 12 de julio de 2012, habla del **documento auténtico**, refiriéndose a este en el artículo 244 de la siguiente manera:

“Es auténtico un documento cuando existe certeza sobre la persona que lo ha elaborado, manuscrito, firmado, o cuando exista certeza respecto de la persona a quien se atribuya el documento.

Los documentos públicos y los privados emanados de las partes o de terceros, en original o en copia, elaborados, firmados o manuscritos, y los que contengan la reproducción de la voz o de la imagen, se presumen auténticos, mientras no hayan sido tachados de falso o desconocidos, según el caso.

También se presumirán auténticos los memoriales presentados para que formen parte del expediente, incluidas las demandas, sus contestaciones, los que impliquen disposición del derecho en litigio y los poderes en caso de sustitución.

Así mismo se presumen auténticos todos los documentos que reúnan los requisitos para ser título ejecutivo.

La parte que aporte al proceso un documento, en original o en copia, reconoce con ello su autenticidad y no podrá impugnarlo, excepto cuando al presentarlo alegue su falsedad. **Los documentos en forma de mensaje de datos se presumen auténticos.**

Lo dispuesto en este artículo se aplica en todos los procesos y en todas las jurisdicciones.” (Negrita fuera del texto).

Actualmente, el decreto 2364 del 22 de noviembre de 2012 reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica:

“Artículo 7°. Firma. Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:

- a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación;
- b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma.”

5.5. Importancia del documento electrónico en Colombia

En Colombia se han establecido varias estrategias y campañas de tipo cultural que buscan reducir el consumo de papel, que ofrecen importantes oportunidades en la generación de buenos hábitos en su uso tanto en organizaciones privadas como públicas, lo cual promueve la eficiencia y productividad, reduciendo costos, tiempo y espacios de almacenamiento (T.I.C & línea), lo que se evidenció con el decreto 19 de 2012, por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.

Estas estrategias han propendido generar una eficiente gestión documental a través del uso de la tecnología, pretendiendo demostrar que es posible reducir significativamente los recursos tanto económicos como materiales, consiguiendo así, un mayor resultado con el mínimo de actividad, tanto del ciudadano como de la administración, buscando la celeridad en los trámites.

En el documento electrónico, juega un papel preponderante la manera como se haya generado el mensaje de datos. Si es un simple mensaje de datos que no esté dotado de ningún método que asegure quién ha emitido dicho mensaje, o si este ha sido alterado después del momento de la transmisión, seguramente no podrá contar con la misma eficacia y validez probatoria de un mensaje que cuente con este tipo de medidas de seguridad, como por ejemplo, aquellos que poseen una firma digital que cuenta con un certificado emitido por una entidad certificadora. (Flórez, 2014).

El documento electrónico es importante también, porque al estar nuestro país en una modernidad tardía, poco a poco lo va acercando a una vanguardia, que aunque en principio es difícil de asimilar y comprender, ayuda a abrir un poco la mente frente a nuevas alternativas, lo que permite ampliar los horizontes y dejar el temor de aceptar nuevas tecnológicas, cultivando así la confianza, tanto en el sistema como en las personas que nos rodean.

5.6. Utilización del documento electrónico como medio de prueba en Colombia

La prueba son las razones o motivos que nos conducen al grado de conocimiento de la existencia o inexistencia de un hecho. Los medios de prueba, son los instrumentos, herramientas que sirven

de vehículo para llevarle ese conocimiento al juez. Probar, es pues, la acción y efecto de llevarle al juez el conocimiento sobre unos hechos existentes o inexistentes. (Cuesta Davu, 2015).

El documento es entonces un medio de prueba, pero muchas veces puede ser objeto de prueba, como cuando nos dedicamos a averiguar su autenticidad, es decir, quién es el autor, si el documento fue alterado, en qué momento lo fue, en qué lugar fue otorgado, dónde ha estado el documento como objeto. (Parra Quijano, Tratado de la Prueba Judicial: Los Documentos, 2003, pág. 15). Pero éste, es también fuente de prueba que, llegado el caso de que del conflicto entre las partes derive un litigio, puede ser incorporado al acervo probatorio a través de cierta actividad de los interesados. En consecuencia, tendremos por un lado la fuente de la prueba, que es el documento, y por el otro la prueba documental, que es el medio por el que se busca demostrar algo y se relaciona con la antedicha actividad de las partes. (Calvinho, 2012, pág. 42).

De acuerdo con la Norma NTC/ISO 15489-1, para que sirvan de apoyo a la gestión de las entidades y puedan servir de prueba, los documentos electrónicos deben poseer ciertas

Características

5.6.1. Autenticidad

Como se dijo en el primer capítulo, se refiere a que pueda demostrarse que el documento es lo que afirma ser, que ha sido creado o enviado por la persona que afirma haberlo creado o enviado, y que ha sido creado o enviado en el momento que se afirma. Para garantizar la autenticidad de los documentos, las entidades deben implantar y documentar políticas y procedimientos para el control de la creación, recepción, transmisión, mantenimiento y disposición de los documentos, de manera que se asegure que los creadores de los mismos estén autorizados e identificados y que los documentos estén protegidos frente a cualquier adición, supresión, modificación, utilización u ocultación no autorizadas.

5.6.2. Integridad

Hace referencia al carácter completo e inalterado del documento electrónico. Es necesario que un documento esté protegido contra modificaciones no autorizadas. Las políticas y los procedimientos de gestión de documentos deben decir qué posibles anotaciones o adiciones se pueden realizar sobre el mismo después de su creación y en qué circunstancias se pueden realizar. No obstante, cualquier modificación que se realiza debe dejar constancia para hacerle su seguimiento.

5.6.3. Fiabilidad

Su contenido representa exactamente lo que se quiso decir en él. Es una representación completa y precisa de lo que da testimonio y se puede recurrir a él para demostrarlo. Los documentos de

archivo deben ser creados en el momento o poco después en que tiene lugar la operación o actividad que reflejan, por individuos que dispongan de un conocimiento directo de los hechos o automáticamente por los instrumentos que se usen habitualmente para realizar las operaciones.

5.6.4. Disponibilidad

Se puede localizar, recuperar, presentar, interpretar y leer. Su presentación debe mostrar la actividad que lo produjo. El contexto de los documentos debe ser suficientemente claro y contener la información necesaria para la comprensión de las operaciones que los crearon y usaron. Debe ser posible identificar un documento en el contexto amplio de las actividades y las funciones de la organización. Se deben mantener los vínculos existentes entre los documentos que reflejan una secuencia de actividades.

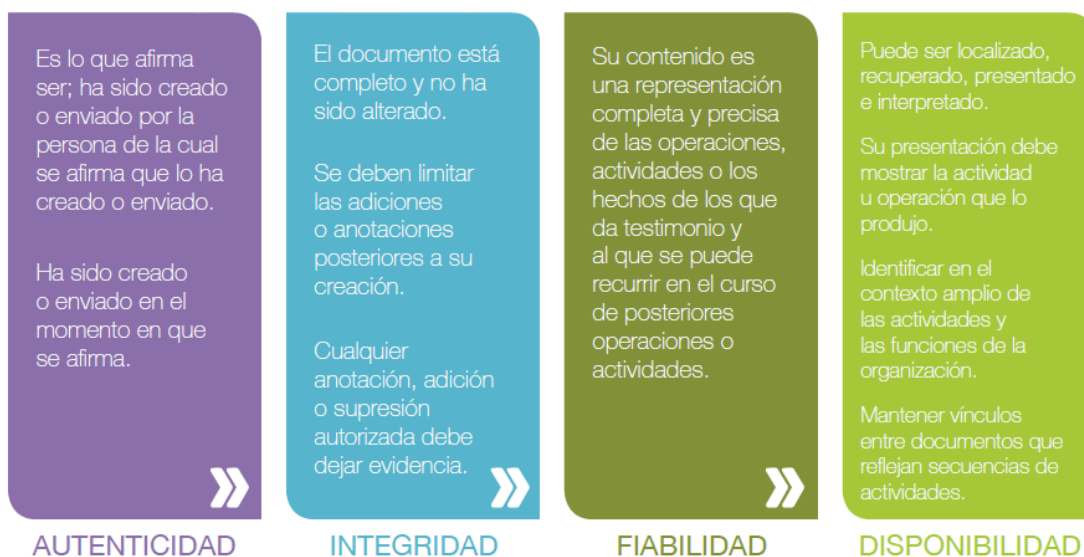


Figura 4

Fuente: (T.I.C & línea).

Para hablar de prueba electrónica necesariamente tenemos que referirnos a mensajes de datos acompañado de la existencia de una firma digital.

El valor probatorio de los mensajes de datos, está ligado con la integridad del documento, o de la información contenida en él, es decir, que su integridad determina su originalidad o autenticidad. Es entonces como ese documento debe garantizar condiciones de idoneidad y aptitud probatoria, y por ende la inalterabilidad, lo que es rol encomendado a los sistemas de traducción criptográfica (escritura oculta en técnicas de cifrado o codificado).

Se siente temor frente a estas clases actuales de documentos por la incertidumbre que se genera, ya que no obstante la existencia de sistemas de seguridad, existen riesgos de manipulación, pérdida de identidad y la posibilidad de presentarse yerros en la transmisión y comprensión de datos.

El documento electrónico como medio de prueba, es una prueba indirecta, objetiva, histórica y con contenido de representación, en ocasiones declarativo y en ocasiones representativo, contiene una declaración o confesión, o un simple acto de voluntad. Es prueba indirecta, en cuanto que el documento es el resultado de un acto humano, pero en sí mismo es una cosa o un objeto; no es un acto representativo, como el testimonio y la confesión, sino un objeto que sirve para representar un hecho cualquiera. (Devis Echandía, 2015).

Puede ser visto y entendido como una confesión extrajudicial, o declaración extrajudicio, la diferencia con el documento material, es que el documento electrónico siempre es un documento extraprocesal, además, es prueba indirecta cuando pruebe la existencia de otro documento original de un acto o negocio jurídico por probar. (Devis Echandía, 2015).

Sin embargo, pese a los esfuerzos que ha hecho la ley 527 de 1999 para corregir la deficiencia legislativa frente al derecho informático, subsiste la anomia especialmente por la ausencia de una reglamentación más general, por cuanto la ley apenas se ocupa del mensaje de datos y la firma digital, en tanto ellas son la expresión más clara del documento electrónico.

Parra Quijano (como se citó en Ramírez Gómez, 2008) señala que la prueba informática puede ser tomada de tres maneras: **a)** Como presunción o indicio; **b)** como complemento de prueba escrita, y bajo este tratamiento en consideración a que la prueba no se desnaturaliza cuando para su conocimiento se acude a otros medios, se abre un panorama amplio para ella dentro de las normas vigentes; y **c)** constituir el comienzo de una prueba escrita, esto es, documento proveniente de un tercero que hace verosímil un hecho.

Cualquiera sea la opción válida para el momento, lo claro es el vacío legal y la necesidad de una política de ese orden sobre el tema, pues si bien hay normatividad, la desconfianza frente a esta no tan nueva forma de documento, sigue existiendo.

Ernesto Rengifo sostiene que, el valor probatorio del documento es incontestable. Con base en una interpretación lógica y funcional del derecho, la forma electrónica debe ser asimilada a la forma escrita. En consecuencia, en un proceso judicial el documento electrónico constituirá plena prueba de lo que está representando, si la persona contra quien se dirige o se esgrime no lo controvierte. Además, no ha de olvidarse que la Ley Estatutaria de la Administración de Justicia equipara el documento electrónico al documento original, si está garantizada su autenticidad e integridad.

Frente al aspecto probatorio, la Ley 527 de 1999, se refiere así:

ARTÍCULO 10. *Admisibilidad y fuerza probatoria de los mensajes de datos.* Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la

otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.⁴

En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.

ARTÍCULO 11. *Criterio para valorar probatoriamente un mensaje de datos.* Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

Teniendo en cuenta lo anterior, Jairo Parra Quijano, en la I Convención Internacional de Derecho Informático, Documentación y Documento Electrónico , 2006, indaga sobre el valor probatorio de los documentos electrónicos, refiriéndose así:

5.6.4.1.1.1.1. El documento electrónico se puede clasificar en documento público y documento privado. Documento público es el otorgado por funcionario público en ejercicio de su cargo o con su intervención. Documento privado es el que no reúne los requisitos para ser documento público. El documento público se presume auténtico.

5.6.4.1.1.1.2. Debemos afirmar que el escrito electrónico privado, que tiene firma digital, ingresa al mundo explosivo del proceso como auténtico y además íntegro, siempre y cuando se cumpla con lo que preceptúa el artículo 28 de la Ley 527 de 1999.

ARTÍCULO 28. *Atributos jurídicos de una firma digital.* Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

PARÁGRAFO. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquella incorpora los siguientes atributos:

1. Es única a la persona que la usa.
2. Es susceptible de ser verificada.

⁴ Hoy, en el Código General del Proceso, Capítulo IX del Título IV, Libro Segundo, Sección Segunda, artículos 243 a 274.

3. Está bajo el control exclusivo de la persona que la usa.
4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.
5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

5.6.4.1.1.1.3. Pero como se debe afrontar la realidad, lo cierto es que las personas realizan una serie de actos y además se comunican utilizando el correo electrónico sin que el documento tenga firma digital. ¿Qué valor probatorio tienen esos documentos privados sin ningún tipo de firma?

Como hay tanta confusión con relación a esta última hipótesis planteada, es necesario que tomemos partido si se puede tener como un principio de prueba por escrito o como indicio. Niego rotundamente (dice Parra Quijano) cualquiera de las dos hipótesis, por cuanto que se trata de una ostensible confusión de lo que son estas dos instituciones.

En efecto, cuando nos referimos a un principio de prueba por escrito, no estamos indagando sobre la autenticidad, sino sobre el contenido del documento. Resulta pertinente transcribir lo que hemos escrito en otra parte:

- El principio de prueba por escrito, como su nombre lo indica, no es sino un principio de prueba; quiere ello decir que no se puede confundir el principio de prueba por escrito con el acto mismo o contrato.
- La diferencia entre el acto mismo que solemos llamar contrato y el principio de prueba por escrito, consiste en que el primero es preconstituido y completo en su parte dispositiva, reúne todos los requisitos exigidos por la Ley, para que pueda con él invocarse del deudor incumplido o que no ejecuta totalmente su obligación, la prestación a que está obligado.
- Se llama prueba preconstituida, el escrito que se hace en el momento de la formación del contrato, a fin de que las partes, previendo futuras dificultades en la ejecución y entendimiento de sus obligaciones, se reserven la prueba de sus derechos. En el principio de prueba por escrito no se reúnen todos los elementos que debe reunir el contrato, la falta o declaración del objeto, o no enuncia completamente la cosa debida; entonces, a diferencia del acto o contrato propiamente dicho, el principio de prueba apenas da margen a la posibilidad de que el contrato se celebró; lo hace verosímil y permite reconstruirlo y completarlo en sus elementos con testigos, indicios y demás medios de prueba.

Hernando Devis Echandía, por su parte, arguye que para hablar de principio de prueba por escrito, es menester que se reúnan los siguientes requisitos:

- a) Que provenga de la parte a quien se opone o de su representante o causante.
- b) Que goce de autenticidad o que ésta se pruebe.
- c) El escrito debe hacer verosímil o probable el hecho alegado.

Como se puede observar fácilmente, no se puede hablar que un documento electrónico no firmado sea un principio de prueba por escrito, por cuanto es un concepto equivocado. (Entre otras cosas con relación al principio de prueba por escrito, es necesario establecer su autenticidad).

Tampoco es un indicio, por los siguientes motivos:

El indicio es un hecho, que por inferencia y utilizando las Reglas de la Experiencia conduce a otro hecho, que es el que interesa para la investigación. Mientras que el documento no firmado es declarativo, contiene declaraciones y debe ser apreciado como documento que no cabe duda que lo es; otra cosa es establecer su autenticidad e integridad.

Si nos preguntamos qué es ese escrito electrónico, la respuesta es obvia, es un documento, pero surge la segunda pregunta: ¿qué debemos hacer para que adquiera autenticidad?

Tendríamos dos respuestas:

1. Una genérica para todo tipo de legislación. Aportar el documento electrónico en soporte papel, es decir, ya impreso y afirmar que fue elaborado (identificar al elaborador), y acompañar un soporte electrónico con el documento. Individualizar el documento, las circunstancias en que se emitió, con qué ocasión y se puede acompañar al mismo certificado sobre si existe la cuenta de correo y para quién está creada y habilitada. Si la parte contra la cual se exhibe el documento guarda silencio a pesar de la imputación como autor, el documento adquiere autenticidad y se considera en su integridad (esa es la razón de individualizarlo).
2. Otra solución es presumirlo auténtico, cuando tiene signos de “Individualidad Electrónica”, y quien niegue la autenticidad soporta la carga de la prueba de desvirtuar esos signos de individualidad electrónica, utilizando la prueba pericial por ejemplo.

Entonces, ¿cómo se puede probar ante el juez el envío o recepción de correo electrónico, la circulación de ciertas marcas en la red o la procedencia de un mensaje de cierta persona?

Esto, de conformidad con nuestro sistema de libertad probatoria, por cualquier medio legal. Se recomienda usar un sistema confiable de almacenamiento en un medio inalterable. Guardar la información en un medio permanente e inalterable, hará más fácil demostrar un reclamo en caso de disputa. (Rengifo García, 2000, pág. 45).

5.7. Uso de la firma (electrónica y digital) para otorgar validez al documento electrónico

La facilitación del acceso a Internet ha auxiliado la expansión de las nuevas tecnologías y la actividad documental por vías electrónicas. Para establecer la autenticidad de un documento,

importa a menudo conocer la autoría. A la tradicional firma ológrafa y otros medios que desde antaño se utilizan a tal fin –como la firma a ruego, testigos, sellos, etc. – se le añaden hoy otras maneras para dejar constancia de ello, donde la innovación tecnológica ha hecho lo suyo: la firma digital, la electrónica, el PIN (Personal Identification Number), la clave, la contraseña y la huella digital, entre otros. (Calvinho, 2012).

Por otro lado, vemos necesario ampliar el concepto de validez, para el cual el jurista y iusfilósofo dinamarqués Alf Ross, tiene tres diferentes funciones y significados:

Primero, el término es usado en las corrientes exposiciones doctrinarias del Derecho vigente para indicar si un acto jurídico, por ejemplo, un contrato, un testamento o una orden administrativa, tiene o no los efectos jurídicos deseados. Se dice que el acto es inválido, o nulo si no los tiene. Esta función es interna, en el sentido de que afirmar que un acto es válido es afirmar algo “según” un sistema de normas dado. El enunciado es un juicio jurídico que aplica reglas jurídicas a determinados hechos.

Segundo, el término es usado en la teoría general del Derecho para indicar la existencia de una norma o un sistema de normas. La validez de una norma en este sentido significa su existencia efectiva o realidad, por oposición a una regla meramente imaginada o a un mero proyecto. Esta función es externa en el sentido de que afirmar que una regla o un sistema de reglas existe, es afirmar algo acerca de la regla o del sistema. El enunciado no es un juicio sino una aseveración fáctica que se refiere a un conjunto de hechos sociales.

Tercero, “validez” en ética y en derecho natural, como hecho visto, se usa para significar una cualidad apriorística, especialmente moral, llamada también la “fuerza obligatoria” del derecho, que da lugar a una obligación moral correspondiente. (Ross, 2008, pp. 214, 215).

Así las cosas, el artículo 7 de la Ley 527 de 1999, que hace referencia a la firma, establece que cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:

- a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación;
- b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.

En Colombia se han reglamentado dos mecanismos de firma: la firma electrónica y la firma digital.

- La firma electrónica representa un medio de identificación electrónico flexible y tecnológicamente neutro que se adecúa a las necesidades de la sociedad. Corresponde a métodos tales como códigos, contraseñas, datos biométricos o claves criptográficas privadas, que permitan identificar a una persona en relación con un mensaje, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la

firma, teniendo en cuenta todas las circunstancias del caso, así como cualquier acuerdo pertinente. (Ministerio de Comercio, 2012).

- La firma digital se entenderá, según el artículo segundo de la Ley 527 del 18 de agosto de 1999, como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación

De conformidad con el **principio de equivalencia funcional**, en los casos que se exija firma manuscrita en los documentos elaborados en físico, es decir, en papel, los documentos electrónicos deben satisfacer el mismo requisito. La firma electrónica permite proporcionar al documento firmado:

- a. Identificación:** avalar la identidad del firmante de manera única, demostrando que es él, y nadie más, quien ha firmado el documento.

Existen dos tipos de finalidades de la autenticación:

- a.1. Identificación del origen de los datos:** el identificado tiene relación con los datos consignados, le pertenecen y lo vinculan con el mensaje enviado.
- a.2. Identificación de entidades:** permite comparar los datos enviados con los datos almacenados en las bases y que han sido enviados anteriormente.

- b. Integridad:** asegurar que el contenido de un mensaje de datos ha permanecido completo e inalterado, independiente de los cambios que hubiera podido sufrir el medio en el que está contenido como resultado del proceso de su transmisión, archivo o presentación.
- c. No Repudio:** es la garantía de que no puedan ser negados los mensajes en una comunicación electrónica.

Existen dos tipos:

- c.1. No repudio en origen,** de tal manera que el emisor no pueda negar el mensaje que ha enviado así quiera negar tal comunicación.
- c.2. No repudio en destino,** que garantiza al emisor que su comunicación ha sido recibida sin que el receptor pueda negar tal comunicación.

El concepto general de firma electrónica incluye cualquier método o símbolo basado en medios electrónicos que tuviera por finalidad identificar a una persona, sin que tenga que dar integridad al mensaje que acompaña.

Dentro de las firmas electrónicas encontramos la firma digital, que corresponde al nivel más alto de seguridad. (T.I.C & línea). Lo anterior debido a que el modo simple y convencional de la firma electrónica, hizo que se desarrollara la CCP (Criptografía de Clave Pública) para

dar origen a las firmas electrónicas avanzadas, calificadas o reconocidas, también llamadas firmas digitales.

Requisitos para la existencia jurídica del documento electrónico

Al respecto se refiere Hernando Devis Echandía (2015), en su libro Teoría General de la Prueba Judicial, señalando como requisito los siguientes:

- a) Que se trate de un objeto con aptitud representativa originada mediante un acto humano. No hace falta que se tenga la intención de pre constituir una prueba, ni que sea declarativo.
- b) Que represente un hecho ordinario; que sea la expresión o representación de un pensamiento, un deseo, un acto de voluntad, una narración sobre hechos naturales o humanos.
- c) Que esté establecida o presumida su autenticidad. Este requisito es indispensable, así se trate de instrumentos declarativos o dispositivos, una fotografía, un documento electrónico, el juez deberá estar completamente seguro de la autenticidad del documento, para si quiera considerarlo como medio de prueba. En el documento electrónico su autenticidad implica la certeza sobre la persona quien los suscribe.
- d) Que no exista prueba legalmente válida en contra: la fuerza probatoria del documento y el mérito de las pruebas en contrario deben de ser subvaloradas.
- e) Que el contenido del documento sea convincente. Que el documento sirva para darle al juez por si solo o conjuntamente con otras pruebas, el convencimiento sobre los hechos investigados, o que se pretenden demostrar.
- f) Que no se haya llevado el proceso de obtención del documento bajo violación de reserva o secreto que la ley consagrado.
- g) Que tenga valor probatorio. Este requisito es consecuencia de los anteriores, rige para todo tipo de pruebas. No puede existir un medio de prueba, ni por tanto, un documento en estricto sentido, sin ninguna justificación probatoria; pero el que la tenga no significa necesariamente resulte eficaz para probar el hecho que se quiso documentar, es decir, para reproducirle al juez convencimiento sobre tal hecho.

5.8. Repaso del documento electrónico en algunas legislaciones de Latinoamérica (Derecho Comparado)

Con base en la tesis “La realidad latinoamericana en gestión de documentos electrónicos” de Aida Mendoza Navarro (2006), realizaremos un útil repaso, que nos permite observar en

términos generales el estado y tratamiento que ha tenido el documento electrónico, la firma digital y su autenticidad, en algunas legislaciones de Latinoamérica:

Argentina

En Argentina la Ley N° 11.672, de 1995 Complementaria Permanente de Presupuesto, fue sustituida en su artículo 49, por el artículo 30 de la Ley 24.624 del 28 de diciembre de 1995, la cual legisla sobre el uso de los medios informáticos para la documentación financiera. El reglamento de la citada Ley, aprobado por Decisión Administrativa 43/96 sobre soporte electrónico u óptico indeleble: “Designa los medios de memorización de los datos, cuya tecnología conlleve a la modificación irreversible de su estado físico y garantice la estabilidad, perdurabilidad, inmutabilidad e inalterabilidad.”

Adicionalmente, El 12 de noviembre del 2001, la Ley 25.5068 estableció el uso de la firma digital y la firma electrónica. En su artículo 5° establece el cumplimiento de la exigencia legal de conservar documentos, registros o datos, conforme a la legislación vigente, la que podrá quedar satisfecha con la conservación de los documentos digitales firmados digitalmente y su certificación se hace conforme a los procedimientos legales correspondientes.

Brasil

En Brasil El Decreto N° 3.505/2000 establece una política de seguridad de la información en los órganos y entidades de la Administración Pública Federal que tiene como presupuestos básicos concienciar a la Administración Pública sobre la importancia de la información procesada y sobre el riesgo de su vulnerabilidad. El artículo 3° legisla sobre las garantías para la información ‘asegurando la confidencialidad, integridad, autenticidad, no repudio y disponibilidad de los datos e información’, y de esta manera hace referencia a los sistemas de información, lo que incluye los documentos electrónicos.

El artículo 6 del Decreto N° 3.587/00, establece las medidas necesarias para que los documentos gestionados electrónicamente sean equivalentes en su validez, reconocimiento y autenticidad que los originarios en papel.

Chile

En cuanto a Chile, la ley 19.799 de 26 de marzo del 2002, legisla sobre los documentos electrónicos, la firma electrónica y los servicios de certificación de dicha firma. Ésta regula los documentos electrónicos y sus efectos legales, la utilización en ellos de la firma electrónica, la

prestación de servicios de certificación de estas firmas y el procedimiento de acreditación al que podrán sujetarse los prestadores del servicio de certificación, con el objeto de garantizar la seguridad en su uso. El artículo 3 de esta ley consagra que los documentos electrónicos que tengan la calidad de instrumento público, se requiere la suscripción mediante firma electrónica avanzada que es aquella certificada por un prestador acreditado, creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere; permite la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría. Estos documentos pueden presentarse en juicio y, en el evento de que sean usados como medio de prueba, los documentos públicos harán fe plena de acuerdo con las reglas generales.

Costa Rica

De otro lado, Costa Rica ha sido un país más bien escéptico y reacio frente a la administración de documentos electrónicos, y por lo tanto, antes de legislar ampliamente sobre la materia expidió una “Directriz de regulaciones técnicas generales para la administración de documentos electrónicos, aplicables al Sistema Nacional de Archivos de Costa Rica” la cual precede a la ley 8454 de certificados, firma digitales y documentos electrónicos, que es una de las más recientes en Latinoamérica, y se aplica a toda clase de transacciones y actos jurídicos, públicos o privados, salvo disposición legal en contrario. Uno de sus objetivos es la desregulación de trámites. Dicha ley, reconoce a los documentos electrónicos fuerza probatoria en las mismas condiciones que a los documentos físicos.

Ecuador

Mientras en Ecuador, la ley de Comercio Electrónico, firmas y mensajes de datos, N° 67 del 2002, regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y la telemática, la prestación de servicios electrónicos a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas. Dentro de los principios generales se establece que los mensajes de datos tendrán igual valor jurídico que los documentos escritos, dejando su eficacia, valoración y efectos al cumplimiento de lo establecido en la ley y su reglamento. En cuanto a la firma electrónica, tiene igual validez que una firma manuscrita y se le reconocen los mismos efectos jurídicos en relación con los datos consignados en documentos escritos, y es admitida como prueba en juicio. La norma comprende equiparadamente la firma electrónica y digital que otros países legislan por separado.

México

En México por decreto del 8 de abril de 2003 se reformaron y adicionaron diversas disposiciones del Código de Comercio en materia de firma electrónica. El artículo 89 instituye la Firma Electrónica y la Firma Avanzada, la primera produce los mismos efectos jurídicos que la firma

autógrafa, siendo admisible como prueba en juicio. La segunda establece algunos requisitos taxativos entre ellos se demanda que los datos de creación de la firma están bajo el control exclusivo del firmante y que sea posible detectar cualquier alteración de la firma. En la Ley Federal de Responsabilidades Administrativas de los servidores públicos se menciona los archivos electrónicos. En el Código Federal de Procedimientos Civiles se adiciona el artículo 210-A que a partir de su segundo párrafo demanda la fiabilidad del método en que se generó la información para gozar de fuerza probatoria, además debe ser accesible para posterior consulta siempre que se mantenga íntegra.

Perú

Para el caso de Perú, El Decreto Legislativo N° 681 del 11 de octubre de 1991 fue el primer dispositivo legal sobre la materia y fue reglamentado por el Decreto Supremo N° 009-92-JUS de 1992. Comenzando en la empresa privada y luego en la Administración Pública.

La ley 26612 de 17 de mayo de 1996, en su artículo 3° añade al artículo 5° del Decreto Legislativo No 681 el inciso e) por el cual autoriza el uso de la firma ‘informática’; ésta deberá ser inalterable, fija, durable y comprobable su autenticidad en forma indubitable, pero, además modifica el artículo 234 del Código Procesal Civil, reconociendo la calidad de documento público o privado en medios informáticos y de la telemática en general y según el artículo 9° éstos pueden ser utilizados para cualquier tipo de transferencia de datos y otros servicios de valor añadido conservando su valor probatorio.

Uruguay

En Uruguay se resalta la ley 16.736 de 5 de enero de 1996, sobre las administraciones públicas que insta a impulsar el empleo y aplicación de medios informáticos y telemáticos para el desarrollo de sus actividades garantizando a los administrados el acceso a las informaciones de su interés. En las actuaciones administrativas la firma autógrafa puede ser sustituida por contraseñas o signos informáticos adecuados. Más adelante por el Decreto 382/2003, se reglamenta el uso de la firma digital y el reconocimiento de su eficacia jurídica, siempre que esté debidamente autenticada por claves u otros procedimientos seguros de acuerdo a la tecnología informática, se otorga idéntico valor probatorio al que tiene la firma manuscrita con respecto al documento en soporte de papel.

Venezuela

Finalmente, en Venezuela el decreto N° 1.204 del 2001 otorga 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. Se entiende que los documentos en formato electrónico gozarán de eficacia probatoria

en tanto se haya conservado su integridad y cuando la información contenida en dicho mensaje de datos esté disponible.

6. Conclusiones

Con base en la anterior investigación, es posible resaltar las siguientes conclusiones:

La disciplina jurídica no debe estar rezagada ante el avance tecnológico. Antes bien, sin transgredir los principios de legalidad, seguridad jurídica, economía procesal, entre otros, debe valerse de éste para facilitar y gestionar a través de una mayor economía de sentido los diferentes trámites y etapas que permiten su utilización en el ejercicio del derecho.

Si bien desde el año 1999 el Congreso de la República expidió una Ley que definiera y reglamentara el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, todavía hay quienes se rehúsan a aceptar y hacer parte de su realidad ésta era digital, apartándose de la facilidad y eficacia que se obtiene con su buen uso, la mayoría de las ocasiones, por la desconfianza que genera, especialmente relacionadas con su autenticidad.

Cuando se aporta un documento electrónico a un proceso, se hace independiente de otra prueba, pues tiene entidad propia y autónoma que tiene peso por sí solo, por lo que no es necesario valerse de un dictamen pericial, testimonio u otro tipo de prueba. Ahora bien, si ese documento electrónico aportado no cuenta con firma digital, se deberá establecer su autenticidad, lo que no significa que no sea válido.

Con la existencia del documento electrónico no se le está quitando veracidad y autenticidad al documento tradicional, por el contrario, se está demostrando que ambos pueden coexistir. Lo que se quiere significar es que con la debida aplicación y utilización del documento electrónico, la tramitología se verá ampliamente reducida, representando un ahorro energético, un ahorro material (papel), y un ahorro económico.

En los casos que se exija firma manuscrita en los documentos elaborados en físico, es decir, en papel, los documentos electrónicos deben satisfacer el mismo requisito a través de la firma digital, esto gracias al principio de equivalencia funcional.

Referencias

- Calvinho, G. (Julio - Septiembre de 2012). Problemática probatoria de los documentos y correos electrónicos utilizados en el tráfico comercial. *Foro de Derecho Mercantil*(36), 39-65.
- Congreso. (22 de Diciembre de 1993). *Ley 98*, Por medio de la cual se dictan normas sobre democratización y fomento del libro colombiano. Obtenido de

- <http://www.secretariassenado.gov.co/>
http://www.secretariassenado.gov.co/senado/basedoc/ley_0098_1993.htm
- Congreso. (20 de Diciembre de 1995). *Ley 223*, Por la cual se expiden normas sobre racionalización tributaria y se dictan otras disposiciones. Obtenido de <http://www.secretariassenado.gov.co/>:
http://www.secretariassenado.gov.co/senado/basedoc/ley_0223_1995.html
- Congreso. (7 de Marzo de 1996). *Ley 270*, Estatutaria de la Administración de Justicia. Obtenido de <http://www.secretariassenado.gov.co/>:
http://www.secretariassenado.gov.co/senado/basedoc/ley_0270_1996.html#
- Corbetta, P. (2010). *Metodologías y técnicas de investigación social*. Recuperado el 2016, de <https://diversidadlocal.files.wordpress.com/>:
<https://diversidadlocal.files.wordpress.com/2012/09/metodologc3ada-y-tc3a9cnicas-de-investigacic3b3n-social-piergiorgio-corbetta.pdf>
- Cuesta Davu, A. A. (14 de Julio de 2015). Prueba. Medio de Prueba. Probar. *Apuntes de clase de Derecho Probatorio*. Medellín: UNAULA, Univeridad Autónoma Latinoamericana.
- Devis Echandía, H. (2015). *Teoría General de la Prueba Judicial* (Sexta ed., Vol. II). Bogotá: Temis S.A.
- Flórez, G. D. (21 de Marzo de 2014). *La validez jurídica de los documentos electrónicos en Colombia a partir de sus evolución legislativa y jurisprudencial*. Recuperado el Diciembre de 2016, de <http://www.unilibre.edu.co>: <http://www.unilibre.edu.co/verbaiuris/31/la-validez-juridica-de-los-documentos-electronicos-en-colombia-a-partir-de-su-evolucion-legislativa-y-jurisprudencial.pdf>
- Marzal, M. Á., & Gonzales, A. (julio-diciembre de 2010). *Del documento al hiperdocumento. Una visión "funcional" de un concepto en evolución*, Revista Signo y Pensamiento. (P. U. Javeriana, Editor) Recuperado el 2016, de <https://dialnet.unirioja.es>:
<http://www.redalyc.org/articulo.oa?id=86020052006>
- Mendoza Navarro, A. L. (Noviembre de 2006). La realidad latinoamericana en gestión de documentos electrónicos. Oviedo, España.
- Ministerio de Comercio, I. T. (22 de Noviembre de 2012). *Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones*. Recuperado el 2016, de <http://wsp.presidencia.gov.co/Normativa/Decretos/2012/Documents/NOVIEMBRE/22/DECRET%202364%20DEL%2022%20DE%20NOVIEMBRE%20DE%202012.pdf>
- Palacio Ochoa, M. M., & Rojas Jimenez, M. M. (2005). Valor probatorio del documento electrónico en el sistema legal colombiano. (U. A. Unaula, Ed.) Medellín.
- Parra Quijano, J. (2003). *Tratado de la Prueba Judicial: Los Documentos* (Tercera ed.). Bogotá: Librería Ediciones del Profesional LTDA.
- Parra Quijano, J. (2006). I Convención Internacional de Derecho Informático, Documentación y Documento Electrónico . En U. E. Colombia (Ed.), *El documento electrónico y su alcance probatorio*. Bogotá.

- Pedauque, R. T. (2003). *Documento: forma, signo y medio, re-formulaciones de lo digital*. Recuperado el 2016, de http://archivesic.ccsd.cnrs.fr/sic_00001160/fr/:
http://archivesic.ccsd.cnrs.fr/sic_00001160/document
- Presidencia. (06 de Agosto de 1970). *Decreto 1400*, Por el cual se expide el Código de Procedimiento Civil. Obtenido de <http://www.secretariasenado.gov.co/>:
http://www.secretariasenado.gov.co/senado/basedoc/codigo_procedimiento_civil.html
- Presidencia. (5 de Diciembre de 1995). *Decreto 2150*, Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública. Obtenido de <http://www.secretariasenado.gov.co/>:
http://www.secretariasenado.gov.co/senado/basedoc/decreto_2150_1995.html
- RAE. (s.f.). <http://www.rae.es/>. Recuperado el Diciembre de 2016, de <http://dle.rae.es/?id=4QjqWMu>
- Ramírez Gómez, J. F. (2008). *La Prueba Documental* (Octava ed.). Medellín: Señal Editora.
- Rengifo García, E. (2000). Comercio electrónico, documento electrónico y seguridad jurídica. En U. E. Colombia, *Comercio electrónico* (pág. 29). Bogotá: Universidad Externado de Colombia.
- Ross, A. (2008). El concepto de validez y el conflicto entre el positivismo jurídico y el derecho natural. (R. Culzoni, Ed.) *Academia. Revista sobre enseñanza del Derecho*(12), 351.
- T.I.C, M. d., & línea, D. d. (s.f.). *Cero papel en la administración pública*, Archivo General de la Nación. (A. C. Administrativa, Editor, & D. A. Pública, Productor) Recuperado el 2016, de <http://programa.gobiernoenlinea.gov.co/>: http://programa.gobiernoenlinea.gov.co/apc-aa-files/Cero_papel/guia-1-cero-papel.pdf
- Turismo, M. d. (22 de Noviembre de 2012). *Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones*. Obtenido de <http://wsp.presidencia.gov.co/Normativa/Decretos/2012/Documents/NOVIEMBRE/22/DECRET O%202364%20DEL%2022%20DE%20NOVIEMBRE%20DE%202012.pdf>
- Turismo, M. d. (22 de Noviembre de 2012). *Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones*. Obtenido de <http://wsp.presidencia.gov.co/Normativa/Decretos/2012/Documents/NOVIEMBRE/22/DECRET O%202364%20DEL%2022%20DE%20NOVIEMBRE%20DE%202012.pdf>

Anexos

Anexo 1:

LEY 527 DE 1999

(Agosto 18)

Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

El Congreso de Colombia

DECRETA:

PARTE I

PARTE GENERAL

CAPITULO I

Disposiciones generales

ARTÍCULO 1º. *Ámbito de aplicación.* La presente ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en los siguientes casos:

- a) En las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales;
- b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo.

ARTÍCULO 2º. *Definiciones.* Para los efectos de la presente ley se entenderá por:

- a) *Mensaje de datos.* La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax;
- b) *Comercio electrónico.* Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; todo tipo de operaciones financieras, bursátiles y de seguros; de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera;
- c) *Firma digital.* Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave

del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación;

d) *Entidad de Certificación*. Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales;

e) *Intercambio Electrónico de Datos (EDI)*. La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto;

f) *Sistema de Información*. Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

ARTÍCULO 3º. Interpretación. En la interpretación de la presente ley habrán de tenerse en cuenta su origen internacional, la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe.

Las cuestiones relativas a materias que se rijan por la presente ley y que no estén expresamente resueltas en ella, serán dirimidas de conformidad con los principios generales en que ella se inspira.

ARTÍCULO 4º. Modificación mediante acuerdo. Salvo que se disponga otra cosa, en las relaciones entre partes que generan, envían, reciben, archivan o procesan de alguna otra forma mensajes de datos, las disposiciones del Capítulo III, Parte I, podrán ser modificadas mediante acuerdo.

ARTÍCULO 5º. Reconocimiento jurídico de los mensajes de datos. No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos.

CAPITULO II

Aplicación de los requisitos jurídicos de los mensajes de datos

ARTÍCULO 6º. Escrito. Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas prevén consecuencias en el caso de que la información no conste por escrito.

ARTÍCULO 7º. Firma. Reglamentado por el Decreto Nacional 2364 de 2012. Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:

- a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación;
- b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma.

ARTÍCULO 8º. Original. Cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si:

- a) Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma;
- b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que la información no sea presentada o conservada en su forma original.

ARTÍCULO 9º. Integridad de un mensaje de datos. Para efectos del artículo anterior, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido, será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

ARTÍCULO 10. Admisibilidad y fuerza probatoria de los mensajes de datos. Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.

En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.

ARTÍCULO 11. *Criterio para valorar probatoriamente un mensaje de datos.* Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

ARTÍCULO 12. *Conservación de los mensajes de datos y documentos.* Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre que se cumplan las siguientes condiciones:

1. Que la información que contengan sea accesible para su posterior consulta.
2. Que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y
3. Que se conserve, de haber alguna, toda información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento.

No estará sujeta a la obligación de conservación, la información que tenga por única finalidad facilitar el envío o recepción de los mensajes de datos.

Los libros y papeles del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta.

ARTÍCULO 13. *Conservación de mensajes de datos y archivo de documentos a través de terceros.* El cumplimiento de la obligación de conservar documentos, registros o informaciones en mensajes de datos, se podrá realizar directamente o a través de terceros, siempre y cuando se cumplan las condiciones enunciadas en el artículo anterior.

CAPITULO III

Comunicación de los mensajes de datos

ARTÍCULO 14. *Formación y validez de los contratos.* En la formación del contrato, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos.

ARTÍCULO 15. *Reconocimiento de los mensajes de datos por las partes.* En las relaciones entre el iniciador y el destinatario de un mensaje de datos, no se negarán efectos jurídicos,

validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de mensaje de datos.

ARTÍCULO 16. *Atribución de un mensaje de datos.* Se entenderá que un mensaje de datos proviene del iniciador, cuando éste ha sido enviado por:

1. El propio iniciador.
2. Por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje, o
3. Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.

ARTÍCULO 17. *Presunción del origen de un mensaje de datos.* Se presume que un mensaje de datos ha sido enviado por el iniciador, cuando:

1. Haya aplicado en forma adecuada el procedimiento acordado previamente con el iniciador, para establecer que el mensaje de datos provenía efectivamente de éste, o
2. El mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio.

ARTÍCULO 18. *Concordancia del mensaje de datos enviado con el mensaje de datos recibido.* Siempre que un mensaje de datos provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y el destinatario, este último tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá proceder en consecuencia.

El destinatario no gozará de este derecho si sabía o hubiera sabido, de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la transmisión había dado lugar a un error en el mensaje de datos recibido.

ARTÍCULO 19. *Mensajes de datos duplicados.* Se presume que cada mensaje de datos recibido es un mensaje de datos diferente, salvo en la medida en que duplique otro mensaje de datos, y que el destinatario sepa, o debiera saber, de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el nuevo mensaje de datos era un duplicado.

ARTÍCULO 20. *Acuse de recibo.* Si al enviar o antes de enviar un mensaje de datos, el iniciador solicita o acuerda con el destinatario que se acuse recibo del mensaje de datos, pero no se ha acordado entre éstos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante:

- a) Toda comunicación del destinatario, automatizada o no, o

b) Todo acto del destinatario que baste para indicar al iniciador que se ha recibido el mensaje de datos.

Si el iniciador ha solicitado o acordado con el destinatario que se acuse recibo del mensaje de datos, y expresamente aquél ha indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, se considerará que el mensaje de datos no ha sido enviado en tanto que no se haya recepcionado el acuse de recibo.

ARTÍCULO 21. *Presunción de recepción de un mensaje de datos.* Cuando el iniciador recepcione acuse recibo del destinatario, se presumirá que éste ha recibido el mensaje de datos.

Esa presunción no implicará que el mensaje de datos corresponda al mensaje recibido. Cuando en el acuse de recibo se indique que el mensaje de datos recepcionado cumple con los requisitos técnicos convenidos o enunciados en alguna norma técnica aplicable, se presumirá que ello es así.

ARTÍCULO 22. *Efectos jurídicos.* Los artículos 20 y 21 únicamente rigen los efectos relacionados con el acuse de recibo. Las consecuencias jurídicas del mensaje de datos se regirán conforme a las normas aplicables al acto o negocio jurídico contenido en dicho mensaje de datos.

ARTÍCULO 23. *Tiempo del envío de un mensaje de datos.* De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido cuando ingrese en un sistema de información que no esté bajo control del iniciador o de la persona que envió el mensaje de datos en nombre de éste.

ARTÍCULO 24. *Tiempo de la recepción de un mensaje de datos.* De no convenir otra cosa el iniciador y el destinatario, el momento de la recepción de un mensaje de datos se determinará como sigue:

a) Si el destinatario ha designado un sistema de información para la recepción de mensaje de datos, la recepción tendrá lugar:

1. En el momento en que ingrese el mensaje de datos en el sistema de información designado; o
2. De enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, en el momento en que el destinatario recupere el mensaje de datos;

b) Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar cuando el mensaje de datos ingrese a un sistema de información del destinatario.

Lo dispuesto en este artículo será aplicable aun cuando el sistema de información esté ubicado en lugar distinto de donde se tenga por recibido el mensaje de datos conforme al artículo siguiente.

ARTÍCULO 25. *Lugar del envío y recepción del mensaje de datos.* De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido en el lugar donde el

iniciador tenga su establecimiento y por recibido en el lugar donde el destinatario tenga el suyo. Para los fines del presente artículo:

- a) Si el iniciador o destinatario tienen más de un establecimiento, su establecimiento será el que guarde una relación más estrecha con la operación subyacente o, de no haber una operación subyacente, su establecimiento principal;
- b) Si el iniciador o el destinatario no tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.

PARTE II

COMERCIO ELECTRONICO EN MATERIA DE TRANSPORTE DE MERCANCIAS

ARTÍCULO 26. Actos relacionados con los contratos de transporte de mercancías. Sin perjuicio de lo dispuesto en la parte I de la presente ley, este capítulo será aplicable a cualquiera de los siguientes actos que guarde relación con un contrato de transporte de mercancías, o con su cumplimiento, sin que la lista sea taxativa:

- a) I. Indicación de las marcas, el número, la cantidad o el peso de las mercancías.
- II. Declaración de la naturaleza o valor de las mercancías.
- III. Emisión de un recibo por las mercancías.
- IV. Confirmación de haberse completado el embarque de las mercancías;
- b) I. Notificación a alguna persona de las cláusulas y condiciones del contrato.
- II. Comunicación de instrucciones al transportador;
- c) I. Reclamación de la entrega de las mercancías.
- II. Autorización para proceder a la entrega de las mercancías.
- III. Notificación de la pérdida de las mercancías o de los daños que hayan sufrido;
- d) Cualquier otra notificación o declaración relativas al cumplimiento del contrato;
- e) Promesa de hacer entrega de las mercancías a la persona designada o a una persona autorizada para reclamar esa entrega;
- f) Concesión, adquisición, renuncia, restitución, transferencia o negociación de algún derecho sobre mercancías;
- g) Adquisición o transferencia de derechos y obligaciones con arreglo al contrato.

ARTÍCULO 27. *Documentos de transporte.* Con sujeción a lo dispuesto en el inciso 3o. del presente artículo, en los casos en que la ley requiera que alguno de los actos enunciados en el artículo 26 se lleve a cabo por escrito o mediante documento emitido en papel, ese requisito quedará satisfecho cuando el acto se lleve a cabo por medio de uno o más mensajes de datos.

El inciso anterior será aplicable, tanto si el requisito en él previsto está expresado en forma de obligación o si la ley simplemente prevé consecuencias en el caso de que no se lleve a cabo el acto por escrito o mediante un documento emitido en papel.

Cuando se conceda algún derecho a una persona determinada y a ninguna otra, o ésta adquiera alguna obligación, y la ley requiera que, para que ese acto surta efecto, el derecho o la obligación hayan de transferirse a esa persona mediante el envío o utilización de un documento emitido en papel, ese requisito quedará satisfecho si el derecho o la obligación se transfiere mediante la utilización de uno o más mensajes de datos, siempre que se emplee un método confiable para garantizar la singularidad de ese mensaje o esos mensajes de datos.

Para los fines del inciso tercero, el nivel de confiabilidad requerido será determinado a la luz de los fines para los que se transfirió el derecho o la obligación y de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

Cuando se utilicen uno o más mensajes de datos para llevar a cabo alguno de los actos enunciados en los incisos f) y g) del artículo 26, no será válido ningún documento emitido en papel para llevar a cabo cualquiera de esos actos, a menos que se haya puesto fin al uso de mensajes de datos para sustituirlo por el de documentos emitidos en papel. Todo documento con soporte en papel que se emita en esas circunstancias deberá contener una declaración en tal sentido. La sustitución de mensajes de datos por documentos emitidos en papel no afectará los derechos ni las obligaciones de las partes.

Cuando se aplique obligatoriamente una norma jurídica a un contrato de transporte de mercancías que esté consignado, o del que se haya dejado constancia en un documento emitido en papel, esa norma no dejará de aplicarse, a dicho contrato de transporte de mercancías del que se haya dejado constancia en uno o más mensajes de datos por razón de que el contrato conste en ese mensaje o esos mensajes de datos en lugar de constar en documentos emitidos en papel.

PARTE III

FIRMAS DIGITALES, CERTIFICADOS Y ENTIDADES DE CERTIFICACION

CAPITULO I

Firmas digitales

ARTÍCULO 28. *Atributos jurídicos de una firma digital.* Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

PARÁGRAFO. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:

1. Es única a la persona que la usa.
2. Es susceptible de ser verificada.
3. Está bajo el control exclusivo de la persona que la usa.
4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.
5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

CAPITULO II

Entidades de certificación

ARTÍCULO 29. *Características y requerimientos de las entidades de certificación.* Modificado por el art. 160, Decreto Nacional 019 de 2012. Podrán ser entidades de certificación, las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero y las cámaras de comercio, que previa solicitud sean autorizadas por la Superintendencia de Industria y Comercio y que cumplan con los requerimientos establecidos por el Gobierno Nacional, con base en las siguientes condiciones:

- a) Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como entidad de certificación;
- b) Contar con la capacidad y elementos técnicos necesarios para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en esta ley;
- c) Los representantes legales y administradores no podrán ser personas que hayan sido condenadas a pena privativa de la libertad, excepto por delitos políticos o culposos; o que hayan sido suspendidas en el ejercicio de su profesión por falta grave contra la ética o hayan sido excluidas de aquélla. Esta inhabilidad estará vigente por el mismo período que la ley penal o administrativa señale para el efecto.

ARTÍCULO 30. *Actividades de las entidades de certificación.* Modificado por el art. 161, Decreto Nacional 019 de 2012. Las entidades de certificación autorizadas por la Superintendencia de Industria y Comercio para prestar sus servicios en el país, podrán realizar, entre otras, las siguientes actividades:

1. Emitir certificados en relación con las firmas digitales de personas naturales o jurídicas.

2. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos.
3. Emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la presente ley.
4. Ofrecer o facilitar los servicios de creación de firmas digitales certificadas.
5. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.
6. Ofrecer los servicios de archivo y conservación de mensajes de datos.

ARTÍCULO 31. *Remuneración por la prestación de servicios.* La remuneración por los servicios de las entidades de certificación serán establecidos libremente por éstas.

ARTÍCULO 32. *Deberes de las entidades de certificación.* Las entidades de certificación tendrán, entre otros, los siguientes deberes:

- a) Emitir certificados conforme a lo solicitado o acordado con el suscriptor;
- b) Implementar los sistemas de seguridad para garantizar la emisión y creación de firmas digitales, la conservación y archivo de certificados y documentos en soporte de mensaje de datos;
- c) Garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor;
- d) Garantizar la prestación permanente del servicio de entidad de certificación;
- e) Atender oportunamente las solicitudes y reclamaciones hechas por los suscriptores;
- f) Efectuar los avisos y publicaciones conforme a lo dispuesto en la ley;
- g) Suministrar la información que le requieran las entidades administrativas competentes o judiciales en relación con las firmas digitales y certificados emitidos y en general sobre cualquier mensaje de datos que se encuentre bajo su custodia y administración;
- h) Modificado por el art. 162, Decreto Nacional 019 de 2012. Permitir y facilitar la realización de las auditorías por parte de la Superintendencia de Industria y Comercio;
- i) Elaborar los reglamentos que definen las relaciones con el suscriptor y la forma de prestación del servicio;
- j) Llevar un registro de los certificados.

ARTÍCULO 33. *Terminación unilateral.* Salvo acuerdo entre las partes, la entidad de certificación podrá dar por terminado el acuerdo de vinculación con el suscriptor dando un preaviso no menor de noventa (90) días. Vencido este término, la entidad de certificación revocará los certificados que se encuentren pendientes de expiración.

Igualmente, el suscriptor podrá dar por terminado el acuerdo de vinculación con la entidad de certificación dando un preaviso no inferior a treinta (30) días.

ARTÍCULO 34. *Cesación de actividades por parte de las entidades de certificación.* Modificado por el art. 163, Decreto Nacional 019 de 2012. Las entidades de certificación autorizadas pueden cesar en el ejercicio de actividades, siempre y cuando hayan recibido autorización por parte de la Superintendencia de Industria y Comercio.

CAPITULO III

Certificados

ARTÍCULO 35. *Contenido de los certificados.* Un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:

1. Nombre, dirección y domicilio del suscriptor.
2. Identificación del suscriptor nombrado en el certificado.
3. El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
4. La clave pública del usuario.
5. La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
6. El número de serie del certificado.
7. Fecha de emisión y expiración del certificado.

ARTÍCULO 36. *Aceptación de un certificado.* Salvo acuerdo entre las partes, se entiende que un suscriptor ha aceptado un certificado cuando la entidad de certificación, a solicitud de éste o de una persona en nombre de éste, lo ha guardado en un repositorio.

ARTÍCULO 37. *Revocación de certificados.* El suscriptor de una firma digital certificada, podrá solicitar a la entidad de certificación que expidió un certificado, la revocación del mismo. En todo caso, estará obligado a solicitar la revocación en los siguientes eventos:

1. Por pérdida de la clave privada.
2. La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido.

Si el suscriptor no solicita la revocación del certificado en el evento de presentarse las anteriores situaciones, será responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe exenta de culpa que confiaron en el contenido del certificado.

Una entidad de certificación revocará un certificado emitido por las siguientes razones:

1. A petición del suscriptor o un tercero en su nombre y representación.
2. Por muerte del suscriptor.
3. Por liquidación del suscriptor en el caso de las personas jurídicas.
4. Por la confirmación de que alguna información o hecho contenido en el certificado es falso.
5. La clave privada de la entidad de certificación o su sistema de seguridad ha sido comprometido de manera material que afecte la confiabilidad del certificado.
6. Por el cese de actividades de la entidad de certificación, y
7. Por orden judicial o de entidad administrativa competente.

ARTÍCULO 38. *Término de conservación de los registros.* Los registros de certificados expedidos por una entidad de certificación deben ser conservados por el término exigido en la ley que regule el acto o negocio jurídico en particular.

CAPITULO IV

Suscriptores de firmas digitales

ARTÍCULO 39. *Deberes de los suscriptores.* Son deberes de los suscriptores:

1. Recibir la firma digital por parte de la entidad de certificación o generarla, utilizando un método autorizado por ésta.
2. Suministrar la información que requiera la entidad de certificación.
3. Mantener el control de la firma digital.
4. Solicitar oportunamente la revocación de los certificados.

ARTÍCULO 40. *Responsabilidad de los suscriptores.* Los suscriptores serán responsables por la falsedad, error u omisión en la información suministrada a la entidad de certificación y por el incumplimiento de sus deberes como suscriptor.

CAPITULO V

Superintendencia de Industria y Comercio

ARTÍCULO 41. *Funciones de la Superintendencia.* Derogado por el art. 176, Decreto Nacional 019 de 2012. La Superintendencia de Industria y Comercio ejercerá las facultades que legalmente le han sido asignadas respecto de las entidades de certificación, y adicionalmente tendrá las siguientes funciones:

1. Autorizar la actividad de las entidades de certificación en el territorio nacional.
2. Velar por el funcionamiento y la eficiente prestación del servicio por parte de las entidades de certificación.
3. Realizar visitas de auditoría a las entidades de certificación.
4. Revocar o suspender la autorización para operar como entidad de certificación.
5. Solicitar la información pertinente para el ejercicio de sus funciones.
6. Imponer sanciones a las entidades de certificación en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio.
7. Ordenar la revocación de certificados cuando la entidad de certificación los emita sin el cumplimiento de las formalidades legales.
8. Designar los repositorios y entidades de certificación en los eventos previstos en la ley.
9. Emitir certificados en relación con las firmas digitales de las entidades de certificación.
10. Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y prácticas comerciales restrictivas, competencia desleal y protección del consumidor, en los mercados atendidos por las entidades de certificación.
11. Impartir instrucciones sobre el adecuado cumplimiento de las normas a las cuales deben sujetarse las entidades de certificación.

ARTÍCULO 42. *Sanciones.* Derogado por el art. 176, Decreto Nacional 019 de 2012. La Superintendencia de Industria y Comercio de acuerdo con el debido proceso y el derecho de defensa, podrá imponer según la naturaleza y la gravedad de la falta, las siguientes sanciones a las entidades de certificación:

1. Amonestación.
2. Multas institucionales hasta por el equivalente a dos mil (2.000) salarios mínimos legales mensuales vigentes, y personales a los administradores y representantes legales de las entidades de certificación, hasta por trescientos (300) salarios mínimos legales mensuales vigentes, cuando se les compruebe que han autorizado, ejecutado o tolerado conductas violatorias de la ley.

3. Suspender de inmediato todas o algunas de las actividades de la entidad infractora.
4. Prohibir a la entidad de certificación infractora prestar directa o indirectamente los servicios de entidad de certificación hasta por el término de cinco (5) años.
5. Revocar definitivamente la autorización para operar como entidad de certificación.

CAPITULO VI

Disposiciones varias

ARTÍCULO 43. *Certificaciones recíprocas.* Los certificados de firmas digitales emitidos por entidades de certificación extranjeras, podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley para la emisión de certificados por parte de las entidades de certificación nacionales, siempre y cuando tales certificados sean reconocidos por una entidad de certificación autorizada que garantice en la misma forma que lo hace con sus propios certificados, la regularidad de los detalles del certificado, así como su validez y vigencia.

ARTÍCULO 44. *Incorporación por remisión.* Salvo acuerdo en contrario entre las partes, cuando en un mensaje de datos se haga remisión total o parcial a directrices, normas, estándares, acuerdos, cláusulas, condiciones o términos fácilmente accesibles con la intención de incorporarlos como parte del contenido o hacerlos vinculantes jurídicamente, se presume que esos términos están incorporados por remisión a ese mensaje de datos. Entre las partes y conforme a la ley, esos términos serán jurídicamente válidos como si hubieran sido incorporados en su totalidad en el mensaje de datos.

PARTE IV

REGLAMENTACION Y VIGENCIA

ARTÍCULO 45. La Superintendencia de Industria y Comercio contará con un término adicional de doce (12) meses, contados a partir de la publicación de la presente ley, para organizar y asignar a una de sus dependencias la función de inspección, control y vigilancia de las actividades realizadas por las entidades de certificación, sin perjuicio de que el Gobierno Nacional cree una unidad especializada dentro de ella para tal efecto.

ARTÍCULO 46. *Prevalencia de las leyes de protección al consumidor.* La presente ley se aplicará sin perjuicio de las normas vigentes en materia de protección al consumidor.

ARTÍCULO 47. *Vigencia y derogatoria.* La presente ley rige desde la fecha de su publicación y deroga las disposiciones que le sean contrarias.

El Presidente del honorable Senado de la República,

FABIO VALENCIA COSSIO.

El Secretario General del honorable Senado de la República,

MANUEL ENRÍQUEZ ROSERO.

El Presidente de la honorable Cámara de Representantes,

EMILIO MARTÍNEZ ROSALES.

El Secretario General de la honorable Cámara de Representantes,

GUSTAVO BUSTAMANTE MORATTO.

REPUBLICA DE COLOMBIA GOBIERNO NACIONAL

Publíquese y ejecútese.

Dada en Santa Fe de Bogotá, D. C., a 18 de agosto de 1999.

ANDRES PASTRANA ARANGO

El Ministro de Desarrollo Económico,

Fernando Araújo Perdomo.

La Ministra de Comercio Exterior,

Martha Lucía Ramírez de Rincón.

La Ministra de Comunicaciones,

Claudia De Francisco Zambrano.

El Ministro de Transporte,

Mauricio Cárdenas Santamaría.

DIARIO OFICIAL: Santafé de Bogotá, Sábado 21 de agosto de 1999. Año CXXXV No. 43.673

Anexo 2:

DECRETO 2364 DE 2012

(Noviembre 22)

Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.

EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA

En uso de las atribuciones constitucionales, y en particular, las previstas en el numeral 11 del artículo 189 de la Constitución Política y,

CONSIDERANDO:

Que uno de los lineamientos estratégicos del Plan Nacional de Desarrollo 2010 - 2014 "*Prosperidad para todos*" es la reglamentación del uso de la firma electrónica.

Que la firma digital se encuentra definida en el literal c) del artículo 2° de la Ley 527 de 1999 y reglamentada en el Decreto 1747 de 2000 y ha sido considerada como una especie de la firma electrónica.

Que en el artículo 7° de la Ley 527 de 1999 se consagró el equivalente electrónico de la firma.

Que se ha considerado al comercio electrónico como motor de crecimiento de la economía del siglo XXI y factor que contribuye a fomentar la competitividad empresarial de las Pymes y Mi Pymes a través del uso de las tecnologías de información y comunicación.

Que para impulsar el desarrollo del comercio electrónico, internacionalmente se ha recomendado promover enfoques apropiados para el reconocimiento legal de firmas electrónicas bajo el principio de neutralidad tecnológica, previsto en el numeral 6 del artículo 2° de la Ley 1341 de 2009.

Que la firma electrónica representa un medio de identificación electrónico flexible y tecnológicamente neutro que se adecúa a las necesidades de la sociedad.

Que de conformidad con el artículo 15.6 del Tratado de Libre Comercio suscrito con los Estados Unidos de América, aprobado por la Ley 1143 de 2007, no se podrá adoptar o mantener legislación sobre autenticación electrónica que impida a las partes en una transacción electrónica determinar en forma mutua los métodos apropiados de autenticación o que les impida establecer, ante instancias judiciales o administrativas, que la transacción electrónica cumple con cualquier requerimiento legal con respecto a la autenticación.

Que ante la evolución de las innovaciones tecnológicas, es necesario establecer criterios para el reconocimiento jurídico de las firmas electrónicas independientemente de la tecnología utilizada.

Que en el documento Conpes 3620 de 2009 se recomendó promover el uso de la firma electrónica como esquema alternativo de la firma digital.

Que el artículo 244 del Código General del Proceso adoptado mediante la Ley 1564 de 2012, establece que se presumen auténticos los documentos en forma de mensajes de datos.

Que se hace necesario reglamentar la firma electrónica para generar mayor entendimiento sobre la misma, dar seguridad jurídica a los negocios que se realicen a través de medios electrónicos, así como facilitar y promover el uso masivo de la firma electrónica en todo tipo de transacciones.

DECRETA:

Artículo 1°. *Definiciones.* Para los fines del presente decreto se entenderá por:

1. Acuerdo sobre el uso del mecanismo de firma electrónica: Acuerdo de voluntades mediante el cual se estipulan las condiciones legales y técnicas a las cuales se ajustarán las partes para realizar comunicaciones, efectuar transacciones, crear documentos electrónicos o cualquier otra actividad mediante el uso del intercambio electrónico de datos.
2. Datos de creación de la firma electrónica: Datos únicos y personalísimos, que el firmante utiliza para firmar.
3. Firma electrónica. Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.
4. Firmante. Persona que posee los datos de creación de la firma y que actúa en nombre propio o por cuenta de la persona a la que representa.

Artículo 2°. *Neutralidad tecnológica e igualdad de tratamiento de las tecnologías para la firma electrónica.* Ninguna de las disposiciones del presente decreto será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método, procedimiento, dispositivo o tecnología para crear una firma electrónica que cumpla los requisitos señalados en el artículo 7° de la Ley 527 de 1999.

Artículo 3°. *Cumplimiento del requisito de firma.* Cuando se exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea tan confiable como apropiada para los fines con los cuales se generó o comunicó ese mensaje.

Artículo 4°. *Confiable de la firma electrónica.* La firma electrónica se considerará confiable para el propósito por el cual el mensaje de datos fue generado o comunicado si:

1. Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante.
2. Es posible detectar cualquier alteración no autorizada del mensaje de datos, hecha después del momento de la firma.

Parágrafo. Lo dispuesto anteriormente se entenderá sin perjuicio de la posibilidad de que cualquier persona:

1. Demuestre de otra manera que la firma electrónica es confiable; o

2. Aduzca pruebas de que una firma electrónica no es confiable.

Artículo 5°. Efectos jurídicos de la firma electrónica. La firma electrónica tendrá la misma validez y efectos jurídicos que la firma, si aquella cumple con los requisitos establecidos en el artículo 3° de este decreto.

Artículo 6°. Obligaciones del firmante. El firmante debe:

1. Mantener control y custodia sobre los datos de creación de la firma.
2. Actuar con diligencia para evitar la utilización no autorizada de sus datos de creación de la firma.
3. Dar aviso oportuno a cualquier persona que posea, haya recibido o vaya a recibir documentos o mensajes de datos firmados electrónicamente por el firmante, si:
 - a) El firmante sabe que los datos de creación de la firma han quedado en entredicho; o
 - b) Las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho.

Parágrafo. Se entiende que los datos de creación del firmante han quedado en entredicho cuando estos, entre otras, han sido conocidos ilegalmente por terceros, corren peligro de ser utilizados indebidamente, o el firmante ha perdido el control o custodia sobre los mismos y en general cualquier otra situación que ponga en duda la seguridad de la firma electrónica o que genere reparos sobre la calidad de la misma.

Artículo 7°. Firma electrónica pactada mediante acuerdo. Salvo prueba en contrario, se presume que los mecanismos o técnicas de identificación personal o autenticación electrónica según el caso, que acuerden utilizar las partes mediante acuerdo, cumplen los requisitos de firma electrónica.

Parágrafo. La parte que mediante acuerdo provee los métodos de firma electrónica deberá asegurarse de que sus mecanismos son técnicamente seguros y confiables para el propósito de los mismos. A dicha parte le corresponderá probar estos requisitos en caso de que sea necesario.

Artículo 8°. Criterios para establecer el grado de seguridad de las firmas electrónicas. Para determinar si los procedimientos, métodos o dispositivos electrónicos que se utilicen como firma electrónica son seguros, y en qué medida lo son, podrán tenerse en cuenta, entre otros, los siguientes factores:

1. El concepto técnico emitido por un perito o un órgano independiente y especializado.
2. La existencia de una auditoría especializada, periódica e independiente sobre los procedimientos, métodos o dispositivos electrónicos que una parte suministra a sus clientes o terceros como mecanismo electrónico de identificación personal.

Artículo 9°. Vigencia. El presente decreto rige a partir de su publicación en el *Diario Oficial*.

Publíquese y cúmplase.

Dado en Bogotá D. C., a 22 de noviembre de 2012.

JUAN MANUEL SANTOS CALDERÓN

El Ministro de Comercio, Industria y Turismo,

Sergio Díaz-Granados Guida.

NOTA: Publicado en el Diario Oficial 48622 de noviembre 22 de 2012.