



Atribución-NoComercial 2.5 Colombia (CC BY-NC 2.5)

La presente obra está bajo una licencia:
Atribución-NoComercial 2.5 Colombia (CC BY-NC 2.5)
Para leer el texto completo de la licencia, visita:
<http://creativecommons.org/licenses/by-nc/2.5/co/>

Usted es libre de:



Compartir - copiar, distribuir, ejecutar y comunicar públicamente la obra
hacer obras derivadas

Bajo las condiciones siguientes:



Atribución — Debe reconocer los créditos de la obra de la manera especificada por el autor o el licenciante (pero no de una manera que sugiera que tiene su apoyo o que apoyan el uso que hace de su obra).



No Comercial — No puede utilizar esta obra para fines comerciales.

Requisitos jurídicos para la validez jurídica de la prueba digital.

Dayan Paola Parra Sichaca¹

Universidad Católica de Colombia

Resumen

Las evidencias contienen pruebas, estas podrán ser digitales, que serán utilizados durante el proceso judicial y para que sean admitidos en un proceso judicial deberán ser cuidadoso y escrupulosos con su manejo.

Por lo anterior, la finalidad de este trabajo es dar a conocer la normatividad interna y externa que regula el tema de prueba digital, exponer los diferentes medios y tipos de pruebas electrónicos o digitales e indicar cuales serias los requisitos indispensables para hacerla valida.

Palabras clave: Evidencia, Prueba, Digital, Electrónico, Valoración, Colombia.

Abstract

The evidence contains evidence, these may be digital, which will be used during the judicial process and to be admitted in a judicial process must be careful and scrupulous with their handling. Therefore, the purpose of this work is to publicize the internal and external regulations that regulate the issue of digital proof, expose the different means and types of electronic or digital tests that exist and indicate which would be the essential requirements to make it valid.

Key words: Evidence, Test, Digital, Electronic, Assessment, Colombia.

¹ Artículo de reflexión presentado por Dayan Paola Parra Sichaca, estudiante de Derecho con materias culminadas identificada con el código 2111117, correo institucional dpparra17@ucatolica.edu.co, como requisito para optar al título de Abogado de la Universidad Católica de Colombia, bajo la asesoría del Doctor German Darío Flórez, docente de la facultad de Derecho en Propiedad Intelectual, 2019.

Sumario:

Introducción, 1. Concepto de prueba digital y evidencia electrónica, 1.1 Evidencia electrónica, 1.2. prueba digital, 1.3 Precedente del concepto de prueba digital en la legislación colombiana, 2. Medios de prueba en el ámbito digital, 3. Tipos de pruebas electrónicos o digitales, 3.1 Documento electrónico, 3.2 Mensaje de datos, 3.3 Diferencia entre mensaje de datos y documento electrónico, 3.4 Los actos de comunicación procesal por medios electrónicos o informáticos, 4. Paso a paso de la prueba digital, 5. Fases de la prueba digital, 6. Método para hacer admisible la prueba digital, 6.1 Autenticidad, 6.2 Confiabilidad, 6.3 Suficiencia, 6.4 Apego y respeto por las leyes y reglas del poder judicial, 7. Modalidad para allegar la prueba digital, 8. Momento para presentar la prueba digital, 9. Cadena de custodia en las pruebas digitales, 10. Valoración, Conclusiones, Referencias bibliográficas

INTRODUCCIÓN

El mundo está evolucionando y el uso de las redes de comunicación es cada vez más intenso, hasta el punto en que se utilizan para relacionarse socialmente y profesionalmente ya que las actividades cotidianas requiere el uso de la tecnología, por lo que el uso de la digitalización se impuso, generando como efecto el remplazo del papel y para ello la norma lo debe regular, como ejemplo, Colombia en 1999 incluye en la normatividad (Ley 527 de 1999) definiciones de contenido técnico y jurídico, abriendo camino para hablar de temas como: prueba digital o prueba electrónica y/o evidencia digital y la ley anti trámites (Ley 962 de 2005), la cual agiliza los procedimientos judiciales, con el objetivo de generar un mínimo de seguridad jurídica en el momento de efectuar transacciones o negocios jurídicos por medio de la tecnología. Es por ello que surja la necesidad de probar o acreditar las actuaciones legítimas.

Por tal efecto, la utilización de los medios tecnológicos (correo electrónico, teléfonos móviles, redes sociales, etc.) impactan el ámbito probatorio y es por ello que debe existir una adaptación de las nuevas tecnologías en la legislación colombiana, específicamente en el tema de prueba digital y de esta manera poner en práctica y de forma efectiva el uso de las tecnologías en el desarrollo de las etapas que se sigue ante las autoridades judiciales o administrativas.

No obstante, aunque existe normatividad que regule la materia, en Colombia aún sigue la problemática en cuanto a la valoración de las pruebas digitales, ya que generan dudas sobre su confidencialidad, la integridad y la autenticidad de la información ante el Juez.

En consecuencia, en cualquier proceso judicial, se debe fortalecer las garantías procesales de la prueba digital en el contexto jurídico colombiano, su regulación y las herramientas jurídicas que tiene el juez en su labor de admitir y valorar pruebas para que cumplan con requisitos de seguridad (Carvajal, 2015), legalidad, confidencialidad, autenticidad e integridad de la información. Por lo anterior, el trabajo de investigación analizara de la prueba digital los diferentes componentes para que sea útil y admisible en un proceso judicial o administrativo (Agudelo 2018).

1. CONCEPTO DE PRUEBA DIGITAL Y EVIDENCIA ELECTRÓNICA

La prueba digital y la evidencia electrónica es un elemento intangible, lo cual requiere ciertas características que son necesarias realizarlas antes de poder confirmar su validez.

De acuerdo a la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial de España, artículo 230 señalaba que “Podrán utilizarse en el proceso cualesquiera medios técnicos de documentación y reproducción, siempre que ofrezcan las debidas garantías de autenticidad”. De acuerdo a De Ros & Méndez serán reguladas en cuando a la forma de utilización.

Con el pasar del tiempo, las herramientas tecnologías surgen o evolucionan, por lo tanto, la legislación no encasilla los medios electrónicos que pueden llegar hacer utilizados como prueba digital en el futuro. Alcanza

La Ley de España (2014), limita el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, artículo 18 numeral 4 de la Constitución de España.

Por lo anterior, concuerdo en que los diferentes procesos judiciales, se debe utilizar cualquier medio probatorio, en tanto se garantizara su legitimidad y siempre y cuando no se vulneren los derechos fundamentales (Carnelutti, 1982) y en lo que respecta a Colombia, estos serían al buen nombre a su intimidad personal y familiar (art.15 C.P), al derecho a la honra (art.21 C.P) y al debido proceso (art. 29).

En consecuencia, en primer lugar, se debe entender como prueba procesal, como el conjunto de actividades realizadas en un proceso con la finalidad de obtener la convicción del Juez o Tribunal sobre determinados hechos relevantes para la decisión de cuestiones sometidas a enjuiciamiento, siempre y cuando se garantice los derechos fundamentales del investigado.

Por otro lado, Carnelutti (1982) hace la diferencia entre fuente de prueba y medio de prueba, los primeros, son las herramientas que el Juez utiliza para verificar las afirmaciones fácticas de las partes y son los previstos, con carácter limitado por el legislador y los segundos, esto es la parte, el testigo, el documento, la cosa que ha de ser examinada y el conocimiento técnico del perito.

De acuerdo a lo anterior, es importante dar a conocer las diferencias entre los conceptos de evidencia electrónica y prueba digital, para evitar errar en los estrados judiciales.

1.1 Evidencia electrónica:

Desde el plano jurídico, la evidencia logra precisarse como un modo en que un hecho está probado o refutado ante un estrado judicial (Flórez, s.f, p.8)

Cano, J. J. C. (2015) señala que la evidencia electrónica es “Cualquier información que, sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático” (HB:171 2003 Guidelines for the Management of IT Evidence), por lo tanto, Cano entiende que cualquier registro generado por o almacenado en un sistema computacional puede ser utilizado como evidencia en un proceso judicial.

La prueba digital es la especie y la evidencia electrónica es el género, significa que la evidencia electrónica se refiere tanto a la prueba digital como a la recabada mediante el uso de medios análogos, ejemplo: la grabación de una conversación telefónica en una cinta magnetofónica.

Adicionalmente, de acuerdo a la investigación de Evidencia Digital: contexto, situación e implicaciones nacionales, menciona una definición uniforme y universal del concepto de evidencia digital o electrónica, del profesor Cano, afirma que: “un tipo de evidencia física, construida por campos magnéticos y pulsos eléctricos que pueden ser recolectados y analizados con herramientas y técnicas especiales”. (Mosquera, Certain & Cano, s.f.)

Respecto de la definición norteamericana de “searching and seizing computers and obtaining electronic evidence in criminal investigations”, señala que; una evidencia que contiene texto puede ser dividida en tres (3) categorías; el primero; Registros generados por computador o en equipos de tecnología informática (registros de auditoría, registros de transacciones, registro de eventos, etc.) el segundo: Registros no generados sino simplemente almacenados en computadores (correos electrónicos, imágenes, etc.), tercer y último: Registros híbridos que incluyen tanto generados por computador como almacenados en los mismos (hojas de cálculo, vistas parciales de datos, consulta especializadas en bases de datos, etc.)

En 2000, Mateu De Ros y Cendoya Méndez de Vigo establecen que; “los documentos generados electrónicamente gozarán de la validez y de la eficacia de un documento original, siempre y cuando se garantice su autenticidad, integridad y el cumplimiento de los requisitos exigidos por las leyes procesales” ... (p. 378).

Jeimy Cano (2015) manifiesta que la evidencia digital es la materia prima para los investigadores donde la tecnología informática es parte fundamental del proceso. No obstante, teniendo en cuenta el uso de la tecnología, detalla las características propias de la evidencia digital, las cuales son (M., 2015):

- Es volátil
- Es anónima
- Es suplicable
- Es alterable y modificable
- Es eliminable

Dichas características, genera una ardua labor por parte de los especialistas en temas de informática forense, tanto en procedimientos como técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia

De acuerdo a lo anterior, se considera que, la evidencia digital compila todos los medios análogos y toda información que se encuentre recopilada en forma digital, cuya utilidad podría llegar a ser utilizada como prueba.

1.2 Prueba digital (PD):

De acuerdo al estudio de Ronderos, J. G. R., & Sanctions Officer, la prueba digital es toda información con valor probatorio que es almacenada o transmitida de forma digital o binaria. Los archivos como Word, Excel o PDF son creados por una persona, mientras que los logs es información que no es generada por una persona directamente, pero es el resultado de su accionar, por ejemplo, la base de datos, computador, página web en el celular, acceso al sistema, compra de apps en iPhone. La prueba digital está contenida en formatos lógicos, por lo tanto, se debe aplicar diferentes procedimientos y requerimientos probatorios.

En 2017, Delgado Martín establece que la prueba digital se debe destacar los siguientes elementos; 1. Se refiere a cualquier clase de información; 2 la información debe ser reproducida, almacenada o transmitida por medio electrónicos; 3. Los efectos de la información deben acreditar hechos.

De acuerdo al derecho comparado, se trae a colación la legislación en Estado Unidos el cual establece que para ser admisible la prueba digital en una Corte la evidencia debe ser pertinente y adecuada, y su valor probatorio debe tener fuerza suficiente para que sobrepase cualquier recelo, no obstante, la prueba digital puede llegar a presentar inconvenientes especiales, ya que podría ser duplicada, alterada y para evitar que se vea afectada la pertinencia de la prueba, se debe cumplir unos requisitos, definidos por las reglas federales de evidencia o cumplir los test de Daubert o Frye, para que sea judicialmente considerada (Rico, 2007, p.600).

La legislación colombiana ha evolucionado en el mundo tecnológico, ya que el mundo es cambiante y por ende la Ley también debe ir al paralelo o incluso adelantarse a está, como, por

ejemplo, regulación de los nuevos medios de prueba y su admisibilidad. El sistema jurídico admite la libertad de la prueba, pero debe ser útil, oponible y que se permita su valoración bajo el criterio de la sana crítica, está podrá ser debatida o refutada por cualquiera de las partes, buscando demostrar la verdad verdadera (Giraldo, Escudero, Camacho, Duarte y González, 2015). y convencer al juez de un hecho en un pleito judicial por medio de cualquier prueba digital, siempre y cuando este revestida de autenticidad e integridad.

1.3 Precedente del concepto de prueba digital en la legislación colombiana:

1. Ley 98 de 1993 “Por medio de la cual se dictan normas sobre democratización y fomento del libro colombiano”, conocida también como “Ley del Libro” señalaba la Ley la diferencia entre las publicaciones en papel y aquellas realizadas por medios electromagnéticos.

En el artículo 2, equipara las publicaciones tradicionales a las publicaciones mediante medios electromagnéticos, lo siguiente: *“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 de papel o publicado en medios electromagnéticos.*

2. La Ley 270 de 1996 Estatutaria de la Administración de Justicia, artículo 95 señala: *“Tecnología al servicio de la Administración de Justicia. El Consejo Superior de la Judicatura debe propender por la incorporación de tecnología avanzada al servicio de la administración de justicia.* Esta noción se enfocará principalmente a mejorar la práctica de 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. Demás circulares y decretos han mencionado tangencialmente el tema de manera similar (Mosquera, J. A. M. G., Certain, A. F. C. J., & Cano, J. J. C. (s.f.).
3. Circular 14 de mayo de 1997 expedida por la Secretaria de Justicia de la Presidencia de la República determinó que el derecho de petición de los ciudadanos que se realice mediante

el uso de las herramientas tecnológicas modernas, debe ser asumido como si fuese una petición de la que trata el artículo 23 de la Constitución Política de Colombia.

4. Decreto 2150 de 1995 “*Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.*”: Norma mediante el cual se suprimen y reforman regulaciones y trámites innecesarios que existían en la Administración Pública. Específicamente el artículo 26 “ *Utilización del sistema electrónico de archivo y transmisión de datos*” obliga a la entidades de la Administración Pública implementar un sistema de transmisión electrónica de datos con la finalidad de que los usuarios remitan o reciban información requerida a sus actuaciones frente a la administración y aclara que no se podrá limitar el uso de tecnologías para el archivo documental respecto de los particulares sin que esto interfiera en el procedimiento interno de cada entidad.
5. Por su lado, la Ley 223 del 20 de diciembre de 1996 “*Por la cual se expiden normas sobre racionalización tributaria y se dictan otras disposiciones*”, artículo 37, eleva la factura electrónica a la categoría de factura de venta, estableciendo para el efecto, lo siguiente:

ARTÍCULO 37. *Adicionase 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 ventas 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.

6. Decreto 1094 de 1996: Ley que introduce la definición de factura electrónica, adicionalmente menciona que todos los equipos de computación de almacenamiento, comunicaciones y software que son empleados para administrar en la red y cuyos buzones electrónicos deben estar en Colombia, dicha Ley es ratificada en el Decreto 1165 de 1996 y regula los requisitos y aplicación de la factura electrónica.

7. Ley 527 de 1999: Ley sobre los documentos electrónicos, el cual, los considero como prueba equiparándolos con la factura electrónica, cuya representación es igual a un documento tributario generado electrónicamente, reemplazando al documento físico y con igual valor legal.

Con la misma ley culminó la costumbre de que se debe creer solo en lo que se encuentra soportado en papel y con ello la política de cero papeles incrementará, dando el paso al manejo de documentos informáticos, convirtiendo una sociedad que, sin tener papeles, tiene mucha más información, con la misma validez y seguridad que proporciona el papel.

Además de lo antes señalado, se encuentran disposiciones con el artículo 6 de la Ley 527 de 1999, el cual señala que: *“cuando una norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, siempre y cuando, la información que contiene sea accesible para su posterior consulta.*

En el mismo sentido, se encuentra el artículo 8 de la ley en comento, señala que cuando una norma requiera que la información sea presentada en forma original, ese requisito se quedará satisfecho si cumple los siguientes requisitos: 1. que pueda garantizar que la información se ha conservado íntegra desde cuando se generó por primera vez y 2. Que al requerirse que la información sea presentada, esta pueda ser mostrada a quien deba presentarse.

Requisitos relacionados con la capacidad de un mensaje de datos pueda ser almacenado y su inalterabilidad, los cuales serán tenidos en cuenta por cualquier Juez al momento de valorar una prueba digital.

Rincón Cárdenas (2015) establece que cuando se cumplan los requisitos señalados anteriormente mencionados que trae la ley, serán relacionados con la labor de las entidades de certificación y con las pruebas complementarias que puedan desprenderse, como lo son las declaraciones e inspecciones con peritos dirigidas a examinar el terminal electrónico donde se generó o recibió un mensaje de datos. No obstante, por economía procesal resulta

de mayor valor entender que, salvo la impugnación del documento electrónico original, certificado o no, el juez debe admitir como prueba sin hacer reflexiones extraordinarias al respecto, para evitar que la prueba electrónica sea imposible de valorar.

De la misma manera, el artículo 9 de la ley 527 de 1999 señala que: “*se considerará que la información consignada en un mensaje de datos es íntegra si ha permanecido completa e inalterada, o si se ha adicionado algún endoso o cambio que sea inherente o propio de su mismo proceso de comunicación, archivo o presentación.* Por lo anterior las entidades de certificación en su labor será de gran importancia, como terceros de confianza legitimados para certificar la integridad de los mensajes de datos, no significa que un mensaje de datos que no se encuentre certificado por una entidad de confianza, no sea válido jurídico y probatoriamente, al contrario, será tenido en cuenta como prueba ante cualquier autoridad administrativa o judicial.

Flórez (s.f.) en un estudio sobre “*La validez jurídica de los documentos electrónicos en Colombia a partir de sus evolución legislativa y jurisprudencial*”, trabajó sobre la Ley 527 de 1999 “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” manifestó que;

Colombia ha sido uno de los países pioneros en América del Sur que implementó la Ley modelo sobre Comercio Electrónico, logrando ampliar temas esenciales para el desarrollo del comercio electrónico, Mensaje de Datos, Sistemas de Información (art.2), Reconocimiento Legal de los Mensajes de Datos (art.5), el Principio de Equivalente Funcional de Documentos Escritos, la Firma Manuscrita y del Documento Original (arts.6,7,8 y 28), la Eficacia Probatoria de la Prueba Digital (arts. 10 y 11), el Criterio de Integridad Necesario para la admisión del mensaje de datos en el ámbito administrativo y judicial (art.9), La Formación de los Contratos Celebrados por Medios Electrónicos (art.14), el Acuse de Recibo, presunciones legales, efectos jurídicos, tiempo de envío y recepción de los mensajes de datos (arts. 20 al25), Comercio Electrónico en materia de transporte de mercancías (arts. 26 y 27) y todo lo referente al Régimen de Firmas Electrónicas.

Dicha Ley fue demandada por inconstitucionalidad de forma parcial, sentencia C-662 de 2000 Corte Constitucional, artículos 10, 11, 12, 13, 14, 15, 27, 29, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 y 45, alegando la parte actora que los certificados emitidos por las entidades de certificación sobre los documentos firmados digitalmente se estaba lesionando la Constitución Política de Colombia, artículo 131, alusivo a la función de dar fe pública y su resorte exclusivo en cabeza de notarios. De igual manera, enarboló dicha demanda, manifestado que al modificar el Código de Procedimiento Civil no podría proceder por medio de una Ley ordinaria sino a través del procedimiento especial que corresponde a las leyes estatutarias.

La Corte en la sentencia, contextualiza la importancia de la Ley de Comercio Electrónico y las ventajas para Colombia, se refirió a la Ley Modelo sobre Comercio Electrónico, como herramienta básica para la expansión del comercio electrónico a través de los mensajes de datos y particularmente en el correo electrónico, cubriéndolos de un grado de confiabilidad y seguridad jurídica igual al de los documentos escritos en papel y de la misma forma el Tribunal Constitucional, recomendó que la Comisión de las Naciones Unidas para el desarrollo del Desarrollo Mercantil, implemente una Ley como modelo para los ordenamientos jurídicos de los países con el fin de agilizar las relaciones comerciales internacionales, así como para otorgar la seguridad de las relaciones jurídicas entre particular en el entorno digital.

De la misma forma, definió el mensaje como “*información obtenida por medios análogos en el ámbito de comunicación modernas, bajo la configuración de los progresos técnicos que tengan contenido jurídico*” definición de mucha importancia ya que sirve como referencia de la semejanza que debe existir entre un documento físico y los documentos digitales con la finalidad de que tengan los mismos efectos jurídicos (derechos y obligaciones), recalcando los beneficios de los mensajes de datos. Como ejemplo, su inalterabilidad en el tiempo, capacidad de almacenamiento, la afirmación de derechos y obligaciones jurídicas entre los otorgantes y la facilidad de acceso para su posterior consulta, entre otros.

El Tribunal Constitucional estudió los cargos elevados por la actora:

“... estableció que las entidades certificadoras, al ser las encargadas de facilitar las transacciones electrónicas a través de sus funciones de verificación y certificación de documentos electrónicos firmados digitalmente, ejercen un servicio público el cual puede ser prestado tanto por entidades públicas como privadas, tanto nacionales como extranjeras, y en particular por las cámaras de comercio, de acuerdo con el artículo 365 de la Constitución Nacional y el artículo 29 de la ley 527 de 1999, el cual fue modificado por el artículo 160 del Decreto 19 de 2012 siempre que cumplan con los requisitos de acreditación del Organismo Nacional de Acreditación, conforme a la reglamentación expedida por el gobierno nacional (Artículo 29 Ley 527 de 1999)..”

Por lo anterior, se entiende que las entidades certificadoras, ejerce una labor de certificación técnica para quienes utilizan los sistemas de información electrónica, respecto a la confidencialidad, autenticidad, integridad y no repudiación de los mensajes de datos firmados digitalmente.

(Florez, s.f.) Concluye que, gracias a la jurisprudencia mencionada:

“se les da plena validez a los mensajes de datos, siempre y cuando de ellos se desprendan los elementos necesarios para identificar al emisor del mensaje, verificar que el documento generado y enviado por el emisor será el mismo que recibió el receptor de este, garantizado que el generador del mensaje de datos no pueda desconocer el envío de dicho mensaje y, en ciertos casos de privación de la información. Lo anterior significa que los documentos electrónicos gozan de plena validez jurídica para todos los efectos de acuerdo con el principio del equivalente funcional siempre y cuando sean generados a través de una firma digital y podrán contar con su respectivo certificado digital. Solo de esta forma los mensajes de datos podrían tener la misma validez de los generados por medios físicos firmados de manera manuscrita.

Adicionalmente, la Corte Constitucional en sentencia C-562 de 2000, Magistrado Ponente Vladimiro Naranjo Mesa, expone a la facilidad de reconocer una información allegada a sedes administrativas y judiciales en forma de mensaje de datos, señaló:

“No cuestiona la Corte el hecho de que el documento contentivo de la presente acusación haya sido enviado por telefax a la sede de la Corporación, pues entiende que, gracias a los avances tecnológicos que se han presentado en el campo de las comunicaciones, al orden jurídico interno se han venido incorporando algunas preceptivas que, amparadas también en los principios de eficacia, economía, celeridad y primacía de lo sustancial, le otorgan plena validez a ciertos actos procesales que se realizan bajo esa modalidad de mensaje de datos. Recientemente, se expidió la Ley 527 de 1999, por medio de la cual se define y reglamenta-entre otros el acceso y uso de los mensajes de datos, en cuyo artículo 10 ° se le reconoce “fuerza obligatoria y probatoria” a toda información que se alegue a las actuaciones administrativas y judiciales “en forma de un mensaje de datos”.

8. En el Código General del Proceso, Ley 1564 de 2012, artículo 164, habla de que toda decisión judicial debe fundarse en una prueba, pero esta prueba debe ser regular, significa que las pruebas deben ser conocidas o habituales y oportunamente allegadas al proceso. Para saber con seguridad cuáles son esas pruebas habituales, están descritas en el artículo 165 del Código General del Proceso y señala que son; la declaración de parte, la confesión, el juramento, el testimonio de parte, el dictamen pericial, la inspección judicial, los indicios, los informes, los documentos y cualesquiera otros medios que sean útiles para la formación del convencimiento del juez (subrayado fuera de texto).

En consecuencia, la prueba digital entra en el acápite subrayado, lo que significa que son un medio probatorio válido en la legislación colombiana.

2. MEDIOS DE PRUEBA EN EL ÁMBITO DIGITAL

Los medios de prueba se pueden ver desde dos perspectivas, la primera es aquella entendida como la actividad del juez o de otras personas, que suministran, al primero, el conocimiento de los hechos del proceso; y el segundo como los instrumentos y órganos que suministran al juez ese convencimiento, es decir, los elementos personales y materiales de la prueba (Echandia ,2015 p.45)

Así mismo, en los medios de prueba electrónica hay dos clases, la primera, es la información almacenada en un dispositivo electrónico y la segunda, es la que se transfiere por redes de comunicación, ejemplo el internet, telefonía fija o móvil.

Respecto a este último (comunicación) Delgado Martín (2017), manifiesta;

” Cuando la información se transmite en un proceso de comunicación, es decir, aquel proceso de transmisión de información entre un transmisor y un receptor a través de redes de comunicación abiertas o restringidas como Internet, telefonía fija, móvil u otras. Este tipo de información tendrá especial relevancia en la investigación y prueba de los delitos, pero también puede resultar de interés en otros órdenes jurisdiccionales.

Por lo anterior, se entiende en que toda información que se envíe por cualquier medio de comunicación entre dos o más personas, será importante en la investigación y tenida en cuenta en materia probatorio, penal, civil, contencioso administrativo y social.

En 2017, Echeverry establece que, el término de prueba electrónica es cualquier valor probatorio de la información almacenada o transmitida en formato digital, dicha evidencia podría convertirse en un factor indispensable dentro de un proceso, no obstante, en la mayoría de los casos se pueden volver frágiles y volátiles.

En otras palabras y siguiendo la línea de pensamiento de Marín y Echeverry, el medio de prueba, es la forma en cómo voy a introducir la evidencia digital al proceso, por lo tanto, se debe evitar que se pierda, se elimine o se deteriore.

3. TIPOS DE PRUEBAS ELECTRÓNICOS O DIGITALES

Acuario (s.f) en su estudio, menciona dos clases de pruebas digitales, la primera es; constante y la segunda es volátil. La primera se entiende como aquella prueba que se encuentra almacenada en un medio informático que mantiene preservada la información incluso después de apagada. La volátil es aquella evidencia que se encuentra temporalmente alojada en la memoria RAM, o en CACHE y la información se pierden cuando el computador es apagado.

De igual forma en el desarrollo de la tecnología está en constante transformación al igual que el manejo de las herramientas electrónicas o digitales, por ende, la prueba de carácter digital está siendo utilizado cada vez más, como son los instrumentos informáticos, de comunicaciones y multimedia, móviles, tabletas, ordenadores, dispositivos USB, ZIP, CD-ROM, DVD, reproductores de MP3 o MP4, navegadores, servidores PDAs, entre otras. No obstante, el estudio de Delgado Martín (2017) arroja que las principales fuentes de la prueba digital, son el correo electrónico, el SMS, la mensajería instantánea o mensaje de datos la cual se entenderá como escrita (Peña, 2001), las redes sociales y otros elementos web.

Delgado Martín (2017) señala que la prueba es la información contenida o transferida por medios electrónicos, en cambio el medio de prueba será la forma a través de la cual la información entra en el proceso.

El Ministerio de Tecnologías y Comunicaciones – MinTic de Colombia, identifica como posibles fuentes de datos:

- Computadoras de escritorio y portátiles
- Servidores (Web, DHCP, Email, Mensajería Instantánea, VoIP Servers, FTP o cualquier servicio de filesharing).
- Almacenamiento en red
- Medios internos como externos: Firewire, PCMCIA, Discos Ópticos y Magnéticos, Discos Duros Extraíbles, Memorias SD y MicroSD
- Cámaras digitales, dispositivos celulares, Grabadoras de video y audio.

Respecto a seguridad informática, existen otras fuentes adicionales de información como lo son:

- Logs de dispositivos de seguridad informática como IDS, Firewalls, Plataformas de Antispam, Proxy, estén ubicados o no dentro de los dispositivos o consolidados en algún sistema SIEM.
- Logs de dispositivo de red como switches o routers.
- Logs de proveedores de servicio (que pueden obtenerse bajo órdenes judiciales únicamente)

De igual forma se debería tener en cuenta cualquier sistema que registre información, como fuente de datos.

Por otro lado, es indispensable mencionar los objetos no susceptibles de registro (artículo 223 del CCP) específicamente los archivos de las personas indicadas en los numerales precedentes que contengan información confidencial y relativa al indiciado, imputado o acusado, acogiendo los documentos digitales, videos, grabaciones, ilustraciones, entre otros de los cuales sean relevantes a los fines de restricción. (Daza, 2016 p.36)

En 2000, Mateu De Ros y Cendoya Méndez de Vigo, establecen en su estudio que el profesor GUASP, clasifica los medios de prueba como:

- Pruebas personales o factor humano, cuando el medio es proporcionado por una persona, estando incluida la confesión, la testifical y la pericial. Se incluyen los documentos públicos y los privados (Mosquera, Certain & Cano, s.f.).

La evidencia puede ser un testimonio de una persona que tiene conocimiento de un registro de servidor de seguridad o un disco duro que contiene datos.

- Pruebas reales, cuando el instrumento probatorio viene dado por una cosa, distinguiendo entre documento y monumento, según pueda ser o no desplazado a la presencia del Juez. Se incluye el reconocimiento judicial

Por lo tanto, no existirá prueba digital en el proceso, sin que primero se allegue por un medio probatorio, en cuyo caso será proporcionado mediante un testigo o un documento.

3.1 Documento electrónico

Devis Echandia, doctrinante nacional, señala que el documento es *“toda cosa que sirve de prueba histórica indirecta y representativa de un hecho cualquiera”*, y Carnelutti (1982) manifiesta que *“el documento no es solo una cosa, sino una cosa representativa, o que sea capaz de representar un hecho”*

Por lo anterior, En 2015, Rincón Cárdenas señaló el documento electrónico como *“la representación en forma electrónica de hechos relevantes, susceptibles de ser representados en una forma humanamente comprensible”*

El Consejo de Europa 95/144 CE, consideran que lo esencial es la información incorporada en el registro electrónico y la admisibilidad en el proceso del documento electrónico como medios de prueba en el proceso existe desde hace años una aceptación jurisprudencial del valor probatorio de esta clase de herramientas probatorio, incorporándolos dentro de un concepto amplio de documento.

Sentencia de la Sala Tercera del Tribunal Supremo de España de 1997, dichas sentencias, señalan que la firma manuscrita o autógrafa no es el único procedimiento admisible en Derecho para garantizar la autenticidad de un documento, estas pueden ser como los trazados gráficos que conceden autoría y obligan, como lo son, las claves, los códigos, los signos y, en algunos casos los sellos con firmas. Por otro lado, señalan que los documentos sin firma, pueden producir efectos jurídicos ya que, la firma es un elemento, pero a veces no esencial, en cuanto existen documentos sin firma que tienen valor probatorio, como ejemplo los libros comerciantes.

La ley de Enjuiciamiento Civil de España a diferencia de Colombia, señalo en su legislación la diferencia entre documento y documento electrónico, cuya definición se refiere a los documentos electrónicos, como instrumento y no como “documento”, cuya función es archivar, conocer o reproducir palabras, datos, cifras y operaciones matemáticas, artículos 265, 299 y 384, dicha Ley hace la distinción es entre escritos, documentos y los medios e instrumentos.

Por lo anterior, un documento electrónico es un mueble por ende puede ser trasladado de un lugar a otro, el cual representa un hecho o un acto del hombre, puede ser creado, diferenciado su

originalidad y autenticidad, su procedencia podrá ser privado y público, de acuerdo a los términos de la Ley Colombiana.

3.2 Mensaje de datos

En Colombia la Ley 527 de 1999, artículo 2, define el mensaje de datos como “*la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otro, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax*”.

La Corte Constitucional, se refirió al contenido del mensaje de datos en la sentencia del 8 de junio de 2000, M.P. Fabio Morón Díaz, de la siguiente manera la noción de “mensaje” comprende la información obtenida por medios análogos en el ámbito de las técnicas de comunicación moderna, bajo la configuración de los progresos técnicos que tengan contenido jurídico.

En la definición de mensajes de datos, hace referencia a los “medios similares”, con la finalidad de dejar abierto a todos los avances tecnológicos que se generen con el tiempo.

El concepto de datos es amplio y abarca varios ámbitos entre esos la transacción electrónica, que puede ser consultada posteriormente y que puede ser o no alterada, cuyo soporte puede ser físico o digital, que para ser utilizada se requiere de la utilización de un medio electrónico y puede tener incidencia real y directa sobre la voluntad (Davara, 2001, p. 188).

El mensaje de datos debe tener el mismo tratamiento de los documentos consignados en papel, significa, que debe darse la misma eficacia jurídica, puesto que el mensaje de datos comporta con los mismos criterios de los documentos (Rincón, 2015).

Para que un mensaje de datos pueda ser tenido en cuenta como prueba judicial o extrajudicial, se encuentra expresamente en el artículo 10 de la Ley 527 de 1999 señala; “ *los mensajes de datos serán admisibles como medios de prueba y con la fuerza probatoria otorgada en el Código Procedimiento Civil (hoy Código General del Proceso) a los documentos, recordando que en toda*

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

La ley colombiana (Ley 527 de 199, artículos 5 y 10) no negará la 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, allí debe entrar a evaluar la confiabilidad en la forma en que se haya generado, archivado, comunicado y conservado a fin de garantizar su autenticidad e integridad (Contreras, 2015).

Las características esenciales del mensaje de datos son Cárdenas (2015): 1. es una prueba de la existencia y naturaleza de la voluntad de las partes de comprometerse; 2. es un documento legible que puede ser presentado ante las entidades públicas y los tribunales; 3. admite su almacenamiento e inalterabilidad en el tiempo; 4. facilita la revisión y posterior auditoría para los fines contables, impositivos y reglamentarios; 5, afirma derechos y obligaciones jurídicas entre los intervinientes y es accesible para su ulterior consulta.

Por otro lado, los mensajes de datos salvaguardan la integridad de la información, gracias a los sistemas de protección como son; la criptografía, firmas digitales, huellas digitales y las empresas certificadoras encargadas de proteger la información en diversas etapas de la transacción, dentro del marco de la autonomía. Adicionalmente, cuando el contenido de un mensaje de datos sea completo y esté alterado, pero exista algún anexo inserto, este no afectara su originalidad, asimilable como el sobre utilizado para enviar ese documento “original” (Rincón Cárdenas, 2015, p.62).

En consecuencia, de lo anterior, es de vital importancia los mensajes de datos ya que es el soporte electrónico base, bajo el cual se representa y se prueban las relaciones que establezcan los medios electrónicos.

Con lo anterior, Rincón Cárdenas (2015) extrae lo siguiente (p. 71): 1. el mensaje de datos obliga a quien lo genera y vincula a sus destinatarios: 2. El mensaje de datos tiene valor y fuerza

probatoria al relacionarse de una prueba contenida en un documento, culminando la discusión sobre la admisibilidad como prueba de los documentos electrónicos, afiliado con el uso del télex y del telefax y seguida con la utilización de tecnología como el EDI e Internet: 3. y último, ya no se tendrá como original exclusivamente el papel escrito, sino también el mensaje de datos que tenga las características propias (Sentencia C-662 de 2000).

3.3 Diferencia entre mensaje de datos y documento electrónico (Rincón Cárdenas, 2015. (p. 72)

Mensaje de datos	Documento electrónico
<p>Cualquier tipo de información (signo, símbolo, imagen, sonido, palabra, letra), que pueda ser creada, transmitida, utilizada y almacenada por cualquier tipo de tecnológico.</p> <p>El tipo de información podrá o no significar o representar algo.</p>	<p>Representa hechos, ideas o actos generados por los seres humanos, incorporados a un soporte electrónico.</p> <p>Su origen podrá ser privado o público, dependerá del agente generador.</p> <p>En los casos en que la Ley exige solemnidades para entender que un documento electrónico se deberá cumplir con los requisitos de la ley, como puede ser la incorporación al documento de la firma electrónica que el legislador requiera.</p>

3.4 Los actos de comunicación procesal por medios electrónicos o informáticos

En Europa en la Ley 1 de 2000 “Enjuiciamiento Civil de España”, artículo 162, señala;

“cuando los juzgados o tribunales y las partes o los destinatarios de los actos de comunicación dispusieron de medios electrónicos que permitan el envío y la recepción de escritos y documentos, de forma tal que esté garantizada la autenticidad de la comunicación y de su contenido y quede constancia fehaciente de la remisión y recepción

íntegras y del momento en que se hicieron, los actos de comunicación podrán efectuarse por aquellos medios, con el acuse de recibo que proceda”

En Colombia, la Ley 1437 de 2011” Código de Procedimiento Administrativo y de lo Contencioso Administrativo”, artículo 56, mencionan la notificación electrónica “Las autoridades podrán notificar sus actos a través de medios electrónicos, siempre que el administrado haya aceptado este medio de notificación.”, los actos administrativos electrónicos, artículo 57“ *Las autoridades, en el ejercicio de sus funciones, podrán emitir válidamente actos administrativos por medios electrónicos siempre y cuando se asegure su autenticidad, integridad y disponibilidad de acuerdo con la ley.*”. Archivo electrónico de documentos, artículo 58 “*Cuando el procedimiento administrativo se adelante utilizando medios electrónicos, los documentos deberán ser archivados en este mismo medio. Podrán almacenarse por medios electrónicos, todos los documentos utilizados en las actuaciones administrativas*”. Expediente electrónico, artículo 59 “*Reglamentado parcialmente por el Decreto Nacional 2609 de 2012. El expediente electrónico es el conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan...*”, creación de una dirección electrónica o sede electrónica, artículo 60. Recepción de documentos electrónicos por partes de las autoridades, con la finalidad de constatar el acuse de recibido de las comunicaciones por medio de correo electrónico, artículo 62.

Por lo anterior, se observa que, respecto del derecho en lo contencioso administrativo, se implementó el sistema digital para la comunicación de los pronunciamientos de la administración judicial y administrativa ya sea por una página web o un correo electrónico y crear un mecanismo para asegurarse si lo remitido fue entregado con éxito o no, de igual forma la creación de archivos y expedientes digitales, para salvaguardar los documentos electrónicos relacionados con el proceso.

En el Código de Procedimiento Penal, Ley 906 de 2004, numeral 5, artículo 146, señala que “Cualquier documento utilizado durante la audiencia que se realice a través de dispositivo de audio-vídeo, debe poder transmitirse por medios electrónicos. Tendrán valor de firmas originales aquellas que consten en documentos transmitidos electrónicamente”.

De acuerdo al Código General del proceso, Ley 1564 de 2013 admite cualquier medio digital en los procesos judiciales, siempre y cuando se garantice la autenticidad y la originalidad del intercambio o acceso a la información parágrafo tercero, artículo 103;

“USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES. En todas las actuaciones judiciales deberá procurarse el uso de las tecnologías de la información y las comunicaciones en la gestión y trámite de los procesos judiciales, con el fin de facilitar y agilizar el acceso a la justicia, así como ampliar su cobertura. Las actuaciones judiciales se podrán realizar a través de mensajes de datos. La autoridad judicial deberá contar con mecanismos que permitan generar, archivar y comunicar mensajes de datos. En cuanto sean compatibles con las disposiciones de este código se aplicará lo dispuesto en la Ley 527 de 1999, las que lo sustituyan o modifiquen, y sus reglamentos.”

En consecuencia, lo que se busca con la Ley 1564 es facilitar y agilizar el acceso a la justicia en todos los procesos judiciales y la tecnología es una herramienta de gran valor y utilidad para tal fin.

Sin embargo, de acuerdo a la norma y jurisprudencia planteada en el subtítulo de precedentes de la legislación en Colombia, se puede inferir que en el ámbito normativo y jurisprudencial en Colombia, no resuelve las inquietudes en relación a la evidencia digital, no obstante, la Ley 906 de 2004 y el Decreto 2770 de 2004 reglamentaron el sistema acusatorio, nombrando en el art. 424, numerales 6 y 7, la grabación computacional y el mensaje de datos, como documentos y por ende serían pruebas documentales. Art. 426 describe los métodos de autenticación e identificación de documentos, numeral 3 certificados digitales emitidos por entidades de certificación como instrumento capaz de lograr ser válido, probatoriamente. Respecto del tema de autenticación en el art. 425 señala que cuando se está frente a un documento verdadero (salvo en prueba en contrario) y se tiene certeza de la persona quien lo elaboro, firmo, produjo, etc., por algún otro procedimiento se tendrá como auténtico.

En conclusión, la Ley 527 de 1999 y la Ley 906 del 31 de agosto de 2004 son aportes legislativos de alta importancia en el tema probatorio y tecnológico y aunque es un avance, no lo es en el tema probatorio, esto es, saber con seguridad cómo se debe allegar a un proceso ni cuáles son los requisitos para que se considere auténtica ya que la ley 527 de 1999 habla en el contexto mercantil y no probatorio y aunque la Ley 906 de 2004 menciona concepto de evidencia digital, el tema de incorporación y valoración en un proceso judicial no es comprensible. Por lo tanto, a falta de dicha regulación, es inevitable recurrir al derecho probatorio, con la finalidad de hacer una investigación de los requisitos legales para la aceptación e incorporación y la modalidad de presentación de las pruebas digitales. (Mosquera, J. A. M. G., Certain, A. F. C. J., & Cano, J. J. C. (s.f.))

Además de lo antes señalado, se trae a colación el Código de Procedimiento Administrativo de lo Contencioso Administrativo, Ley 1437 de 2011, Artículo 40 señala que, las pruebas durante el proceso (antes de que se profiera la decisión de fondo), se podrán aportar, pedir y practicar pruebas de oficio a petición del interesado sin requisitos especiales. Respecto del auto que decida la solicitud de pruebas aportadas, no procederá recurso alguno. El interesado tendrá la oportunidad procesal para controvertir las pruebas aportadas o practicadas dentro de la actuación, antes de que se dicte una decisión de fondo.

Los gastos que genere la práctica de pruebas serán asumidos por quien las solicitó. En el caso en que varios serán los interesados, se distribuirá los gastos por porcentajes iguales.

Todos los medios de prueba señalados en el Código General del Proceso, Ley 1564 de 2012 (art. 164), serán admisibles, como bien se citaron en el subcapítulo “2.3 Precedente del concepto evidencia digital en la legislación colombiana, numeral 6”:

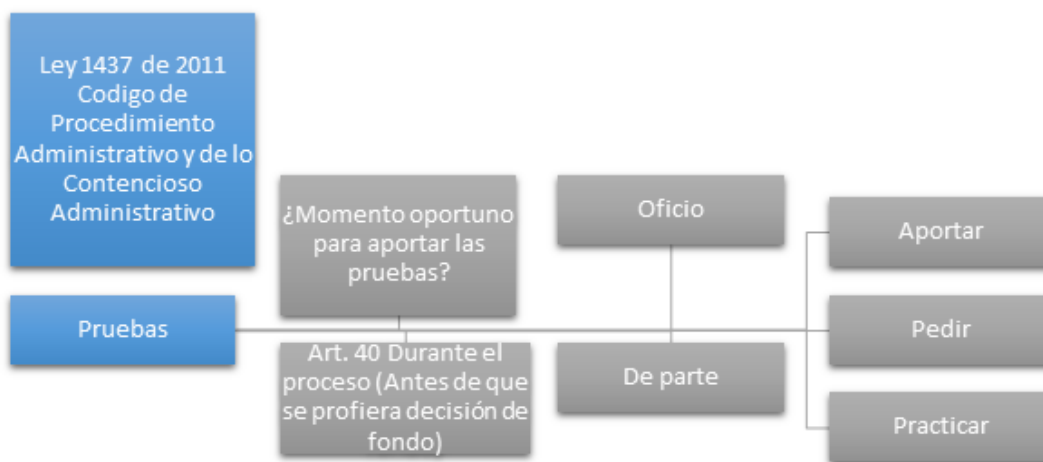
“...la declaración de parte, la confesión, el juramento, el testimonio de parte, el dictamen pericial, la inspección judicial, los indicios, los informes, los documentos y cualesquiera otros medios que sean útiles para la formación del convencimiento del juez”

Gráfico 1. Medios de prueba admisibles



Fuente: elaboración propia

Gráfico 2. Momento para aportar pruebas

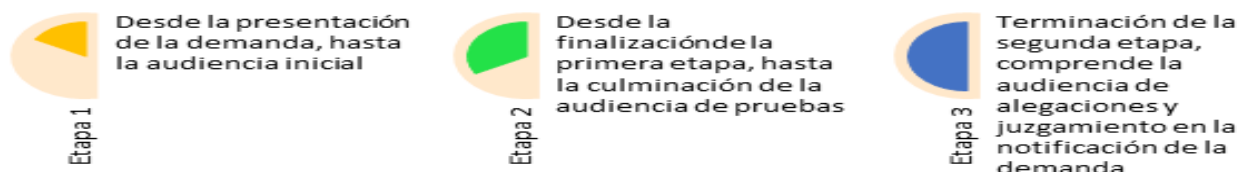


Fuente: elaboración propia

Gráfico 3. Etapas del proceso

Ley 1437 de 2011 Código del Procedimiento Administrativo y de lo Contencioso Administrativo

- Art. 179 Etapa.

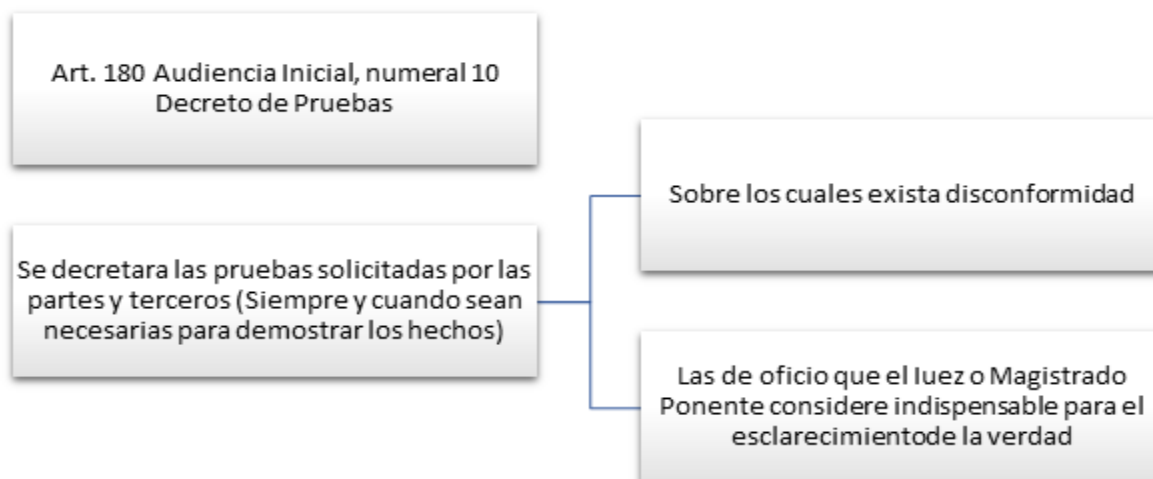


Fuente: elaboración propia

Gráfico 4. Decreto de pruebas

Ley 1437 de 2011 Código del Procedimiento Administrativo y de lo Contencioso Administrativo

- Art. 180 Audiencia Inicial



Fuente: elaboración propia

Gráfico 5. Audiencia de pruebas



Fuente: elaboración propia

Al momento de finalizar la audiencia de pruebas, el juez señala fecha y hora para la audiencia de alegaciones y juzgamiento.

- En un término no mayor a 20 días.
- Sin perjuicio que, por considerarse innecesaria, ordene la presentación por escrito de los alegatos dentro de los diez (10) días siguientes.
- Caso en el cual dictara sentencia en el término de veinte (20) días siguientes al vencimiento para presentar alegatos.
- Ministerio Público podrá presentar el concepto si a bien lo tiene.

4. PASO A PASO DE LA PRUEBA DIGITAL

No importa el orden jurisdiccional, ya que toda prueba digital debe cumplir las siguientes fases (Giraldo. M.C):

1. Obtención de la información o datos, la cual debe ser lícita, sin violación a los derechos fundamentales.

Existe una metodología general del procedimiento de prueba digital creada por el Ministerio de Tecnologías de la Información y las Comunicaciones. (s.f), esta es:

- a. Aislamiento de la escena: Limitar el acceso a la zona del incidente para evitar alteración en la prueba.
 - b. Identificación de fuentes de información: Los datos relacionados con un hecho deben identificarse, evaluarse y controlar la escena y así, proceder con el siguiente paso:
 - c. Examinación y recolección de información: Aplican las técnicas y herramientas forenses se aplican a los datos recolectados para extraer la información importante, evitando alterar la integridad de los datos
 - d. Análisis de datos: Hacer un análisis de la información relevante que se obtuvo en el paso de examinación, concentrándose a buscar las respuestas para el caso, correlacionando los hechos, archivos y los datos hallados.
 - e. Reporte: Reporte de los resultados del análisis que puede concluir los procedimientos que llevaron a cabo, si quedaron verificaciones pendientes, mejoras, cambios.
2. Incorporación de la información o datos al proceso: La prueba debe ser importante o relevante, es decir debe pertenecer al caso real, para acreditar los hechos, En esta fase se debe cumplir los siguientes requisitos:
- Pertinente o útil: La prueba debe demostrar el hecho.
 - Idoneidad: La prueba debe ser conducente, significa que debe ser determinante, ser realmente lo que pretender ser.
 - Inoponible: La ley lo da, por cierto
 - Lícita: No puede ir en contra de la Ley
 - Auténtica: Puede llegar hacer autentica por medio de un testimonio, el ejemplo lo elaboró UniColombia (s.f.) en su trabajo “La Evidencia Digital o la prueba electrónica”, señala que, puede llegar hacer el administrador de red que ha protegido en el servidor de seguridad los registros inmediatamente después de un ataque y da testimonio que los datos de registro presentados en la corte coinciden con los datos que veía en los registros de esa fecha y hora. El oficial de policía que llego a la escena puede testificar que él empaqueto de equipo que contiene los archivos de registro y los entregó al laboratorio de pruebas. El técnico de análisis

forense que tomó posesión de la computadora puede testificar que él lo recibió de dicha persona y que utilizó métodos de análisis forense estándar para hacer una copia a nivel de bits del disco que contiene los registros.

- Necesidad de prueba: Su importancia es indispensable ya que con esta se confirma o se desvirtúa una afirmación, hipótesis, buscando la verdad formal (Acuario s.f.).
- Efectiva: Se habla de efectividad cuando la prueba respeta la protección de datos personales, la intimidad personal y la libertad de expresión

3. Valoración de los datos o de la información incorporada: Consiste en que el Juez es quien practica y valora la prueba (inmediación).

5. FASES DE LA PRUEBA DIGITAL (Martín, 2017)

Obtención de la prueba	<ul style="list-style-type: none"> • Licitud
Incorporación al proceso	<ul style="list-style-type: none"> • Pertinencia y necesidad. • Licitud. • Cumplimiento de los requisitos procesales (admisibilidad procedimental)
Valoración de la prueba	<ul style="list-style-type: none"> • Impugnación. • Autenticidad • Integridad o exactitud

La legislación colombiana Ley 527 señala que todo documento electrónico debe contar con unos atributos jurídicos para otorgarle plena validez jurídica y probatoria, estos son (Rincón, 2015):

- a. Escrito: Cuando una norma solicite que la información esté por escrito, dicho requisito quedará satisfecho con un mensaje de datos, siempre y cuando la información que contenga dicho mensaje de datos sea asequible para su posterior consulta, lo cual obliga a que se deba conservar en medio seguro la información.
- b. Original: Cuando una norma requiera que la información presentada en su forma original, esa obligación quedará satisfecha si cumple los siguientes requisitos: 1. que se garantice que la información se ha conservado íntegra desde el momento en que se generó por primera vez; 2. que al requerirse que la información sea presentada, esta pueda ser exhibida a quien lo solicite.

“Lo que se puede entender con esta disposición es que para el caso de documentos electrónicos el criterio de original está dado por su inalterabilidad y posterior consulta, a diferencia de los documentos por escrito, los cuales se considera como único original el primer ejemplar (Morales- s.f.).

Como ejemplo traigo un caso de firma electrónica de Amani (2004) :

Dos personas desean intercambiar un mensaje digitalmente firmado deberán seguir un proceso, el cual es invisible al usuario por cuanto es realizado de manera automática por el computador.

Luis quiere enviarle un documento a Sofía, para ello tendrá entonces que seguir los pasos siguientes: 1-Luis redacta el documento. 2-Lo ejecuta a través de un programa de computación unidireccional denominado „Hash Function“ (por ejemplo, MD5) para crear el resultado „hash“. 3-Firma el resultado „hash“ del documento, utilizando su clave privada y empleando tecnología de encriptación de clave pública como RSA. 4-Combina el documento con la Firma para obtener un nuevo documento firmado. 5-Envía el documento firmado a Sofía. Una vez recibido el documento, Sofía puede leerlo, pero no puede estar segura de que el documento no haya sido alterado o que 53 ciertamente provenga de Luis. Para comprobar lo antes lo antes descrito, Sofía deberá seguir los pasos señalados a continuación: 1-

Sofia separa el documento de la firma. 2-Lo ejecuta a través del mismo programa de computación, unidireccional de tipo „hash“ (como la MD5) usado por Luis para obtener un resultado „hash“ el documento. 3.Obtiene la clave pública de Luis de un proveedor de servicios de certificación. 4-Utiliza la clave pública de Luis para descifrar su firma (una vez más el algoritmo de encriptación de clave pública, tal como RSA.) 5-Compara el resultado „hash“ obtenido luego de descifrar la firma digital de Luis, con el resultado „hash“ obtenido del documento. Si los resultados „hash“ son iguales, entonces ella podrá estar segura de que el documento fue enviado por Luis y que no ha sido modificado. Si los resultados „hash“ hubiesen resultado distintos, entonces sabría que el documento adolecía de algún vicio. Como el ejemplo lo indica, la firma digital goza de ventajas sobre la firma autógrafa. (p. 161)

4. Integridad: Si la información reposada en un mensaje de datos está completa e inalterable, o si se ha adicionado algún endoso o cambio que este sea inherente o propio de su mismo proceso de comunicación, archivo o presentación se considerará íntegro. Los atributos escrito y original, depende de la integridad, ya que sin este no se podrá hacer valer un documento electrónico ante la autoridad judicial o administrativa.

Para conservar la integridad se debería solicitar:

- No apagar el sistema: La información contenida en el memorial volátil (RAM) podría perderse.
- No desconectar el sistema de la red: Un hacker podría cubrir sus pistas mediante la supresión de los archivos de registro y otros datos probatorios.
- No ejecutar ningún programa ya que un hacker podría haber dejado un programe que borre los datos cuando se active algún evento, eso es cerrar o abrir un programa.
- No abrir archivos para examinarlos, modifica fecha y hora.

Lo anterior, está basado en el estudio realizado por Mauricio Curre Días publicado en la UNICOLOMBIA “La Evidencia Digital o la prueba electrónica”, recomienda que la mejor manera de

preservar una evidencia digital en su estado original es conectar el ordenador a otro ordenador en que se pueda copiar la información digital.

6. MÉTODO PARA HACER ADMISIBLE LA PRUEBA DIGITAL

En el trabajo de Mosquera, J. A. M. G., Certain, A. F. C. J., & Cano, J. J. C. (s.f.) manifiesta que J. Cano se basó en autores como Sommer y Casey y recuerda que en las legislaciones modernas son cuatro (4) los criterios que se deben tener en cuenta y analizar al momento de decidir sobre la admisibilidad de la prueba digital: la autenticidad, la confiabilidad, la completud o suficiencia y el apego y respeto por las leyes y reglas del poder judicial.

De acuerdo a lo anterior, y al trabajo de “Evidencia Digital: contexto, situación e implicaciones nacionales”, se expondrá cada uno de los criterios:

6.1 Autenticidad

La autenticidad es un requisito para que sea aceptada la evidencia digital y para que se considere auténtica debe cumplir dos condiciones, el primero que la evidencia haya sido generada y registrada en el lugar de los hechos y la segunda que no esté alterado los medios originales, significa que los registros atañen a la realidad. En el Código General del Proceso (Ley 1564 de 2012) en el art.165 considera el documento como medios de prueba entre otros y cualesquiera que sean útiles para la formación del convencimiento del juez, no obstante, la presunción de autenticidad de la prueba puede afectarse en su creación, procesamiento, almacenamiento, recuperación y eliminación, generado un impacto dentro de un proceso judicial.

Es aquella evidencia que ha sido generada y registrada en lugares relacionados con el caso, específicamente en la escena del posible delito (Echeverry, 2017).

Del mismo modo la garantía de autenticidad de la identificación del firmante se logra por la particularidad de las gráficas de cada persona, demostrables de los exámenes periciales.

La integridad del contenido del documento de lo que se comunica, garantía en la constancia fehaciente de la emisión y recepción íntegras del escrito o documento que se comunica y garantía de constancia del momento en que se realiza la comunicación (De Ros & Méndez, 2000).

Por otro lado, se debe cumplir con los requisitos de fondo exigidos por la ley, respecto del acto que se instituye en el documento, según su especie y calidad, y adicionalmente deberá reunir los requisitos formales establecidos por la ley para el valor de ciertos actos en consideración a la naturaleza de ellos, consentimiento y causa lícitos de acuerdo a trabajado por González (2013).

6.2 Confiabilidad

Es confiable la evidencia digital cuando viene de fuentes creíbles y verificables. Significa que la prueba digital es confiable siempre y cuando el sistema que la haya generado no haya sido violado y estaba en correcto funcionamiento al momento de recibir, almacenar o generar la prueba.

El valor probatorio de la prueba digital, debe reunir los mismos requisitos que se refieren a la esencia instrumentales probatorias propias de todo acto o contrato, como: ser un instrumento público o privado, reconocido por el ordenamiento jurídico y reunir los requisitos de eficiencia que establecen los códigos de procedimiento para que sean creíbles y ostentan valor probatorio en juicio (Rincón Cárdenas,2015).

De igual modo, contestaría a diferentes inquietudes que se pretende demostrar en los registros electrónicos, ejemplo: ¿Cómo se diseñó la estrategia de registro y su almacenamiento? ¿Cómo se registran, recogen y analizan?

6.3 Suficiencia

De acuerdo a la publicación de (Echeverry, 2017), se refiere a la presencia de toda evidencia necesaria para adelantar el caso.

Confiabilidad y suficiencia se armonizan ya que una prueba es suficiente si esta es completa y para que sea completa se requiere instrumentos de integridad, sincronización y centralización que admita percibir una *imagen completa de la situación objeto de análisis*.

Se reitera que la prueba digital o electrónica tendrá valor probatorio que el juez en su libertad probatoria le otorgue y se deberá tener en cuenta la confiabilidad en tres aspectos, estos son: la forma que se generó, la forma como se ha conservado y la forma como se identifique el iniciador. (Rincón Cárdenas, 2015)

6.4 Apego y respeto por las leyes y reglas del poder judicial

Toda evidencia digital debe obedecer con los criterios de autenticidad, confiabilidad y suficiencia y debe acatar la normatividad del sistema jurídico colombiano. Entendiendo que no procederá ninguna prueba digital sin que cumpla con los requisitos normativos. El art. 168 del Código General del Proceso manifiesta cuando se rechaza de plano, *“El juez rechazará, mediante providencia motivada, las pruebas ilícitas, las notoriamente impertinentes, las inconducentes y las manifiestamente superfluas o inútiles”*. Art 176 C.G.P señala que la pruebas se aprecian en conjunto, eso significa que en una sola diligencia se practicarán todas las pruebas que se admitieron con antelación *“Las pruebas deberán ser apreciadas en conjunto, de acuerdo a las reglas de la sana crítica, sin perjuicio de las solemnidades prescritas en la ley sustancial para la existencia o validez de ciertos actos...”*

El doctor Antonio Rocha en su libro *“De la prueba en derecho”*, señala: La prueba será impertinente cuando no están aludidas al objeto del proceso y no tiene que ver con los hechos que

involucra la litis. Será inconducente o impertinente la prueba cuando se pretende probar un hecho que, aún demostrado, no sería de naturaleza para influir en la decisión de la litis.

Por último, una prueba superflua es aquella que no desempeña ninguna utilidad en el proceso, sinónimo de inútil y no podrá lograr convencer al juez, respecto de lo que quiere demostrar.

Por lo anterior, se entiende que las pruebas deben de ser conducentes, por ende, se debe emplear el medio de prueba legal, lícito, eficiente para corroborar los hechos que se pretende hacer valer.

Así mismo, hace referencia a los procedimientos internacionalmente aceptados para recolección, aseguramiento, análisis y reporte de la evidencia digital. Si bien es cierto que los Códigos de Procedimiento Civil y Penal contiene disposiciones normativas que establecen la manera de aportar una prueba a un proceso, en el campo internacional existen iniciativas como las de la IOCE, el *Digital Forensic Research Workshop*, donde se establecen marcos de acción y lineamientos que cobijan la evidencia en medios electrónicos (ADALID, & Echeverry, J. J. E, 2019).

Se entenderá por eficacia probatoria (Cárdenas, 2015), cuando aparte de ser válido, reúne los requisitos de idoneidad y es conducente para probar un hecho un acto, tendiendo por seguridad su autenticidad, y si es otorgado fuera del país, se deberá cumplir las autenticaciones previstas en la ley, por último, no puede estimar prueba legalmente válida en contra, agregando además que el autor del documento tenga la capacidad requerida para suscribir el acto documentado.

El profesor Devis Echandia, señala que, el objeto de la prueba está limitado a los hechos pasados presentes y futuros y los que puedan asimilarse a estos.

Pero además de lo anterior, lo importante en la valoración de la prueba es: “(i) la confiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje, (ii) la confiabilidad de la forma en que se haya conservado la integridad de la información, (iii) la forma en la que se identifique a su iniciador o autor y (iv) cualquier otro factor pertinente. (Ley 527 de 1999, artículo 11)

7 MODALIDAD PARA ALLEGAR LA PRUEBA DIGITAL

La prueba digital se presenta como regla general en medio electrónico, esto es en un CD ROM, memoria, disco duro etc., y para demostrar su inalterabilidad y autenticidad, se trae a colación la Ley 527 de 1999, artículo 8 “*Original*” señala que se entera como original un documento electrónico cuando se garantice que este ha conservado la integridad de la información a partir del momento en que se generó por primera vez. Anteriormente se explicó que los documentos electrónicos gozan de la misma presunción de auténticos como los documentos físicos hasta que se compruebe lo contrario y esto se hace utilizando la firma electrónica, deshabilitando los permisos de edición, o revisando los metadatos. (Mosquera, J. A. M. G., Certain, A. F. C. J., & Cano, J. J. C. (s.f.).

8 MOMENTO PARA PRESENTAR LA PRUEBA DIGITAL

El momento correcto para allegar la prueba está señalada en el Código General del Proceso, esto es al momento de proyectar la demanda, artículo 82, numeral 6. La petición de las pruebas que se pretenda hacer valer, con indicación de los documentos que el demandado tiene en su poder, para que este lo aporte. Así mismo, en el artículo 84 de la misma ley en el numeral 3, manifiesta que se deben allegar las pruebas extraprocesales y los documentos que se pretenda hacer valer y se encuentren en poder del demandante, señala *Anexos de la demanda*, manifiesta que la demanda debe adjuntar las pruebas. De igual forma en el momento de la contestación de la demanda, numeral 5, la contestación de la demanda deberá acompañarse de las pruebas que pretenda hacer valer. Art. 101 *Oportunidad y trámite de las excepciones previas*, en el escrito deberán acompañar todas las pruebas que se pretenda hacer valer y que se encuentren en poder del demandado.

No obstante, la ley 1564 de 2012 en su artículo 170 *Decreto y práctica de prueba de oficio* permite que el juez decrete pruebas de oficio, en las oportunidades probatorias del proceso y de los incidentes y antes de fallar, cuando sean necesarias para esclarecer los hechos objeto de la controversia o de acuerdo al artículo 98 cuando advierta fraude, colusión o cualquier otra situación similar.

La evidencia electrónica se ha venido utilizando con más cotidianidad en los estrados judiciales y por ende se ha tecnificado en su fuerza probatoria y es por ello que las partes dentro de un proceso

deben colocar a disposición del juez, la mayor cantidad posible de evidencias que ayuden a probar el hecho y eliminen cualquier alteración de la prueba (Abogacía Española Consejo General & Díez, 2015).

9 CADENA DE CUSTODIA EN LAS PRUEBAS DIGITALES

En nuestra legislación colombiana, la Ley 527 de 1999, señala las condiciones para conservar los mensajes de datos y de los documentos, estos son (art.12):

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.

La conservación de mensajes de datos y archivo de documentos a través de terceros (art.13) se podrá hacer siempre y cuando se cumplan las condiciones del artículo 12 de la misma ley.

Por lo anterior y de acuerdo a lo señalado en el artículo 250 de la Constitución Política, la custodia es un deber impuesto a la Fiscalía General de Nación, para que se garantice la transparencia de las pruebas que van dirigida al proceso penal.

Los servidores públicos y los particulares que tengan contacto o relación con las pruebas, como ejemplo se tiene la recolección, envío, manejo, análisis y conservación de estos elementos. La cadena de custodia, se inicia en el lugar donde se obtiene, encuentre o recaude el elemento físico de prueba y finaliza por orden de la autoridad competente ((Mosquera, J. A. M. G., Certain, A. F. C. J., & Cano, J. J. C. (s.f.)

Respecto de pruebas digitales, la cadena de custodia es indispensable ya que por su naturaleza (un chat, mensaje de texto, correo electrónico etc.) cualquier archivo se puede modificar , en

consecuencia la norma ISO/IEC 27037:2012 “Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence” dirigida al procedimiento de la actuación pericial en las etapas de recolección, identificación y secuestro de la evidencia digital no se adentra en la etapa de análisis de la evidencia.

La Fiscalía General de la Nación en su manual de Sistema de cadena de custodia, señala “Para garantizar la integridad de archivos digitales, en su recolección, se deben emplear programas que permitan calcular valores HASH (es un código que se puede generar para verificar un archivo, ejemplo es como la cédula de un archivo) y almacenarlos en medios que en lo posible no permitan su modificación o daño”, significa que es tiene una garantía de inalterabilidad de los documentos digitales. (Adalid, 2018).

Las personas que utilizan la tecnología y/o de comunicación, generan actividades mediante dispositivos electrónicos, de manera consciente o inconsciente, con voluntad o sin ella (González, 2000) que son útiles para la investigación de actuaciones ilícitas, generando entornos digitales. La investigación en este tipo de entorno digital incrementa la eficacia de la persecución y la prueba del delito y es allí cuando el Estado puede llegar a tener acceso en el entorno digital de una persona, con injerencia en sus derechos fundamentales, siempre que concurren tres requisitos, que la injerencia este prevista por la ley (legalidad), que su finalidad sea legítima (legitimidad del fin) y por último, que sea necesaria en una sociedad democrática para consecución de ese fin (necesidad) (Fiaschi (s.f) p. 366).

10 VALORACIÓN

En la valoración de las pruebas se tendrá en cuenta la Ley 527 de 1999 artículo 9 en el cual se entenderá que la información depositada en un mensaje de datos (entendiendo que son cualquier tipo de información (signo, símbolo, imagen, sonido, palabra, letra), que pueda ser creada, transmitida, utilizada y almacenada por cualquier tipo de tecnológico) esta íntegra, si esta permaneció completa e inalterado. Por otro lado, en el artículo 10, deja con claridad la admisibilidad de los mensajes de datos como medio de prueba y su fuerza probatoria y en cualquier actuación judicial o administrativa y por ende no se negará la validez, eficacia o fuerza obligatoria y probatoria.

Respecto de los criterios para la valoración, se encuentran señalados en el artículo 11, los cuales son; la sana crítica, 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.

La valoración probatoria en la evidencia digital no se debe aislar los elementos probatorios, esto es; la utilidad, conducencia y pertinencia (requisitos intrínsecos de la prueba), los cuales serán tenidos en cuenta en cualquier juicio de admisibilidad de evidencia y proteger la formalidad de la prueba y evitar que se obstruya y dificulte la actividad probatoria y así proteger la formalidad de la prueba y buscando que se impida la obstrucción la actividad probatoria. Universidad del Externado y Contreras (2015).

La autenticidad se debe asegurar y su autoría y quien promueve la verificación debe proponer los medios de prueba disponibles. Toda prueba que se allegue al proceso pasaran a ser o no admisibles y cada una reviste una particular importancia y esto es que el interesado debe producir o, si no están en su posesión, debe indicar en lugar donde se encuentran y el juez del proceso, deberá darle custodia y posterior a ello nombrar un consultor técnico (Sentis, 1980, p. 335)

Finalmente, Eugenio Picón de Peritos Ingenieros Informáticos (s.f.), manifiesta es su estudio que para ratificar la prueba digital es necesaria la realización de una prueba pericial informática y para garantizar su eficacia en el proceso se debería contratar un ingeniero en informática con los conocimientos técnicos necesarios para emitir un dictamen ya que ofrece garantías ante el tribunal.

CONCLUSIONES

En Colombia existe regulación frente al tema de prueba digital, nuestra legislación ha dejado abierta la posibilidad de acoplar nuestro mundo jurídico al avance tecnológico, pero esto no es suficiente, la posibilidad de implementar un procedimiento electrónico, buscando ventajas de celeridad y simplicidad de procedimientos, no es descabellada, es algo real y seguro, que va a pasar y que incluso está pasando. Es por ello, que es necesario mantener un conocimiento detallado de

las normas y regulaciones legales asociadas con las pruebas y el derecho procesal, así como de las técnicas y los procesos que permita una seguridad jurídica en la información digital recaudada., la integridad de los medios y la presentación idónea de las pruebas digitales.

No obstante, se debe actualizar o crear nuevas normas que regulen los acontecimientos que se vayan generando con el pasar del tiempo, para que se pueda implementar los sistemas análogos, los digitales de grabación y reproducción audio video, ya que, por su menor costo, y por la política de ahorro de papel, seguramente se implementara el sistema digital, por lo que la documentación en el derecho probatorio lo será en soporte electrónico conservada en las memorias de los ordenadores.

La investigación hace una recopilación de la información, esto es; la ley, la jurisprudencia y la doctrina, para sí lograr determinar las características de la misma y su utilidad.

REFERENCIAS BIBLIOGRAFICAS

Doctrina

Abogacía Española Consejo General, & Díez, A. D. R. R. (2015, 29 julio). La actividad probatoria reforzada en las evidencias digitales. Recuperado de <https://www.abogacia.es/2015/06/29/la-actividad-probatoria-reforzada-en-las-evidencias-digitales/>

Adalid, & Echeverry, J. J. E. (2019) ¿Cómo lograr que una evidencia digital tenga validez jurídica? Recuperado de <https://www.adalid.com/evidencias-digitales-validez-juridica/>

Agudelo Giraldo O. A. (Ed.) (2018). La pregunta por el método: derecho y metodología de la investigación. Bogotá. Editorial Universidad Católica.

Amani Reveron, G. A. (2004). Aspectos generales de la firma electrónica en Venezuela. Revista nueva época: 10(23), 149-169

Carvajal, J. E. (2015). Derecho, seguridad y globalización. Bogotá, Colombia. Universidad Católica de Colombia.

Carnelutti, F. (1982) La prueba civil. Buenos Aires: Depalma

- Cano, J. J. C. (2015). *Computación Forense Descubriendo Los Rastros Informáticos* (2ª ed.). Bogotá, Colombia: Alfaomega
- Davara Rodríguez M. (2001). *Manual de derecho informático*. (3ª ed.). Pamplona, España: Arazandi
- Daza, A. (2016). *Reglas de producción de las pruebas y regla de exclusión en sede de casación penal*. Bogotá, Colombia: Universidad Católica de Colombia
- Delgado Martín, J. D. M. (2017). La prueba digital. Concepto, clases, aportación al proceso y valoración. Recuperado de <https://diariolaley.laley.es/home/DT0000245602/20170411/La-prueba-digital-Concepto-clases-y-aportacion-al-proceso>
- Echeverry, J. J. E. (2017). ¿Cómo lograr que una evidencia digital tenga validez jurídica? Recuperado, de <https://www.adalid.com/evidencias-digitales-validez-juridica/>
- Fiaschi F. (s.f). *Investigación tecnológica y prueba digital en todas las jurisdicciones*. Recuperado de https://www.academia.edu/35899985/Investigacion_tecnologica_y_prueba_digital_en_todas_las_jurisdicciones
- Flórez, G. D. F. (s.f.). La validez jurídica de los documentos electrónicos en Colombia a partir de su evolución legislativa y jurisprudencial. Recuperado de <http://www.lexbase.biz/revistauniversitaria/ulibre%20bogota/verba%20iuris%2031/1a%20validez.pdf>
- Flórez, G. D.F. (s.f.). Algunas nociones básicas sobre la evidencia digital en el contexto del

comercio electrónico, desde la perspectiva anglosajona y su visión en Colombia. Recuperado de https://repository.ucatolica.edu.co/bitstream/10983/18297/1/Evidencia-digital-distribucion-musical-y-derecho-de-consumo_Cap01.pdf

Giraldo, C. G. M., Escudero, C. E. M., Camacho, G. C. T., Duarte, M. D. H., & González, G. G. A. (2015). Derecho Probatorio. Bogotá, Colombia: Universidad Católica de Colombia

Grupo de Estudios en Internet, Comercio electrónico, Telecomunicaciones e Informática. (2011). *DERECHO & TIC 10.0*. Bogotá, Colombia: Temis S.A.

González Cuellar N. G. C. S. (2013). Garantías constitucionales de la persecución penal.

Recuperado de

https://www.academia.edu/35899985/Investigacion_tecnologica_y_prueba_digital_en_todas_las_jurisdicciones

Mateu De Ros, R. M. R., & Cendoya Méndez de Vigo, J. M. C. M. V. (2000). *Derecho de Internet Contratación Electrónica y Firma Digital*. E: Aranzandi.

Ministerio de Tecnologías de la Información y las Comunicaciones. (s.f.). Seguridad y Privación de la Información. Recuperado de https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

Morales, F. M. S. (s.f.). Validez de la prueba electrónica, un estudio sobre la firma digital y electrónica. Recuperado de <https://repository.ucatolica.edu.co/bitstream/10983/13779/4/VALIDEZ%20DE%20LA%20PRUEBA%20ELECTRONICA.pdf>

Mosquera, J. A. M. G., Certain, A. F. C. J., & Cano, J. J. C. (s.f.). Evidencia Digital: contexto, situación e implicaciones nacionales. Recuperado de <http://www.lexbase.biz/revistauniversitaria/uandes/dercnt/gecti%20n-1/evidencia%20digital%20cano.htm>

Peña Valenzuela, D. P. V. (2001). *Aspectos legales de Internet y del comercio electrónico*. Bogotá, Colombia: Dupre Editorial Ltda.

Picón Eugenio, Peritos Ingenieros Informáticos. (s.f.). La prueba electrónica. Su validez y eficacia procesal, Recuperado de <https://peritoinformatico.es/blog/prueba-electronica-validez-procesal/#Los-4-requisitos-para-asegurar-la-validez-probatoria-de-una-evidencia-digital>

Rincón Cárdenas, E. R. C. (2015). *Derecho del Comercio Electrónico y de Internet* (2ª ed.). Bogotá, Colombia: Legis S.A.

Ronderos, J. G. R., & Sanctions Officer. (2015). La prueba digital en el contexto jurídico actual. Recuperado de https://www.deceval.com.co/portal/page/portal/Home/Marco_Legal/Eventos/Presentacion_Deceval_JGRFINAL.pdf

Sentis Melendo, S & Liebman, E (1980). *Manual de derecho procesal civil*. Buenos Aires. Ed. Buenos Aires

Unicolombia. (s.f.). La Evidencia Digital o la prueba electrónica. Recuperado de <https://www.unicolombia.edu.co/2364-2/>

Universidad del Externado, & Contreras, A. F. C. (2015, 22 julio). Departamento de Derecho Informático. Recuperado de <https://derinformatico.uexternado.edu.co/evidencias-digitales-y-su-valor-probatorio/>

Sentencias

Corte Constitucional, Sala Plena (2000), Sentencia C-662. (MP: Fabio Morón Díaz)

Corte Constitucional, Sala Plena (2000) Sentencia C-562. (MP: Vladimiro Naranjo Mesa)

Normatividad

Código Procedimiento Penal (Código) Ley 906 de 2004. Legis.

Código General del Proceso (Código) Ley 1564 de 2012. Legis.

Constitución política de Colombia [Const.] (1991) Artículo 23 [Titulo II]. 2da Ed. Legis.

Constitución de España. España. Boletín Oficial del Estado, 29 de diciembre de 1987, número 311, pp. 6.

Ley 98 de 1993, por medio de la cual se dictan normas sobre democratización y fomento del libro colombiano. Bogotá: Congreso de Colombia.

Ley 270 de 1996, por el cual se dicta el estatuto de la Administración de Justicia. Bogotá: Congreso de Colombia.

Ley 527 de 1999, 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. Bogotá: Congreso de Colombia.

Ley 1564 de 2012, por la cual se expide el Código General del Proceso. Bogotá: Congreso de Colombia.

Ley 1437 de 2011, por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. Bogotá: Congreso de Colombia.

Ley 1/2000, de 7 de enero de 2000, de Enjuiciamiento Civil. Boletín Oficial del Estado, Referencia BOE-A-2000-323.