HACIA UN JUICIO EN LÍNEA EN LA JURISDICCIÓN DE LO CONTENCIOSO-ADMINISTRATIVO EN COLOMBIA

"Line to a trial in the administrative jurisdiction in Colombia"

Dra. Ana Yasmín Torres Torres*
Fecha de entrega: 03/16 /2013
Fecha de Aprobación: 05/ 23/2013

TORRES TORRES, Ana Yasmín (2013) Artículo: "HACIA UN JUICIO EN LÍNEA EN LA JURISDICCIÓN DE LO CONTENCIOSO ADMINISTRATIVO EN COLOMBIA", En Principia Iuris 19. Universidad Santo Tomás. Tunja

RESUMEN**

La evolución tecnológica que se requiere a nivel mundial, consiste en minimizar el uso del papel con miras en la desmaterialización del proceso y así obviar la impresión y uso de los documentos físicos, todo ello en procura de la adopción de los procesos electrónicos, mediante los cuales se busca salvaguardar la información y confiabilidad de los procesos así como también obtener información de manera práctica, tanto de los sujetos procesales y sus apoderados, como de los empleados y funcionarios de los despachos judiciales.

PALABRAS CLAVE

Documentos electrónico, equivalencia funcional, Neutralidad Tecnológica, Internet, Firma Digital, Firma Electrónica, notificaciones electrónicas, expediente electrónico, medios electrónicos, plan de justicia digital.

* Doctora en Derecho de la Universidad Carlos III de Madrid, Magistrada Auxiliar de la Presidencia del Consejo de Estado. AI/AE. Mail: anayasmint@hotmail.com

** Artículo de investigación el cual es una producción original e inédita, resultado del proyecto de investigación denominado "Hacia un juicio en linea en la jurisdiccion de lo Contencioso Administrativo en Colombia", que se adelanta en el Centro de Investigaciones de la Universidad Santo Tomás, Seccional Tunja, Facultad de Derecho, vinculado a la línea de investigación en Derecho Administrativo y Responsabilidad Estatal.

El método utilizado en este estudio es de carácter documental con base a los predicados de la ley, la doctrina existente y la respectiva jurisprudencia.

ABSTRACT

Technological evolution is required globally, is to minimize the use of paper towards the dematerialization of the process and thus obviate the use of printing and physical documentation, all in pursuit of the adoption of electronic processes mean you which seeks to safeguard the information and reliability of processes as well as practical information for both the parties to the proceedings and their agents, and employees and officers of the judicial offices.

KEYWORDS

Electronic documents, functional equivalence Technological Neutrality, Internet, Digital Signature, Digital Signature, electronic notifications, electronic record, electronic, digital justice plan.

METODOLOGÍA

Analítico Descriptivo de Orden Legal.

SUMARIO

1. Introducción. 2. Los medios electrónicos en la legislación colombiana. 2.1 Análisis normativo. 2.2 Principio de la equivalencia funcional. 2.3 Validez y valor probatorio de los documentos electrónicos. 2.4 Entidades de certificación. 2.5 Firmas electrónicas y firmas digitales. 3. Los nombres de dominio y su regulacion. 3.1 Definición. 3.2 Clasificación. 3.3 Registro. 4. El proceso contencioso-administrativo online. 4.1. Normatividad. 4.2 Herramientas tecnológicas requeridas. 4.3 Seguridad. 5. Conclusiones. 6. Referencias Bibliográficas.

1. INTRODUCCIÓN.

El uso de las nuevas tecnologías en la sociedad, ha traído como consecuencia que el legislador deba pronunciarse sobre estos avances a fin de crear un ambiente ágil y seguro dentro de los procesos judiciales que actualmente se presentan.

Por esta razón, dentro de la ley 1437 de 2011 (Código de Procedimiento Administrativo y de lo Contencioso-Administrativo) y la ley 1564 de 2012 (Código General del Proceso) se han incluido la utilización de los medios electrónicos en los procesos contenciosos.

Sin embargo a la fecha, esta jurisdicción no cuenta con una plataforma tecnológica adecuada que permita adelantar el proceso contencioso-administrativo online de manera ágil, eficiente y segura para los operadores judiciales, generando un atraso respecto de otros países.

Por lo anterior, se requiere adelantar las gestiones administrativas y técnicas necesarias para que con las herramientas que nos brinda la legislación actual y de acuerdo con el presupuesto con el que cuente la rama, la jurisdicción contenciosa Administrativa pueda

ofrecer un procedimiento administrativo online seguro confiable e inalterable, que contribuya al buen desarrollo de las finalidades de la rama judicial, consistentes en la observancia de la ley, con la satisfacción del deber cumplido por parte de los funcionarios y empleados judiciales y la tranquilidad del usuario y apoderados en la transparente resolución de un asunto de su interés y de otro lado disponer de un sistema que vaya a la par con los avances tecnológicos.

Ahora bien, la necesidad de acciones técnicas encaminadas a la sistematización del aparato jurisdiccional con el expediente electrónico, no es un capricho sino que obedece a un mandato legal previsto en Parágrafo del artículo 186 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, el cual contempla que un término que no supere los cinco años a partir de la vigencia de la norma dicha, deben concretarse las condiciones técnicas y tecnológicas, que a nuestro juicio, pone al sistema judicial Colombiano a la par de muchos países, que han dejado en la historia el sistema escritural.

En este contexto, es oportuno señalar que para lograr un juicio en línea, se requiere de una inmensa responsabilidad, tal vez mucha más de la que podemos imaginar, ya que pese a la creación constante de mecanismos de seguridad, la realidad cotidiana muestra nuevas formas de transgredir la privacidad y confiabilidad en el campo de la tecnología, por ello se hacen imperiosos los recursos técnicos, pero aún más los humanos para dinamizarla, de tal manera que sea implantada la tranquilidad y confianza de los usuarios, operadores judiciales y funcionarios en la administración de justicia, que va desde confianza en un sistema eficiente, como en la pronta resolución del asunto, con un desgaste mínimo tanto de las partes como del aparato jurisdiccional.

2. LOS MEDIOS ELECTRÓNICOS EN LA LEGISLACIÓN COLOMBIANA.

2.1 Análisis normativo.

Desde el año 1966 la Comisión de las Naciones Unidas para la Unificación del Derecho Mercantil Internacional (UNCITRAL)[1], delegó en grupos la redacción de convenciones y leyes, que posteriormente fueron adoptados dentro de las diferentes legislaciones, todo ello con el fin de propender por la armonización y unificación de la normatividad que rige la contratación internacional.

La UNCITRAL, luego de examinar las observaciones que realizaron los gobiernos y organizaciones interesadas en el asunto, presentaron el texto definitivo de la Ley Modelo de la CNUDMI sobre comercio electrónico, normatividad que fue aprobada en el 29º período de sesiones y cuya promulgación ayudó de manera significativa a todos los Estados para fortalecer la legislación y así reglamentar el uso de métodos de comunicación y almacenamiento de información, a fin de sustituir la utilización del papel.

1 La CDUNMDI/UNCITRAL es el principal órgano jurídico del sistema de las Naciones Unidas en el ámbito del derecho mercantil internacional. Órgano jurídico de composición universal, dedicado a la reforma de la legislación mercantil a nivel mundial durante más de 40 años. La función de la CNUDMI consiste en modernizar y armonizar las reglas del comercio internacional. www.uncitral.org.

Colombia, con base en la ley modelo de la UNCITRAL, fue el primer país de Latinoamérica en regular el comercio electrónico, lo hizo con la expedición de la ley 527 de 18 de agosto 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, se establecen las entidades de certificación y se dictan otras disposiciones[2].

Sin embargo, con anterioridad a la expedición de la ley 527 de 1999, la legislación ya se había pronunciado sobre la validez y utilización de los medios electrónicos en diferentes áreas del derecho, atendiendo como antes se ha afirmado, a la necesidad de aparejar la realidad judicial al avance de la tecnología y la exigencia de una justicia ágil y eficaz, por tanto vale la pena hacer referencia a las disposiciones anteriores y posteriores a la promulgación de la ley 527 de 1999 así:

- El decreto 2527 del 27 de julio de 1950[3] establece en el artículo 5º que la copia de un documento o de cualquier pieza de un archivo microfilmado tendrá el mismo valor probatorio que la ley le otorga al original así copiado, siempre que la microfilmación se haya hecho de acuerdo con las normas de este decreto.

- El decreto 1167 de 14 de mayo de 1980[4] estableció en el artículo 7º que los archivos del Registro Nacional de Valores e Intermediarios podrían conservarse por cualquier medio técnico adecuado que garantizara su reproducción exacta.

- El artículo 1° del decreto 1094 de 1996[5] define la factura electrónica como "el documento computacional que soporta una transacción de venta de bienes o prestación de servicios, transferido bajo un lenguaje estándar universal denominado Edifact de un computador a otro".

- La ley 270 del 7 de marzo de 1996[6] (Ley Estatutaria de la Administración de Justicia) en su artículo 95 se refiere al uso de la tecnología al servicio de la Justicia. Específicamente, la norma dispone que el Consejo Superior de la Judicatura debe propender a la incorporación de tecnología de avanzada al servicio de la administración de justicia, con miras a mejorar la práctica

2 Posteriormente, mediante decreto 1747 de 2000, se reglamentó la LCCE en lo relacionado con las entidades de certificación, los certificados y las firmas digitales. Así mismo se expidió la resolución 26930 de 2000, por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores.

3 Decreto 2527 de 27 de julio de 1950, "Por el cual se autoriza el procedimiento de microfilm en los archivos y se concede valor probatorio a las copias fotostáticas de los documentos microfilmados". Publicado en el Diario Oficial 28641 de 1950.

4 Decreto 1167 de 14 de mayo de 1980, "Por el cual se determinan las pautas conforme a las cuales se organizará el Registro Nacional de Valores e Intermediarios". Publicado en el Diario Oficial 35524 de 1980.

5 Decreto 1090 de 21 de junio de 1996, por medio del cual se reglamenta el artículo 616-1 del Estatuto Tributario. Publicado en el Diario Oficial 42814 de 1996.

6 Ley 270 de 7 de marzo de 1996, "Estatutaria de la Administración de Justicia". Publicado en el Diario Oficial 42745 de 1996.

de las pruebas, la formación, conservación y reproducción de los expedientes y la comunicación entre los despachos. Precisa la norma que los documentos emitidos por medios técnicos, electrónicos, informáticos y telemáticos, 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, por su parte, deben garantizar la identificación y el ejercicio de la función judicial por el órgano que la ejerce, y la confidencialidad, privacidad y seguridad de los datos de carácter personal que contengan, en los términos que establezca la ley.

- El decreto 1487 del 12 de agosto de 1999[7] autorizó el "Sistema de Declaración y Pago Electrónico" de la Dirección de Impuestos y Aduanas Nacionales (DIAN) y estableció algunos criterios operativos para presentar las declaraciones tributarias y pagar los impuestos por vía electrónica.

- Ley 527 del 18 de agosto de 1999[8], 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, se establecen las entidades de certificación y se dictan otras disposiciones.

- Decreto 1747 de 2000[9], reglamenta la ley 527 de 1999 en lo relacionado con las entidades de certificación, los certificados y las firmas digitales y Resolución 26930 de 2000[10], por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores.

- Ley 599 de 2000[11], por la cual se expide el Código Penal Colombiano, reconoce el bien jurídico del derecho de autor e incorpora conductas relacionadas indirectamente con el delito informático.

- Ley 633 de 2001[12] establece en el artículo 91 que todas las páginas

7 Decreto 1487 de 12 de agosto de 1999. Autorizó el "Sistema de Declaración y Pago Electrónico". Publicado en el Diario Oficial 43667 de 1999.

8 Ley 527 de 18 de agosto de 1999. "Por medio del cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico, y se establecen las entidades de certificación y se dictan otras disposiciones". Publicado en el Diario Oficial 43.673 de 1999.

9 Decreto 1747 de 2000 "Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales" Publicado en el Diario Oficial No. 44.160, de 2000.

10 Resolución 26930 de 2000 "Por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores". Superintendencia de Industria y Comercio, octubre 26 de 2000.

11 Ley 599 de 24 de julio de 2000 "por la cual se expide el Código Penal". Publicado en el Diario Oficial No. 44.097 de 2000.

12 Ley 633 de 29 de diciembre de 2001 "Por la cual se expiden normas en materia tributaria, se dictan disposiciones sobre el tratamiento a los fondos obligatorios para la vivienda de interés social y se introducen normas para fortalecer las finanzas de la Rama Judicial". Publicado en el Diario Oficial No. 44.275 de 2000.

Web y sitios de Internet de origen colombiano que operan en el Internet y cuya actividad económica sea de carácter comercial, financiero o de prestación de servicios, deberán inscribirse en el Registro Mercantil y suministrar a la Dirección de Impuestos y Aduanas Nacionales DIAN, la información de transacciones económicas que esta entidad requiera.

- Ley 962 de 2005[13] incorpora el principio de neutralidad tecnológica en el uso de la factura electrónica reglamentada a través del Decreto 1929 de 2007[14].

- Ley 1150 de 2007[15], crea el sistema Electrónico para la Contratación Pública (SECOP).

- Ley 1221 de 2008[16], regula la promoción del Teletrabajo como un instrumento de generación de empleo y autoempleo.

- Ley 1273 de 2009[17], tipifica diversos delitos informáticos y sanciona el hurto por estos medios.

- Ley 1341 de 2009[18], es el marco general del sector de las telecomunicaciones, en la cual se definen los principios y conceptos de la sociedad de la información como referente para la formulación de políticas.

- Ley 1480 de 2011[19], más conocida como el nuevo estatuto del consumidor, esta norma establece en varias de sus normas la protección al consumidor materia de comercio Electrónico.

- Ley 1437 de 2011[20], nuevo código administrativo y de lo contencioso Administrativo, esta norma en diversos artículos prevé la utilización de medios electrónicos en las etapas del proceso administrativo y contencioso-administrativo.

13 Ley 962 del 8 de julio de 2005. "Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos". Publicado en el Diario Oficial No. 46.023 de 2005.

14 Decreto 1929 del 29 de mayo de 2007. "Por medio del cual se modifica el artículo 616-1 del Estatuto Tributario". Publicado en el Diario Oficial No. 46.643 de 2007.

15 Ley 1150 del 16 de julio de 2007. "Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos". Publicado en el Diario Oficial 46.691 de 2007.

16 Ley 1221 del 16 de julio de 2008. "Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones". Publicado en el Diario Oficial No. 47.052 de 2008.

17 Ley 1273 del 5 de enero de 2009. "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Publicado en el Diario Oficial No. 47.223 de 2009.

18 Ley 1341 del 30 de julio de 2009. "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones". Publicado en el Diario Oficial No. 47.426 de 2009.

19 Ley 1480 del 12 de octubre de 2011. "Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones". Publicado en el Diario Oficial No. 48220 de 2011.

20 Ley 1437 del 18 de enero de 2011. "Por la cual se expide el código administrativo y de lo contencioso Administrativo". Publicada en el Diario Oficial No. 47.956 de 2011.

- Decreto 19 de 2012[21]. En este decreto se suprimen procedimientos y trámites innecesarios existentes en la Administración Pública. En lo que respecta a las entidades de certificación, modifica los artículos 29 y 30 de la ley 527 de 1999 y deroga los artículos 41 y 42 de la misma ley.

- Decreto 734 de 2012[22], mediante este decreto se reglamenta el Estatuto General de Contratación de la Administración Pública, así mismo regula en el capítulo II, la contratación pública electrónica con el objeto de reglamentar la sustanciación de las actuaciones, la expedición de los actos administrativos, los documentos, contratos y en general los actos derivados de la actividad precontractual y contractual provenientes de las modalidades de selección de licitación pública y selección abreviada de menor cuantía, en lo referente al trámite, notificación y publicación de tales actos por medio del Sistema Electrónico para la Contratación Pública, Secop Transaccional, etapa 1.

- Ley 1564 de 2012[23], mediante la cual fue creado el Nuevo Código General del Proceso. Esta norma regula en varios de sus apartes la utilización de medios electrónicos, de la firma electrónica y la firma digital entre otros.

- Decreto 2364 de 2012[24], reglamenta el uso de la firma electrónica definida en el artículo 7 de la ley 527 de 1999 y establece los requisitos para su utilización y validez. Aplica el principio de equivalencia funcional y neutralidad tecnológica.

Como podemos observar, en Colombia ya se ha regulado la utilización de los medios electrónicos en las diferentes áreas del Derecho y especialmente con la promulgación del nuevo Código Administrativo y de lo Contencioso-Administrativo así como también el nuevo Código General del Proceso se inicia una etapa de cambios positivos que propende por una justicia ágil y oportuna.

2.2 Principio de la equivalencia funcional.

El Principio de equivalencia funcional es considerado como la piedra angular del comercio electrónico; de él se derivan las disposiciones fundamentales que regulan esta nueva actividad mercantil.

21 Decreto 19 de 10 de enero de 2012. "Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública" Publicado en el Diario Oficial No. 48.308 de 2012.

22 Decreto 734 de 13 de abril de 2012, "Por el cual se reglamenta el Estatuto General de Contratación de la Administración Pública y se dictan otras disposiciones". Publicado en el diario oficial No. 48.400 de 2012.

23 Ley 1564 de 12 de julio de 2012. "Por la cual se expide el código general del proceso y se dictan otras disposiciones". Publicada en el Diario Oficial No. 14489 de 2012.

24 Decreto 2364 de 22 de noviembre de 2012 por medio del cual se reglamenta el artículo 7 de la ley 527 de 1999 sobre firma electrónica y se dictan otras disposiciones.

La doctrina[25] ha definido este principio como podemos observar a continuación:

> *"La función jurídica que en toda su extensión cumple la instrumentación escrita y autógrafa – o eventualmente su expresión oral - respecto de cualquier acto jurídico, la cumple igualmente su instrumentación electrónica a través de un mensaje de datos, con independencia del contenido, dimensión, alcance y finalidad del acto así instrumentado. La equivalencia funcional, en suma, implica aplicar a los mensajes de datos electrónicos una pauta de no discriminación respecto de las declaraciones de voluntad o ciencia manual, o gestualmente efectuadas por el mismo sujeto". Illescas, R. (2001).*

El denominado principio de equivalencia funcional supone un paso más concreto respecto del principio de no discriminación. Contiene una manifestación afirmativa de la producción efectiva de determinados efectos jurídicos de una información que consta en soporte electrónico. (Madrid, P. 1998)

Podemos decir entonces que en virtud de este principio no se debe discriminar a los mensajes de datos independientemente del soporte en el que se encuentren ya que las funciones que cumplen los documentos en papel, igualmente las pueden ofrecer las consignadas en medios electrónicos e incluso con una seguridad mayor a la brindan los medios tradicionales[26].

La legislación colombiana consagra el principio de la equivalencia funcional entre los documentos escritos y los documentos electrónicos, en el artículo 5º de la LCCE, a cuyo tenor literal se expresa que

> *"No se negará efecto jurídico, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos", entendiendo por 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)[27], Internet, el correo electrónico, el telegrama, el télex o el telefax"[28].*

25 Rico, M. (2007). Derecho de las Tecnologías. Buenos Aires: Ediciones la Roca. Pág. 274; Gutiérrez, M. (2002). Consideraciones sobre el tratamiento jurídico del comercio electrónico /En/ Internet, comercio electrónico y telecomunicaciones, Colombia. Legis. Pág. 187.

26 Al respecto, la LMCUCE, se basa en el reconocimiento de que los requisitos legales que prescriben el empleo de la documentación tradicional con soporte de papel constituye el principal obstáculo para el desarrollo de medios modernos de comunicación, así que en la preparación de esta ley se estudió la posibilidad de ampliar el alcance de conceptos como "escrito", "firma" y "original" con miras a dar entrada al empleo de técnicas basadas en la informática. (NACIONES UNIDAS, ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para la incorporación al derecho interno de 1996 con el nuevo artículo 5 bis aprobado en 1998, New York, 1999. p. 20.)

27 (Un amplio estudio relacionado con los aspectos técnicos del EDI y la mecánica operativa de la trasmisión electrónica de Documentos se puede encontrar en Barcelo, R. 2000)

28 COLOMBIA. Ley 527 de 1999, publicada en el Diario Oficial No. 43.673 del 21 de agosto de 1999, op, cit, Artículo 2º Núm. a).

El mensaje electrónico según este artículo, es un documento y participa de la naturaleza de los escritos, siempre y cuando se pueda materializar en papel escrito por los procedimientos técnicos adecuados (Moreno, M. 1999). La fórmula negativa del artículo antes trascrito, establece claramente el principio de la equivalencia funcional entre los documentos escritos de forma autógrafa y los mensajes de datos electrónicos, pues se trata de establecer no ya la equiparación absoluta entre el soporte material y el electrónico, habida cuenta de su diversa naturaleza, sino entre las funciones comerciales y jurídicas que uno y otro puedan desempeñar.

> Posteriormente, el artículo 6º de la misma ley nos dice que *"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"*[29].

Así pues, la ley no trata de consagrar un equivalente informático para todo tipo de documento emitido sobre papel, sino lo que pretende es, que una vez conocida la función que desempeñan los requisitos formales propios de la documentación tradicional, tratar de precisar cuáles de estos criterios permiten la atribución a este de un reconocimiento legal equivalente al de la documentación sobre papel (Martín Castro, M. P. 2000).

El único requisito que establece la ley, a fin de equiparar los mensajes de datos a la información que conste por escrito, es que esta información sea accesible para su posterior consulta, sin embargo no establece el término por el cual deba permanecer la información para efectos de dicha consulta.

De otra parte, los documentos electrónicos están en capacidad de brindar similares niveles de seguridad que el papel[30] y, en la mayoría de los casos, un mayor grado de confiabilidad y rapidez, especialmente con respecto a la identificación del origen y el contenido de los datos, siempre que se cumplan los requisitos técnicos y jurídicos plasmados en la ley.

El principio de la equivalencia funcional se ha expandido por todos los sectores negociales y hasta donde le ha sido permitido por la ley, actualmente es el principio más importante y desarrollado por todas las legislaciones que regulan el comercio electrónico.

2.3 Validez y valor probatorio de los documentos electrónicos

La ley 527 de 1999 estableció en su artículo 10 que:

29 COLOMBIA. Ley 527 de 1999, publicada en el Diario Oficial No. 43.673 del 21 de agosto de 1999, op., cit, Artículo 2º Núm. a).

30 Una vez promulgada la LCCE, la Corte Suprema de Justicia, se pronunció sobre las demandas presentadas vía fax estableciendo que "Nos encontramos ante un nuevo instrumento legal, que representa un avance jurídico, ágil y acorde con la modernidad, con el desarrollo tecnológico, que se ajusta a los conceptos procesales sobre cumplimiento de los términos y a las calidades intrínsecas de un documento. Así pues, se le ha dado plena validez a los mensajes de datos, afirmando que son documentos con la misma fuerza jurídica que cualquier otro, y deben ser considerados como medios de prueba, ya que cumplen los requisitos de los escritos en papel". Colombia, Corte Suprema de Justicia, Sala de Casación Laboral, Jurisprudencia No. 13015. (Magistrado Ponente José Roberto Herrera Vergara; Diciembre 3 de 1999.)

> *"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 solo hecho de que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original".*

Podemos decir entonces que de conformidad con la LCCE, los documentos electrónicos son admitidos como medios de prueba, sin ningún tipo de discriminación sobre su naturaleza y sobre el proceso en el que se presenten[31].

La LMCUCE no discriminó ningún campo especial del derecho, pues su finalidad es la de aplicar esta tecnología a todas las ramas del mismo. Efectivamente, la Corte Constitucional entendió dicho espíritu y en sentencia del 8 de junio de 1998, se refirió a la necesidad de actualizar el régimen normativo, para otorgar fundamento jurídico al intercambio electrónico de datos. Agrega la misma corporación que con la promulgación de nuevas normas, su propósito no es otro que actualizar la legislación nacional y ponerla a tono con las nuevas realidades de comunicación e interacción imperantes y para darle fundamento jurídico, no sólo a las transacciones comerciales sino también fuerza probatoria a los mensajes de datos. Más adelante resalta y taxativamente declara que el mensaje de datos como tal, debe recibir el mismo tratamiento de los documentos consignados en papel, es decir, debe dárseles la misma eficacia jurídica por cuanto el mensaje de datos comparte los mismos criterios de un documento.

La legislación colombiana se ha caracterizado por una excesiva reverencia a los formalismos. En ese sentido, múltiples normas determinan numerosas solemnidades que deben cumplirse con anterioridad a la celebración de diferentes actos y contratos, y el papel de las notarías es de gran importancia al momento de dar constancia de los actos jurídicos celebrados.

Sin embargo esta cultura jurídica, respecto de las nuevas tecnologías, está

31 En marzo de 2001, la Corte Constitucional debía pronunciarse si concedía o no una acción de tutela teniendo en cuenta los siguientes hechos: A un docente pensionado de la Universidad del Valle, no se le pagaba su pensión, o se le pagaba por partes, trayéndole dificultades para atender sus necesidades básicas, como alimentación, pago de servicios públicos, su manutención y la de su familia. El accionante solicitó que se le pagara la pensión, obligación asumida directamente por la Universidad y que se le previniera a ésta para pagar cumplidamente. El Juez Penal Municipal negó la tutela aduciendo que no se demostró que se afectara el mínimo vital del peticionario. El accionante envió facturas presentadas para probar la afectación del mínimo vital, por correo electrónico. Por ésta razón el juez observó el pago de altos costos por la utilización de internet, considerando como lujos y comodidades que se dan las personas que tienen dinero, al igual que por el hecho de tener una finca y DirecTV. En segunda instancia, el Juzgado Penal del Circuito confirmó la decisión, porque consideró que no afectó el núcleo esencial de la tercera edad. Respecto al tema de nuestro interés, la Corte aclaró que el uso del internet no ubica a las personas en alta situación económica. El internet, el uso del teléfono y otros medios, hacen parte del mejoramiento de la calidad de vida de las personas. Por lo expuesto anteriormente se revocó la sentencia de segunda instancia ya que sus razonamientos carecen de valor jurídico. Se concedió la tutela, se ordenó el pago completo de las mesadas y se previno para que no vuelva a incurrir en mora. COLOMBIA. Corte Constitucional. Tutela T- 410 de marzo 29 de 2001. M.P. Marco Gerardo Monroy Cabra.

cambiando gracias a la facilidad del acceso a los medios tecnológicos sin embargo aún no es muy usual que se presenten como medios de prueba los mensajes de datos ni los documentos en formato electrónico; no obstante, al ser una práctica ya casi generalizada, en muy poco tiempo deberán valorarse estos medios de prueba en los diferentes procesos judiciales.

Así mismo es importante resaltar que como se mencionó anteriormente, actualmente contamos con nuevas normas que otorgan validez y valor probatorio a los medios electrónicos como son entre otras la ley 1395 de 2010[32], Ley 1437 de 2011[33] y la ley 1564 de 2012.

En lo que respecta a la jurisprudencia, ya en los últimos años, aunque no son muchos los pronunciamientos de las Cortes sobre la validez del documento electrónico y el principio de la equivalencia funcional, vale resaltar los siguientes:

> a. En providencia proferida por el Consejo de Estado, Sala de lo Contencioso Administrativo, de fecha 23 de Julio de 2008, la Magistrada María Inés Ortiz Barbosa, al resolver un recurso consideró que las pruebas aportada por el actor, consistentes en fallos proferidos por la Organización Mundial del Comercio los cuales fueron consultados e impresos por el actor y autenticados posteriormente ante el Notario Sexto del Círculo de Bogotá, tienen plena validez y constituyen un medio probatorio que merece ser valorado de la misma forma que los contemplados en las normas del Código de Procedimiento Civil[34].

---

32 Ley 1395 de 2010, por la cual se adoptan medidas en materia de descongestión judicial, establece en su artículo Art. 432, que las audiencias se registrarán mediante un sistema de grabación electrónica o magnetofónica. Así mismo establece la implementación de la notificación por medios electrónicos, de acuerdo con la reglamentación que para el efecto expida el Consejo Superior de la Judicatura.

33 Esta norma otorga la posibilidad a los particulares de utilizar diferentes medios electrónicos para presentar peticiones a las autoridades, en lo que respecta a los procedimientos administrativos establece que estos pueden ser adelantados por medios electrónicos y crean mecanismos antes no contemplados en ninguna norma como lo son el documento público en medio electrónico, las notificaciones electrónicas dentro del procedimiento administrativo, El acto administrativo electrónico, el archivo electrónico de documentos, el expediente electrónico, la sede electrónica y las sesiones virtuales de comités, consejos y demás organismos colegiados quienes quedan facultados para votar y decidir en conferencia virtual. Esta ley es clara en establecer que será admisible la utilización de medios electrónicos para efectos probatorios, de conformidad con lo dispuesto en las normas que regulan la materia y en concordancia con las disposiciones de este Código y las del Código de Procedimiento Civil.

34 Considero igualmente el despacho que otros documentos tienen carácter reservado solo para los miembros de la OMC y para visualizarlos es necesaria una contraseña, en atención a ello se entiende que la documentación oficial publicada por vía electrónica no presenta alteración en su contenido, sin embargo, algunos documentos están incompletos. Por este caso se estima procedente tener como prueba los mensajes de datos que se aportaron impresos y que fueron descargados de la página oficial de la OMC, entidad reconocida a nivel internacional, circunstancia que ofrece similares niveles de seguridad, autenticidad e integridad a los que tendrían las copias auténticas de los fallos en los casos de Japón, Corea y Chile que se solicitaron por conducto del Ministerio de Relaciones Exteriores al Departamento Suizo de Justicia y Policía y que hasta la fecha no han sido allegadas al plenario. (Colombia, Consejo de Estado. Sala de lo Contencioso Administrativo, Sección Cuarta, Bogotá, D.C. Radicación Número: 19001-23-31-000-2001-04311-01 (14858). (Consejera Ponente María Inés Ortiz Barbosa; Veintitrés (23) de Julio de dos mil ocho (2008). Actor: Guinness Udv Colombia S.A. y Otros, Demandado: Departamento del Cauca).

b. La Corte Suprema de Justicia, Sala de Casación Civil, en sentencia de fecha 16 de diciembre de 2010, analiza como medio probatorio un disco compacto C.D, que contenía un mensaje de datos enviado desde la dirección electrónica del ex esposo de la demandante al correo electrónico del demandado, aunque el mensaje de datos fue allegado oportunamente, la primera instancia considero que "el correo electrónico al que hace referencia el cargo formulado, carece de autenticidad, amén de que no aparece fijada a él la firma digital de su autor; y por otro lado que el presunto autor del mensaje no reconoció haber sido quien lo envió. En la segunda instancia el magistrado ponente hace un análisis de lo que la doctrina y la ley han denominado como mensaje de datos así como también de las características que éste debe reunir y distingue entre firma electrónica y firma digital, concluyendo que como el tan aludido mensaje de datos no contaba con firma electrónica o digital no era posible dar validez al mismo. Y que además era deber de demandado haber demostrado por otros medios que el mensaje de datos provenía del ex esposo de la demandante.[35]

c. Auto proferido por el Consejo de Estado, de fecha 19 de mayo de 2011, con ponencia del Consejero Víctor Hernando Alvarado Ardila, quien al resolver recurso de súplica, estableció que los escritos memoriales que se envíen vía fax a los diferentes despachos judiciales, se entenderán recibidos el día en que fueron enviados aun cuando se hayan recibido por posterioridad a las 5:00 de la tarde, hora en que termina la atención al público[36].

2.4 Entidades de certificación.

Una autoridad de certificación, entidad certificadora, autoridad emisora, proveedor o prestador de servicios de certificación o simplemente certificador, es una entidad dedicada a la emisión de certificados que contienen información sobre algún hecho o circunstancia del sujeto del certificado, en el caso de los certificados de clave pública, certificados que vinculan un par de claves con una persona determinada de forma segura cubriendo así la necesidad de servicios de terceras partes de confianza en el comercio electrónico de los tenedores de pares de claves asimétricas[37].

35 Colombia, Corte Suprema de Justicia.Sala de Casación Civil, Ref.: Expediente No.11001 3110 005 2004 01074 01). (Magistrado Ponente Pedro Octavio Munar Cadena; dieciséis (16) de diciembre de dos mil diez (2010).

36 En el auto en mención se estableció: Así las cosas, el término que tenía para sustentar el recurso de apelación la parte demandada, inició a partir del 4 de junio de 2010 es decir vencía el 9 de junio de 2010, y aun cuando la secretaría puso sello de recibo de 10 de junio, lo cual en principio haría extemporánea la sustentación del recurso por la hora del recibo, de acuerdo con la tesis trascrita anteriormente, los escritos memoriales que se envíen vía fax a los diferentes despachos judiciales, se entenderán recibidos el día en que fueron enviados aun cuando se hayan recibido por posterioridad a las 5:00 de la tarde, hora en que termina la atención al público. La Sala concluye que la parte demandada sustentó el recurso de apelación dentro de su oportunidad, esto es el 9 de junio de 2010, no obstante el informe de secretaría indique haberlo recibido el 10 del mismo mes y año. Consejo de Estado, sección segunda, Auto de fecha 19 de mayo de 2011, radicación: 19001233100020020131202 (0609-2010)

37 Martínez Nadal Apolonia. Comercio Electrónico, firma digital y autoridades de certificación. Civitas 2001, p. 149.

La ley 527 de 1999 la define como aquella persona que una vez autorizada por la autoridad competente 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[38].

Si bien en un principio fueron creadas mediante la ley 527 de 1999[39], posteriormente el decreto 19 de 2012, les modificó su reglamentación, estableciendo que: *Podrán ser entidades de certificación, las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero y las cámaras de comercio, que cumplan con los requerimientos y sean acreditados por el Organismo Nacional de Acreditación conforme a la reglamentación expedida por el Gobierno Nacional. El Organismo Nacional de Acreditación de Colombia suspenderá o retirará la acreditación en cualquier tiempo, cuando se establezca que la entidad de certificación respectiva no está cumpliendo con la reglamentación emitida 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."

Así mismo establece el artículo 161 del Decreto 19 de 2012 que las entidades de certificación una vez acreditadas por el Organismo Nacional de Acreditación de Colombia para prestar sus servicios en el país, podrán realizar, entre otras, las siguientes actividades:

38 Ley 527 de 1999, artículo 2° numeral d.

39 Las entidades de certificación fueron posteriormente reglamentadas mediante el decreto Decreto 1747 de 2000, el cual las clasificó en entidades de certificación abiertas y cerradas definiéndolas así: Las entidades de certificación abiertas son aquellas que ofrecen servicios propios de las entidades de certificación. Su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor y recibe remuneración por los servicios prestados.

Entidad de certificación cerradas: son entidades que ofrece servicios propios de las entidades de certificación pero sólo para el intercambio de mensajes entre la entidad y el suscriptor, sin exigir remuneración por ello. Con base en esta reglamentación varias entidades como la Sociedad Cameral de Certificación Digital Certicámara, S.A., Gestión de Seguridad Electrónica S.A. y Andes Servicio de Certificación Digital S. A., optaron por la creación de entidades de certificación abiertas, mientras que entidades como el Banco de la República, Dirección de Impuestos y Aduanas Nacionales – DIAN y Ecopetrol, crearon entidades de certificación cerradas.

1. *Emitir certificados en relación con las firmas electrónicas o 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 y de documentos electrónicos transferibles.*
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 Ley 527 de 1999.*
4. *Ofrecer o facilitar los servicios de generación de los datos de creación de las 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 o facilitar los servicios de generación de datos de creación de las firmas electrónicas.*
7. *Ofrecer los servicios de registro, custodia y anotación de los documentos electrónicos transferibles.*
8. *Ofrecer los servicios de archivo y conservación de mensajes de datos y documentos electrónicos transferibles.*
9. *Cualquier otra actividad relacionada con la creación, uso o utilización de firmas digitales y electrónicas".*

Estas entidades de certificación deben pagar los costos para su correspondiente acreditación y son auditadas por el ONAC, pueden dejar de ejercer sus actividades siempre y cuando garanticen la continuidad del servicio a quienes ya lo hayan contratado, directamente o a través de terceros, sin costos adicionales a los servicios ya cancelados.

2.5 Firmas electrónicas y firmas digitales.

La firma electrónica[40] es definida como un *"método o símbolo basado en medios electrónicos utilizado o adaptado por una parte con la intención de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita"*[41].

MARTÍNEZ NADAL[42] considera que en este concepto amplio y tecnológicamente indefinido tendrían cabida técnicas tan simples como un nombre u otro elemento identificativo incluido al final de un mensaje electrónico, y de tan escasa seguridad que

40 En su 29º período de sesiones (1996), la CNUDMI decidió incluir en su programa los asuntos relacionados con las firmas numéricas y las entidades certificadoras. Así que se pidió al grupo de trabajo sobre comercio electrónico (C-E) que examinara la conveniencia y viabilidad de preparar un régimen uniforme sobre temas como los son la base jurídica que sustenta los procesos de certificación, incluida la tecnología incipiente de autenticación y certificación numéricas; la aplicabilidad del proceso de certificación; la asignación del riesgo y la responsabilidad de los usuarios, prestadores y terceros en el contexto del uso de técnicas de certificación; las cuestiones concretas de certificación mediante el uso de registros y la incorporación por remisión. El 5 de julio de 2.001, durante su 34º período de sesiones realizado en la ciudad de Viena (Austria), fue aprobado el texto de la ley Modelo de la CNUDMI sobre firmas electrónicas, en adelante LMCUFE y la guía para su incorporación al derecho interno de cada estado.

41 IRIARTE AHON Erick, "Firma digital y certificado digital. El proyecto peruano", Revista electrónica de derecho informático, septiembre de 1999. http://publicaciones.derecho.org/redi/No._14_-_septiembre_de_1999/9.

42 MARTÍNEZ NADAL, Apol-lònia, Firma electrónica, certificados y Entidades de Certificación, op. cit. p. 41.

plantea la cuestión de su valor probatorio a efectos de su autenticación, aparte de su nula aportación respecto de la integridad del mensaje. Tan es así, que podría dudarse de su condición de firma, por su nula o escasa utilidad.

Mediante la firma electrónica se permite al receptor de unos datos transmitidos por medios electrónicos (documento electrónico) verificar su origen (autenticación) y comprobar que están completos y no han sufrido alteración (integridad). Es decir, se acredita la autoría (genuidad) y la integridad del contenido (autenticidad) del documento electrónico[43].

La Ley 527 de 1999 nos dice que la firma electrónica constituye una serie de datos electrónicos que se adhieren al mensaje de datos para corroborar quién envió el mensaje y a su vez quién lo recibió[44]. El artículo 7 de la ley 527 de 1999 fue reglamentado por el decreto 2364 de 2012, el cual establece que la firma electrónica comprende cualquier tipo de tecnología como lo son códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permitan 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.

La pieza clave de la regulación de las firmas electrónicas es la determinación de sus efectos jurídicos, que repercuten no sólo sobre la información por medios electrónicos de negocio jurídico sino, entre otros, sobre la documentación electrónica de actos y declaraciones de voluntad en general, proyectándose sobre sectores muy diversos del ordenamiento jurídico (Administrativo, Procesal, Civil, etc.). Tiende a imponerse la atribución a la firma electrónica para los datos consignados electrónicamente, del mismo valor jurídico que tiene la firma manuscrita para los datos firmados en papel, al tiempo que, con carácter general, se proclama que el mero hecho de que una firma se presente en forma electrónica, no debe ser determinante para que se le nieguen efectos jurídicos. La equiparación de efectos con la firma manuscrita encuentra su fundamento en que la firma electrónica es susceptible de ser (como mínimo) tan fiable y precisa como la tradicional firma manuscrita, por lo que su plena eficacia aparece subordinada al cumplimiento de ciertos requisitos de seguridad[45].

---

43 MORENO NAVARRETE, Miguel Ángel, Contratos Electrónicos, op. cit p.105.

44 El artículo 7º de la Ley 527 de 1999 establece: 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.

45 DE MIGUEL ASENSIO, Pedro A., Derecho Privado de Internet, Madrid: Civitas, 2000, p. 341.

En la medida que la firma electrónica se configura como instrumento que permite satisfacer tales exigencias, al aparecer como equivalente funcional de la firma manuscrita, puede contribuir a superar plenamente para las transacciones en internet las dificultades inherentes a la ausencia en ese contexto de la firma manuscrita, cumpliendo las funciones básicas de ésta en el ámbito contractual, que son construir un signo de identificación personal y representar la voluntad de obligarse[46].

En tal sentido, la firma electrónica que reúna los requisitos del artículo 7º de la Ley 527 de 1999, reglamentado por el Decreto 2364 de 2012, surte los mismos efectos jurídicos que la firma manuscrita en papel[47].

Así las cosas, podemos decir que todas aquellas firmas que se encuentren en formato electrónico y que sean útiles para autenticar el documento, se pueden considerar como firma electrónica. Esta firme incluye cualquier tipo de tecnología desde las más simples como son los códigos y contraseñas hasta las más avanzadas como son los métodos biométricos[48], sin discriminar ningún tipo de tecnología.

Firma Digital

Las firmas digitales son tecnológicamente específicas, pues se crean utilizando un

46 Vid. CAVANILLAS MÚGICA, Santiago, Introducción al tratamiento jurídico de la contratación por medios electrónicos (EDI). En: Actualidad Informática Aranzadi, No. 10, 1994, p. 3.

47 MADRID PARRA, Agustín, Adecuación de la regulación del Comercio Electrónico en la realidad práctica. En Derecho del Comercio Electrónico, Madrid, La ley. 2001. p. 213. Vid. MATEUS DE ROS, Rafael; CENDOYA MÉNDEZ DE VIGO Juan Manuel. Derecho de Internet, contratación electrónica y firma digital. Madrid: Aranzadi 2000.

48 Los métodos biométricos son aquellos métodos de identificación que se basan en medir las particularidades biológicas de una persona, para establecer su identidad. A título ejemplificativo, la información biométrica puede consistir en la estructura vascular de la retina, la estructura visible del iris, la composición espectral de la voz, la imagen facial o la dinámica de posición, velocidad y presión de generación de una firma manuscrita. La información biométrica es única pero no es secreta: cualquier persona puede grabar la voz de otro, u obtener las huellas digitales de otra persona de, por ejemplo, un vaso. Por ello los métodos biométricos pueden utilizarse para la identificación de una persona para autorizar su acceso a una instalación física o su ingreso a un sistema informático propietario (como ser un sistema para transferir fondos electrónicamente entre un banco y otro) pero por sí solos no son utilizables para firmar digitalmente pues no conllevan un secreto no compartido. Por ello los mecanismos de firma que los utilizan en forma exclusiva crean firmas digitales que podrían ser desconocidas por el firmante. Sin embargo, los métodos biométricos pueden utilizarse en conjunto con la criptografía de clave pública para crear firmas digitales. Normalmente la clave privada del firmante se guarda en un archivo en disco o en una tarjeta inteligente con microchip ("smartcard"). La clave privada debe almacenarse, pues es binaria y de considerable longitud, por lo cual no puede ser memorizada por su titular. Por ello y a fin de impedir su utilización por un tercero, la clave privada se protege encriptándola con criptografía simétrica basada en una clave nemotécnica de acceso suministrada por el titular de la clave privada y sólo conocida por él. Es factible utilizar métodos biométricos para asistir en la protección de dicha clave privada, es decir para activar la clave privada para la creación de una firma por su titular. Adicionalmente los métodos biométricos tienen el beneficio de que, al requerir la presencia física del titular de una clave privada para activarla, impiden que una persona divulgue su frase de acceso y por ello su clave privada a un tercero conocido y confiable (por ejemplo, a su secretaria) a fin de que el tercero impersone al titular cuando éste está ausente, por ejemplo de vacaciones, para que firme en su lugar". Informe de la Comisión Redactora del Anteproyecto de Ley de Firma Digital Argentino. http://www.ulpiano.com/FD_Informe.htm Página consultada el día 4 de julio de 2.006.

sistema específico de criptografía[49]. Este sistema de criptografía asimétrica permite: a) *Confidencialidad*, es decir, enviar mensajes secretos a través de canales inseguros, como internet, sin necesidad de comunicación previa de una clave secreta compartida: el emisor de un mensaje cifra los datos utilizando la clave pública del receptor que es accesible para cualquiera, y estos datos sólo pueden ser descifrados por el receptor con su propia clave privada.

De esta forma, utilizando la clave pública del destinatario, de conocimiento público, el remitente puede estar seguro de que sólo el destinatario, el tenedor de la clave privada correspondiente, puede descifrar el mensaje, obteniéndose así confidencialidad. Ello tiene la ventaja de que personas que no se conocen previamente pueden intercambiar mensajes cifrados, sin que exista la necesidad de un intercambio seguro de claves secretas compartidas, pues, simplemente, se elimina la necesidad de intercambiarlas.

Y, precisamente, esta confidencialidad que la criptografía puede proporcionar ha planteado, y sigue planteando problemas, pues entra en conflicto con el interés público de poder intervenir determinadas comunicaciones en determinadas situaciones, posibilidad que no existiría, en principio, si no se tuviera acceso a la clave privada. De ahí las restricciones comerciales a la venta y exportación de productos criptográficos y las diversas iniciativas existentes en distintos países tendientes a conseguir que las autoridades públicas puedan intervenir también comunicaciones electrónicas cifradas, iniciativas basadas en la exigencia de depósito de las claves privadas, o en la disminución de la calidad de las claves comercializadas, de forma que a partir de la clave pública pueda obtenerse, de ser necesario, la correspondiente clave privada[50].

b) Realizar firmas digitales, que proporcionan autenticidad, integridad y no rechazo de origen, y que puedan resultar

49 La palabra criptografía proviene del griego kryptos, que significa esconder y gráphein, escribir, es decir, escritura escondida. Es la ciencia que se ocupa de transformar mensajes en forma aparentemente ininteligibles y devolverlos a su forma original. La criptografía ha sido usada a través de los años para mandar mensajes confidenciales cuyo propósito es que sólo las personas autorizadas puedan entender el mensaje. Desde sus inicios, la criptografía llegó a ser una herramienta muy usada en el ambiente Militar. En la Segunda Guerra Mundial tuvo un papel determinante ENIGMA, una máquina de cifrado que tuvo gran popularidad. Al terminar la guerra, las agencias de seguridad de las grandes potencias invirtieron muchos recursos para su investigación. La criptografía, como la conocemos hoy, surgió con la invención de la computadora. La criptografía actual se inicia en la segunda mitad de la década de los años 70. No es hasta la invención del sistema conocido como DES (Data Encryption Standard) en 1976, que se dio a conocer más ampliamente, principalmente en el mundo industrial y comercial. Posteriormente con el sistema RSA (Rivest, Shamir y Adleman) en 1978, se abre el comienzo de la criptografía en un gran rango de aplicaciones: en transmisiones militares, en transacciones financieras, en comunicación de satélite, en redes de computadoras, en líneas telefónicas, en transmisiones de televisión, etcétera.

50 "La mayor ventaja de la criptografía asimétrica es que se puede cifrar con una clave y descifrar con la otra, pero este sistema tiene bastantes desventajas: a) Para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso. b) Las claves deben ser de mayor tamaño que las simétricas. c) El mensaje cifrado ocupa más espacio que el original". http://es.wikipedia.org. Página consultada el día 29 de enero de 2007.

tanto o más útiles, válidas y eficaces en el comercio y en los procedimientos legales como la firma escrita sobre papel. En este caso, la clave privada se utiliza para crear una firma digital y una clave pública para verificar la firma digital.

La criptografía asimétrica utiliza dos claves complementarias llamadas clave privada y clave pública. Lo que está codificado con una clave privada necesita su correspondiente clave pública para ser descodificado y viceversa; lo codificado con una clave pública sólo puede ser descodificado con su clave privada.

La criptografía asimétrica está basada en la utilización de números primos muy grandes. Si multiplicamos entre sí dos números primos muy grandes, el resultado obtenido no puede descomponerse eficazmente, es decir, utilizando los métodos aritméticos más avanzados en los ordenadores más avanzados, sería necesario utilizar durante miles de millones de años tantos ordenadores como átomos existen en el universo. El proceso será más seguro cuanto mayor sea el tamaño de los números primos utilizados. Los protocolos modernos de encriptación, tales como SET y PGP, utilizan claves generadas con números primos de un tamaño tal, que los hace completamente inexpugnables.

Cuando el texto a cifrar es bastante extenso, se hace necesario el empleo de las funciones hash, las cuales son una herramienta fundamental en la criptografía, usadas principalmente para resolver el problema de la integridad de los mensajes, así como la autenticidad de mensajes y de su origen.

Por ello, las firmas basadas en la criptografía de clave pública son consideradas seguras, por cuanto permiten satisfacer, en principio, las exigencias de autoría e integridad necesarias para que el mensaje y su firma electrónica sean vinculantes para el firmante y exigibles ante los tribunales, e incluso es posible que determinados criptosistemas de clave pública utilizados con función de firma digital puedan ser, si así se desea, para obtener confidencialidad[51].

En la legislación colombiana, el artículo 2º, literal c) de la LCCE, nos la define 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"*.

Posteriormente, en su artículo 28, establece claramente el principio de la equivalencia funcional entre la firma digital y la firma manuscrita, siempre y cuando la firma digital incorpore determinados atributos:

a) Que sea única a la persona que la usa: dicha firma debe corresponder de manera exclusiva a una sola persona (que puede ser natural o jurídica), de acuerdo con la propuesta de C-E sobre firmas digitales, entidades de certificación y certificados digitales, de nuestro país, para cumplir con este requisito debe a su vez tener las siguientes características: *"1. La clave privada sólo puede ser conocida por el firmante; 2. La firma digital es creada mediante la aplicación de una función*

51 Ibidem.

unidireccional creando un compendio digital, para luego cifrarlo con su llave privada; y 3. Si el tiempo para deducir la clave privada a partir de la clave pública es superior al intervalo de tiempo (sic) entre la fecha de creación de las claves y la fecha de expiración del documento firmado".

b) Ser susceptible de verificación: implica la posibilidad mediante medios digitales, de verificar la identidad del autor y de los datos.

c) Estar bajo el control exclusivo de la persona que la usa: es decir, la persona que adquiere una firma digital debe contar con el pleno control del manejo de la llave privada y si decide dársela a otra, será responsabilidad única de este sujeto. En el caso de las personas jurídicas, el representante legal o quien haga sus veces, será el encargado de manejar la clave.

d) Que esté ligada a la información o mensaje, de tal manera que si estos son cambiados, la firma digital es invalidada: el mensaje y la firma como se envían en un mismo carácter, si es alterado el contenido, cambia la configuración, impidiendo que la firma se desactualice.

La firma digital cumple así los requisitos establecidos para reemplazar la firma manuscrita, inclusive puede llegar a ser más segura, debido a que no sólo da certeza sobre el originador, sino que garantiza la integridad del mensaje, mediante la utilización de una clave privada manejada por el emisor y una clave pública que verifica el envío del mensaje, la integridad del mismo y a su autor, por parte del receptor.

La firma digital consigue iguales, si no superiores, efectos que la firma manuscrita, pues da integridad, autenticidad y, en definitiva, no rechazo de origen. En este sentido, desde sus inicios las diversas iniciativas legislativas existentes sobre firma digital realizan un reconocimiento de los efectos de la misma, equiparándola, con más o menos exigencias, a la firma manuscrita y estableciendo determinadas presunciones o reglas de atribución a su favor. La firma digital es el instrumento que permitirá, entre otras cosas, determinar de forma fiable si las partes que intervienen en una transacción, son las que dicen ser, y si el contenido del contrato ha sido alterado o no posteriormente[52].

52 RIVAS ALEJANDRO, Javier, Aspectos Jurídicos del Comercio Electrónico en internet. Pamplona: Aranzadi, 1999, p. 93.

Así como también nuevos conceptos jurídicos como los certificados, firma electrónica[53] y firma digital[54], de igual manera señala la competencia para la vigilancia y control de estas entidades en cabeza de la Superintendencia de Industria y Comercio.

3. LOS NOMBRES DE DOMINIO Y SU REGULACIÓN.

3.1 Definición.

Los nombres de dominio, son utilizados, para poder acceder y estar en contacto con todas las páginas Web, así como para poder reconocer e individualizar cada máquina que esté en conexión. Dicho sistema se compone en direcciones univocas para transferir los datos en Internet, mediante dominios que son el nombre nemotécnico que se asigna a un DSN y se utiliza en las direcciones de correo electrónico y como medio de localización de una Web en Internet, los nombres de dominio son en sí las direcciones con las que establecemos contacto para acceder al contenido de las páginas a las que pertenece dicha dirección, como por ejemplo www.ramajudicial.gov.co.

Funcionan mediante un número asignado por el sistema básico de intercomunicación en la red, denominado Internet protocolo IP; estos números buscando satisfacer las necesidades de los navegantes y su incursión fácil a la red, se suplieron con códigos expresados en palabras, las cuales desplazaron los números de los códigos I.P, permitiendo una mayor identificación de las direcciones, pues con estas asignaciones los navegantes de Internet recuerdan las palabras para establecer conexión con cualquier dirección de la Red.

Es claro entonces que la función del DNS o sistemas de Nombres de Dominio, es la de permitir un fácil acceso a Internet, ya que la relación de los nombres con una marca o con una frase conocida, hace fácil la entrada a dicho sitio.

---

53 La firma electrónica es definida como un método o símbolo basado en medios electrónicos utilizado o adaptado por una parte con la intención de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita. se trata de un concepto amplio de firma, que podría ser predicable de cualquier método o signo que permita la identificación de una persona, aún fuera del ámbito de la electrónica, incluye desde el uso de tecnologías simples como la firma escaneada, hasta tecnologías avanzadas como los métodos biométricos definidos como aquellos métodos de identificación que se basan en medir las particularidades biológicas de una persona, para establecer su identidad, así mismo se pueden utilizar tecnologías como código de barras, tabletas de firma electrónicas, etc. Vid. MARTÍNEZ NADAL, Apol-lònia, Firma electrónica, certificados y Entidades de Certificación, op. cit. p. 41; ILLESCAS ORTIZ, Rafael, Derecho de la contratación electrónica, op. cit. p. 78; MORENO NAVARRETE, Miguel Ángel, Contratos Electrónicos. Madrid, Marcial Pons, 1999, p.105.

54 Las firmas digitales se definen 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. Esta firma es tecnológicamente específicas, pues se crean utilizando un sistema específico de criptografía asimétrica Vid. RIVAS ALEJANDRO, Javier, Aspectos Jurídicos del Comercio Electrónico en internet. Pamplona: Aranzadi, 1999, p. 93; IRIARTE AHON, ERICK: "Firma digital y certificado digital, el proyecto peruano", en Revista Electrónica de Derecho Informático, septiembre de 1999 (http://publicaciones.derecho.org/redi/No._14). En algunos países se denominan firma electrónica avanzada, es el caso de Chile, España, México entre otros.

En principio fueron equiparables a una dirección postal o a un número de teléfono[55], actualmente la doctrina[56] y la jurisprudencia europea mayoritaria reconocen la posibilidad de que los nombres de dominio alcancen un carácter distintivo susceptible de protección jurídica[57].

3.2 Clasificación.

El sistema de los nombres de dominio está compuesto por diferentes niveles, los cuales corresponden a palabras que en orden jerárquico, permiten realizar su clasificación. Comienza por la designación con las letras "http" correspondientes al protocolo de transferencia de máximo texto, utilizando para comunicar entre si, a todos los equipos conectados a la red, luego la www o Word Wide Web que significa el código de la red en Internet.

Estas dos denominaciones son las iniciales de un nombre de dominio, las cuales dan apertura a las palabras claves para la identificación de dicha dirección que como lo mencionamos anteriormente, corresponde a números I.P trasladados a letras. Posteriormente se continúa con los dominios de segundo y primer nivel como podemos ver a continuación:

3.2.1 Dominios de segundo nivel (sld).

Esta clase de dominios corresponden a la palabra clave de la dirección, pues es la que identifica un Web side de todos los demás. En el comercio se utilizan generalmente los nombres comerciales de un establecimiento de comercio, o las marcas de un producto, las cuales al ser recordados por los usuarios permiten la búsqueda rápida de una página. También se utiliza en nombre de algún elemento que identifique la página o el nombre de la organización localizada en Internet. Quien escoge el segundo nivel, es el mismo dueño del dominio, quien debe tener precaución al momento de registrarlo, ya que puede tener problemas jurídicos si se llega a tratar de una palabra protegida por la propiedad intelectual. Por otra parte, es importante escoger un dominio apropiado para el sitio o negocio que se pretende instalar en la Web, pues de lo llamativo que sea el nombre, dependerán en parte las visitas realizadas.

3.2.2 Nombres de dominio de primer nivel (tld).

Los dominios de primer nivel o nivel superior conocidos como TLD son aquellos que se encuentran localizados al final de la dirección hasta el último punto, son

55 En Alemania se puede observar el caso Kerpen, Hürth y Pulheim del Landgericht de Köln, en sentencia de fecha 17 de diciembre de 2006. www.netlaw.de/urteile/lgk_2:htm.

56 Para CARBAJO CASCON, el nombre de dominio no es a priori más que un expediente técnico mnemotécnico dentro de un sistema o medio de comunicación telemático como lo es el Internet; una dirección alfanumérica que hace posible la comunicación fluida de la información entre los distintos equipos informáticos de todo el mundo conectados a la red por un mismo protocolo de comunicación. Sin embargo dadas las características especiales del nombre de dominio a su función esencialmente técnica (localización de equipos informáticos por los humanos de manera rápida y fácil) se haya superpuesto otra función complementaria de carácter identificador y distintivo. CARBAJO CASCON, F. Conflictos entre signos distintivos y nombres de dominio en Internet. Navarra. Aranzadi. 2002, p. 69.

57 Una de las primeras decisiones judiciales al respecto fue el memorándum y la orden del Distrito de New York, de 28 de octubre de 1994, dictados en el caso MTV Networks V. Curry, Alemania, BGH, sentencia 18.12.1985, y sentencia de Hanseastischen Oberlandesgericht Hamburg de 16 de septiembre de 1982. En Italia, la ordinanza del Tribunale di Napoli No. 3992 de 24 de marzo de 1999, entre otros.

importantes porque identifican donde se encuentra registrado el dominio. Estos niveles están divididos en otros que individualizan el dominio dependiendo de los niveles que tenga. Dicha división está organizada de la siguiente forma:

3.2.2.1 Dominios genéricos:

Buscan identificar a la compañía o institución, dependiendo del área o actividad a que se dedica o de acuerdo a la clase de servicios que distribuye en la World Wide Web. Las siglas o abreviaturas genéricas existentes actualmente para identificar las actividades específicas en la red son entre otros:

- .**aero** Industria del transporte a reo
- .**com** Fines comerciales
- .**museum** Museos
- .**net** Infraestructura de red
- .**org** Organizaciones
- .**gov** Gobiernos y Entidades Públicas (En inglés)
- .**gob** Gobiernos y Entidades Públicas (En español)
- .**edu** Educación
- .**mil** Organizaciones militares (Ejército, Armada, Fuerza Aérea)

3.2.2.2 Dominios territoriales.

Son los específicos para cada país[58], amplían la posibilidad de registro de nombres de dominio, y básicamente lo que hacen es facilitar la ubicación de las páginas en Internet cuando los operadores tengan presencia física y sean reconocidos en ese territorio, además permiten que empresas con presencia en diferentes territorios tengan páginas de Internet en cada uno de ellos.

Por razones exclusivamente técnicas, solo es posible registrar un mismo SDL en cada TDL, sea genérico o territorial, abierto o restringido. La justificación es evidente: conocido el carácter universal del medio, cada equipo informático conectado a Internet ha de tener una dirección única e inequívoca para todo el mundo, a fin de poder ser localizado y conectado desde cualquier punto de la red independientemente del lugar geográfico desde el que tenga lugar la conexión.

3.3 Administración y registro.

Con el crecimiento de Internet y su consecuente internacionalización,

58 Entre otros podemos mencionar: .ar: Argentina, .be: Bélgica, .bf: Burkina Faso, .bg: Bulgaria, .bh: Bahrain, .bi: Burundi, .bj: Benin, .bm: Bermuda, .bn: Brunei Darussalam, .bo: Bolivia, .br: Brasil, .ch: Suiza, .de: Alemania, .dk: Dinamarca, .dm: Dominica, .do: República Dominicana, .dz: Argelia, .ec: Ecuador, .ee: Estonia, .eg: Egipto, .es: España, .gp: Guadalupe, .gq: Guinea Ecuatorial, .kr: República de Corea, .lt: Lithuania, .lu: Luxemburgo, .gl: Latvia, .ly: Líbia, .ma: Marruecos, .mc: Mônaco, .md: República de Moldova, .mg: Madagascar, .mh: Islas Marshall, .mk: Macedônia, .ml: Mali, .mm: Myanmar, .mn: Mongólia, .mo: Macau, .mp: Islas Mariana del Norte, .mq: Martinique, .mr: Mauritânia, .ms: Monserrat, .mt: Malta, .mu: Mauritânia, .mv: Maldivas, .mw: Malawi, .mx: México, .my: Malásia, .mz: Mozambique, .ni: Nicarágua, .gi: Holanda, .no: Noruega, .np: Nepal, .nr: Nauru, .nu: Niue, .nz: Nueva Zelanda, .pa: Panamá, .pe: Perú, .pr: Puerto Rico, .se: Suecia, .to: Tonga, .tp: Timor Oriental, .tr: Turquía, .tt: Trinidad y Tobago, .tv: Tuvalu, .tw: Taiwan, .tz: Tanzania, .ua: Ukrania, .ug: Uganda, .uk: Reino Unido, .um: Islas US Minor Outlying .us: Estados Unidos, .uy: Uruguay, .uz: Uzbekistán, .va: Ciudad del Vaticano, .vc: San Vicente y Las Grandinas, .ve: Venezuela, .vg: Islas Virgen, .vi: Islas Virginia, .vn: Vietnam, .vu: Vanuatu, .wf: Islas Wallis y Futuna, .ws: Samoa Occidental, .ye: Yemen, .yt: Mayotte, .yu: Yugoslavia, .za: Sudáfrica.

el gobierno Norteamericano desde un principio estuvo encargado de la administración del sistema de nombres de dominio[59]. Posteriormente y por la presión de otros gobiernos que plantearon que no había justificación alguna para que la IANA (Internet Asisigned Numbers Authority) tuviera el control de una parte tan importante del Internet como es el sistema de nombres de dominio, acepto la necesidad de delegar esta función en un ente de carácter privado. El resultado fue la formación de ICANN (Internet Corporation for asisigned Names and Numbers) en octubre de 1998, con el fin de que asumiera la responsabilidad del manejo del Internet en términos técnicos y con el objetivo que asignara los nombres de dominio y los números I.P.

La Corporation for Assigned Names and Numbers (ICANN), es una entidad sin ánimo de lucro constituida conforme a la Nonprofit Public Benefit Corporation Law de California (EE.UU.), cuyo objeto es administrar el espacio de direcciones IP y el sistema de nombres de dominio. En Colombia, el 24 de diciembre de 1991 la IANA delegó a la Universidad de Los Andes la administración del servicio de registro de nombres de dominio bajo la denominación .co y posteriormente la ICANN, en 1998, reiteró dicha delegación.

Sin embargo, el Ministerio de Comunicaciones solicitó un concepto al Consejo de Estado en relación con el carácter público o privado del dominio .co y la competencia del Estado Colombiano para regularlo. Al respecto el Consejo de Estado con ponencia del Doctor CÉSAR HOYOS SALAZAR, conceptuó que el dominio .co, aunque sea administrado por una entidad privada, como lo es la Universidad de Los Andes, tiene un notorio interés público[60].

A raíz de este concepto, se expidió la ley 1065 de 2006, la cual en su artículo 1º establecía que *"La administración del registro de*

59 Cuando Internet era patrocinada por el Departamento de Defensa de los Estados Unidos (DOD), éste fundó el Centro de información de red del Departamento de Defensa (DDN NIC-Departament of Defense Network Information Center) responsable de la administración y registro de todos los nombres y direcciones. Luego, en 1993, la Fundación Nacional de Ciencias (NSF-National Science Foundation) asumió esa responsabilidad sobre los nombres y direcciones no militares, mientras el DDN NIC conservó la responsabilidad sobre los nombres y direcciones militares. La Fundación antes indicada creó el Servicio de registro InterNIC (InterNIC Registration Service), como principal autoridad mundial sobre nombres y direcciones, pero dado que tal centralización generaba situaciones de ineficiencia, InterNIC optó por delegar su autoridad en registros regionales y éstos en registros nacionales. Durante el período comprendido entre 1972 y 1994, el gobierno Norteamericano estuvo encargado de la administración del sistema de nombres de dominio, para lo cual decidió los dominios que se crearían y determinó, a su discreción, quienes se encargarían de su administración y manejo. Para ese momento, IANA (Internet Asisigned Numbers Authority) era la autoridad encargada de administrar los números I.P., los nombres de dominios y otros parámetros utilizados en Internet.

60 El consejo de Estado considero que "La administración del dominio .co y el derivado registro de los nombres de dominio en Colombia, para la red de la Internet, es un asunto relacionado intrínsecamente con las telecomunicaciones y en consecuencia, existe la competencia del Gobierno nacional, a través del Ministerio de Comunicaciones, para su planeación, regulación y control, de conformidad con las normas citadas en precedencia y las concordantes del decreto 1130 de 1999, con mayor razón cuanto que el dominio .co, como se explicó en el punto 2.5, constituye un recurso de interés público, respecto del cual el Estado colombiano debe velar por su adecuada utilización para hacer prevalecer el interés general, de acuerdo con el principio instituido por el artículo 1º de la Constitución Política. COLOMBIA. Sala de Consulta y Servicio Civil, Magistrado Ponente: César Hoyos Salazar, Diciembre 11 de 2001, radicación No. 1376.

nombres de dominio.co es aquella actividad a cargo del Estado, que tiene por objeto la organización, administración y gestión del dominio.co, incluido el mantenimiento de las bases de datos correspondientes, los servicios de información asociados al público, el registro de los nombres de dominio, su funcionamiento, la operación de sus servidores y la difusión de archivos de zona del dominio, y demás aspectos relacionados, de conformidad con las prácticas y definiciones de los organismos internacionales competentes. Parágrafo. Para los efectos de esta ley, el nombre de dominio de Internet bajo el código de país correspondiente a Colombia -.co-, es un recurso del sector de las telecomunicaciones, de interés público, cuya administración, mantenimiento y desarrollo estará bajo la planeación, regulación y control del Estado, a través del Ministerio de Comunicaciones, para el avance de las telecomunicaciones globales y su aprovechamiento por los usuarios"[61].

Por medio de la Resolución 00284 del 21 de febrero de 2008, el Ministerio de Tecnologías de la Información y las Comunicaciones adopta el modelo operativo para la administración del dominio .co, mantiene la política en cabeza del Ministerio de Comunicaciones y se tercerizan las funciones del Registro para lo cual se debe adelantar un proceso de selección objetivo. Por lo anterior, se adelantó licitación pública 0002 de 2009 y por contrato de concesión, se seleccionó como administrador del dominio del nivel superior .Co a la empresa privada Cointernet S.A.S[62].

.CO Internet SAS, es una entidad de carácter privado, que por contrato de concesión con el Estado Colombiano, tiene la Responsabilidad de administración del dominio, básicamente cumple con tres funciones: Promoción, administración y operación del dominio .CO. En desarrollo de estas Responsabilidades es quien establece y administra las relaciones con los registradores y define el modelo de contraprestaciones; Establece y maneja las relaciones con el ICANN y demás organizaciones de soporte a la gestión de los ccTLDs, al igual que participa como invitado permanente en el Consejo Asesor de Políticas y; es responsable por la operación técnica del dominio.

En lo que respecta al registro cualquier persona natural o jurídica, nacional o extranjera, puede registrar los dominios .CO. De acuerdo a las mejores prácticas internacionales, y a la liberalización de políticas de los principales ccTLD, no hay ningún requisito de documentación para registrar un dominio .CO Esta regla general tiene como única excepción los dominios de Usuario Restringido como .org.co, .edu.co, .mil.co, y .gov.co (próximamente .gob.co), para los que se han establecido algunos requisitos que deben cumplir sus potenciales titulares. El precio depende de cada registrador (comercializador) y del paquete de servicios que éste ofrezca al usuario; sin embargo, cabe anotar que el

61 Esta ley fue derogada mediante la ley 1341 de 2009, art. 73. La ley 1341 de 2009 es el marco general del sector de las telecomunicaciones, en la cual se definen los principios y conceptos de la sociedad de la información como referente para la formulación de políticas.

62 A la fecha esta empresa tiene 10 empresas registradoras acreditadas para ofrecer registros en el dominio .CO, estas son: Registradores nacionales: mi.com.co, dominio amigo. Registradores internacionales: dotster,enom, internetx, goo dady.com,melbournelt, network solutions, opensrs, register.com

precio al por mayor que cobra .CO Internet a sus registradores guarda relación con el precio de los principales dominios del mercado internacional[63].

Los dominios de usuario restringido .org.co, .edu.co, .mil.co, y .gov.co (próximamente .gob.co), tienen un esquema especial de precios, en virtud del cual son gratuitos los dominios bajo .mil.co, .gov.co (próximamente .gob.co) y los dominios de las instituciones educativas públicas. Por su parte, los dominios bajo el .org.co y .edu.co, de instituciones privadas, tienen un precio de $30.000 por año.

Como podemos observar la Rama judicial pueden registrar su dominio gov.co directamente en la página .CO Internet sin costo alguno y solo se requiere allegar Fotocopia del certificado del RUT y Decreto de creación o resolución de la entidad Solicitante[64].

4. EL PROCESO CONTENCIOSO ADMINISTRATIVO ONLINE.

4.1 Normatividad.

Con el fin de analizar las normas que regulan los medios tecnológicos en el Código de procedimiento administrativo y de lo contencioso administrativo (CPACA) así como también el Código General del proceso (C.G.P) a continuación y de manera comparativa estudiaremos los diferentes temas que considero relevantes para adelantar un juicio en línea:

a). Principio de la equivalencia funcional:

El C.P.A.C.A en la primera parte del código en varios de sus artículos establece la equivalencia funcional entre los documentos manuscritos y los documentos electrónicos, así mismo establece que los documentos públicos autorizados o suscritos por medios electrónicos tienen la validez y fuerza probatoria que le confieren a los mismos las disposiciones del Código de Procedimiento Civil y que las reproducciones efectuadas a partir de los respectivos archivos electrónicos se reputarán auténticas para todos los efectos legales[65]. Así mismo establece en la segunda parte del código que todas las actuaciones judiciales susceptibles de surtirse en forma escrita se podrán realizar a través de medios electrónicos, siempre y cuando en su envío y recepción se garantice su autenticidad, integridad, conservación y posterior consulta, de conformidad con la ley. En lo que respecta a la utilización de firmas digitales o electrónicas el Código

63 De acuerdo con las nuevas políticas de Registro, el usuario puede ahora registrar y administrar sus dominios a través de los principales registradores del mundo, y encontrará servicios de valor agregado y precios más competitivos. Se elimina la documentación y los trámites requeridos en el proceso de registro. Los usuarios en Colombia y alrededor del mundo estarán en capacidad de seleccionar y adquirir en línea su nombre de dominio preferido, en cuestión de minutos. – Para los dominios de usuario restringido se seguirá exigiendo la presentación de documentación de soporte. Es posible registrar un dominio o varios de manera fácil para promocionar servicios distintos y/o productos distintos. Se puede registrar un dominio por períodos de un año hasta 5 años. Es posible transferir nombres de dominio a otros titulares y/o entre registradores y se automatiza el procedimiento de registro el cual pasa a ser completamente en línea. http://www.cointernet.com.co/dominios/faq/registro-de-dominios-nuevos

64 http://www.cointernet.com.co/dominios/uso-restringido

65 Ley 1437 de 2011, articulo 55.

no establece regulación al respecto, por lo cual nos remitiríamos en un principio a la ley 527 de 1999 y posteriormente al C.G.P. una vez éste entre en vigencia.

La ley 1564 de 2012, en lo que respecta al principio de la equivalencia funcional se remite a la ley 527 de 1999 y además establece que, se presumen auténticos los memoriales y demás comunicaciones cruzadas entre las autoridades judiciales y las partes o sus abogados, cuando sean originadas desde el correo electrónico suministrado en la demanda o en cualquier otro acto del proceso. Así mismo en varios de sus apartes establece las reglas para la valoración de los documentos electrónicos[66]. Es de gran relevancia en el C.G.P el artículo 103 el cual establece que 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. Así mismo establece que las actuaciones judiciales se podrán realizar a través de mensajes de datos y que la autoridad judicial deberá contar con mecanismos que permitan generar, archivar y comunicar mensajes de datos. Para dar cumplimiento a lo anterior la Sala Administrativa del Consejo Superior de la Judicatura debe adoptar las medidas necesarias para procurar que al entrar en vigencia este código todas las autoridades judiciales cuenten con las condiciones técnicas necesarias para generar, archivar y comunicar mensajes de datos[67].

Respecto a las firmas, el C.G.P. en varios de sus apartes regula aspectos relacionados con las firmas digitales y electrónicas. En relación con los poderes la ley establece que esos se pueden conferir con mensaje de datos con firma digital[68]. Sin embargo, para la presentación de las demandas esta ley es más flexible ya que establece que las demandas que se presenten en mensaje de datos no requerirán de la firma digital definida por la Ley 527 de 1999 y que solo bastará que el suscriptor se

66 Ley 1564. Artículo 243. Distintas clases de documentos. 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. Artículo 244. Documento auténtico. 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. Artículo 247. Valoración de mensajes de datos. Serán valorados como mensajes de datos los documentos que hayan sido aportados en el mismo formato en que fueron generados, enviados, o recibidos, o en algún otro formato que lo reproduzca con exactitud. La simple impresión en papel de un mensaje de datos será valorada de conformidad con las reglas generales de los documentos.

67 El Plan de Justicia Digital estará integrado por todos los procesos y herramientas de gestión de la actividad jurisdiccional por medio de las tecnologías de la información y las comunicaciones, que permitan formar y gestionar expedientes digitales y el litigio en línea. El plan dispondrá el uso obligatorio de dichas tecnologías de manera gradual, por despachos judiciales o zonas geográficas del país, de acuerdo con la disponibilidad de condiciones técnicas para ello. Ley 1564 Artículo 103.

68 Ley 1564 Artículo 74. Poderes. Inciso 5.

identifique con su nombre y documento de identificación en el mensaje de datos[69]. En lo que respecta a los funcionarios la norma establece que los funcionarios y empleados judiciales deberán usar, en todos sus actos escritos, firma acompañada de antefirma y que podrán usar firma electrónica, de conformidad con el reglamento que expida el Consejo Superior de la Judicatura[70].

Se concluye de lo anterior que tanto el CPACA como el CGP en su articulado desarrollan el principio de la equivalencia funcional entre los documentos escritos y los mensajes de datos otorgando la posibilidad a los operadores judiciales de acudir a los medios tecnológicos en las diferentes etapas del proceso.

b). Presentación de demandas y memoriales:

El CPACA no regula específicamente la presentación de demandas y memoriales vía electrónica, sin embargo el artículo 186 establece que todas las actuaciones judiciales susceptibles de surtirse en forma escrita se podrán realizar a través de medios electrónicos, siempre y cuando en su envío y recepción se garantice su autenticidad, integridad, conservación y posterior consulta, de conformidad con la ley y que la autoridad judicial deberá contar con mecanismos que permitan acusar recibo de la información recibida, a través de este medio. De lo anterior se concluye que es viable presentar demandas y memoriales por medios electrónicos y que se requiere que la jurisdicción cuente con herramientas tecnológicas necesarias para garantizar los requisitos exigidos en la Ley.

El C.G.P. en el artículo 82 establece que es viable presentar las demandas por medio de mensajes de datos posteriormente establece que en donde se haya habilitado un Plan de Justicia Digital, no será necesario presentar copia física de la demanda y que atendiendo las circunstancias particulares del caso, el juez podrá excusar al demandante de presentar la demanda como mensaje de datos[71]. Posteriormente el artículo 109 regula la presentación y trámite de memoriales e incorporación de escritos y comunicaciones y establece que las autoridades judiciales llevarán un estricto control y relación de los mensajes recibidos que incluya la fecha y hora de recepción. También mantendrán el buzón del correo electrónico con disponibilidad suficiente para recibir los mensajes de datos. En relación con la fecha de recibido establece que los memoriales, incluidos los mensajes de datos, se entenderán presentados oportunamente si son recibidos antes del cierre del despacho del día en que vence el término[72].

Además de ser viable la presentación de demandas y memoriales por medios electrónicos, el C.G.P. establece que no obstante lo dispuesto en la Ley 527 de 1999, se presumen auténticos los memoriales y

69 Ley 1564 Artículo 82. Requisitos de la demanda. Salvo disposición en contrario, la demanda con que se promueva todo proceso deberá reunir los siguientes requisitos: Parágrafo segundo. Las demandas que se presenten en mensaje de datos no requerirán de la firma digital definida por la Ley 527 de 1999. En estos casos, bastará que el suscriptor se identifique con su nombre y documento de identificación en el mensaje de datos.

70 Ley 1564 Artículo 105.

71 Ley 1564 Artículo 102.

72 Ley 1564 Artículo 109.

demás comunicaciones cruzadas entre las autoridades judiciales y las partes o sus abogados, cuando sean originadas desde el correo electrónico suministrado en la demanda o en cualquier otro acto del proceso[73].

c). Notificaciones:

En relación con las notificaciones el C.P.A.P.A. establece que las entidades públicas de todos los niveles, las privadas que cumplan funciones públicas y el Ministerio Público que actúe ante la jurisdicción, deben tener un buzón de correo electrónico exclusivamente para recibir notificaciones judiciales[74]. El auto admisorio de la demanda y el mandamiento de pago contra las entidades públicas y las personas privadas que ejerzan funciones propias del Estado se deben notificar personalmente a sus representantes legales o a quienes estos hayan delegado la facultad de recibir notificaciones, o directamente a las personas naturales, según el caso, y al Ministerio Público, mediante mensaje dirigido al buzón electrónico para notificaciones judiciales a que se refiere el artículo 197 de este Código. De esta misma forma se deberá notificar el auto admisorio de la demanda a los particulares inscritos en el registro mercantil en la dirección electrónica por ellos dispuesta para recibir notificaciones judiciales[75].

Respecto a las notificaciones por estado la norma establece que los autos no sujetos al requisito de la notificación personal se notificarán por medio de anotación en estados electrónicos para consulta en línea bajo la responsabilidad del Secretario. La inserción en el estado se hará el día siguiente al de la fecha del auto[76], el estado se insertará en los medios informáticos de la Rama Judicial y debe permanecer allí en calidad de medio notificador durante el respectivo día. De las notificaciones hechas por el estado el Secretario debe dejar certificación con su firma al pie de la providencia notificada y enviar un mensaje de datos a quienes hayan suministrado su dirección electrónica[77]. En relación con las sentencias, éstas se notificarán, dentro de los tres (3) días siguientes a su fecha, mediante envío de su texto a través de mensaje al buzón electrónico para notificaciones judiciales[78]. Finalmente en relación con las notificaciones el CPACA establece que además de los casos contemplados en los artículos anteriores, se podrán notificar las providencias a través de medios electrónicos, a quien haya aceptado expresamente este medio de notificación y en este caso, la providencia a ser notificada se debe remitir

73 Ley 1564 Artículo 103 parágrafo 2º.

74 Ley 1437 Artículo 197

75 Ley 1437 de 2011. Artículo 199.

76 En la anotación en los estados electrónicos se hará constar: 1. La identificación del proceso. 2. Los nombres del demandante y el demandado. 3. La fecha del auto y el cuaderno en que se halla. La fecha del estado y la firma del Secretario. Ley 1437 de 2011 Artículo 199.

77 De los estados que hayan sido fijados electrónicamente se conservará un archivo disponible para la consulta permanente en línea por cualquier interesado, por el término mínimo de diez (10) años. Cada juzgado dispondrá del número suficiente de equipos electrónicos al acceso del público para la consulta de los estados. Ley 1437 de 2011 Artículo 201.

78 Ley 1437 de 2011. Artículo 203.

por el Secretario a la dirección electrónica registrada y para su envío se deberán utilizar los mecanismos que garanticen la autenticidad e integridad del mensaje. Así mismo se presumirá que el destinatario ha recibido la notificación cuando el iniciador recepcione acuse de recibo o se pueda por otro medio constatar el acceso del destinatario al mensaje y el Secretario hará constar este hecho en el expediente[79].

Al respecto, el C.G.P. establece que para la práctica de la notificación personal se procederá así: (…) Las personas jurídicas de derecho privado y los comerciantes inscritos en el registro mercantil deberán registrar en la Cámara de Comercio o en la oficina de registro correspondiente del lugar donde funcione su sede principal, sucursal o agencia, la dirección donde recibirán notificaciones judiciales. Con el mismo propósito deberán registrar, además, una dirección electrónica. Esta disposición también se aplicará a las personas naturales que hayan suministrado al juez su dirección de correo electrónico. Si se registran varias direcciones, la notificación podrá surtirse en cualquiera de ellas. La parte interesada remitirá una comunicación a quien deba ser notificado, a su representante o apoderado, por medio de servicio postal autorizado por el Ministerio de Tecnologías de la Información y las Comunicaciones, en la que le informará sobre la existencia del proceso, su naturaleza y la fecha de la providencia que debe ser notificada, previniéndolo para que comparezca al juzgado a recibir notificación dentro de los cinco (5) días siguientes a la fecha de su entrega en el lugar de destino. Cuando se conozca la dirección electrónica de quien deba ser notificado, la comunicación podrá remitirse por el secretario o el interesado por medio de correo electrónico. Se presumirá que el destinatario ha recibido la comunicación cuando el iniciador recepcione acuse de recibo. En este caso, se dejará constancia de ello en el expediente y adjuntará una impresión del mensaje de datos[80].

En relación con la notificación por aviso establece que el Artículo 292 que cuando se conozca la dirección electrónica de quien deba ser notificado, el aviso y la providencia que se notifica podrán remitirse por el secretario o el interesado por medio de correo electrónico. Se presumirá que el destinatario ha recibido el aviso cuando el iniciador recepcione acuse de recibo. En este caso, se debe dejar constancia de ello en el expediente y adjuntará una impresión del mensaje de datos[81]. Las notificaciones de autos y sentencias que no deban hacerse de otra manera se cumplirán por medio de anotación en estados que elaborará el secretario. La inserción en el estado se hará al día siguiente a la fecha de la providencia y cuando se cuente con los recursos técnicos los estados se publicarán por mensaje de datos, caso en el cual no deberán imprimirse ni firmarse por el secretario[82].

d). Expediente judicial electrónico

En la primera parte de la ley 1437 de 2011, se define el expediente electrónico como el conjunto de documentos electrónicos

79 De las notificaciones realizadas electrónicamente se conservarán los registros para consulta permanente en línea por cualquier interesado. Ley 1437 de 2011. Artículo 205.

80 Ley 1564 de 2012. Artículo 291.

81 Ley 1564 de 2012. Artículo 292.

82 Ley 1564 de 2012. Artículo 293.

correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan, que el foliado de los expedientes electrónicos se llevará a cabo mediante un índice electrónico, firmado digitalmente por la autoridad, órgano o entidad actuante, según proceda y que este índice garantizará la integridad del expediente electrónico y permitirá su recuperación cuando se requiera. En lo que respecta al expediente judicial electrónico, el artículo 186 establece que la Sala Administrativa del Consejo Superior de la Judicatura adoptará las medidas necesarias para que en un plazo no mayor de cinco (5) años, contados a partir de la vigencia del presente Código, sea implementado con todas las condiciones técnicas necesarias el expediente judicial electrónico, que consistirá en un conjunto de documentos electrónicos correspondientes a las actuaciones judiciales que puedan adelantarse en forma escrita dentro de un proceso.

Como se puede observar el C.P.A.C.A. propende por la implementación del expediente electrónico en las diferentes entidades así como también la implementación del expediente judicial electrónico en la jurisdicción Contencioso-Administrativa.

El nuevo C.G.P, en su artículo 103 es más ambicioso al establecer que se debe implementar el plan de justicia digital el cual deberá estar integrado por todos los procesos y herramientas de gestión de la actividad jurisdiccional por medio de las tecnologías de la información y las comunicaciones, que permitan formar y gestionar expedientes digitales y el litigio en línea. Posteriormente en los artículos 125 y 324 regula aspectos relacionados con el denominado expediente digital, por lo cual se puede concluir que aunque el C.P.A.C.A utiliza el término expediente judicial electrónico y el C.G.P hace referencia al expediente digital básicamente lo que se pretende es la implementación de un juicio en línea que esté al alcance de las diferentes jurisdicciones.

e). Audiencias y diligencias

La ley 1437 de 2011 en su artículo 183. *"Actas y registro de las audiencias y diligencias"*, establece que las audiencias y diligencias serán presididas por el Juez o Magistrado Ponente. En el caso de jueces colegiados podrán concurrir los magistrados que integran la sala, sección o subsección si a bien lo tienen. Tratándose de la audiencia de alegaciones y juzgamiento esta se celebrará de acuerdo con el quórum requerido para adoptar la decisión.

Para efectos de su registro se tendrán en cuenta las siguientes reglas:

(…)
3. Se deberá realizar una grabación del debate, mediante cualquier mecanismo técnico; dicha grabación deberá conservarse en los términos que ordenan las normas sobre retención documental.

En igual sentido se pronuncia la ley 1564 de 2012, Artículo 107 *"Audiencias y diligencias"*, el cual establece que las audiencias y diligencias se sujetarán a las siguientes reglas:

(…)

4. Grabación. La actuación adelantada en una audiencia o diligencia se grabará en medios de audio, audiovisuales o en cualquiera otro que ofrezca seguridad para el registro de lo actuado.

5. Publicidad. Las audiencias y diligencias serán públicas, salvo que el juez, por motivos justificados, considere necesario limitar la asistencia de terceros.

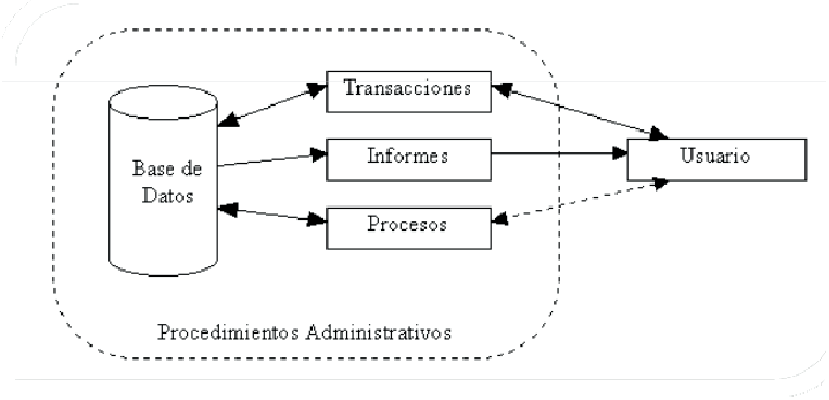
El Consejo Superior de la Judicatura deberá proveer los recursos técnicos necesarios para la grabación de las audiencias y diligencias.

6. Prohibiciones. Las intervenciones orales no podrán ser sustituidas por escritos.

(…)
Solo cuando se trate de audiencias o diligencias que deban practicarse por fuera del despacho judicial o cuando se presenten fallas en los medios de grabación, el juez podrá ordenar que las diligencias consten en actas que sustituyan el sistema de registro a que se refiere el numeral 4 anterior o que la complementen.

Como se puede observar, el nuevo Código Contencioso-Administrativo y el Nuevo Código general del proceso regulan taxativamente la utilización de los medios electrónicos en la Jurisdicción, haciéndose imperativo proceder a la implementación de los mismos de manera prioritaria.

ILUSTRACIÓN 1. ELEMENTOS DE UN SISTEMA DE INFORMACIÓN



4.2 HERRAMIENTAS TECNOLÓGICAS REQUERIDAS.

El proceso contencioso-administrativo online requiere de diversas herramientas tecnológicas y un correcto procedimiento para su implementación (Etapas de desarrollo, pruebas e implantación), por lo anterior solo enunciaré aquellas que considero necesarias para el desarrollo y buen funcionamiento de la plataforma:

En primera instancia, debe existir la necesidad de organizar de manera coherente, sistematizar y controlar algún o algunos procesos; la información a ser organizada debe provenir de actos, hechos y decisiones. Un Sistema de

Información[83] debe estar compuesto por un conjunto de elementos que deben cubrir satisfactoriamente las necesidades que permitan el buen desempeño de la organización que lo ha implementado o lo hará a futuro.

El éxito de un impecable sistema de información, se basa, en primera instancia, en hacer una correcta recolección de información sobre los procesos, usuarios y administración de los datos que se manipulan entre los dos primeros. **ES MUY IMPORTANTE** que se gestione la implementación a la par del sistema de información, de un **Sistema de Gestión Documental**, el cual garantizará el correcto uso de la información (documentos) y asegurará su contenido, así como los permisos de visualización.

La creación de un sistema de información requiere de personal profesional capacitado, así como las herramientas de Software para poder crearlo. Es necesario resaltar que existen diferentes aplicaciones de software para el desarrollo de un Sistema de Información (en adelante S.I.) siendo un gran motivo a decidir el factor económico y si se opta por Software libre o propietario[84]. El tiempo que conlleve el desarrollo del S.I. solo podrá ser definido por la empresa o el grupo destinado a su desarrollo teniendo en cuenta los requerimientos que se hayan solicitado y su nivel de complejidad, teniendo un tiempo aproximado de desarrollo de 8 meses. El tiempo es una variable que puede verse afectada por el número de personas que estén trabajando en el proyecto y la relación entre el usuario y la empresa desarrolladora para el intercambio de información.

Como ejemplos meramente ilustrativos, podremos nombrar herramientas de desarrollo privativas tales como Visual Studio 2012 (Microsoft)[85] para la construcción del S.I., y SharePoint (Microsoft)[86] para la Gestión documental. Por su contraparte encontramos a Netbeans Java (Sun MicroSystems)[87] para la construcción del S.I. y Open KM[88] como gestor documental.

Ahora bien, habiendo conocido la temática implícita para el desarrollo del S.I. debemos soportar esto con una estructura de Hardware robusta y que sea proyectada con el fin de escalonar y ampliarse debido a la naturaleza del proyecto (Justicia en Línea), ya que su demanda será creciente y por su complejidad requerirá que se manejen protocolos de seguridad y respaldo.

Servidor de aplicaciones: Será la máquina encargada de alojar el Sistema de Información, la cual soportará la totalidad de solicitudes que se hagan en tiempo

83 http://www.slideshare.net/rulascch/sistemas-de-informacin-16167190

84 http://helenalh.blogspot.com/2011/10/semejanzas-y-diferencias-y-ventajas-e.html

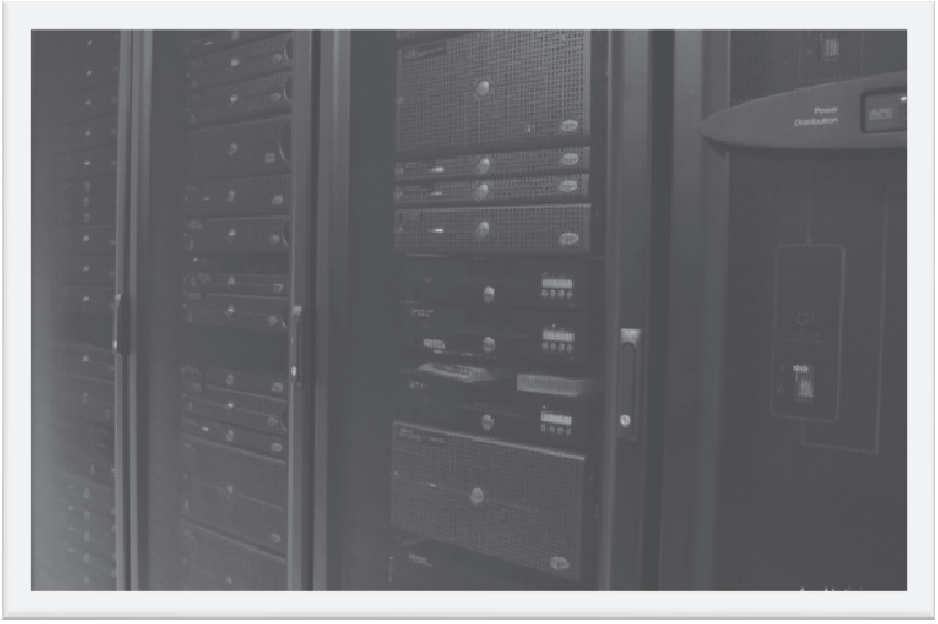
85 http://www.microsoft.com/visualstudio/esn/whats-new#story-whats-new

86 http://sharepoint.microsoft.com/es-es/Paginas/default.aspx

87 http://netbeans.org/index_es.html

88 http://www.openkm.com/es/

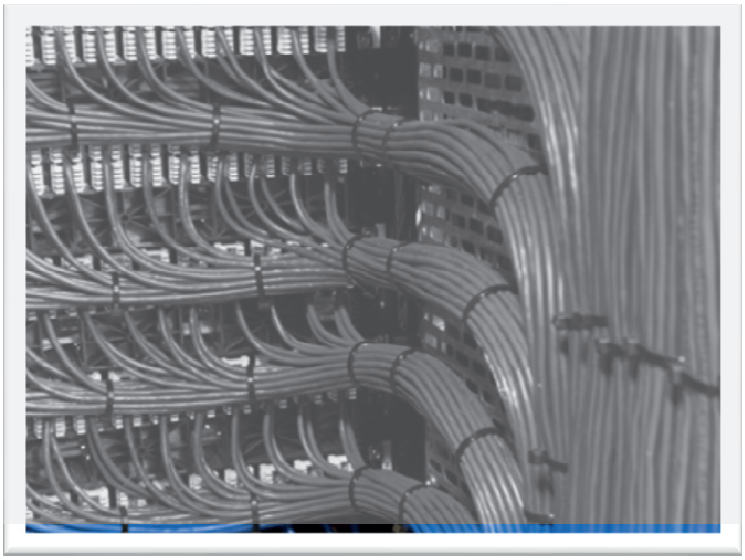
real al sistema para Ingresar, Consultar o Modificar información y que deberá estar disponible las 24 horas del día de todos los días del año. Debe contar con Discos Duros espejos para el respaldo de la aplicación y un Centro de Cómputo[89] que preserve su funcionamiento.



Servidor de almacenamiento (storage): Equipo(s) destinado(s) al almacenamiento de los datos e información generados a partir del uso del Sistema de Información sea cual sea su contenido (Documentos o material multimedia tal como audio, imágenes o video)

89 http://www.fcca.umich.mx/descargas/apuntes/Academia%20de%20Informatica/Adm%C3%B3n%20de%20Centros%20de%20Computo%20%20%20R.C.M/UNIDAD%20I.pdf

Cableado estructurado: Implementado con normas IEEE[90] que garanticen el cumplimiento de estándares para certificaciones nacionales e internacionales.



Access point(s) (aps): O puntos de acceso que permitirán el acceso de manera inalámbrica a la red y a la aplicación por parte de los usuarios usando sus propios dispositivos móviles (Portátiles, Tablets o Smartphones) lo que redunda en una inversión menor de equipos de cómputo para colocar a disposición del público.[91]

90 http://standards.ieee.org/

91 http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps10492/ps10597/cisco_small_business_wireless_access_point_brochure_spanish.pdf

Equipo de cómputo: Permitirán a los usuarios dentro de las instalaciones hacer uso del Sistema de información y deben contar con requisitos mínimos tales como (recomendados) Sistema Operativo Windows 7, Memoria RAM Mínima de 4 Gigas, Disco Duro de 320 GigaBytes, Procesador Core i5 de Segunda Generación o Similar.

Canal de internet dedicado: Permitirá que las consultas hechas a través de Internet sean realizadas de una manera rápida y efectiva sin retrasar la respuesta al usuario y garantice una navegabilidad de calidad en el Sistema de Información[92].

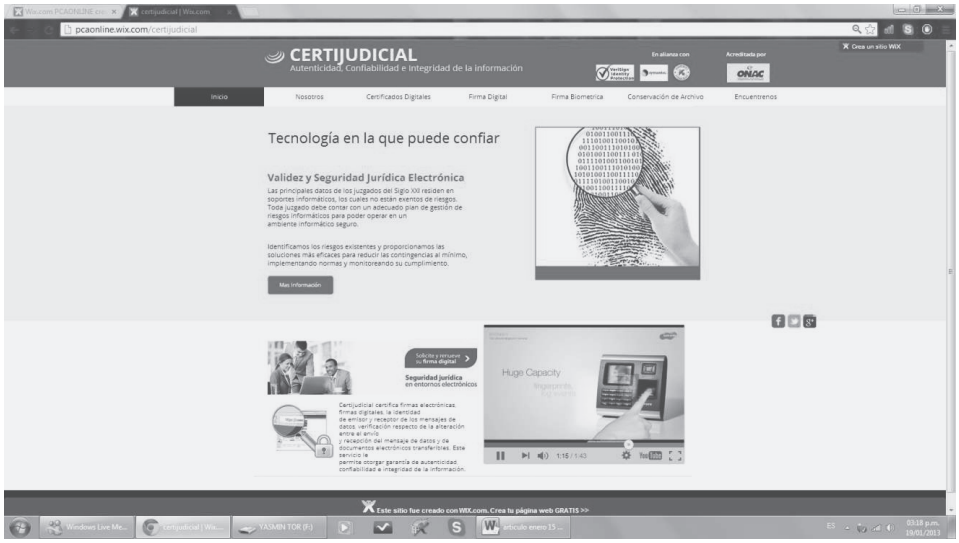
Dispositivos biométricos: que garantizarán niveles de seguridad y reconocimiento de acuerdo a su clase.[93]

Cámaras de video: Que permitan la continua vigilancia no solo de los equipos mencionados, sino también y en un uso diferente, la transmisión vía Web de eventos relacionados con el Sistema de Información (Tales como audiencias o cualquier tipo de evento que necesite hacerse virtual y remotamente accesible). Deben contar con requerimientos mínimos tales como la posibilidad de captar imágenes en alta definición (HD) y tener buen desempeño en ambientes de baja luminiscencia.

92 http://www.une.com.co/empresas/internet/internet-dedicado

93 http://www.articulo.org/articulo/49962/sistemas_biometricos_y_autenticacion.html

4.3 SEGURIDAD



La ley 527 de 1999 creó y reglamentó las entidades de certificación, las firmas digitales y las firmas electrónicas. Estas entidades de certificación también llamadas terceros de confianza, se encargan de garantizar la seguridad jurídica y tecnológica de las transacciones y comunicaciones.

Posteriormente el Decreto 19 de 2012, modificó los artículos 29 y 30 y derogó los artículos 41 y 42 de la ley 527 de 1999[94]. Así mismo se le otorgó la competencia al Organismo Nacional de Acreditación de Colombia ONAC, para acreditar a las entidades de certificación conforme a la reglamentación expedida por el Gobierno Nacional, normatividad que a la fecha de presentación de este artículo no ha sido expedida.

Aunque no han tenido mayor acogida, las entidades de certificación han sido de gran utilidad tanto en entidades del sector público como en entidades del sector privado para otorgar seguridad y confianza a la entidad y a los suscriptores[95]. Es por esto que en aras de contar con

94 Decreto 19 de 2012. Artículos 160, 161,162 y 163.

95 Las siguientes son algunas de las entidades de certificación que han cumplido con los requisitos exigidos en la ley 527 de 1999, en el decreto 1747 de 2000 y la resolución 26930 de 2000 de la Superintendencia de Industria y Comercio. 1. CERTICÁMARA, S.A., entidad de certificación abierta, página web: www.certicamara.com, autorizada mediante resoluciones Nos. 1007 (2002.01.24) y 9887 (2007.04.13.). 2. Instituto Colombiano de Codificación y Automatización Comercial, entidad de certificación cerrada, página web: www.iaccolombia.org, autorizada mediante resolución No. 25352 del 31 de agosto de 2002. 3. BANCO DE LA REPÚBLICA, entidad de certificación cerrada, página web: www.banrep.gov.co, autorizada mediante resolución No. 6372 del 28 de Febrero de 2003. 4. A TODA HORA S.A., entidad de certificación cerrada, autorizada mediante resolución No. 29844 del 22 de octubre de 2003. 5. UAE DIRECCIÓN DE IMPUESTOS Y ADUANAS NACIONALES – DIAN, entidad de certificación cerrada, página web: www.dian.gov.co, autorizada mediante resolución No. 36119 del 30 de diciembre de 2005. 6. ECOPETROL S.A, entidad de certificación cerrada, página web: www.ecopetrol.com.co.

herramientas tecnológicas que nos permitan avanzar hacia la adopción del tan anhelado expediente judicial electrónico[96] y el Plan de Justicia Digital[97], considero que lo conveniente de acuerdo a la ley 527 de 1999, sería la creación de una entidad de certificación cerrada que a manera de ejemplo de denominado CERTIJUDICIAL, para la Rama Judicial.

Esta entidad de certificación una vez acreditada por el Organismo Nacional de Acreditación se encargara de CERTIFICAR aspectos de gran importancia en el intercambio de mensajes entre la rama judicial y los suscriptores sin exigir remuneración por ello y dentro de sus funciones encontraríamos:

a. CREACIÓN DE FIRMAS DIGITALES Y ELECTRONICAS PARA LOS SUSCRIPTORES. El usuario tendrá la opción de crear firmas seguras en consecuencia podrá elegir entre crear una firma digital basada en criptografía asimétrica con clave pública y clave privada o crear una firma electrónica basada en características biométricas como lo son la huella digital, reconocimiento del iris, de voz y de rostro entre otros.

b. EMITIR CERTIFICADOS DE FIRMAS DIGITALES O ELECTRÓNICAS DE PERSONAS NATURALES O JURÍDICAS. CERTIJUDICIAL certificará la identidad del iniciador y destinatario de un mensaje de datos sin necesidad de acudir a la función notarial.

c. EMITIR CERTIFICADOS SOBRE LA INTEGRIDAD DE LA INFORMACIÓN[98]: CERTIJUDICIAL certificará que entre

96 El artículo 186 del C.P.A.CA, establece que todas las actuaciones judiciales susceptibles de surtirse en forma escrita se podrán realizar a través de medios electrónicos, siempre y cuando en su envío y recepción se garantice su autenticidad, integridad, conservación y posterior consulta, de conformidad con la ley. La autoridad judicial deberá contar con mecanismos que permitan acusar recibo de la información recibida, a través de este medio. Parágrafo. La Sala Administrativa del Consejo Superior de la Judicatura adoptará las medidas necesarias para que en un plazo no mayor de cinco (5) años, contados a partir de la vigencia del presente Código, sea implementado con todas las condiciones técnicas necesarias el expediente judicial electrónico, que consistirá en un conjunto de documentos electrónicos correspondientes a las actuaciones judiciales que puedan adelantarse en forma escrita dentro de un proceso.

97 La ley 1564 de 2012, en sus artículos 37, 39, 42, 89,125, 324 de la ley 1564 menciona la utilización del Plan de Justicia Digital, en especial el artículo 103 parágrafo primero establece que La Sala Administrativa del Consejo Superior de la Judicatura adoptará las medidas necesarias para procurar que al entrar en vigencia este código todas las autoridades judiciales cuenten con las condiciones técnicas necesarias para generar, archivar y comunicar mensajes de datos. El Plan de Justicia Digital estará integrado por todos los procesos y herramientas de gestión de la actividad jurisdiccional por medio de las tecnologías de la información y las comunicaciones, que permitan formar y gestionar expedientes digitales y el litigio en línea. El plan dispondrá el uso obligatorio de dichas tecnologías de manera gradual, por despachos judiciales o zonas geográficas del país, de acuerdo con la disponibilidad de condiciones técnicas para ello.

98 Ley 527 de 1999 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.

el envío y recepción del mensaje de datos la información no fue alterada y que el contenido de la información cuenta con la aprobación del firmante, de esta manera evitaremos que el autor del mensaje de datos niegue su autoría o manifieste no ser el documento que él firmo inicialmente.

d. ESTAMPADO CRONOLÓGICO:
Con base en la hora legal colombiana, CERTIJUDICIAL certificará la hora de creación, modificación y recepción de un mensaje de datos impidiendo su posterior alteración. De esta manera tendremos certeza al momento de rechazar alguno escrito cuando se presente fuera del término establecido en la ley.

e. OFRECER LOS SERVICIOS DE ARCHIVO Y CONSERVACIÓN DE MENSAJES DE DATOS.

CERTIJUDICIAL prestará el servicio de archivo y conservación de los mensajes de datos en condiciones de seguridad y confianza para cuando esta información sea requerida ya sea por el juez o por las partes.

CERTIJUDICIAL otorgará a los usuarios de la Rama Judicial y a los operadores judiciales la autenticidad, e integridad de la información y brindara la seguridad y confianza requerida por los jueces y por las partes para una administración de justicia, recta, trasparente y eficiente.

Podemos concluir entonces, que de conformidad con la normatividad vigente es necesario y prioritario implementar un proceso contencioso-administrativo on line en la jurisdicción de lo contencioso administrativo. Así mismo y como se expuso es viable crear nuestra propia página web, con los contenidos adecuados para brindar a la jurisdicción un procedimiento ágil y eficiente que propenda por la recta administración de Justicia.

5. REFERENCIAS BIBLIOGRÁFICAS

-ALCOVER GARAU, GUILLERMO: "La firma electrónica como medio de prueba (valoración jurídica de los criptosistemas de claves asimétricas)", en Cuadernos de Derecho y Comercio, 1994, abril, núm. 13.

-BARRIUSO RUIZ, CARLOS: La contratación electrónica, Madrid, Dykinson, 1998.

-BETTONI TRAUBE, ALEJANDRO: "La contratación electrónica en la nueva ley de certificados, firmas digitales y documentos electrónicos", en Revista Ivstitia, San José, núm. 229, 2006.

-CANELO, CAROLA, y otros: "El documento electrónico. Aspectos procesales", en Revista Chilena de Derecho Informático, núm. 4, mayo de 2004.

-CARABAJO CASCON, FERNANDO. Localización, identificación y distinción en la red. La problemática entre signos distintivos y nombres de dominio de Internet. En el comercio electrónico, editorial Edisofer, Madrid, España, 2001.

-CRUZ RIVERO, DIEGO: "Análisis de los antecedentes del concepto de Firma electrónica como equivalente de la firma manuscrita", en Revista de la Contratación Electrónica, núm. 60, 2005.

-DAVARA RODRÍGUEZ, MIGUEL ÁNGEL: Derecho informático, Pamplona, Aranzadi, 2008.

-DE LA CUADRA MARTÍNEZ, JUAN MIGUEL/ECHAVARRÍA BARRERO, JOSÉ MARÍA: "Comercio Electrónico. Requisitos

generales para su desarrollo", en Régimen jurídico de Internet, Madrid, La Ley, 2002.

-DE MIGUEL ASENSIO, PEDRO A.: Derecho privado de Internet, Madrid, Civitas, 2000.

-GIANNANTONIO, ETTORE: "El valor jurídico del documento electrónico", en Informática y derecho. Apuntes de doctrina informática, Vol. I, Buenos Aires, Depalma, 1991.

-GUTIÉRREZ GÓMEZ, MARÍA CLARA: "Consideraciones sobre el tratamiento jurídico del comercio electrónico", en Internet, comercio electrónico y telecomunicaciones, Bogotá, Editorial Legis, 2002.

-HERRERA BRAVO, ADOLFO: El documento electrónico. Algunas vías de aplicación en el derecho probatorio chileno, Santiago de Chile, La ley Ltda., 1999.

-ILLESCAS ORTIZ, RAFAEL: Derecho de la contratación electrónica, Madrid, Civitas, 2001.

-IRIARTE AHON, ERICK: "Firma digital y certificado digital, el proyecto peruano", en Revista Electrónica de Derecho Informático, septiembre de 1999 (http://publicaciones.derecho.org/redi/No._14)_.

-MADRID PARRA, AGUSTÍN; GUERRERO LEBRON, Mª JESÚS: Derecho patrimonial y tecnología, Madrid, Marcial Pons, 2007.

-MARTÍNEZ NADAL, APOLONIA: Comercio electrónico, firma digital y autoridades de certificación, 2ª ed., Madrid, Civitas, 2000.

-MORENO NAVARRETE, MIGUEL ÁNGEL: Contratos electrónicos, Madrid, Marcial Pons, 1999.

-PEÑA VALENZUELA, DANIEL: Aspectos legales de Internet y del comercio electrónico, Bogotá, Dupré Editores, 2001.

-REMOLINA ANGARITA NELSON: "Desmaterialización, documento electrónico y centrales de registro", en Internet, comercio electrónico y telecomunicaciones, Santa Fe de Bogotá, Legis, 2002.

-RENGIFO GARCÍA, ERNESTO: "Comercio electrónico, documento electrónico y seguridad jurídica", en Seminario sobre Derecho del Comercio Electrónico, Santafé de Bogotá, Universidad Externado de Colombia, ponencia presentada el 23 de septiembre de 1999.

-RIBAGORDA GARNACHO, ARTURO/ RAMOS ÁLVAREZ, BENJAMÍN: Avances en criptología y seguridad de la información, Madrid, Ediciones Díaz de Santos S. A., 2004..

-RICO CARRILLO, MARILIANA: Derecho de las tecnologías, Buenos Aires, Ediciones la Rocca, 2007.

-RINCÓN CÁRDENAS, ERIC: "Últimos retos para el derecho privado: las nuevas tecnologías de la información", en Revista Estudios Socio-Jurídicos, núm. 2, Bogotá, Universidad del Rosario, 2004.

-RIVAS ALEJANDRO, JAVIER: Aspectos jurídicos del comercio electrónico en Internet, Pamplona, Aranzadi, 1999.

-ZUBIETA URIBE, HELMANN: "Los mensajes de datos y las entidades de certificación", en Internet, comercio electrónico y telecomunicaciones, Santa Fe de Bogotá, Legis, 2002.

LEYES Y DECRETOS

LEYES:

-Ley 270 de 1996, Diario Oficial 42745 de 1996.

-Ley 527 de 1999, Diario Oficial 43.673 de 1999.

-Ley 599 de 2000, Diario Oficial No. 44.097 de 2000.

-Ley 633 de 2001 Diario Oficial No. 44.275 de 2000.

-Ley 962 de 2005, Diario Oficial No. 46.023 de 2005

-Ley 1150 de 2007, Diario Oficial 46.691 de 2007.

-Ley 1221 de 2008, Diario Oficial No. 47.052 de 2008.

-Ley 1273 de 2009, Diario Oficial No. 47.223 de 2009

-Ley 1341 de 2009, Diario Oficial No. 47.426 de 2009.

-Ley 1480 de 2011, Diario Oficial No. 48220 de 2011.

-Ley 1437 de 2011, Diario Oficial No. 47.956 de 2011.

-Ley 1564 de 2012, Diario Oficial No. 14489 de 2012.

DECRETOS:

-Decreto 2527 de 1950, Diario Oficial 28.641 de 1950.

-Decreto 1167 de 1980, Diario Oficial 35524 de 1980.

-Decreto 1090 de 1996, Diario Oficial 42814 de 1996.

-Decreto 1487 de 1999, Diario Oficial 43667 de 1999.

-Decreto 1747 de 2000, Diario Oficial 44.160 de 2000.

-Decreto 4149 de 2004, Diario Oficial No. 45762 de 2004.

-Decreto 1929 de 2007, Diario Oficial No. 46.643 de 2007.

-Decreto 19 de 2012, Diario Oficial No. 48.308 de 2012.

RESOLUCIONES:

-Resolución 26930 de 2000. Superintendencia de Industria y Comercio, octubre 26 de 2000.

PÁGINAS WEB

-www.uncitral.org

-www.cointernet.com.co

-www.ipm.com.pe

-www.slideshare.net/rulascch/sistemas-de-informacin-16167190

-helenalh.blogspot.com/2011/10/semejanzas-y-diferencias-y-ventajas-e.html