Mecanismos de validación de identidad y firma electrónica certificados en la adquisición de productos o servicios comercializados en medios electrónicos

NADYA LUCÍA MUSA MURILLO

Director:
Juan Miguel Ángel
Docente Investigación

Magister en Derecho Informático y Nuevas Tecnologías

UNIVERSIDAD EXTERNADO DE COLOMBIA
FACULTAD DE DERECHO
MAESTRÍA EN DERECHO INFORMÁTICO Y NUEVAS TECNOLOGÍAS
BOGOTÁ D.C
2019

Contenido

Introducción

Décadas atrás la sociedad colombiana no hubiera concebido llevar a cabo transacciones, operaciones, procesos y trámites a través del uso de medios electrónicos y mucho menos que estos últimos, en el desarrollo de actividades comerciales, entrarán a reemplazar procesos materializados. Sin embargo, situaciones como éstas que en su momento generaron múltiples interrogantes, han encontrado respuesta a la Ley 527 de 1999 y al Decreto 2364 de 2012, toda vez que hoy por hoy es posible llevar a cabo procesos de firmado en medios electrónicos

Bajo el panorama mencionado y reconociendo que nos encontramos inmersos en la Era Digital, el presente trabajo tiene la intención de presentar bajo un caso hipotético, el estado del arte en Colombia entorno a la regulación en materia de mecanismos de validación de identidad y firmas electrónicas, analizando algunos tipos particulares a la luz del caso planteado, con el fin de establecer si en Colombia contamos con mecanismos robustos y débiles y cuáles son las recomendaciones a la hora de escoger uno u otro mecanismo.

El uso de mecanismos más o menos robustos puede ser determinante a la hora de comercializar servicios en medios electrónicos, siempre se ha pensado que la firma digital es el mecanismo más fuerte, sin embargo, en la actualidad se presentan otros mecanismos lo suficientemente robustos como la firma biométrica a través de la huella, la cual se encuentra en una dicotomía entre lo establecido en la Resolución 5633 de 2016 y el Decreto 2364 de 2012 o también las claves.

El reto en medios electrónicos siempre será el mismo: garantizar que los trámites o actividades que se adelanten en estos entornos, además de cumplir la normativa relativa a su naturaleza, cuenten con la seguridad jurídica y técnica suficiente que permita mitigar riesgos en el curso de la operación. De esta forma, la suplantación de identidad, falsificación del documento electrónico, indisponibilidad de la información electrónica y la no confidencialidad de la misma, serán riesgos

a examinar al momento de determinar qué herramientas electrónicas deben apoyar el desarrollo de la transacción, con el fin de evitar su ocurrencia.

I. Mecanismos de autenticación electrónica y firmas electrónicas

1.1.Lineamientos y normativa a nivel internacional

El desarrollo que se ha gestado en el ordenamiento jurídico colombiano en torno a los conceptos de validación de identidad y firmas electrónicas, así como la participación de Entidades de Certificación Digital, en calidad de terceros de confianza, tienen como antecedentes los avances que se han surtido en el ámbito internacional.

Estos avances se fundamentan en una serie de iniciativas y desarrollos normativos, que en principio parten de que los Estados, a través de sus Gobiernos, adopten estrategias que promuevan el uso de las tecnologías de la información y las comunicaciones en aras de contar con Gobiernos más transparentes, abiertos, participativos e innovadores que permitan acercar al sector público y privado con los ciudadanos, lo cual necesariamente redunda en que tanto en el sector público como en el sector privado se implementen mecanismos electrónicos que permitan adelantar procesos, trámites, servicios y operaciones desmaterializadas, es decir, que nacen y surten su ciclo de vida en el entorno electrónico.

En primer lugar, es importante resaltar que la Organización de Naciones Unidas (ONU) estableció los Objetivos de Desarrollo Sostenible que se configuran en puntos de referencia, así como lineamientos básicos, en materia internacional, frente a la consolidación y formulación de las políticas públicas de los países miembros, encaminadas principalmente a propender por la igualdad y con ello erradicar la pobreza, siendo así que dentro de dichos objetivos es claro que la utilización de las Tecnologías de la Información y las Comunicaciones (TIC) se constituyen en una oportunidad de progreso para tal fin.

Ahora bien, la autenticación electrónica, que es el pilar para llevar a cabo la validación de identidad y la firma en medios electrónicos, tiene como propósito en el marco de las TIC, impulsar las acciones necesarias para avanzar en los Objetivos de Desarrollo Sostenible -ODS[1], permitiendo el goce de derechos a través del uso de TIC. Lo anterior, teniendo presente de antemano, que las tecnologías de la información y comunicaciones tiene el potencial de generar las herramientas necesarias para fortalecer la gobernabilidad democrática, reducir la pobreza, facilitar la generación de desarrollo económico, así como del crecimiento urbano ordenado, entre otros beneficios.

En segundo lugar, para efectos del sector público, también es importante señalar que Organización para la Cooperación y el Desarrollo Económicos (OECD, siglas en inglés) generó unas recomendaciones para el Desarrollo de Estrategias de Administración Digital elaborado por el grupo de trabajo de Gobierno Electrónico de la Organización para la Cooperación y el Desarrollo Económicos (OECD, siglas en inglés); dicho documento plantea una distinción entre lo que significa el Gobierno Electrónico y el Gobierno Digital.

Frente al Gobierno Electrónico, la OCDE menciona que consiste en el uso de las TIC´s por parte de las Administraciones Públicas, particularmente el internet, como una herramienta para lograr un mejor Gobierno. Ahora bien, frente al Gobierno Digital, menciona que consiste en el uso de tecnologías digitales como un elemento que debe ser integrado en la modernización de las estrategias gubernamentales con el fin de crear valor público. En ese sentido, se sustenta bajo el concepto de Administración Pública digital que comprende a los actores del Gobierno, organizaciones no gubernamentales, sector privado, asociaciones ciudadanas y a los agentes que

[1] Objetivos de Desarrollo Sostenible. Disponible en https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

proveen la producción y acceso a la información y servicios a través de interacciones con el Gobierno[2].

De esta forma, el citado documento de la OCDE estipula 12 recomendaciones para que sean tenidas en cuenta por aquellos Gobiernos que tienen el objetivo de desarrollar e implementar estrategias de gobierno digital. Estas son:

1. Asegurar mayor transparencia, apertura e integración de procesos y operaciones del gobierno (Ensure greater transparency, openness and inclusiveness of government processes and operations).
2. Fomentar el compromiso y participación de actores públicos, privados y de la sociedad civil en la formulación de políticas, y diseño y entrega de servicios públicos (Encourage engagement and participation of public, private and civil society stakeholders in policy making and public service design and delivery).
3. Crear una cultura orientada a la información en el sector público (Create a data-driven culture in the public sector).
4. Reflejar en enfoque a la gestión de riesgos para direccionar los problemas en seguridad digital y privacidad, e incluir la adopción de medidas de seguridad efectivas y apropiadas (Reflect a risk management approach to addressing digital security and privacy issues, and include the adoption of effective and appropriate security measures).
5. Asegurar el liderazgo y el compromiso político hacia la estrategia (Secure leadership and political commitment to the strategy).

[2] OECD, Recommendation of the Council on Government Strategies, Public Governance and Territorial Development Directorate. 15th July 2014. Disponible en http://www.oecd.org/gov/public-innovation/Recommendation-digital-government-strategies.pdf

6. Asegurar el uso coherente de tecnologías digitales en los ámbitos políticos y niveles de gobierno (Ensure coherent use of digital technologies across policy areas and levels of government).

7. Establecer marcos organizacionales y de gobernanza efectivos para coordinar la implementación de la estrategia digital en y dentro de los niveles de gobierno (Establish effective organizational and governance frameworks to co-ordinate the implementation of the digital strategy within and across levels of government).

8. Fortalecer la cooperación internacional con otros gobiernos (Strengthen international co-operation with other governments).

9. Desarrollar casos de negocio claros para soportar la financiación y orientar la implementación de proyectos de tecnología digital (Develop clear business cases to sustain the funding and focused implementation of digital technologies projects).

10. Reforzar las capacidades institucionales para administrar y monitorear la implementación de proyectos (Reinforce institutional capacities to manage and monitor projects' implementation).

11. Procurar tecnologías digitales basadas en la evaluación de los activos existentes (Procure digital technologies based on assessment of existing assets).

12. Asegurar que los marcos jurídicos y normativos generales permiten oportunidades digitales para ser aprovechadas (Ensure that general and sector-specific legal and regulatory frameworks allow digital opportunities to be seized).[3]

[3] OECD, Recommendation of the Council on Government Strategies. Disponible en https://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf

En tercer lugar, es importante tener en cuenta que la Comisión de Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), que es "principal órgano jurídico del sistema de las Naciones Unidas en el ámbito del derecho mercantil internacional…dedicado a la reforma de la legislación mercantil a nivel mundial"[4], tiene como finalidad emitir recomendaciones a los países miembros de Naciones Unidas respecto a la legislación mercantil, en aras que adopten al interior de sus ordenamientos jurídicos, normas que desarrollen materias relativas, por ejemplo, a comercio electrónico, firmas electrónicas, etc. Todo ello con el fin de lograr la uniformidad y estandarización de conceptos. Es así que su función consiste en "modernizar y armonizar las reglas del comercio internacional"[5].

Atendiendo lo anteriormente señalado, la CNUDMI profirió dos leyes modelos que han sido cardinales frente al uso de medios electrónicos y el robustecimiento jurídico de las transacciones que se llevan a cabo a través de este entorno, mediante el uso de mecanismos tecnológicos que provean validez jurídica y probatoria. Estas leyes modelos son las de Comercio Electrónico de 1996 y la de Firmas Electrónicas de 2001, las cuales precisamente reconocen que "un número creciente de transacciones comerciales internacionales se realizan por el medio de comunicación habitualmente conocido como comercio electrónico, en el que se usan métodos de comunicación, almacenamiento y autenticación de la información sustitutivos de los que utilizan papel"[6]. De esta forma, estas leyes modelos introducen conceptos jurídicos en la esfera internacional, tales como el de mensajes de datos, equivalencia funcional, autenticación electrónica, firma electrónicas, terceros intermediarios, entre otros.

---

[4] Comisión de Naciones Unidas para el Derecho Mercantil Internacional. Disponible en https://uncitral.un.org/es/about
[5] Ibidem.
[6] Ley Modelo de la CNUDMI sobre Firmas Electrónicas de 2001, página 8. Disponible en http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf

En primera instancia, respecto a Frente a la Ley de Comercio Electrónico de 1996, es de anotar que la CNUDMI ha señalado que "los objetivos de la Ley Modelo, entre los que figuran el de permitir o facilitar el empleo del comercio electrónico y el de conceder igualdad de trato a los usuarios de mensajes consignados sobre un soporte informático que a los usuarios de la documentación consignada sobre papel, son esenciales para promover la economía y la eficiencia del comercio internacional. Al incorporar a su derecho interno los procedimientos prescritos por la Ley modelo para todo supuesto en el que las partes opten por emplear medios electrónicos de comunicación, un Estado estará creando un entorno legal neutro para todo medio técnicamente viable de comunicación comercial"[7].

Ahora bien, la CNUDMI ha planteado que la manera de lograr precisamente esa igualdad en el trato respecto al entorno físico y el entorno electrónico se sustenta en el principio de Equivalencia Funcional que permite equiparar, desde el punto de vista jurídico, a los documentos, transacciones, operaciones, trámites, entre otros, que se llevan a cabo en medios electrónicos con respecto a sus homólogos en papel. Al respecto, es de anotar que la CNUDMI indica que "un mensaje de datos no es, de por sí, el equivalente de un documento de papel, ya que es de naturaleza distinta y no cumple necesariamente todas las funciones imaginables de un documento de papel. Por ello se adoptó en la Ley Modelo un criterio flexible que tuviera en cuenta la graduación actual de los requisitos aplicables a la documentación consignada sobre papel: al adoptar el criterio del "equivalente funcional", se prestó atención a esa jerarquía actual de los requisitos de forma, que sirven para dotar a los documentos de papel del grado de fiabilidad, inalterabilidad y rastreabilidad que mejor convenga a la función que les haya sido atribuida"[8]. De esta forma, la equivalencia

[7] Ley Modelo de la CNUDMI sobre Comercio Electrónico de 1996, p 17. Disponible en https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf
[8] Ibidem, p 28.

funcional no consiste en afirmar que el mensaje de datos, operación, transacción o trámite electrónico sea exactamente igual a su homólogo en papel, sino simplemente indicar que es posible equipararlos desde sus diferentes entornos.

De lo previamente descrito, se desprende que la equivalencia funcional, como fue explicada, puede comprender varias manifestaciones, dentro de las cuales se encuentra la de "Firma" que tiene como punto de partida la autenticación electrónica. Al respecto, desde años atrás "El creciente empleo de técnicas de autenticación electrónica en sustitución de las firmas manuscritas y de otros procedimientos tradicionales de autenticación ha planteado la necesidad de crear un marco jurídico específico para reducir la incertidumbre con respecto a las consecuencias jurídicas que pueden derivarse del empleo de dichas técnicas modernas (a las que puede denominarse en general "firmas electrónicas")"[9]. De esta forma, frente a los procesos de validación de identidad que se surten en el entorno físico y los mecanismos de firma manuscritos, los cuales por ejemplo, pueden ser llevados a cabo por empresas en el sector financiero que ofrecen sus servicios y productos a usuarios en el mercado y que ahora tienen la intención que sean ofrecidos a través de canales virtuales, el concepto de autenticación electrónica y de firma electrónica, eje central de esta temática.

En desarrollo de lo anteriormente expuesto, la CNUDMI a través del artículo 7º de su Ley Modelo de Comercio Electrónico, consagra el equivalente funcional de Firma, estableciendo que esta última tiene diversas funciones, a saber: "identificar a una persona; dar certeza a la participación personal de esa persona en el acto de firmar; y asociar a esa persona con el contenido de un documento. Se observó que una firma podía desempeñar además diversas otras funciones, según

[9] Ley Modelo de la CNUDMI sobre Firmas Electrónicas de 2001, página 8. Disponible en http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf p 19

la naturaleza del documento firmado. Por ejemplo, podía demostrar la intención de una parte contractual de obligarse por el contenido del contrato firmado; la intención de una persona de reivindicar la autoría de un texto; la intención de una persona de asociarse con el contenido de un documento escrito por otra; (…)"[10] (subrayado fuera del texto). En consecuencia, la firma electrónica, que incorpora necesariamente un proceso de validación de identidad y que una persona se vincule con lo que está firmando, se convierte en el equivalente de una firma manuscrita.

Aunado a lo anterior, la Ley Modelo de Comercio Electrónica también trae a colación un concepto que, de igual forma, redunda en brindar mayor robustez a las operaciones, trámites, transacciones o documentos que se llevan al entorno electrónico, este concepto es el de "intermediario". El intermediario en relación con un determinado mensaje de datos es "toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él", siendo así que dentro de estos se encuentran "los operadores de las redes y otros intermediarios pueden prestar servicios adicionales "con valor añadido" como los de formatear, traducir, consignar, autenticar, certificar y archivar los mensajes de datos y prestar además servicios de seguridad respecto de las operaciones electrónicas"[11]. De esta forma, estos intermediarios se convierten en terceros de confianza que pueden blindar jurídica y técnicamente las transacciones que se surten en medios electrónicos.

Por otra parte, se encuentra la Ley Modelo de Firmas Electrónica de la CNUDMI de 2001 que también respalda lo descrito previamente. Al respecto, indica que la firma electrónica ha sido reconocida como el género dentro del cual se encuentran diversos especies o tipos de firmas electrónicas, como por ejemplo la firma digital, la firma biométrica (que hace uso de datos

[10] Ley Modelo de la CNUDMI sobre Comercio Electrónico de 1996, p 17. Disponible en https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf
[11] Ibidem.

biométricos), el usuario y contraseña, los one time passwords (OTP), el PIN, entre otros[12], todos estos mecanismos que permiten validar la identidad de una persona y que esta última se vincule con el contenido de lo que está firmando.

Ahora bien, dicha ley señala que debe darse una neutralidad tecnológica en el uso de los mecanismos de autenticación electrónica, por lo cual "este enfoque neutral con los medios técnicos, utilizado también en la Ley Modelo de la CNUDMI sobre Comercio Electrónico, tiene la finalidad de abarcar, en principio, todas las situaciones de hecho en que se genera, archiva o comunica información, con independencia de cuál sea el soporte en el que se consigne la información (véase la Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, párr. 24). Las palabras "entorno jurídico neutro", utilizadas en la Ley Modelo de la CNUDMI sobre Comercio Electrónico, reflejan el principio de la no discriminación entre la información consignada sobre papel y la información comunicada o archivada electrónicamente. La nueva Ley Modelo refleja asimismo el principio de que no debe discriminarse ninguna de las diversas técnicas que pueden utilizarse para comunicar o archivar electrónicamente información, un principio a veces denominado "de neutralidad tecnológica"[13].

De igual forma, ha señalado la CNUDMI que "Ante la evolución de las innovaciones tecnológicas, la Ley Modelo establece criterios para el reconocimiento jurídico de las firmas electrónicas independientemente de la tecnología utilizada (a saber, firmas electrónicas basadas en la criptografía asimétrica; los dispositivos biométricos (que permiten la identificación de personas por sus características físicas, como su geometría manual o facial, las huellas dactilares, el reconocimiento de la voz o el escáner de la retina, etc.); la criptografía simétrica; la utilización de

[12] Ley Modelo de la CNUDMI sobre Firmas Electrónicas de 2001. Disponible en http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf
[13] Ibidem.

números de identificación personal (NIP); la utilización de "contraseñas" para autenticar mensajes de datos mediante una tarjeta inteligente u otro dispositivo en poder del firmante; versiones digitalizadas de firmas manuscritas; la dinámica de firmas; y otros métodos, como la selección de un signo afirmativo en la pantalla electrónica mediante el ratón)"[14].

Aunado a lo anterior, la Ley Modelo sobre Firmas Electrónicas señaló en materia de infraestructura de clave pública que una forma de resolver algunos de los problemas que se presentan en ésta son "el empleo de uno o más terceros para vincular a un firmante identificado o el nombre del firmante a una clave pública determinada. El tercero se conoce en general, en la mayoría de las normas y directrices técnicas, como "entidad certificadora", "prestador de servicios de certificación" o "proveedor de servicios de certificación" (en la Ley Modelo, se ha elegido el término de "prestador de servicios de certificación"). En unos cuantos países, esas entidades certificadoras están siendo organizadas en forma jerárquica en lo que suele denominarse una infraestructura de clave pública (ICP)". En ese sentido, de lo antes expuesto se desprende que la figura de entidades de certificación digital, es decir, aquellos terceros de confianza que pueden ser certificadores frente a terceros, respecto a mecanismos de autenticación electrónica, validación de identidad y firmas electrónicas, son reconocidas por el marco jurídico internacional.

Es de resaltar que la CNUDMII también hace énfasis, en su Ley Modelo de Firmas Electrónicas, respecto al papel que ejercen las entidades de certificación digital en el entorno electrónico, al indicar que "las autoridades gubernamentales y legislativas están preparando leyes sobre cuestiones relacionadas con las firmas electrónicas, incluido el establecimiento de infraestructuras de clave pública (ICP) (…)".

[14] Ibidem, p 43.

La ICP o PKI fue un estándar que se consagró en la Ley Modelo de Firmas Electrónicas, siendo así que se reconoció que el mismo necesariamente exigía la presencia de una proveedor o prestador de servicios de certificación digital, en aras de vincular mediante un certificado digital, un par de claves a un posible firmante. Estos proveedores o terceros de confianza, reconocidos por las leyes modelo de la CNUDMI, tienen como función principal "vincular una clave pública con un titular determinado. El "receptor" del certificado que desee confiar en una firma numérica creada por el tenedor que figura en el certificado puede utilizar la clave pública indicada en ese certificado para verificar si la firma numérica fue creada con la clave privada correspondiente"[15].

Así las cosas, en razón a la importancia de este estándar, resulta necesario involucrar a un prestador de servicios de certificación digital que garantice las transacciones comerciales en medios electrónicos. Al respecto, es importante recordar que la estructura jerárquica de cualquier entidad de certificación se divide de la siguiente manera:

- La autoridad de certificación (CA): es la entidad encargada de generar los certificados mediante la ejecución de operaciones criptográficas sobre medios de almacenamiento y procesamiento seguros, normalmente implementados en un módulo de seguridad en hardware.
- La autoridad de registros (RA): es la entidad encargada de administrar la relación entre entidades finales y certificados digitales, es decir mantiene el registro de los usuarios que solicitan certificados ante la entidad de certificación.

[15] Ibidem.

El reconocimiento que realizó la CNUDMI sobre el citado tipo de entidades, llevó a que en la Ley 527 de 1999 que hace parte del ordenamiento jurídico colombiano, se incorporara la figura de las Entidades de Certificación Digital, como proveedores de servicios de certificación digital.

1.2. Autenticación Electrónica: caracteres a nivel internacional

La Autenticación Electrónica consiste en validar la identidad de una persona cuando adelanta trámites ante una entidad, ya sea del sector público o privado, por medios electrónicos, con el objetivo de mitigar el riesgo de suplantación de su identidad, lo cual implica que necesariamente el atributo de autenticidad se torna vital a la hora de interactuar en el entorno electrónico. De esta forma, la autenticación electrónica es "el proceso de establecer confianza en las identidades de los usuarios presentadas electrónicamente ante un sistema de información"[16].

Ahora bien, es importante tener presente que la autenticación electrónica puede abarcar no solo la verificación de respecto a la identidad del usuario con el cual se está interactuando en medios electrónicos, sino también la autenticación de la integridad del mensaje de datos, documento electrónico, trámites o transacción, es decir, que la información o la transacción no haya sido modificada o alterada desde la primera vez en que se generó.

La revisión respecto al tipo mecanismos de autenticación electrónica que deben ser utilizados en determinada transacción u operación, necesariamente conlleva el análisis de un escenario jurídico y un escenario tecnológico, en el marco de un análisis fuerte de riesgos por parte de la entidad que desea emplear el mecanismo de autenticación electrónica y firma electrónica para el ofrecimiento de sus servicio y productos al público. Por una parte, técnicamente, se debe evaluar si el mecanismo a utilizar que se encuentra respaldado por un hardware y software o solo software, permite

[16] National Institute of Standards and Technology – NIST (5), Abril 2006.

identificar de manera confiable al usuario del trámite, de tal manera que dicho mecanismo sea lo más seguro posible. Por otra parte, jurídicamente se buscará que el mecanismo cumpla los requisitos previstos en la normativa.

En aras de determinar los mecanismos de autenticación electrónica, la Comisión de Naciones Unidas para el Derecho Mercantil Internacional ha establecido que existen diversos tipos de factores de autenticación electrónica, así:

"Los métodos de autenticación y firma electrónicas pueden clasificarse en tres categorías, a saber: los que se basan en lo que el usuario o el receptor sabe (por ejemplo, contraseñas, números de identificación personal (NIP)), los basados en las características físicas del usuario (por ejemplo, biométrica) y los que se fundamentan en la posesión de un objeto por el usuario (por ejemplo, códigos u otra información almacenados en una tarjeta magnética. En una cuarta categoría se podría incluir a diversos tipos de métodos de autenticación y firma que, sin pertenecer a ninguna de las categorías arriba citadas, podrían también utilizarse para indicar el iniciador de una comunicación electrónica (por ejemplo, un facsímil de una firma manuscrita, o un nombre mecanografiado en la parte inferior de un mensaje electrónico). Entre las tecnologías que se utilizan en la actualidad figuran las firmas digitales en el marco de una infraestructura de clave pública (ICP), dispositivos biométricos, NIP, contraseñas elegidas por el usuario o asignadas, firmas manuscritas escaneadas, firmas realizadas por medio de un lápiz digital, y botones de pulsación del tipo de "sí" o "aceptar" o "acepto""[17].

[17] Comisión de las Naciones Unidas para el Derecho Mercantil Internacional en su documento de "fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas". Disponible en https://www.uncitral.org/pdf/spanish/texts/electcom/08-55701_Ebook.pdf

De esta forma, existen diversos mecanismos de autenticación electrónica que permitirán la validación de identidad de un usuario en el entorno electrónico y que adicionalmente podrán, servir como mecanismos de firma electrónica, con base en los cuales el usuario se obligue con la transacción, con los términos y condiciones de adquisición de un producto o servicio o incluso con la aceptación de un contrato.

Ahora bien, los factores de autenticación, se definen de conformidad con los siguientes criterios:

- **"Algo que el usuario sabe":** Son patrones que memoriza el usuario y que él únicamente conoce. Estos patrones pueden ser cadenas de texto alfanuméricas, números o trazados (ejemplos: contraseñas, número de identificación personal-PIN).
- **"Algo que el usuario tiene":** Son elementos físicos que el usuario tiene en su poder, como por ejemplo la tarjeta de identificación, teléfono celular, token físico, entre otros.
- **"Algo que el usuario es":** Son características físicas únicas e irrepetibles asociadas al usuario, como por ejemplo la identificación de la persona mediante su huella dactilar, el patrón retiniano, el rostro, la voz, la secuencia de ADN, la rúbrica.

Es de resaltar que los sistemas de autenticación que contemplan los tres factores son los más robustos en cuanto a seguridad. El sistema puede contemplar los tres factores para identificarse ante él, o bien, combinaciones entre factores.

En virtud de lo expuesto anteriormente, son muchas las posibilidades para hacer uso de mecanismos de autenticación electrónica, sin embargo, la escogencia de uno u otro mecanismo debe verse enmarcada en los siguientes planteamientos:

- Técnicamente ningún mecanismo o herramienta tecnológica es cien por ciento segura.

- Es necesario conocer el trámite o proceso que requiere ser adelantado por parte de la compañía que va a implementar el mecanismo de autenticación electrónica y firma electrónica y los riesgos jurídicos asociados al mismo, a fin de determinar si resulta necesario contar con métodos más robustos o menos robustos que brinden determinado grado de seguridad en el proceso de validación de identidad que adelantará la compañía ante sus usuarios.
- Atendiendo lo anterior, es importante contar, por una parte, con la definición del proceso donde funcionará el mecanismo, y por otra, con una matriz de riesgos que le permita identificar el tipo de riesgos que desea mitigar, su probabilidad de ocurrencia y las acciones que actualmente implementa para mitigarlos.

Es de resaltar que en el plano internacional se han gestado avances en materia de cómo clasificar estos riesgos y por lo tanto la seguridad requerida para efectos, tienen como fundamento el Reglamento de la Unión Europea No. 910/2014 del Parlamento Europeo y del Consejo del 23 de julio de 2014 que desarrolla lo concerniente a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado.

Es de suma importancia tener en cuenta que el Reglamento de la Unión Europea no solo estableció los niveles de seguridad en el marco de mecanismos de autenticación o identificación electrónica, sino que además estableció qué tipo de mecanismos se debían usar para adelantar trámites y servicios electrónicos con el Estado en aras de generar la máxima seguridad.

Este Reglamento consagra distintos tipos de niveles de seguridad de identificación electrónica, señalando que un sistema de identificación electrónica deberá especificar los niveles de seguridad bajo, sustancial y alto para los medios de identificación electrónica expedidos en virtud del mismo.

En ese sentido, “el nivel de seguridad bajo se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado limitado de confianza en la identidad pretendida o declarada de una persona; el nivel de seguridad sustancial se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado sustancial de confianza en la identidad pretendida o declarada de una persona; el nivel de seguridad alto se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado de confianza en la identidad pretendida o declarada de una persona superior al medio de identificación electrónica con un nivel de seguridad sustancial”[18].

En virtud de lo antes señalado es importante tener en cuenta que el Reglamento establece que “si un Estado miembro requiere una firma electrónica avanzada con el fin de utilizar un servicio en línea ofrecido por un organismo del sector público, o en nombre del mismo, dicho Estado miembro reconocerá las firmas electrónicas avanzadas, las firmas electrónicas avanzadas basadas en un certificado cualificado de firma electrónica y las firmas electrónicas cualificadas por lo menos en los formatos o con los métodos definidos en los actos de ejecución contemplados en el apartado. Si un Estado miembro requiere una firma electrónica avanzada basada en un certificado cualificado con el fin de utilizar un servicio en línea ofrecido por un organismo del sector público, o en nombre del mismo, dicho Estado miembro reconocerá las firmas electrónicas avanzadas basadas en un certificado cualificado y las firmas electrónicas cualificadas por lo menos en los formatos o con los métodos definidos en los actos de ejecución”[19]. De esta forma se observa que ante trámites o servicios que sean prestados por el Estado es importante contar con altos niveles de seguridad, por

[18] REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, p 16. Disponible en https://www.boe.es/doue/2014/257/L00073-00114.pdf
[19] Ibidem, p 28.

tal motivo, la firma electrónica avanzada (es decir la firma digital) y la firma electrónica cualificadas son de suma relevancia si se desea satisfacer un nivel de confianza y seguridad alto.

En este orden de ideas, los niveles de seguridad desarrollados por la Directiva de la Unión Europea, implica que para los riesgos bajos se encontrarían las firmas electrónicas simples, y nombre de usuario y contraseña; para riesgos medio, se encontraría la biometría o los certificados electrónicos emitidos por entidades de certificación digital. Finalmente, para riesgos altos, tal y como lo señala Reglamento se deberán utilizar mecanismos como firmas electrónicas avanzadas y cualificadas, cuyas homólogas en otras legislaciones son las firmas digitales.

Por último, es importante recordar que todos y cada uno de estos mecanismos son válidos jurídicamente desde que garanticen atributos jurídicos como son la autenticidad e integridad. De esta manera, determinar la aplicación de uno u otro, debe ser revisado con bastante detalle pues no se puede desconocer que existe el principio de neutralidad tecnológica, el cual ejercer un rol preponderante en el entorno electrónico.

Este principio ha sido precisamente fuente de mucho desarrollo, especialmente a través de diversos doctrinantes. Dicho principio se reconoce como "(…) un hecho evidente: la tecnología cambia constantemente. Si la ley se "casa" con una tecnología en particular, muy seguramente la norma quedará obsoleta rápidamente. (…). La Ley 527 exige algunos requisitos técnicos fundamentales, pero no señala la tecnología específica que se deba utilizar. Así las cosas, si la ley requiere que se utilicen tecnologías confiables para garantizar la integridad de un mensaje de datos, el operador puede escoger la tecnología que desee, siempre y cuando sea fiable a la luz del Estado de la técnica y del momento histórico que se requiera"[20].

[20] CASTRO, Marcela. Fundamentos de derecho de los negocios para no abogados: Capítulo VII Comercio Electrónico, Nelson Remolina Angarita. Bogotá: Editorial Temis, 2013. p 225.

Ahora bien, asimismo otros doctrinantes han señalado que "una disposición tecnológicamente neutra, en cambio, establece sus disposiciones sobre la base de las funciones que cumple o puede cumplir cualquier tecnología de identificación, sin importar el proceso y la estructura que utiliza para identificar, sin el cumplimiento de los requisitos que exige. (…). Cualquiera sea el acercamiento del ordenamiento jurídico, la finalidad última de la disposición será reconocer valor jurídico a las nuevas tecnologías de identificación. (…). En definitiva, implica una regulación abierta que no establezca impedimentos al uso de una tecnología en particular, en la medida que ella cumpla con los requisitos y funciones básicas que exige. La neutralidad tecnológica deja libre y expedita la decisión abierta del usuario para elegir el proceso de identificación que estime adecuado. Por lo anterior, en la medida que el proceso de identificación se acomode y sea compatible con las disposiciones jurídicas, éstas serán aplicables a dicho proceso"[21]. En ese sentido, es importante tener presente que los usuarios pueden llegar a elegir sus métodos de autenticación, tomando en cuenta los requisitos previstos en su ordenamiento jurídico.

Teniendo en cuenta lo antes señalado, es claro que el principio de neutralidad tecnológica aunque puede tener diversas interpretaciones todas estas válidas y complementarias en cuanto a lo que engloba este principio. Una de estas se refiere a la libre adopción de las tecnologías, y como lo ha dicho la CNUDMI, a alentar el uso de diversos tipos de tecnologías, a reconocer jurídicamente los diversos tipos de tecnologías utilizadas independientemente de la tecnología utilizada, otras se refieren a la no discriminación entre la información consignada sobre papel y la información comunicada o archivada electrónicamente, y otras se refieren a que el usuario sea libre para elegir y escoger sus métodos de autenticación.

[21] TRIVELLI GONZÁLEZ, María Paz. El Principio de Neutralidad Tecnológica en la Ley No 19.799. Disponible en http://www.derechoinformatico.uchile.cl/index.php/RCHDI/article/viewFile/10675/10953

Así las cosas, si bien todos los tipos de firmas electrónicas son válidos jurídicamente y a la luz del ordenamiento jurídico colombiano, sin embargo, es de anotar que no todos los mecanismos de conformidad con la normativa del país donde se encuentre tendrán las mismas características y atributos jurídicos, pues si estos fueran iguales entonces el legislador del país correspondiente no se tomaría la molestia de diferenciarlos.

En este orden de ideas, lo expuesto en el presente capítulo permite concluir que el entorno electrónico desde años atrás viene cobrando mucha importancia. Precisamente, múltiples iniciativas, lineamientos e incluso normas desde el ámbito internacional han venido respaldando el uso de estos medios, lo cual conlleva necesariamente al uso de mecanismos de autenticación electrónica y terceros de confianza que permiten robustecer estas operaciones, transacciones o trámites. De igual forma, son múltiples los tipos de mecanismos de autenticación electrónica y firmas electrónicas que pueden ser utilizados, sin embargo, la escogencia de uno u otro dependerá necesariamente de un análisis exhaustivos, desde el punto de vista de riesgos y de seguridad, por parte de la compañía que desee implementarlos, lo cual no podrá desconocer principios tan importantes en el entorno electrónico, como es la equivalencia funcional.

II. Marco Jurídico Nacional

2.1.Mecanismos de Validación de identidad

La equivalencia funcional es un principio fundamental en medios electrónicos. Es de resaltar que la norma marco en materia de comercio electrónico en el ordenamiento jurídico colombiano es la Ley 527 de 1999 que se desprende de la Ley Modelo de Comercio Electrónico de la Comisión de Naciones Unidas sobre el Derecho Mercantil (CNUDMI).

Previo a entrar a desarrollar el principio de equivalencia funcional, es de suma importancia entablar una breve descripción respecto a la Ley 527 de 1999.

La ley 527 de 1999 constituye el marco jurídico integral y general que autoriza el uso de los mensajes de datos en todas las actividades de los sectores público y privado. Aunque regula aspectos de dicha materia y es conocida como la ley de comercio electrónico, fue redactada de manera que comprenda todas las actividades en que se involucre el uso de mensajes de datos, salvo el contrato de transporte y los documentos de transporte.

Al respecto, es de notar que la Corte, concretamente, señaló que: "(…) la ley 527 de 1999 no se restringe a las operaciones comerciales sino que hace referencia en forma genérica al acceso y uso de los mensajes de datos, lo que obliga a una comprensión sistemática de sus disposiciones con el conjunto de normas que se refieren a este tema dentro de nuestro ordenamiento jurídico"[22].

Ahora bien, la noción de mensajes de datos es el núcleo fundamental de la ley y de los procesos de inmaterialización, toda vez que ellos se convierten en otro medio jurídicamente válido para manifestar la voluntad, así como se convierten en un medio probatorio. De esta forma, un mensaje de datos, de acuerdo a lo previsto en el literal a) del artículo 2 de la Ley 527 de 1999 es aquella "información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax".

Al respecto, es de anotar que de esta noción se desprenden distintitos tipos de mensajes de datos, entre estos, los documentos electrónicos. Los mensajes de datos pueden tener distintas manifestaciones como se desprende de su definición, así, por ejemplo, una manifestación pueden

[22] Corte Constitucional, Sentencia C- 831 de 2001, M.P Alvaro Tafur Gálvis.

ser los documentos electrónicos. Vale recordar, como lo ha indicado la Doctrina, que estos últimos son la representación electrónica de hechos jurídicamente relevantes susceptibles de ser representados en forma humanamente comprensible. Es de notar, que según el artículo 243 de la Ley 1564 de 2012, los documentos son "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". De lo antes citado, es posible evidenciar que un documento es un objeto mueble que no necesariamente se sujeta a un soporte material sino que también puede ser inmaterial toda vez que puede tener carácter representativo o declarativo. De igual forma, vale la pena recordar que el artículo 247 de la citada ley estableció expresamente que "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".

De acuerdo con el artículo 5 de la Ley 527 de 1999, no pueden negarse efectos jurídicos, validez o fuerza obligatoria a cierta información, por el solo hecho de que esté en forma de mensajes de datos. En consecuencia, los mensajes de datos son un medio probatorio reconocido legalmente.

Es de resaltar que la ley 527 de 1999 ha sido enfática no solo en reconocer los efectos jurídicos, validez o fuerza obligatoria a la información generada a través de mensajes de datos, sino también en reconocer la su admisibilidad como medio de prueba, siendo así que el mensaje de datos gozará de fuerza probatoria de acuerdo con lo dispuesto en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil. En ese sentido, la Ley

527 de 1999 reconoce de manera expresa el valor probatorio que tienen los mensajes de datos, dentro de los cuales se encuentran los documentos electrónicos, en materia procesal. Al respecto, es de recordar que si bien el Código de Procedimiento Civil fue derogado por la Ley 1564 de 2012, no obstante esta última ley en su Capítulo IX del Título Único de la Sección Tercera relativa a régimen probatorio dispuso una serie de disposiciones generales en respecto a los mensajes de datos, siendo así que dicha ley reconoció lo desarrollado por la Ley 527 de 1999.

Así las cosas, habiendo descrito a grandes rasgos la esencia y el ámbito de aplicación de la Ley 527, es importante precisar que el principio del equivalente funcional, aunque no está expresamente definido en la Ley 527 de 1999, se caracteriza por lo siguiente: permite que un mensaje de datos (entendido como aquella información almacenada, transformada, generada, enviada, recibida, y en general tratada por medios electrónicos) goce del mismo valor jurídico y probatorio que aquella información transmitida por medios físicos, como es el papel. En ese sentido, dicho mensaje de datos recibirá el mismo tratamiento jurídico que la información soportada en medios físicos.

De conformidad con lo antes mencionado, la equivalencia funcional según lo dispuesto en la Ley 527 de 1999, se compone entonces de cuatro manifestaciones, a saber: (i) Escrito; (ii) Original; (iii) Firma; y (iv) Archivo y Conservación. Así las cosas, conforme a la ley antes citada, el documento electrónico será el equivalente funcional de su homólogo en medios físicos, cuando cumpla las manifestaciones anteriormente indicadas.

En este orden de ideas, una vez descrito el principio de equivalencia funcional, se dará paso a desarrollar cada una de sus manifestaciones.

2.1.1. Equivalente funcional de Escrito

El artículo 6 de la Ley 527 de 1999 establece lo siguiente: "*Artículo 6°. Escrito. Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un*

mensaje de datos, si la información que éste contiene es accesible para su posterior consulta. Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas prevén consecuencias en el caso de que la información no conste por escrito".

Este equivalente se centra en indicar que es necesario que la información pueda ser accesible, es decir, consultada cuando sea necesario. Al respecto, ello supone contar con un hardware, por ejemplo un computador, conforme al cual se pueda verificar que el mensaje de datos existe, y un software, es decir, un programa o sistema que traduzca a un lenguaje inteligible, dicho mensaje de datos. De esta forma, solo contando con un hardware y software se podrá afirmar que el mensaje de datos existe y que está disponible para su consulta.

2.1.2. Equivalente funcional de Original

En el escenario físico "original" es el primer documento creado en el tiempo. Por el contrario, en el entorno electrónico, no se vincula exclusivamente al primer soporte físico creado en el tiempo por cuanto pueden existir múltiples originales. Por el contrario, dicho concepto se vincula con el de "integridad" del contenido del mensaje de datos. El artículo 8 de la Ley 527 de 1999 establece que se garantiza la noción de original en medios electrónicos, cuando: a) Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma y b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar. Es tas manera, es original en el entorno electrónico, aquel documento que goza de integridad, es decir, que no ha sido alterado o modificado desde el primer momento en que se creó y en el formato en que se generó.

2.1.3. Equivalente funcional de Firma

Según el Diccionario de la Real Academia de la Lengua Española (DRAE), la firma es el "nombre y apellido, o título que una persona escribe de su propia mano en un documento, para darle autenticidad o para expresar que aprueba su contenido"[23]. Asimismo, Planiol y Ripert dicen que "la firma es una inscripción manuscrita que indica el nombre de una persona que entiende hacer suyas las declaraciones del acto[24].

Al respecto, surge el reto de garantizar que la firma en medios electrónicos tenga la misma validez jurídica que la firma en medios electrónicos. En cualquiera de estos dos escenarios, la firma siempre estará vinculada con el concepto de "Autenticidad", el cual consiste en garantizar que la persona que está remitiendo un mensaje de datos o que lo está firmando, es realmente quien dice ser.

Es de anotar que a la luz de la jurisprudencia, corporaciones como la Corte Suprema de Justicia han manifestado la importancia de la firma: "La firma es, pues, requisito imprescindible para que un documento tenga valor probatorio, ya que sin ella, salvo aceptación expresa de la parte o de sus causahabientes —según el caso—, no podrá establecerse con certeza quién es el autor, esto es, lisa y llanamente su autenticidad, siendo necesario recordar que, por firma, se entiende "la expresión del nombre del suscriptor o de alguno de los elementos que la integren o de un signo o símbolo empleado como medio de identificación personal" (art. 826, C. de Co.), omnicomprensiva noción —ex lege— que está a tono, en la hora de ahora, con el empleo de los adelantos tecnológicos (cibernéticos, robóticos, informáticos, etc.), en virtud de los cuales se ha desarrollado el concepto de firma electrónica o digital que, según la Ley 527 de 1999, se acota de paso, tiene idéntica fuerza

[23] Diccionario de la Lengua Española. Real Academia Española, Vigésima segunda edición, Madrid, 2001.
[24] PLANIOL, RIPERT, Traite Pratique de Droit Civil Francais, T. VIII, No. 1458

y efectos de la firma manuscrita, cuando se reúnan los requisitos —claro está— allí señalados relativos a la verificación de la individualidad de la misma"[25].

Ahora bien, el concepto de firma electrónica será abordado con mayor detalle en los próximos capítulos.

2.1.4. Equivalente funcional de Archivo y Conservación

Respecto a esta manifestación la Ley 527 en sus artículos 12 y 13 establece que cuando la Ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre y cuando se cumplan con las siguientes condiciones: a. La información debe ser accesible para su posterior consulta. b. El mensaje de datos o documento conservado, debe estar en el formato en el que se haya generado, enviado o recibido, o en un formato que permita verificar que se reprodujo con exactitud la información conservada. c. La conservación la información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o reproducido el documento. De igual forma, establece el inciso final expresamente que "Los libros y papeles del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta". De esta manera, esta manifestación recoge a la de Escrito, por cuanto exige también que la información sea accesible para su posterior consulta y adicionalmente establece una serie de requisitos que deberán cumplirse.

Finalmente, es de resaltar que todas y cada uno de estas manifestaciones, de conformidad con lo previsto en la Ley 527 de 1999, deberán ser garantizadas a través de mecanismos tecnológicos que serán revisados en los próximos capítulos.

[25] Sentencia de casación, Sala de Casación Civil, septiembre 4 de 2000, rad. 5565, M. P.: Jaramillo, C. I. Citada sentencia del 27 de agosto de 2003 (proceso 20166) de la Corte Suprema de Justicia (CSJ), M. P.: Pulido de Barón, M.

2.2. Firmas Electrónicas

La doctrina ha señalado que "la confianza está estrechamente ligada a la seguridad. De no contar con medios electrónicos seguros las actividades no crecerán en las escalas deseables. En el contexto del comercio electrónico, puede entenderse como tener la seguridad de que a empresa va a realizar la transacción con las mismas o mayores garantías de las que tiene en el negocio tradicional. Determinados aspectos que involucran el desarrollo de la confianza y seguridad en el uso de medios electrónicos se puede resumir así: i) Identidad, implica estar seguros de que realizamos negocios con determinada persona y no con otra y que dicha persona existe y tiene capacidad jurídica. ii) confidencialidad, consiste en impedir que personas no autorizadas accedan a la información que queremos proteger. iii) Integridad, consiste en garantizar que los documentos electrónicos no sean alterados, modificados, falsificados o manipulados y iv) no repudio, consiste en tener la certeza de que los mensajes de datos son una forma válida de manifestar la voluntad y un medio de prueba"[26], siendo así que a través del no repudio el emisor no estará en posibilidad de negar el conocimiento de un mensaje de datos ni los compromisos adquiridos a través de este. Particularmente, cuando nos encontramos en medios electrónicos surgen los siguientes riesgos:

2.2.1. Suplantación:

Cuando se está en presencia de trámites, servicios, procesos y procedimientos que se llevan a cabo en papel existe un alto riesgo de suplantación toda vez que la persona que se presenta ante una entidad con el fin de adelantar un trámite o un procedimiento puede no ser quien dice ser, siendo así que se configuran actos fraudulentos. De igual forma, cuando se está en presencia de canales electrónicos de comunicación por ejemplo la red pública de internet, existen riesgos de que la persona con la que interactúe el sistema no sea la quien dice ser. La autenticidad que se refiere al

[26] CASTRO, Marcela. Fundamentos de derecho de los negocios para no abogados. Bogotá: Editorial Temis, 2013. p 212 y 213.

atributo requerido para mitigar el riesgo de suplantación, es un tema de la mayor importancia, pues la determinación del origen de un mensaje de datos es absolutamente necesaria en cualquier comunicación electrónica.

La determinación de la autoría es necesaria para verificar, entre otras cosas, la capacidad y competencia de las partes involucradas en una comunicación electrónica; por ejemplo, la representación legal o poder de representación de la persona jurídica o moral es la única que puede vincular de manera efectiva y legal a dicha persona jurídica o moral con la actuación. Este riesgo se mitiga a través del atributo de seguridad jurídica denominado autenticidad, sobre el cual dentro de la operación financiera desarrollada por medios electrónicos ha sido desarrollado por las Circulares Externas 052 de 2007 y 042 de 2013. La determinación del origen de las manifestaciones en los documentos que se pretenden desmaterializar o inmaterializar también será importante.

2.2.2. Alteración:

Cuando se está en presencia de trámites, servicios, procesos y procedimientos que se materializan en papel existe un alto grado de alteración de la información. De igual forma, los medios electrónicos y en general la información electrónica contenida en distintos tipos de extensiones de archivo por ejemplo, Word, Excel, puf, power point, o cualquier tipo de procesador de texto o imágenes y video son susceptibles a ser modificadas o alteradas. Un ejemplo práctico de ello es el hecho de que una persona sin ningún conocimiento previo en sistemas puede alterar un correo electrónico recibido únicamente sobre escribiendo en el texto y es posible remitirlo o guardarlo con un contenido que no es el original enviado por su emisor.

La integridad que se refiere al atributo requerido para mitigar el riesgo de alteración, consiste en la confirmación de que el mensaje de datos o información electrónica recibida corresponda a la enviada, por cuanto en la comunicación electrónica es susceptible de modificar cualquier parte del

mismo. La integridad hace alusión a que la información enviada a través del mensaje de datos no carezca de alguna de sus partes, como tampoco haya sido transformada.

En tal sentido, este es uno de los requisitos esenciales con los cuales se le da plena validez jurídica al documento electrónico. En el proceso de transmisión o envió de información electrónica existen trasiegos susceptibles de toma no autorizada de la información y posible modificación de la misma, así como la posibilidad de manipulación de la información a lo largo del ciclo de vida en el proceso de conservación y archivo.

2.2.3. Pérdida de confidencialidad:

Cuando se está en presencia de trámites, servicios, procesos y procedimientos que se adelantan en papel existe un alto grado de pérdida de confidencialidad en el manejo de documentos. Es de recordar que en materia de seguridad de la información el eslabón más débil es el ser humano, toda vez que es éste quien manipula de manera indiscriminada información de carácter confidencial, no siguiendo estrategias que le permitan impedir su divulgación, así también puede perder la información contenida en el soporte físico lo cual conlleva altos riesgos. De igual forma, en medios electrónicos la red pública internet, trae consigo innumerables ventajas de comunicación pero a su vez un reto en materia de seguridad y confidencialidad, ya que la información o sistemas en internet se exponen a la posibilidad de ser interceptados por personas no autorizadas. La confidencialidad que se refiere al atributo requerido para mitigar el riesgo de pérdida de confidencialidad implica que la información sólo sea compartida entre las personas u organizaciones autorizadas. La seguridad apropiada depende del nivel de confidencialidad de la información. La tecnología de cifrado de la firma digital y/o electrónica puede ser un camino en búsqueda de dicha garantía.

2.2.4. Conflictos en la fecha y hora:

En medios digitales la fecha y hora en la generación, envío y recepción de información electrónica juega un papel muy importante en materia probatoria, por ejemplo, la fecha y hora de generación de un documento en un procesador de texto vinculará la fecha y hora del computador de su emisor, y esta fecha podría estar errada, desincronizada, o no atender la fecha y hora del país donde se van a producir los efectos jurídicos de la transacción.

Así las cosas, en virtud de lo expuesto en los numerales anteriores, a continuación se presentan los atributos jurídicos que son importantes tener en cuenta en las transacciones en medios electrónicos:

Gráfica 1. Atributos jurídicos a garantizar en el entorno electrónico

ATRIBUTOS JURÍDICOS	EN QUÉ CONSISTE
Autenticidad	Garantizar la identidad del iniciador del mensaje de datos; permite saber si la persona es realmente quien dice ser, mitigando con esto riesgos de suplantación de identidad.
Integridad	Garantizar que el mensaje de datos no haya sido alterado o modificado una vez el mismo se ha creado.
No repudio	Garantiza que la persona no pueda negar el conocimiento de un mensaje de datos ni los compromisos adquiridos a través de este, por cuanto se presume que quería ser vinculado al mismo (presunción legal de la firma digital)
Disponibilidad	Garantizar la consulta de la información en medios electrónicos a lo largo del tiempo, asegurando su trazabilidad.
Confidencialidad	Impedir que terceros no autorizados accedan a la información que reposa en medios electrónicos, protegiendo los datos personales de aquellas personas que se autentican electrónicamente.

2.3. Mecanismos de Autenticación Electrónica y firmas electrónicas

Es importante señalar que el ordenamiento jurídico colombiano reconoce jurídicamente la noción de autenticación electrónica a través de las normas y disposiciones normativas que se presentan a continuación:

NORMAS PRINCIPALES EN AUTENTICACIÓN ELECTRÓNICA			
Temario	**Norma**	**Concepto**	**Definición**
Equipara a los mensajes de datos con los documentos en papel	ley 527 de 1999	Mensaje de datos (Artículos 2º y 5º)	Información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax
		Principio de Equivalencia Funcional (Artículos 6º, 8º, 7º, 28º, 12º y 13º)	Tiene como propósito legitimar los mensajes de datos o documentos electrónicos y equipararlos a los documentos en papel, mediante cuatro manifestaciones: i) escrito, ii) original, iii) firma y iv) archivo y conservación.
Mecanismos Autenticación electrónica	Ley 527 de 1999	Presunción del origen de un mensaje de datos (Artículo 17º)	Se presume que un mensaje de datos ha sido enviado por el iniciador, cuando: a) Haya aplicado en forma adecuada el procedimiento acordado previamente con el iniciador, para establecer que el mensaje de datos provenía efectivamente de éste, o b) El mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio
	Decreto 2364 de 2012 (compilado por el Decreto 1074 de 2015	Firma electrónica pactada mediante acuerdo (Artículo 7º)	Salvo prueba en contrario, se presume que los mecanismos o técnicas de identificación personal o autenticación electrónica según el caso, que acuerden utilizar las partes mediante acuerdo, cumplen los requisitos de firma electrónica. La parte que mediante acuerdo provee los métodos de firma electrónica deberá asegurarse de que sus mecanismos son técnicamente seguros y confiables para el propósito de los mismos. A

			dicha parte le corresponderá probar estos requisitos en caso de que sea necesario.
Firma electrónica	Ley 527 de 1999	Firma Electrónica simple (Artículo 7º)	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.
		Firma Digital (Artículo 28º)	Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo. Parágrafo. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos: 1. Es única a la persona que la usa. 2. Es susceptible de ser verificada. 3. Está bajo el control exclusivo de la persona que la usa. 4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada. 5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.
		Firma Electrónica certificada	Las entidades de certificación acreditadas por el Organismo Nacional de Acreditación de Colombia para prestar sus servicios en el país, podrán realizar, entre otras, las siguientes actividades: 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

		(Artículo 30º, modificado por el artículo 161 del Decreto Ley 019 de 2012)	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.
	Decreto 2364 de 2012 (compilado por el Decreto 1074 de 2015)	Definiciones (Artículo 1º)	Acuerdo sobre el uso del mecanismo de firma electrónica: Acuerdo de voluntades mediante el cual se estipulan las condiciones legales y técnicas alas cuales se ajustarán las partes para realizar comunicaciones, efectuar transacciones, crear documentos electrónicos o cualquier otra actividad mediante el uso del intercambio electrónico de datos. Datos de creación de la firma electrónica: Datos únicos y personalísimos, que el firmante utiliza para firmar. Firma electrónica: Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente. Firmante. Persona que posee los datos de creación de la firma y que actúa en nombre propio o por cuenta de la persona a la que representa.

		Cumplimiento del requisito de Firma (Artículos 3º en concordancia con los artículos 4º, 6 y 8º)	Cuando se exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea tan confiable como apropiada para los fines con los cuales se generó o comunicó ese mensaje.
		Efectos jurídicos de la Firma Electrónica (Artículo 5º)	La firma electrónica tendrá la misma validez y efectos jurídicos que la firma, si aquella cumple con los requisitos establecidos en el artículo 3 de este decreto.
	Decreto Ley 019 de 2012	Entidades de Certificación Digital (Artículo 161º)	Las entidades de certificación acreditadas por el Organismo Nacional de Acreditación de Colombia para prestar sus servicios en el país, podrán realizar, entre otras, las siguientes actividades: 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.

	Decreto 1074 de 2015	Compilación de los Decretos 2364 de 2012 y 333 de 2014	Decreto Único Reglamentario del Sector de Comercio, Industria y Turismo que compila las normas reglamentarias preexistentes que rigen el sector. Específicamente en su artículo 2.2.2.47.1 y siguientes, y en su artículo 2.2.2.48.1.1 y siguientes, compila a los Decretos 2364 de 2012 y 333 de 2014. El artículo 3.1.1 relativo a derogatoria integral establece que el Decreto 1074 regula íntegramente las materias contempladas en él, siendo así que quedan derogadas todas las disposiciones de naturaleza reglamentaria relativas al sector Comercio, Industria y Turismo que versen sobre las mismas materias salvo alguna excepciones, valga mencionar que dentro de esas excepciones no se encuentran los Decretos 2364 de 2012 y 333 de 2014.

De la gráfica previamente indicada, los artículos más significativos en materia de Autenticación Electrónica son el 17º de la Ley 527 de 1999 y 7º del Decreto 2364 de 2012 compilado por el Decreto 1074 de 2015 (Ver Artículo 2.2.2.47.7).

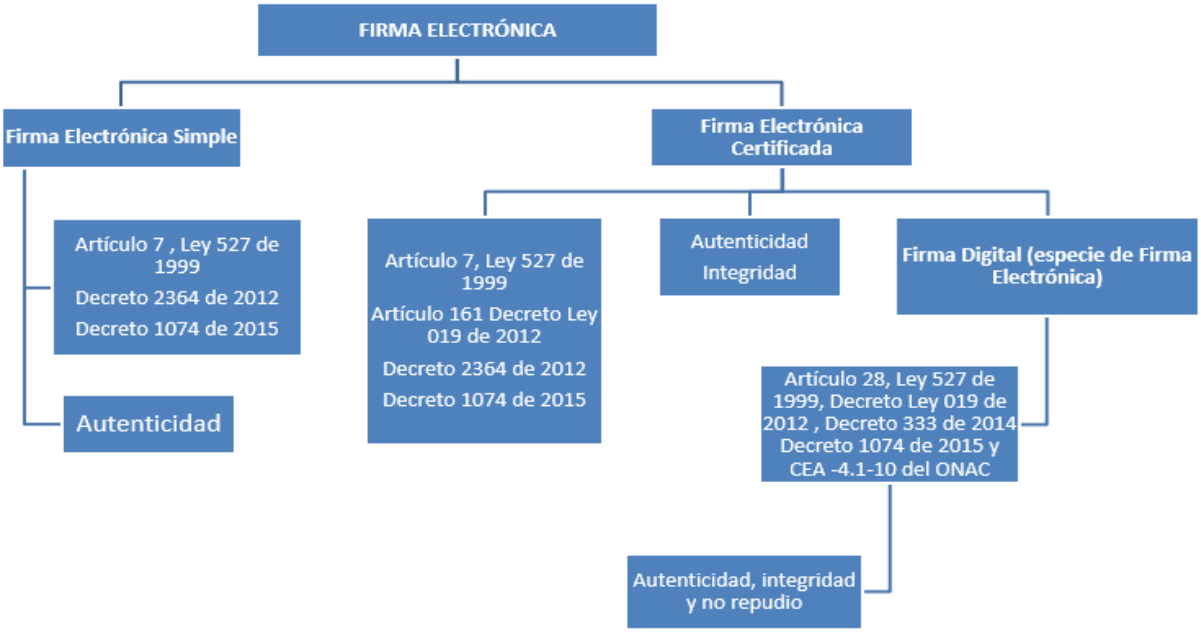
Con base en dichos artículos es posible establecer entonces que la normativa consagra dos presunciones a favor de los mecanismos de autenticación, por una parte, una presunción respecto al origen de la información que sea generada, enviada, recibida, almacenada o comunicada por medios electrónicos (mensajes de datos) cuando se materialice una de las situaciones que presenta el artículo 7º. Por otra parte, una presunción respecto a que los mecanismos de autenticación electrónica cumplen los requisitos de firma electrónica, siendo así que resulta necesario hacer mención a la Firma Electrónica.

El ordenamiento jurídico colombiano a través del artículo 7 de la ley 527 de 1999, el Decreto 2364 de 2012 y el Decreto 1074 de 2015 que compilo al 2364 de 2012, reguló y reglamentó,

respectivamente, el mecanismo de Firma Electrónica. De esta forma, la firma electrónica será válida jurídicamente siempre y cuando el método sea utilizado sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas las circunstancias del caso, así como cualquier acuerdo pertinente.

Teniendo en cuenta lo anterior, a continuación se presentan dos gráficas por medio de las cuales se pretende indicar cuál es el esquema jurídico de la Firma Electrónica en Colombia, cuáles son las características de la Firma Electrónica como mecanismo técnico y qué tipo de firmas electrónicas existen a la luz de la normativa.

a. Esquema jurídico de la Firma Electrónica en Colombia



Tal y como se desprende de lo mencionado previamente es posible establecer que la firma electrónica es un mecanismo técnico que puede ser prestado por cualquier persona que satisfaga los requisitos establecidos en el artículo 7 de la ley 527 de 1999 y el Decreto 2364 de 2012 antes citados, por tal motivo, es posible señalar que la normativa vigente permite el uso e implementación

de firmas electrónicas simples o no certificadas. En ese sentido, la Firma Electrónica simple es aquella provista por una empresa de tecnologías o por cualquier empresa que la desarrolle (que no sea una Entidad de Certificación Digital) y que por lo tanto si bien puede satisfacer un atributo de autenticidad, no necesariamente puede garantizar un atributo de integridad y muy difícilmente un atributo de no repudio. Esta firma no resulta tan segura en la medida en que es provista por una entidad diferente a una entidad de certificación digital.

No obstante lo anterior, la Ley 527 de 1999, el Decreto 019 de 2012 y el Decreto 333 de 2014 compilado por el Decreto 1074 de 2015, dieron un paso significativo a nivel de seguridad jurídica y técnica, así como en materia de imparcialidad, al crear la figura de Entidades de Certificación Digital. De acuerdo con el artículo 2 de la Ley 527 de 1999 estas entidades están facultadas 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. De esta manera, de acuerdo con el artículo 30 modificado por el artículo 161 del Decreto Ley 019 de 2012, estas entidades están en capacidad de prestar servicios de certificación digital y deben cumplir las condiciones y requerimientos[27] establecidos por la Ley 527 de 1999, el Decreto Ley 019 de 2012 y el Decreto 333 de 2014. En ese sentido la Firma Electrónica certificada será aquella provista únicamente por una Entidad de Certificación Digital, por lo cual puede satisfacer los atributos jurídicos de autenticidad e integridad en cuanto goza con el respaldo de un tercero de confianza.

En consecuencia, atendiendo las consideraciones antes presentadas, el legislador forjo el concepto de firma electrónica certificada a través del artículo 30 de la Ley 527 de 1999 modificado por el

27 Artículo 160 Decreto Ley 019 de 2012 reglamentado por el Decreto 333 de 2014.

artículo 161 del Decreto Ley 019 de 2012, como aquella que además de cumplir lo dispuesto en la normativa en materia de firmas electrónicas exige la participación de una entidad de certificación, es decir, un tercero de confianza "parte neutra, ajena a las partes que intervienen en una comunicación, que expide actos denominados certificados, los cuales son manifestaciones hechas como resultado de la verificación que efectúa sobre la autenticidad, veracidad y legitimidad de las claves criptográficas y la integridad de un mensaje de datos"[28] que "certifica técnicamente que un mensaje de datos cumple con los elementos esenciales para considerarlo como tal, a saber la confidencialidad, la autenticidad, la integridad y la no repudiación de la información, lo que, en últimas permite inequívocamente tenerlo como auténtico"[29].

Por último, es de resaltar que dentro de la firma electrónica certificada se encuentra la firma digital, como una de sus especies, que también tendrá unas implicaciones particulares desde el punto de vista jurídico pues goza de presunciones legales (artículo 28 de la Ley 527 de 1999).

b. Características de la Firma Electrónica como mecanismo técnico

28 Corte Constitucional, Sentencia C – 662 de 2000, M.P. Fabio Morón Díaz.
29 Ibid.

Como se mencionaba anteriormente, la Ley 527 en su artículo 7º consagró la manifestación de firma al establecer que "cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si: a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación; b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado. (…)". Al respecto, es de notar que el Decreto 2364 de 2012 establece la reglamentación del artículo 7 de la ley 527 de 1999. Con esta norma se complementa el marco jurídico de los diferentes mecanismos de autenticación y de firma previstos en Colombia. En efecto, el Decreto expedido por el Gobierno Nacional tiene algunas características que benefician el uso de los medios electrónicos, las cuales se describen brevemente:

- Se definen los criterios de confiable y apropiado en el uso de los mecanismos de autenticación. La firma electrónica está definida en la Ley como un mecanismo confiable y apropiable que permite identificar a una persona ante un sistema de información. El Decreto define el alcance de la expresión "confiable" pero no define el concepto "apropiado" y sí por el contrario de "seguridad".
- Se establece la relación de género y especie que existen entre firmas electrónicas y firmas digitales, señalando las diferencias que existen en su tratamiento probatorio, pues en el último mecanismo señalado existe una inversión probatoria.
- Se establece el uso de la firma electrónica mediante acuerdo de las partes de una relación jurídica, pero se establece también de manera clara que éstos mecanismos deben garantizar las condiciones de confiabilidad, siendo así que quien establezca mecanismos de autenticación electrónica deberá garantizar las condiciones de autenticidad e integridad

definidas como alcance del concepto de confiabilidad. Esto redunda en la seguridad los usuarios finales.

- Se destaca la neutralidad tecnológica de los diferentes mecanismos de autenticación, lo que posibilitará el uso de cualquier tipo de tecnología.
- Se definen criterios para determinar la seguridad de la firma electrónica, haciendo una expresa alusión a la necesidad de contar con auditorias técnicas o la intervención de terceros especializados para definir el grado de seguridad de los mecanismos de firma electrónica.
- Los mecanismos de autenticación deben ser tanto confiables como seguros con independencia de quien los provea.
- El rol de un tercero de confianza, como son las entidades de certificación digital, debe ser valorado a fin proveer mecanismos de autenticación electrónica y firmas electrónicas.

Ahora bien, el solo hecho de usar un mecanismo de firma electrónica no es suficiente para considerar que el documento se encuentra válidamente firmado jurídicamente, sino que el mecanismo debe cumplir con dos requisitos valorativos: debe ser confiable y debe ser apropiado. Estos conceptos se deben analizar con respecto al contenido del mensaje de datos que está siendo firmado y con la transacción que se está realizando.

Precisamente, los artículos 3 y 5 del Decreto 2364 de 2012 establecieron que la firma electrónica tendrá la misma validez y efectos jurídicos que la firma si esta es apropiada y confiable para los fines por los cuales se creó o comunicó el mensaje. Al respecto, es de resaltar que el Decreto 2364 de 2012 consagró como “confiable” lo siguiente:

- **Confiable:** Artículo 4 “(…) será confiable si: 1. Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante. 2. Es posible

detectar cualquier alteración no autorizada del mensaje de datos, hecha después del momento de la firma, y agrega el artículo en su parágrafo que lo dispuesto anteriormente se entenderá sin perjuicio de la posibilidad de que cualquier persona: 1. Demuestre de otra manera que la firma electrónica es confiable; o 2. Aduzca pruebas de que una firma electrónica no es confiable. En virtud de lo anterior, y aunado a lo que establece el artículo 7 de la Ley 527 de 1999, es posible establecer que el numeral 1 consagra un atributo jurídico de autenticidad, pues al ser el dato de creación de la firma único y exclusivo a una persona, será posible identificarla, y en esa medida se observa cómo se cobija bajo un concepto de autenticación electrónica. Ahora bien, el numeral 2 consagra un atributo jurídico de integridad, en la medida en que es posible verificar una modificación o alteración al documento electrónico una vez el mismo ha sido firmado electrónicamente.

- **Apropiado:** Si bien el Decreto 2364 de 2012 no define qué se entiende por "apropiado", es de notar que a la luz del Diccionario de la Lengua Española de la Real Academia de la Española (RAE) este término significa "ajustado y conforme a las necesidades de algo". En ese sentido, en el caso de la Firma Electrónica será necesario que la compañía que la implemente haga una evaluación propia respecto a las necesidades que desea satisfacer mediante la implementación de un método técnico de este tipo, y si el mismo se ajusta y es conforme a dichas necesidades. En esa medida si bien la confiabilidad será una característica a satisfacer por parte de quien ofrece el mecanismo de firma electrónica o por parte de la Entidad de Certificación Digital.

De manera seguida, tal y como se puede interpretar del parágrafo del artículo 4 del Decreto 2364 de 2012, las firmas electrónicas como género, a diferencia de la firma digital como una de sus especies, no gozan de presunciones legales, por lo cual desde el punto de vista probatorio se debe

demostrar que el método de firma electrónica empleado es confiable y apropiado como se ha mencionado previamente.

De lo anterior, se colige una importante consecuencia: quien afirme que un mensaje de datos está firmado no solamente debe probar la existencia del mensaje de datos, sino que adicionalmente debe probar que el documento se encuentra debidamente firmado y que dicho mecanismo sea confiable y apropiado. Así, quien afirme que un mensaje de datos se encuentra firmado, debe allegar las pruebas que se establecen en el Decreto 2364 de 2012, a saber:

- Del método de firma utilizado.
- Probar que ese método es confiable para el tipo de transacción.
- Que el método es apropiado para el tipo de transacción.

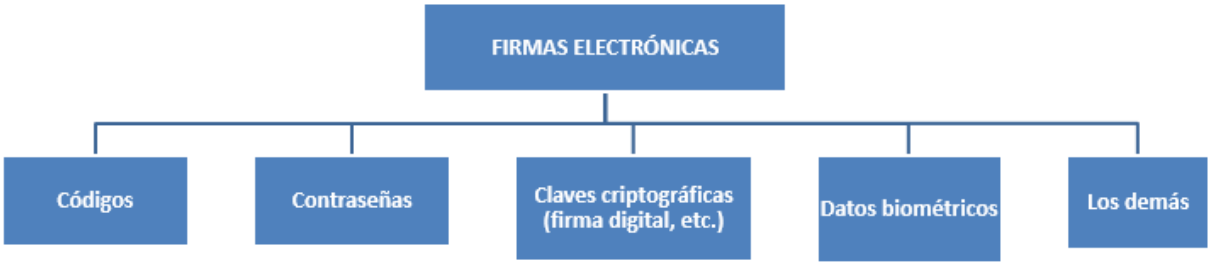
De esta forma, es de resaltar que si no se allegan las pruebas relacionadas con el método de firma, se tomará como un documento no firmado. Ahora bien, si se allegan las pruebas de la firma y estas demuestran que el método fue confiable y apropiado, el tratamiento será el de los documentos firmados y la parte a quien se opone deberá afirmar la falsedad del documento.

Habiendo presentado lo anterior, es importante tener presente si bien todas las firmas electrónicas son válidas jurídicamente, desde que cumplan los postulados de que sean confiables y apropiadas, no necesariamente todas tienen la misma robustez y por lo tanto el análisis de la escogencia de una u otra, deberá obedecer a un criterio de riesgo y de asegurar la transacción que se está llevando a cabo en medios electrónicos.

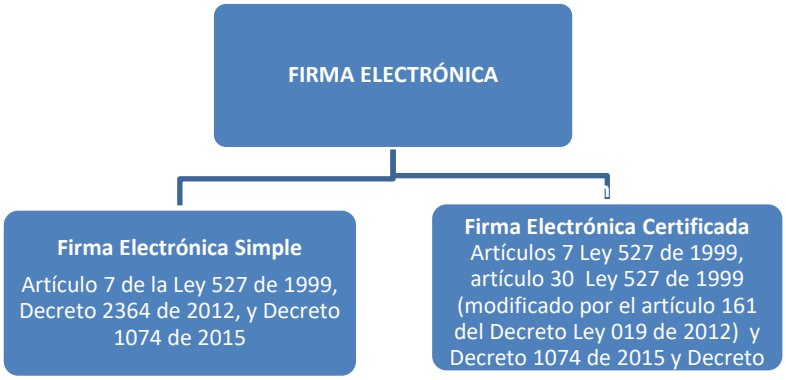
c. Tipos de Firmas Electrónicas y la determinación respecto a cuáles debe aplicar

Ahora bien, la Firma electrónica ha sido reconocida como el género dentro del cual se encuentran diversos especies o tipos de firmas electrónicas, como por ejemplo la firma digital, la firma

biométrica (que hace uso de datos biométricos), el usuario y contraseña, los one time passwords (OTP), el PIN, entre otros[30], así:



Teniendo en cuenta la definición antes señalada es de notar que actualmente el marco jurídico en torno a firmas electrónicas es el siguiente:



Es de resaltar que estos mecanismos deberán cumplir las disposiciones de la Ley 527 de 1999, y del Decreto 2364 de 2012 compilado por el Decreto 1074 de 2015. En concordancia con lo anterior, los artículos 3 y 5 del Decreto 2364 de 2012 establecieron que la firma electrónica tendrá la misma

[30] Ley Modelo de la CNUDMI sobre Firmas Electrónicas de 2001, página 8. Disponible en http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf

validez y efectos jurídicos que la firma manuscrita si ésta es apropiada y confiable[31] para los fines por los cuales se creó o comunicó el mensaje.

De la gráfica anteriormente expuesta es posible evidenciar que el Decreto 2364 de 2012 no establece una lista taxativa de métodos de firma electrónica, por el contrario, se refiere a un listado enunciativo, por lo que cualquier tipo de método de firma electrónica que cumpla con los requisitos reglamentarios dispuestos en el Decreto 2364 de 2012 y demás normativa antes señalada para efectos de firma electrónica, y siempre y cuando el mecanismos de firma sea tanto confiable como apropiado, podrá tenerse como una firma electrónica válida jurídicamente.

Tal y como se desprende de lo mencionado previamente es posible establecer que la firma electrónica es un mecanismo técnico que puede ser prestado por cualquier persona que satisfaga los requisitos establecidos en el artículo 7 de la ley 527 de 1999 y el Decreto 2364 de 2012 antes citados, por tal motivo, es posible señalar que la normativa vigente permite el uso e implementación de firmas electrónicas simples o no certificadas. No obstante lo anterior, la Ley 527 de 1999, el Decreto 019 de 2012, el Decreto 333 de 2014 y el Decreto 1074 de 2015, dieron un paso significativo a nivel de seguridad jurídica y técnica, así como en materia de imparcialidad, al crear la figura de Entidades de Certificación Digital. De acuerdo con el artículo 2 de la Ley 527 de 1999 estas entidades están facultadas 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. De esta manera, de acuerdo con el artículo 30º modificado por el

[31] Decreto 2364, Artículo 4 "(…) será confiable si 1. Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante. 2. Es posible detectar cualquier alteración no autorizada del mensaje de datos, hecha después del momento de la firma, y agrega el artículo en su parágrafo que lo dispuesto anteriormente se entenderá sin perjuicio de la posibilidad de que cualquier persona: 1. Demuestre de otra manera que la firma electrónica es confiable; o 2. Aduzca pruebas de que una firma electrónica no es confiable.

artículo 161º del Decreto Ley 019 de 2012, estas entidades están en capacidad de prestar servicios de certificación digital[32], entre otros, por ejemplo, "emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas", es decir, firmas electrónica que cuentan con el respaldo de certificados digitales y que son, por lo tanto, provistas por Entidades de Certificación Digital, siendo así que estas entidades deben cumplir las condiciones y requerimientos[33] establecidos por la Ley 527 de 1999, el Decreto Ley 019 de 2012 y el Decreto 333 de 2014.

Es evidente que la transición del mundo físico al mundo digital a través del comercio electrónico ha ofrecido múltiples oportunidades, ventajas y facilidades a la sociedad y el Estado, no obstante, como lo han mencionado diversos doctrinantes, este intercambio de información en el mundo electrónico también conlleva riesgos, es así como "se ha establecido que el principal obstáculo para los negocios electrónicos ha sido la falta de confianza en los mecanismos electrónicos. Esto obedece a varios factores: 1) el anonimato de las transacciones electrónicas; 2) la falta de seguridad que garantice la confidencialidad e integridad de la información; 3) el desconocimiento de la tecnología y cómo opera y 4) la barrera cultural"[34]. Precisamente, "garantizar la seguridad en medios electrónicos es quizá el problema más significativo para las personas interesadas en efectuar operaciones de comercio electrónico. En un enfoque más amplio, la confidencialidad, la autenticidad, la integridad y el no repudio son los principales problemas que afectan a los documentos electrónicos"[35].

---

[32] "1. Emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas. (…) 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. (…) 9. Cualquier otra actividad relacionada con la creación, uso o utilización de firmas digitales y electrónicas".

[33] Artículo 160 Decreto Ley 019 de 2012 reglamentado por el Decreto 333 de 2014.

[34] CASTRO, Marcela. Fundamentos de Derecho de los Negocios para no abogados. Bogotá: Editorial Temis, 2013, p 212.

[35] RINCÓN CÁRDENAS, Erick. Derecho del Comercio Electrónico y de Internet. Segunda Edición. Bogotá: Editorial Legis, 2015.

En consecuencia, atendiendo las consideraciones antes presentadas, el legislador forjo el concepto de firma electrónica certificada a través del artículo 30 de la Ley 527 de 1999 modificado por el artículo 161 del Decreto Ley 019 de 2012, como aquella que además de cumplir lo dispuesto en la normativa en materia de firmas electrónicas exige la participación de una entidad de certificación. La Corte Constitucional precisamente reconoció la labor de las Entidades de Certificación Digital y las catalogó como un tercero de confianza, es decir, una parte neutra, ajena a las partes que intervienen en una comunicación, que expide actos denominados certificados, los cuales son manifestaciones hechas como resultado de la verificación que efectúa sobre la autenticidad, veracidad y legitimidad de las claves criptográficas y la integridad de un mensaje de datos"[36] que facilita y garantiza las transacciones comerciales por medios electrónicos o medios diferentes a los estipulados en papel e implican un alta grado de confiabilidad, lo que las hace importantes y merecedoras de un control ejercido por un ente público, control que redunda en beneficio de la seguridad jurídica del comercio electrónico[37]. Así, el tercero de confianza otorga seguridad jurídica y técnica a las transacciones electrónicas, dota de validez jurídica y probatoria a los mensajes de datos, garantizando de manera efectiva que el firmante sea quien dice ser basándose en una serie de verificaciones previas que permiten disminuir el riesgo de suplantación de identidad, que de igual forma garantiza la utilización de medios tecnológicos pertinentes basados en el estado del arte de la ciencia y que por lo tanto tiene la capacidad de emitir certificados digitales sobre dicha firma[38].

En este orden de ideas, las Entidades de Certificación Digital, como son las seis actuales que se encuentran acreditadas por el Organismo Nacional de Acreditación de Colombia (ONAC), a saber:

[36] Corte Constitucional, Sentencia C – 662 de 2000, M.P. Fabio Morón Díaz.
[37] Corte Constitucional, Sentencia C-831 de 2001, M.P. Álvaro Tafur Galvis.
[38] Ibid.

GSE S.A., Thomas Signe S.A.S., Edicom S.A.S., Olimpia IT S.A.S., Certicámara S.A. y Andes S.A. [39] , son terceros de confianza que para ofrecer firmas electrónicas en el mercado, necesariamente cumplen lo dispuesto en la Ley 527 de 1999, el Decreto Ley 019 de 2012 (artículos160 a163), el Decreto 2364 de 2012, el Decreto 1074 de 2015 y el Decreto 333 de 2014, así como deben cumplir una serie de estándares técnicos dispuestos en los Criterios Específicos de Acreditación de Entidades de Certificación Digital Abiertas (CEA) 4.1.-10[40].

Así las cosas, son diversos los mecanismos de firmas electrónicas que pueden ser utilizados, dentro de estos, hablaremos de tres en particular, la firmas digital, la firma biométrica a través de la huella haciendo uso de la biometría expuesta por la Registraduría del Estado Civil y el uso de claves.

c.1. Firma Digital

Un tipo de firma electrónica es la firma digital. Esta última ha sido regulada por la Ley 527 de 1999 y específicamente ha sido reconocida por el Decreto 2364 como una especie de la firma electrónica y obedece particularmente a los factores de autenticación de "algo que el usuario sabe", como puede ser la clave o contraseña para firmar digitalmente, y en algunos casos "algo que el usuario posee", que se refiere a la posesión de un token físico, a través del cual es posible firmar digitalmente.

Este tipo de firma se encuentra definida en el artículo 2 de la Ley 527 de 1999 como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este

[39] Organismo Nacional de Acreditación de Colombia (ONAC), Directorio de Acreditación. Disponible en https://onac.org.co/directorio-de-acreditacion-buscador

[40] Entidades de Certificación Digital, ficha técnica del esquema. ONAC, Disponible en https://onac.org.co/certificacion-de-firmas-digitales

valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

Ahora bien, la existencia de la firma digital tiene sustento en la Ley Modelo de Firmas Electrónicas de la CNUDMI, de la que se ha hablado en párrafos anteriores. En dicha norma internacional, se consagra el método de Infraestructura de Llave Pública, el cual "es una forma de ofrecer confianza en que: a) la clave pública del usuario no ha sido alterada y corresponde de hecho a la clave privada del mismo usuario; b) se han utilizado buenas técnicas de codificación. Para poder ofrecer el grado de confianza descrito más arriba, una ICP puede ofrecer diversos servicios, incluidos los siguientes: a) gestión de las claves criptográficas utilizadas para las firmas numéricas; b) certificación de que una clave pública corresponde a una clave privada; c) provisión de claves a usuarios finales; d) publicación de una guía segura de certificados o claves públicas; e) administración de contraseñas personales (por ejemplo, tarjetas inteligentes) que permitan identificar al usuario con información de identificación personal singular o que permitan generar y almacenar claves privadas individuales; f) comprobación de la identificación de los usuarios finales y prestación de servicios a éstos; g) prestación de servicios de marcado cronológico; y h) gestión de las claves de codificación utilizadas con fines de confidencialidad en los casos en que esté autorizado el empleo de esa técnica"[41].

En ese sentido, este tipo de firma "(…) se crea y verifica utilizando el método de "criptografía de clave pública" que se basa en el empleo de una función algorítmica para generar dos claves diferentes, pero relacionadas entre sí"[42]. Es así como, la firma digital se basa en la criptografía asimétrica, lo que significa que hace uso de una clave pública y una clave privada, es decir, en el

[41] Ley Modelo de la CNUDMI sobre Firmas Electrónicas. Disponible en https://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf, página 30

[42] PEÑA VALENZUELA, Daniel. De la firma manuscrita a las firmas electrónica y digital. Derecho Internacional de los Negocios Tomo V. Universidad Externado de Colombia. Bogotá: 2015. página 128

primer caso se usa un "valor o valores numéricos que utilizados conjuntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos"[43], y en el segundo caso se emplean "valores numéricos que son utilizados para verificar que una firma digital fue generada con la clave privada del iniciador"[44].

Al respecto, es importante resaltar que una firma digital a nivel técnico[45], consiste en lo siguiente:

1. Tomar un conjunto de datos de **cualquier tamaño** y calcularles un resumen de **tamaño fijo**, **único** e **irrepetible** mediante un procedimiento matemático denominado función Hash.

   Hash: *Operación que se realiza sobre un conjunto de datos de cualquier tamaño de tal forma que se obtiene como resultado otro conjunto de datos, de tamaño fijo e independiente del tamaño original que, además, tiene la propiedad de estar asociado directamente a los datos iniciales.*

2. Tomar el certificado digital asociado al firmante, y obtener de este los datos de identidad del firmante, tales como nombre - razón social, número de documento - NIT, cargo, correo electrónico, etc.

3. Realizar un proceso criptográfico asociado al resumen obtenido del conjunto de datos, utilizando la llave privada almacenado dentro del certificado digital.

[43] Numeral 5 del Artículo 3, Decreto 333 de 2014
[44] Numeral 6 del Artículo 3, Decreto 333 de 2014
[45] Entrevista a Camilo Reyes, Director de Factura Electrónica, Certicámara S.A.

4. Anexar al conjunto de datos a firmar el resultado de este proceso criptográfico y además la información de identidad obtenida del certificado digital.

Ahora bien, con el fin de generar firmas digitales, la Ley Modelo en mención, así como el ordenamiento jurídico colombiano, han reconocido la existencia de terceros especializados o como se ha indicado en párrafos anteriores, terceros de confianza.

Dichos terceros tienen como objeto "(…) vincular a un firmante identificado o el nombre del firmante a una clave pública determinada. El tercero se conoce en general, en la mayoría de las normas y directrices técnicas, como "entidad certificadora", "prestador de servicios de certificación" o "proveedor de servicios de certificación" (en la Ley Modelo, se ha elegido el término de "prestador de servicios de certificación"). En unos cuantos países, esas entidades certificadoras están siendo organizadas en forma jerárquica en lo que suele denominarse una infraestructura de clave pública (ICP). Otras soluciones pueden ser, por ejemplo, los certificados emitidos por terceros que confían en la firma"[46].

[46] Ibidem, CNUDIMI, Ley Modelo de Firmas Electrónicas. página 30

Estos proveedores de confianza, tal y como lo indica la Ley Modelo previamente citada, cuentan con diversos niveles jerárquicos de autoridad, que les permite llevar a cabo la generación de firmas digitales de manera confiable e imparcial, al usuario final que las requiera. Es así como pueden contar con una "(…) a) una "entidad principal" única que certificaría la tecnología y las prácticas a todas las partes autorizadas a emitir certificados o pares de claves criptográficas en relación con el empleo de dichos pares de claves, y llevaría un registro de las entidades de certificación subordinadas; b) diversas entidades de certificación, situadas bajo la autoridad "principal" que certificarían que la clave pública de un usuario corresponde en realidad a la clave privada del mismo usuario (es decir que no ha sido alterada); y c) diversas entidades locales de registro, situadas bajo las autoridades de certificación, que reciban de los usuarios peticiones de pares de claves criptográficas o de certificados relativos al empleo de esos pares de claves, y que exijan pruebas de identidad a los posibles usuarios y las verifiquen". De esta manera, en entidades de certificación digital abiertas como la Sociedad Cameral de Certificación Digital Certicámara S.A., se presenta una autoridad de registro (AR), encargada de recibir y tramitar las solicitudes de emisión de certificados de firma digital, así como llevar a cabo el proceso de validación de identidad del usuario, y por otra parte, se encuentra una autoridad de certificación (AC) encargada de llevar a cabo la emisión de los certificados de firma digital, con base en las gestiones llevadas a cabo por la AR[47].

Ahora bien, el contar con el respaldo de un tercero, reconocido como entidad de certificación digital, en quien se encuentra totalmente delegado el proceso de validación de identidad, sin duda hace que dentro de los tipos de firmas electrónicas, la firma digital tenga unas características especiales, pues la emisión y generación de la misma depende en su totalidad de la validación de

[47] Entrevista a Tatiana Hernández, Directora de Identidad Digital, Firmas y Componentes, Certicámara S.A.

identidad exitosa por parte de un tercero de confianza, como son las entidades de certificación digital.

Por otra parte, es importante mencionar lo que la normativa colombiana ha dispuesto para las firmas digitales.

En primer lugar, de la Ley 527 de 1999 y el Decreto 2364 de 2012, se ha establecido que la firma digital garantiza los siguientes atributos jurídicos, los cuales se desprenden de la noción de firma digital consagrada en estas normas:

i) Autenticidad: permite garantizar la identidad del emisor de un mensaje y tener la plena seguridad que quien remite el mensaje de datos es realmente quien dice ser; este proceso se realiza mediante la emisión de un certificado digital que conlleve la participación de una autoridad de registro (AR) y autoridad de certificación (AC) dependientes de una entidad de certificación digital, como se evidenció previamente.

ii) Integridad: permite garantizar que el mensaje de datos no haya sido alterado después de la firma. Al vincularse la firma con la contenida en el mensaje de datos, en caso que esa información cambie, la firma será invalidada. Precisamente a partir de los datos de entrada se crea una cadena que solo puede volverse a crear con esos mismos datos. Estas funciones tienen varias finalidades; entre otras, asegurar la integridad del documento electrónico"[48]

iii) No repudio: permite establecer que el emisor, suscriptor o creador de un mensaje de datos no podrá negar el conocimiento de este último, ni los compromisos adquiridos a través de este, por cuanto se presume que al firmar digitalmente, dicho emisor o suscriptor quería ser vinculado con el contenido de ese mensaje de datos. De esta forma,

[48] Ibidem, PEÑA VALENZUELA, Daniel. página 129

> "mediante los sistemas de identificación del iniciador o destinatario de un mensaje de datos, se asegura que las partes intervinientes de la transacción no puedan negar su intervención en ella y la autoría de su mensaje"[49].

Ahora bien, es de resaltar que la norma también consagra el concepto de certificado de firma digital, al establecer que es "mensaje de datos firmado por la entidad de certificación que identifica, tanto a la entidad de certificación que lo expide como al suscriptor, y contiene la clave pública de este"[50]. En consecuencia, mediante el certificado digital es que es realmente posible firmar digitalmente, pues lo que normalmente usamos para firmar digitalmente que es el token físico, al estilo de una USB, es simplemente el formato de almacenamiento, físico, siendo así que con lo que verdaderamente se firma es con el certificado digital.

Dicho certificado digital, si se puede decir coloquialmente, es un estilo de cédula o identificación particular que relaciona un conjunto de información y los datos personales propios del firmante, siendo así que, como lo dispone el Decreto 333 de 2014, se convierte en un mensaje de datos firmado por la entidad de certificación donde se identifica, tanto a la entidad que lo emitió, así como al suscriptor. Al respecto, vale la pena indicar que la Ley 527 de 1999, reconoce que pueden ser emitidas firmas digitales a personas naturales o jurídicas, sin dar una más amplia clasificación que ésta (artículo 30 de la Ley 527 de 1999). Sin embargo, las entidades de certificación digital abiertas han creado tipologías específicas de acuerdo a la calidad del sujeto quien firma, lo cual se desarrolló a raíz de las necesidades del mercado.

Así, por ejemplo, existen categorías como las siguientes: pertenencia a empresa, representación legal, función pública, profesional titulado, personal natural, entre otras[51], lo cual permite

---

[49] Ibidem. RINCÓN CÁRDENAS, Erick. página 130
[50] Decreto 333 de 2014, artículo 3, numeral 1.
[51] Certificación 16-ECD-001 de la compañía Gestión de Seguridad Electrónica GSE S.A. proferida por el Organismo Nacional de Acreditación de Colombia (ONAC). Disponible en https://onac.org.co/certificados/16-ECD-001.pdf

evidenciar que aunque la firma digital sea la misma en medios electrónicos, no lo es en razón a la calidad en que este firmando el autor del documento. En ese sentido, si Juan Pérez firma como persona natural, tendrá unas implicaciones jurídicas totalmente diferentes, si Juan Pérez firma como representante legal de la Empresa XYZ.

Aunado a lo anterior, es de suma importancia tener en cuenta que el artículo 28 de la Ley 527 de 1999 consagra una serie de características que debe reunir la firma digital.

Dicho artículo dispuso que para que una firma digital tuviera la misma fuerza y efectos que una firma manuscrita, debía incorporar los siguientes atributos: 1) Ser única a la persona que la usa, 2) Debe ser susceptible de ser verificada, 3) Estar bajo el control exclusivo de la persona que la usa, 4) Estar ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada, 5) Estar conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

Las características anteriormente indicadas, son precisamente la base jurídica para indicar el por qué una firma digital cuenta con los atributos jurídicos de autenticidad e integridad, los cuales, vale la pena anotar, aparecen en principio, en todas las firmas electrónicas, de acuerdo a lo que establece el Decreto 2364 de 2012.

No obstante lo anterior, la Ley 527 de 1999, dio un paso más adelante al otorgarle a las firmas digitales unas bondades con las que no cuentan lo demás tipos de firmas electrónicas.

Precisamente, el artículo 28 consagra los atributos jurídicos de la firma digital, estipulando que "Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo (…)". En ese sentido, el artículo 28, que se refiere exclusivamente a la firma digital y no a cualquier tipo de firma electrónica, establece dos presunciones legales, una referida a la autoría y otra referida a la no repudiación.

En el caso de la primera, la persona que firma digitalmente acredita el contenido de lo que está firmando; en el caso de la segunda, la persona cuando firma digitalmente tiene la intención de vincularse al contenido del mensaje de datos que está firmando digitalmente, por lo cual la consecuencia inmediata, y en lo que se enfoca esta última presunción legal, es que no podrá generarse una repudiación o rechazo de aquello que ha firmado el suscriptor.

Al respecto, es de resaltar que el no repudio ha sido algo muy cuestionado, sin embargo es claro que el mismo se encuentra reconocido por las siguientes razones:

En primer lugar, la Ley Modelo sobre Firmas Electrónicas de la CNUDMI hace una diferencia entre la autoría del mensaje de datos frente al hecho de que el iniciador se vincule o asocie con el contenido del mensaje de datos.

En segundo lugar, la Ley 527 de 1999 en su exposición de motivos retoma lo manifestado por la CNUDMI en su Ley Modelo sobre Comercio Electrónico, señalando que "la firma digital debe cumplir idénticas funciones que una firma en las comunicaciones consignadas en papel. En tal virtud, se toman en consideración las siguientes funciones de esta: Identificar a una persona como el autor; Dar certeza de la participación exclusiva de esa persona en el acto de firmar; Asociar a esa persona con el contenido del documento". Nuevamente se observa, cómo el Legislador reconoce en dicha exposición de motivos una clara distinción entre la autoría y el hecho de que el autor se asocie con el contenido del documento, lo cual en el caso de la presunción legal prevista en el artículo 28 de la Ley 527 permitirá concluir que se consagra una presunción de no repudiación.

En tercer lugar, la Corte Constitucional, mediante Sentencia C-662 de 2000, ha reconocido el concepto de repudiación y lo ha diferenciado del concepto autenticidad. Respecto al primero, señala que "es el procedimiento técnico que garantiza que el iniciador de un mensaje no puede

desconocer el envío de determinada información", en cuanto al segundo manifiesta que "es la certificación técnica que identifica a la persona iniciadora o receptora de un mensaje de datos".

En cuarto lugar, la Guía No. 3[52] relativa a Documento Electrónico del Ministerio de Tecnologías de la Información y las Comunicaciones ha indicado que: "De conformidad con el principio de equivalencia funcional, en los casos que se exija firma manuscrita en los documentos elaborados en físico, es decir, en papel, los documentos electrónicos deben satisfacer el mismo requisito. La firma electrónica permite proporcionar al documento firmado: 1. Identificación: avalar la identidad del firmante de manera única, demostrando que es él, y nadie más, quien ha firmado el documento. Existen dos tipos de finalidades de la autenticación: 1.1. Identificación del origen de los datos: el identificado tiene relación con los datos consignados, le pertenecen y lo vinculan con el mensaje enviado. 1.2. Identificación de entidades: permite comparar los datos enviados con los datos almacenados en las bases y que han sido enviados anteriormente. 2. Integridad: asegurar que el contenido de un mensaje de datos ha permanecido completo e inalterado, independiente de los cambios que hubiera podido sufrir el medio en el que está contenido como resultado del proceso de su transmisión, archivo o presentación. 3. No Repudio: es la garantía de que no puedan ser negados los mensajes en una comunicación electrónica. Existen dos tipos: 3.1. No repudio en origen, de tal manera que el emisor no pueda negar el mensaje que ha enviado así quiera negar tal comunicación. 3.2. No repudio en destino, que garantiza al emisor que su comunicación ha sido recibida sin que el receptor pueda negar tal comunicación".

Así las cosas, de lo establecido en la Guía No. 3 del MinTic es posible concluir que se reconoce la existencia del no repudio, al establecer que el mismo es un elemento fundamental que aporta

[52] Guía No. 3 Cero papel en la Administración Pública, Documento electrónico. Ministerio de Tecnologías de la Información y las Comunicaciones. Disponible en https://docplayer.es/3613313-Guia-no-3-cero-papel-en-la-administracion-publica-documentos-electronicos.html

seguridad jurídica y técnica, y que solo puede ser suministrado por la firma digital que es reconocida por este Ministerio como el nivel más alto de seguridad.

Todo lo anteriormente expuesto, será determinante a nivel probatorio, toda vez que gracias a ese atributo de no repudiación, quien haya firmado digitalmente no podrá desconocer el documento que ha firmado, lo cual necesariamente lleva a concluir que probatoriamente la firma digital tiene un peso diferente a los demás tipos de firmas electrónicas por cuanto resulta más robusta jurídicamente. En ese sentido, jurídicamente sí resulta relevante que el mensaje de datos se haya suscrito con firma digital.

c.2. Firma biométrica a través de la huella dactilar

Otro tipo de mecanismo de firma electrónica que puede encontrarse en el mercado es la firma biométrica a través de la huella.

Es importante mencionar, de antemano y a modo de introducción, que las firmas electrónicas que surgen a partir de perfiles biométricos construidos con base en rasgos físicos de las personas, como pueden ser la huella, el iris, la voz, el rostro, entre otros, son un claro ejemplo de que hoy por hoy, la tecnología se adentra en esferas que no están relacionadas únicamente con factores de autenticación, como pueden ser “algo que el usuario sabe” o “algo que el usuario tiene”, sino también en factores como “algo que el usuario es”.

De esta forma, por sí solo, el mecanismo de biometría usualmente se ha usado para identificar a una persona por medio de técnicas matemáticas aplicadas a los rasgos físicos o comportamentales de dicha persona, por lo que se convierte en un mecanismo fuerte de autenticación. Esto quiere decir que este mecanismo al ser aplicado como firma electrónica principalmente se centra en

cumplir con el atributo de autenticidad, debido a que el elemento de firma proviene exclusivamente del iniciador de la firma.

Cada método biométrico tiene debilidades y fortalezas. Son diversos los grados de fortaleza y precisión que ofrece cada uno, siendo así que ningún sistema biométrico está exento de fallas ocasionadas por errores humanos o tecnológicos relacionados con la captura y el procesamiento, o con condiciones humanas como la edad, el envejecimiento, las limitaciones físicas o la facilidad de manipular estos mecanismos en ciertas situaciones.

Aunque existen diferentes tipos de biometría actualmente, para este documento solo se mencionaran los siguientes:

- **Biometría de rúbrica:**

Por si sola la imagen de la rúbrica de firma capturada en medios electrónicos no se puede vincular directamente al firmante, por lo tanto este tipo de firma captura junto con la rúbrica, la velocidad, la presión, la aceleración, los trazos, etc. Por medio de un dispositivo PAD habilitado para leer este tipo de variables. Este tipo de biometría es del tipo comportamental debido a que depende de la manera como el firmante realiza manuscritamente su firma. Debido a que incluye cada una de estas variables, en conjunto forman un patrón biométrico único por cada persona.

- **Biometría de huella:**

La huella digital es un mecanismo comúnmente usado para autenticar a personas ante un sistema. La huella biométrica hace referencia a tomar una serie de características técnicas de la huella denominadas minucias, las cuales son un conjunto de puntos únicos sobre la completitud de la huella que permiten establecer un patrón de la misma. Basado en la premisa que no existen dos huellas idénticas, tampoco existirán dos minucias idénticas y de esta manera permite verificar la

identidad de una persona en medios electrónicos, por medio de la comparación de la minucia de la huella capturada, contra una fuente confiable de comparación.

- **Biometría de rostro:**

La biometría por rostro corresponde a tomar las medidas y proporciones del rostro humano y con base a esto establecer un conjunto de características únicas para cada individuo por medio de una plantilla de acuerdo a las proporciones entre los ojos, la nariz y la boca, los ojos y boca con respecto a las orejas, etc.

- **Biometría de voz:**

La biometría por voz hace referencia a tomar las características técnicas y comportamentales de la voz para generar una huella vocal, tomando en cuenta a través del sonido el tamaño y forma de la boca, garganta y nariz, la tensión de las cuerdas vocales así como también la pronunciación, acento, velocidad de habla, vocalización y movimiento de los labios principalmente.

En este orden de ideas, el concepto de "algo que el usuario es" es un tema intrínsecamente asociado a la biometría, que cada vez toma más y más acogida en Colombia, específicamente en algunos sectores como pueden ser el bancario, notarial, cameral, entre otros. Pero ¿qué es la biometría?, la identificación biométrica consiste en capturar una imagen o las métricas de un individuo en un dispositivo (por ejemplo una cámara o un sensor) y, con un algoritmo, apoyado en hardware y software, se extrae, codifica, almacena y comparan características"[53].

En ese sentido, a través de la biometría es posible tomar los patrones o rasgos físicos únicos e irrepetibles de una persona, todo ello a partir de un proceso de validación de identidad, para

[53] Biometría: conveniente y segura. Edición 1138, Semana Económica, 2018. Asobancaria. Disponible en https://www.asobancaria.com/wp-content/uploads/1138-C-28-05-2018.pdf

construir o conformar un perfil biométrico con el cual es posible generar un mecanismo de firma electrónica, con base en el dato biométrico.

En Colombia particularmente, la biometría de huella, es un mecanismo usado normalmente para autenticar a personas ante un sistema, para lo cual, se recolectan una serie de características denominadas minucias, las cuales son un conjunto de puntos únicos sobre la completitud de la huella que permiten establecer un patrón de la misma. Esta tipo de biometría, que es de interés para el presente trabajo, ha sido abordada bajo dos escenarios que serán revisados a continuación, uno, que cuenta con la participación de la Registraduría (en adelante "RENEC) y otro, sin la participación de RENEC, que es provisto por terceros de soluciones tecnológicas en el sector privado.

En el primer caso, es de resaltar que la RENEC, constitucionalmente tiene la función de registrar la vida civil e identificar a los colombianos, así como organizar los procesos electorales y los mecanismos de participación ciudadana, en orden a apoyar la administración de justicia y el fortalecimiento democrático del país. De esta forma, es con base en este mandato constitucional que esta entidad ha conformado las bases de datos biográficas y biométricas de todos los colombianos, siendo así que allí reposan los datos de la cédula de ciudadanía, tales como: nombres, apellidos, fecha de expedición, entre otros, así como las minucias dactilares.

El Gobierno Nacional, teniendo en cuenta la necesidad de mejorar la prestación de servicios de las Entidades del Estado, expide el Decreto 019 del 10 de enero del 2012 "Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública". Dicho Decreto Ley establece, entre otras cosas, que la Registraduría

Nacional del Estado Civil debe asumir la interrelación y facilitación de consulta de sus bases de datos con otras Entidades.

En virtud de lo antes señalado, se desprende entonces que el Decreto Ley 019 de 2012 estipula las obligaciones en cabeza de la Registraduría Nacional del Estado Civil, a saber:

> "Artículo 18. Verificación de la huella dactilar por medios electrónicos. En los trámites y actuaciones que se cumplan ante las entidades públicas y los particulares que ejerzan funciones administrativas en los que se exija la obtención de la huella dactilar como medio de identificación inmediato de la persona, ésta se hará por medios electrónicos. Las referidas entidades y particulares contarán con los medios tecnológicos de interoperabilidad necesarios para cotejar la identidad del titular de la huella con la base de datos de la Registraduría Nacional del Estado Civil. (…)"

De esta forma, del artículo antes citado, es posible evidenciar que el Decreto Ley 019 de 2012 permite que las entidades públicas y los particulares que ejercen función pública o prestan un servicio público, puedan acceder a la base de datos biográfica y biométrica de la Registraduría Nacional del Estado Civil.

Asimismo, es importante resaltar que la Registraduría Nacional del Estado Civil, ha proferido una serie de resoluciones conforme a las cuales ha descrito asuntos relacionados con el acceso a sus bases de datos biográfica y biométrica, dentro de las cuales es necesario resaltar la 5633 de 2016, por la cual se reglamentan las condiciones y el procedimiento para el acceso a la base de datos de la información que produce y administra la Registraduría Nacional del Estado Civil. Es de resaltar que bajo esta Resolución se establece lo siguiente:

> "ARTÍCULO 3°: Autorización y disposición para el acceso a la información de las bases de datos de la Entidad. La Registraduría Nacional del Estado Civil autorizará y pondrá a disposición de las entidades interesadas, la consulta de las bases de datos que produce y administra para el cumplimiento de las obligaciones constitucionales y legales (entidades públicas y particulares con funciones públicas) o con el objeto social (particulares autorizados por la ley), según el caso. Dicha disposición estará sujeta al ejercicio de la función a su cargo, a la modalidad de prestación del servicio y a la observancia de las limitaciones técnicas de la Registraduría Nacional del Estado Civil, teniendo en cuenta los términos, procedimientos y condiciones establecidas en la presente resolución, garantizando el cumplimiento de las limitaciones de acceso y uso referidas a la protección de datos personales, al derecho de habeas data, privacidad, reserva estadística, asuntos de defensa y seguridad nacional y en general toda aquella información que tenga el carácter de reserva.".

Así las cosas, las entidades que se encuentran habilitadas para acceder a la base de datos de la RENEC para procesos de validación de identidad, son las siguientes:

- Entidades públicas (artículo 18 del Decreto Ley 019 de 2012, Artículo 159 de la Ley 1753 de 2015 y artículo 1 de la Resolución 5633 de 2016).
- Particulares que ejercen función pública (artículo 18 del Decreto Ley 019 de 2012, Artículo 159 de la Ley 1753 de 2015 y artículo 1 de la Resolución 5633 de 2016).
- Particulares que prestan servicios públicos (artículo 18 del Decreto Ley 019 de 2012, Artículo 159 de la Ley 1753 de 2015 y artículo 1 de la Resolución 5633 de 2016).
- Particulares que desarrollen las actividades del artículo 335 (Las actividades financiera, bursátil, aseguradora y cualquier otra relacionada con el manejo, aprovechamiento e

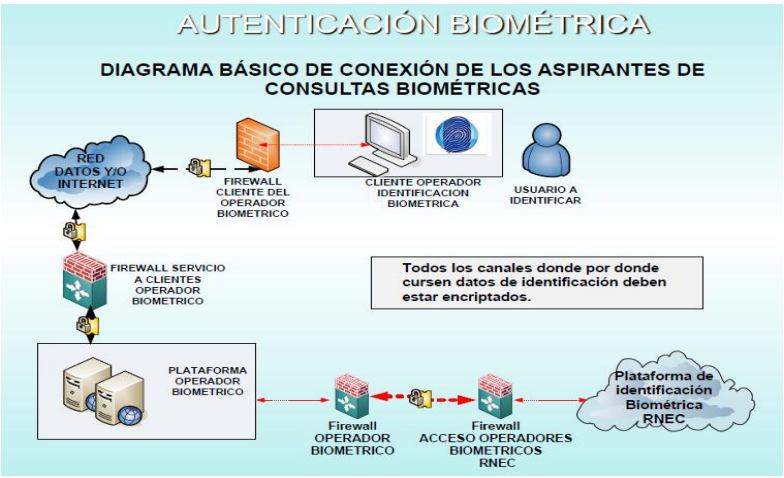
inversión de los recursos de captación a las que se refiere el literal d) del numeral 19 del artículo 150 son de interés público y sólo pueden ser ejercidas previa autorización del Estado, conforme a la ley, la cual regulará la forma de intervención del Gobierno en estas materias y promoverá la democratización del crédito) (Artículo 335 de la Constitución Política, Artículo 159 de la Ley 1753 de 2015 y artículo 1 de la Resolución 5633 de 2016).

- Unidad Administrativa Especial de Gestión Pensional y Contribuciones Parafiscales de la Protección Social (UGPP) (Artículo 159 de la Ley 1753 de 2015 y artículo 1 de la Resolución 5633 de 2016).
- Administradoras del sistema de seguridad social integral en pensiones, salud y riesgos laborales (Artículo 159 de la Ley 1753 de 2015 y artículo 1 de la Resolución 5633 de 2016).

De lo anterior se desprende que en caso de ser una entidad autorizada por la normatividad anteriormente mencionada, tiene, por lo tanto, permitido acceder a la réplica de la base de datos de la RENEC para llevar a cabo validaciones de identidad, para lo cual esta entidad habilitada deberá cumplir los anexos técnicos 1 y 2 que forman parte de la Resolución 5633 de 2016, para lo cual podrá acceder mediante su propia infraestructura o contratar los servicios de un operador biométrico habilitado por RENEC, quien cuenta con el hardware y software exigido por la autoridad para proveer una solución biométrica integral; estos proveedores se encuentran expuestos en la web con el fin de que las entidades puedan escoger el de su preferencia[54].

[54] Operadores biométricos habilitados por la Registraduría Nacional del Estado Civil. Disponible en https://wsp.registraduria.gov.co/biometria/operadores/listar/

A continuación se presenta una gráfica que fue presentada en un evento de la Registraduría Nacional del Estado Civil, donde se explica el modelo técnico y funcional de la validación de identidad contra la base de datos de la Registraduría:



Ahora bien, resulta importante mencionar que la Resolución 5633 de 2016, establece en su artículo 29 que "está totalmente prohibido recolectar, enrolar y almacenar huellas digitales o imágenes de éstas, o complementar bases de datos con la información consultada de las bases de datos de 1a Registraduría Nacional del Estado Civil". Esta disposición normativa ha sido interpretada por la RENEC de manera absoluta, es decir, para esta autoridad hoy por hoy no es posible hacer uso de la minucias dactilares (dato biométrico) para firmar en medios electrónicos, por cuanto, como la ha argumentado la RENEC, la identificación de los colombianos es un tema de seguridad nacional, para lo cual el Estado debe contar con la plena certeza del registro e identificación de los colombianos, y así poder definir y orientar en forma confiable y efectiva las acciones que van en beneficio de la población colombiana.

En razón de lo anterior, es que hoy en día la RENEC desincentiva el uso de soluciones tecnológicas que no involucren la validación de la identidad de la huella contra las bases de datos de esta entidad que es la base de datos más confiable en el Estado colombiano pues cuenta con información

actualizada en tiempo real, al nutrirse de otras bases de datos, como puede ser la de notarías, consulados, etc., y refuerzan especialmente el argumento de que no es viable firmar electrónicamente con las minucias dactilares, toda vez que las mismas quedarían almacenadas en el documento electrónico, estando sujetas a posibles hurtos informáticos y vulneraciones de orden técnico, lo cual pondría en riesgo la seguridad de los colombianos.

Aunque sus argumentos son legítimos, no es menos cierto que existe que la firma biométrica a través de la huella dactilar se encuentra también, hoy por hoy, reglamentada por el Decreto 2364 de 2012, pues dentro de esta normativa se permite el uso de datos biométricos como mecanismos de firma electrónica.

Por último, el segundo tipo de biometría es aquella implementada fuera del marco de la Resolución 5633 de 2016 proferida por la Registraduría, es decir, es aquella que se ampara totalmente en el Decreto 2364 de 2012, donde, vale la pena anotar, la información no es cotejada contra una base de datos confiable como es la de la Registraduría, sino que captura la huella del titular del dato personal para que sea almacenada y pueda utilizarse en múltiples procesos.

c.3. Firma a través de claves

El uso de claves es una de las estrategias más usadas actualmente para realizar procesos de autenticación electrónica. Estas claves también se encuentran contempladas bajo el Decreto 2364 de 2012, como mecanismos de firmas electrónicas que serán válidos, siempre y cuando se garanticen los atributos de “confiable” y “apropiado” que exige el Decreto.

En general se manejan dos tipos de claves para dichos procesos de autenticación, las cuales son:

- **Claves estáticas:**

Corresponden a aquella combinación de caracteres alfabéticos, numéricos y especiales definidos por una persona o un sistema de manera aleatoria y que son asignados también a una persona o sistema con el propósito de autenticarse. Se denominan estáticas porque dicha combinación de caracteres permanece sin alteraciones.

- **Claves dinámicas:**

Corresponden a aquella combinación de caracteres típicamente alfabéticos y numéricos asignados a una persona que tienen la particularidad de ser vigentes solo por cierto periodo de tiempo definidos, implicando que cambien una vez finalizado el tiempo de vigencia.

Aunque dichas claves no provienen de manera natural del firmante, como es el caso de los elementos biométricos, sí se realiza un proceso de asignación de clave por lo cual es algo que conoce el dueño de dicha clave permitiendo establecer en vínculo correspondiente. Para garantizar la integridad del mensaje de datos firmado con algún tipo de clave, se debe establecer un mecanismo complementario enfocado principalmente a cumplir con este objetivo y que a su vez pueda correlacionarse con el mecanismo de firma usado y el mensaje de datos que se está firmando[55].

Un ejemplo claro de este tipo de mecanismos de firma es aquel que se observa en el servicio de renovación del registro mercantil de comerciantes que ofrece la Cámara de Comercio de Bogotá[56], el cual se explicará a continuación.

La clave virtual consiste en la generación de una clave a través de un proceso de validación de identidad, que le permitirá al usuario autenticarse electrónicamente ante sistemas, y que esa misma

[55] Entrevista a Camilo Reyes, Director de Factura Electrónica, Certicámara S.A.
[56] Clave Virtual, Cámara de Comercio de Bogotá https://linea.ccb.org.co/clavevirtual/portalconsulta/default.aspx y https://www.ccb.org.co/Inscripciones-y-renovaciones/Registro-Unico-de-Proponentes/Clave-virtual

clave sea utilizada como mecanismo de firma electrónica.

Es de anotar que se asigna una clave alfanumérica a usuarios de portales transaccionales o recursos tecnológicos de las entidades que adquieren este servicio, debido a que se realiza un proceso de verificación de identidad a personas naturales por medio de la solicitud de datos asociados a su cédula de ciudadanía (nombres, apellidos, número de C.C. y fecha de expedición), y de cuestionarios reto cuyas respuestas son cotejadas contra una fuente confiable de datos (centrales de riesgo tales como Transunion). Todo lo anterior, con el fin de determinar que dicha persona es quien dice ser si aprueba dicho cuestionario. Al respecto, es importante precisar que el proceso de verificación de identidad por medio de preguntas reto, es un mecanismo que permite establecer, de acuerdo con la complejidad de las preguntas e Historial Crediticio y Financiero, un porcentaje de acierto en la identificación de la persona, el cual nunca llega a un 100%.

En ese sentido, en caso de ser exitosa la respuesta a dicho cuestionario, se genera una clave segura que permite hacer autenticación ante sistemas y ser aplicada como mecanismo de firma electrónica. Dicho mecanismo cumple los requisitos jurídicos que exige el Decreto citado respecto a que sea un mecanismo confiable y apropiado, y por lo tanto el equivalente de la firma manuscrita, por lo que el usuario puede firmar documentos con plena validez jurídica.

De lo anterior se desprende que la fuerza probatoria de la firma electrónica, en este caso de la Clave Virtual, se fundamenta nuevamente en el Decreto 2364 de 2012, donde se establece que quien afirme que un mensaje de datos está firmado electrónicamente deberá probar necesariamente la existencia del mensaje de datos y la evidencia de que el mismo se encuentra firmado. En ese sentido, se debe demostrar: i) El método de firma electrónica utilizado y ii) evidencias que permitan

probar que ese método es confiable y apropiado para el tipo de transacción electrónica realizada. Lo anterior se encuentra sustentado jurídicamente en los párrafos precedentes.

Es de anotar que en este tipo de mecanismos de firma electrónica, también pueden participar terceros, como son las centrales de riesgos o incluso también entidades de certificación digital u otros terceros, que provean seguridad jurídica y técnica a la solución.

III. Descripción de la Necesidad- Caso Hipotético:

Una compañía del sector financiero colombiano que ofrece tres productos de su portafolio en medios físicos, a través de sus diferentes oficinas, a saber la entrega de tarjetas de crédito, y la generación de créditos y de seguros, tiene el objetivo de inmaterializar estos dos procesos, es decir, que los mismos, nazcan y surtan su ciclo de vida en medios electrónicos. Para tal fin, desea disponer un canal transaccional a sus usuarios que le permita a estos últimos gestionar la entrega de tarjetas de crédito y seguros de forma ciento por ciento 100% electrónica. Para esto requiere contar con mecanismos que vinculen al usuario con el trámite, así como contar con mecanismos que le permitan a los usuarios dar su consentimiento y aceptación respecto a dichos productos.

Así las cosas, los objetivos del proyecto, son: 1) Disminuir, y si es posible, eliminar, educir el uso de papel, para que se facilite la agilidad en el proceso, así como la conservación y posterior consulta, y 2) Disponer un canal transaccional (portal web) que le permita al usuario gestionar su producto de manera virtual.

En virtud de lo anterior, este proyecto tiene como fin llevar a cabo la adquisición de los siguientes productos en medios electrónicos:

a. **Tarjeta de crédito:**

En la actualidad este trámite se lleva a cabo de manera presencial. Sin embargo, la compañía está interesada en implementar el trámite y adquisición de cada una de sus 10 tipos de tarjeta de crédito desde su portal web. El trámite de gestión de la emisión y aprobación de la tarjeta de crédito es cien por ciento (100%) electrónicos, lo cual permitirá que la entrega del producto, que será realizada en medios físicos, sea mucho más ágil y segura. Ahora bien, junto con el proceso de gestión de la emisión y aprobación de la tarjeta, el título valor que la respaldará deberá ser firmado. Frente a este último ítem, la compañía busca que se demuestre la validez jurídica de la aquiescencia del usuario respecto a la adquisición de la tarjeta y la vinculación con el título valor, en medios electrónicos.

b. Créditos y seguros:

En la actualidad la adquisición y trámite de este producto se realiza de manera ciento presencial. Sin embargo, la compañía está interesada en inmaterializar dicho trámite, para lo esta última busca que se demuestre la validez jurídica de la aquiescencia del usuario respecto a la adquisición del crédito y de los seguros y la vinculación con el título valor, en medios electrónicos para efectos de respaldar el crédito solicitado.

IV. Propuesta de Aplicabilidad

Con base en el caso hipotético presentado anteriormente y las necesidades presentadas en el mismo por parte de la compañía, resulta necesario revisar a la luz de los mecanismos de autenticación y firma electrónica anteriormente expuestos, cuál o cuáles pueden ser el mejor modelo en términos de seguridad jurídica y técnica para la compañía. Lo anterior con el fin de realizar una comparación de los mecanismos tecnológicos que puedan llegar a ser usados.

Criterios	Firma Digital	Firma biométrica de huella con	Claves

		participación de la Registraduría	
Autenticidad	La validación de identidad se encuentra totalmente delegada en un tercero de confianza denominado Entidad de Certificación Digital, toda vez que por norma y por lineamiento del Organismo Nacional de Acreditación de Colombia, únicamente este tipo de entidades pueden emitir certificados de firma digital. Adicionalmente, a diferencia de los demás tipos de firmas electrónicas, la firma digital es la única que goza jurídicamente de la presunción legal de autenticidad. Ahora bien, el proceso de validación de identidad es realizado por la Autoridad de Registro, que necesariamente es un área compuesta por un equipo humano que lleva a cabo la validación de identidad con base en los documentos que sean presentados por el suscriptor para la emisión del tipo de firma digital. En ese sentido, cualquier error humano u omisión por parte del equipo podría	Bajo el supuesto que hoy en día es posible la firma electrónica a través de la huella cotejada contra la base de datos de la RENEC, la validación de identidad tendría la participación de varios actores. Por una parte, el operador biométrico que proveería el software para llevar el cotejo de la huella dactilar, el cual para lograr hacer un cotejo contra la base de datos de la RENEC debe contar con una disponibilidad de sus servicios para permitir este macheo, y por otra parte, participaría la RENEC, quien cuenta con las bases de datos biográfica y biométricas, más confiables a nivel nacional, precisamente por las facultades constitucionales que ostenta. En ese sentido, el proceso de validación de identidad se encuentra bajo el imperio del operador biométrico y la Registraduría.	En este caso la validación de la identidad puede estar en manos de la misma compañía o en manos de un tercero. Si está en manos de la compañía, esta podría ser catalogada como un juez y parte en la emisión del certificado. Por otra parte, si está delegada en terceros, como empresas de tecnología, entidades de certificación digital o centrales de riesgos, se podría generar un mecanismo válido pero que se sustentaría en su emisión a través de las respuestas exitosas de preguntas reto generadas al usuario, las cuales siempre tienen un margen de error, o pueden ser conocidas incluso por personas muy cercanas al usuario. En este caso tampoco se presenta la

	ocasionar una falla en el proceso de validación de identidad.	Las fallas que se puedan dar en el proceso de validación dependerían de: 1) Los errores del software de cotejo de la huella y/o indisponibilidad del servicio por parte del operador biométrico o 2) Algún error que se encuentra en la base de datos biográfica y biométrica de la RENEC. En este caso, se tiene un proceso de validación de identidad a través de biometría, conforme el cual, si la validación de la huella es exitosa, por lo tanto esto podría ser utilizado como mecanismo de firma electrónica de carácter biométrico. Si bien este tipo de firma no gozaría jurídicamente con la presunción legal de no repudio, pues esta únicamente está consagrada para las firmas digitales, no obstante, para un usuario cuyo resultado de validación fue exitoso, repudiar dicho resultado, resultaría sumamente difícil toda vez que se encuentra de por medio la participación de un organismo como es la RENEC. Por lo cual, la	presunción legal de autenticidad.

		compañía del sector financiera podría contar con el apoyo no solo del operador biométrico sino de la misma RENEC.	
Sujetos involucrados en la prestación del servicio	Entidades de Certificación Digital abiertas	Registraduría Nacional del estado Civil y operador biométricos (en caso de no hacer uso de infraestructura propia)	Entidades de Certificación Digital abiertas, empresas de tecnología y centrales de riesgo
Integridad	Esta firma goza de integridad, pues en caso de alterarse la información del documento firmado digitalmente, inmediatamente se invalidaría la firma, tal y como lo señala el artículo 28 de la Ley 527 de 1999	Esta firma también permitiría evidenciar alteraciones sobre el documento firmado a través de este mecanismo, realizadas después del momento de la firma, según lo dispuesto en el artículo 4 del Decreto 2364 de 2012	Esta firma también permitiría evidenciar alteraciones sobre el documento firmado a través de este mecanismo, realizadas después del momento de la firma, según lo dispuesto en el artículo 4 del Decreto 2364 de 2012
No repudio	Es la única que goza de la presunción legal de no repudio prevista en el artículo 28 de la Ley 527 de 1999	Esta firma no gozaría de la presunción legal de no repudio, pues no está consagrado en la norma a su favor, sin embargo, repudiar este tipo de firma dada la intervención de la Registraduría Nacional del Estado Civil, sería sumamente difícil.	Esta firma no gozaría de la presunción legal de no repudio, pues no está consagrado en la norma a su favor.
Presencialidad /No presencialidad	Es un mecanismo de firma no presencial, por lo que goza de usabilidad	Se trataría de un mecanismo presencial, toda vez que se requiere que el usuario a quien se le va a validar la identidad y	Es un mecanismo de firma no presencial, por lo que goza de usabilidad

		quien firmará electrónicamente, asista presencialmente al lugar donde le cotejaran la huella. Su usabilidad no es tan clara.	

Así las cosas, de lo anteriormente expuesto se puede establecer lo siguiente:

- La vinculación del usuario es determinante a la hora de garantizar el atributo jurídico de autenticidad y de ahí en adelante continuar con el proceso de adquisición de los productos en medios electrónicos.
- La relación de un nombre de una persona en un documento no se considera una firma confiable y apropiada porque no necesariamente se requiere del solicitante como iniciador de la firma sino que, de acuerdo al Decreto 2364 de 2012 es necesario que los datos de creación de la firma sean datos únicos y personalísimos.
- Para llevar a cabo lo anterior, se requiere que la entidad financiera incluya la funcionalidad que permita: i) Obtener los datos únicos y personales del usuario que quiere firmar; ii) Generar un documento con el mensaje de datos que se quiera firma que permita su posterior consulta, PDF/A; iii) Invocar el método de firma electrónica con dato personal que provee la herramienta que se establezca para permitir realizar la firma.
- La escogencia de uno u otro mecanismo de firma electrónica depende necesariamente del análisis de riesgos que efectúe el área que va a implementar los mecanismos de firma electrónica en sus procesos. De esta manera, si los riesgos son altos, lo recomendable es hacer uso de mecanismos de firma electrónica robustos jurídicamente, como puede ser la firma digital que goza de las presunciones legales de autenticidad y no repudiación. Ahora bien, si los riesgos

están principalmente asociados a la validación de identidad, de contar con la mayor certeza en materia de validación, un mecanismo como la validación de identidad contra la base de datos de la RENEC y el firmado electrónico a través de las minucias dactilares puede ser el mecanismo más idóneo.

- Se puede llevar a cabo la escogencia de un mecanismo de validación de identidad y posteriormente un mecanismo de firma electrónica, o es posible suministrar únicamente un mecanismo de firma electrónica, que permitiría validar la identidad del usuario y adicionalmente que se vincule con el contenido de lo que está firmando. Es posible reforzar el proceso mediante la mezcla de dos o más factores de autenticación, por ejemplo “algo que el usuario sabe” con “algo que el usuario es”.
- Se recomienda nunca manejar el dato en claro, debe ser un dato cifrado o un resumen (HASH) del dato que permita su posterior cotejo contra una fuente confiable de información.
- La documentación o datos generados puede que estén potencialmente en riesgo de ser alterados posterior a su consulta, firma o aceptación por parte de la entidad financiera, siendo así que se genera una debilidad a la hora de probar que el documento o los datos son los mismos que se firmaron o aceptaron tanto para la entidad como para el usuario.
- El documento que va a ser firmado en medios electrónicos debe permanecer íntegro desde el momento en el que se aplicó la firma por de dicha entidad. Sin embargo, no se podrá garantizar fácilmente de manera inequívoca que el documento efectivamente fue firmado por el usuario, debido a que la acción de firma puede ser generada no necesariamente a partir de la acción iniciadora del firmante.
- La firma digital, permite garantizar que un mensaje de datos permanece íntegro a lo largo del tiempo, debido a que por medio de un procedimiento criptográfico se cifra un código alfanumérico único generado a partir del contenido del documento denominado hash. Si el

documento se llegase a alterar en su contenido, el hash que se calcule a partir de este momento será diferente al hash cifrado, por lo tanto inequívocamente se podrá concluir si el documento es o no el mismo desde el momento de su firma.

- Fortalecimiento de la conservación de la documentación electrónica: cuando se genera y se firma un documento en medios electrónicos y este documento tiene un periodo de vigencia prolongado, por ejemplo mayor a un año, es recomendable usar un elemento complementario a la firma digital, denominado estampado cronológico. Dicho estampado, que también se encuentra reconocido en la norma corresponde a un sello de tiempo que se impone sobre un mensaje de datos, siendo así que aporta un segundo nivel de integridad y se convierte en un anexo de la firma que almacena la fecha y hora exacta de la generación de la firma sobre el documento, según la hora legal colombiana provista por el reloj atómico del Instituto Nacional de Metrología, la cual estará certificada por una entidad de certificación digital acreditada por el ONAC. La estampa garantizará el momento exacto de la firma, y permitirá determinar que desde ese momento se deberá conservar el documento de acuerdo a las tablas de retención documental de la entidad financiera y conservar el estado del documento y de su firma digital.
- Si la compañía desea garantizar la integridad de los documentos que el usuario provee en el módulo de carga de documentos a través del cual este realizando el proceso de adquisición del producto, es recomendable firmarlos digitalmente con el certificado emitido a la entidad financiera y estamparlos cronológicamente para garantizar su integridad desde el momento que el usuario provee el documento, no obstante ésta documentación que provee el usuario hace parte de un expediente electrónico que la entidad financiera deberá empezar a manejar de manera electrónica haciendo uso de las tablas de retención documental que existen para estos documentos.

- Por otra parte, es importante reconocer que el uso de un mecanismo electrónico de firma no necesariamente puede eliminar los vacíos en materia de seguridad, por lo cual, la combinación de factores de autenticación y por lo tanto de mecanismos de firma electrónica, puede robustecer en términos de seguridad, la solución. Así las cosas, se encontraría también pendiente el uso de un tipo de firma electrónica que sea confiable y apropiada. Frente a esto, se recomienda el uso de firmas electrónicas, haciendo uso de métodos como datos biométricos.
- Dichos mecanismos permitirán, de manera inequívoca, demostrar la relación de una persona a un mensaje de datos, siempre y cuando el método usado sea lo suficientemente confiable y seguro. Es decir, el usuario debe estar seguro que la entidad financiera no podrá acceder al método utilizado para firmar en nombre de él, así como debe estar seguro que él es el único que puede inicializar el evento de firma. En consecuencia, la entidad financiera y el usuario deben estar seguros que el método utilizado brinda toda la información para demostrar que el usuario fue el iniciador del evento de firma.
- En este orden de ideas, la firma electrónica combinada con la firma digital con certificado de un tercero de confianza, aumenta su condición de confiabilidad y legalidad y se convierte en un mecanismo muy apropiado toda vez que brinda integridad del contenido del mensaje de datos, integridad del certificado de firma digital, integridad del dato único y personalísimos utilizado para la firma electrónica, autenticidad de los datos utilizados y longevidad a la firma.
- Ahora bien, las pantallas que muestran los términos y condiciones, acuerdos de uso de datos personales o cualquier otro “documento” no necesariamente deberán mostrarse en pantalla en formato pdf pero si el documento generado para firma deberá tener explícitamente el mismo contenido que el mostrado en pantalla.
- Los documentos que se generen se recomienda que estén en formato PDF/A pues este formato permite que la firma digital pueda ser visualizada más fácilmente.

- Así las cosas, el flujo del proceso podría ser el siguiente:

    1. Se valide la identidad del usuario a través del cotejo de su huella dactilar contra la base de datos de la RENEC o a través de preguntas reto, cotejadas contra una central de riesgo.
    2. Con la citada validación de identidad, el usuario tenga la posibilidad de firmar en medios electrónicos ya sea con su huella, para lo cual requerirá siempre la presencialidad, o a través de la emisión de un certificado de firma digital que sea provisto por una entidad de certificación digital.
    3. El usuario acepte términos y condiciones de la plataforma cuando se está registrando (Se realiza una vez), lo cual podrá ser realizado con firma digital o firma biométrica con huella. De requerirse presencialidad, se recomienda que sea a través de la huella, si no hay presencialidad, podrá ser a través de un certificado de firma digital.
    4. El usuario de manera seguida debe aceptar que va a realizar la firma electrónica antes de firmar documentos (Se recomienda hacer una vez), toda vez que el Decreto 2364 de 2012 exige al respecto un acuerdo entre las partes.
    5. Los documentos sean firmados digitalmente por la entidad financiera toda vez que con este mecanismos se obtienen las presunciones legales de autenticidad y no repudiación.
    6. Una vez firmados digitalmente dichos documentos estos sean estampados cronológicamente.
    7. La documentación generada y firmada sea almacena en el sistema de gestión documental que gestiones la entidad financiera o el tercero que tenga contratado para estos fines.
    8. A fin de garantizar el acceso a estas evidencias digitales, la entidad financiera debe exponer una funcionalidad que permita la posterior consulta sobre la información, por parte de sus funcionarios

9. Si algún documento requiere ser enviado al usuario que involucre datos personales, resulta importante que se cifre el documento.

Sumado a lo anterior, se incluyen también otras recomendaciones o sugerencias a la entidad financiera:

- La manifestación de lectura y aceptación que da el usuario final donde confirma lo expuesto por la entidad es una firma electrónica a la luz de la Ley 527 de 1999. Asimismo, se deberá contar con prueba de la autorización otorgada lo cual deberá revisarse a nivel técnico. Efectivamente de los documentos electrónicos debe quedar log transaccional y PDF, que permita comprobar que el usuario y/o cliente entraron al documento y aceptaron los términos y condiciones del producto, encriptado tanto el contenido como la aceptación de los mismos.
- Es importante individualizar y describir de manera particular cada servicio, por lo cual se recomienda que se manejen términos y condiciones por cada producto o servicio ofrecido.
- Que la entidad financiera dé cumplimiento a la Ley 1581 de 2012 respecto al tratamiento de datos personales y cuente con una política de tratamiento de datos personales.
- Emitir títulos valores totalmente inmaterializados para que el trámite sea 100% virtual. Teniendo en cuenta que el ordenamiento jurídico colombiano permite la sustitución del papel por mensajes de datos, y que estos últimos, en virtud del principio de equivalencia funcional deben recibir el mismo tratamiento jurídico que los documentos en papel.
- Teniendo en cuenta la entidad ofrecerá algunos de sus servicios a través de una plataforma electrónica, por lo tanto, estos últimos se encuentran inmersos en el comercio electrónico. Lo anterior, implica que se llevarán a cabo actos, negocios u operaciones de comercio concertadas por medio de mensajes de datos. En ese sentido, resulta de suma importancia

que la entidad tenga en cuenta la Ley 1480 de 2011 reconocida como el Estatuto del Consumidor, así como las disposiciones relativas al consumidor financiero.

- Adicionalmente, la entidad puede atender las recomendaciones que han sido desarrolladas por la Organización para la Cooperación y el Desarrollo Económico (OCDE) relativas a los Lineamientos para la Protección al Consumidor en el Contexto del Comercio Electrónico, las cuales permiten establece una serie de parámetros que será recomendable que esta entidad tenga en cuenta para ofrecer sus servicios en la plataforma en línea. Estos lineamientos son los siguientes:
  - Protección transparente y efectiva: Debe otorgarse a los consumidores que participen en el comercio electrónico una protección transparente y efectiva en el desarrollo de las actividades en línea.
  - Información en línea: Debe proporcionarse de manera precisa, clara y accesible, información suficiente sobre la entidad que está prestando el servicio. De igual forma, debe proporcionarse información precisa y accesible que describa los bienes o servicios ofrecidos, siendo así que el consumidor pueda tomar una decisión informada antes de participar en la transacción y en términos que le permita mantener un adecuado registro de dicha información. Finalmente, debe proporcionarse información suficiente sobre los términos, condiciones y costos asociados con la servicios que serán prestados, que permita a los consumidores tomar una decisión informada antes de participar en las transacciones, lo cual incluirá las políticas, derechos, deberes y responsabilidad con respecto a los contenidos digitales.
  - Procedimiento de confirmación: Debe permitirse al consumidor identificar los bienes o servicios que desea comprar, identificar y corregir cualquier error o modificación de la orden de compra, expresar su consentimiento para realizar la compra de manera

deliberada y razonada, así como de conservar un registro completo y preciso de la transacción.

- Mecanismos de pago: Debe proporcionarse a los consumidores mecanismos de pago seguros y fáciles de utilizar y en consecuencia información sobre el nivel de seguridad que brinden tales mecanismos.
- Ley aplicable y territorialidad: Los servicios deben sujetarse al marco legal vigente sobre ley aplicable y la competencia jurisdiccional. De igual forma, debe proporcionarse a los consumidores un fácil acceso a mecanismos alternativos para un justo y oportuno proceso de resarcimiento y resolución de disputas sin costos o cargos onerosos.
- Privacidad, protección de datos personales: Debe conducirse de acuerdo con los principios de privacidad y protección de datos personales[57].

- Precisamente, como lo establece el artículo 50º de la Ley 1480 de 2011, serán obligaciones de aquellas compañías que ofrezcan productos utilizando medios electrónicos, las siguientes:

  - Informar en todo momento de forma cierta, fidedigna, suficiente, clara, accesible y actualizada su identidad especificando su nombre o razón social, Número de Identificación Tributaria (NIT), dirección de notificación judicial, teléfono, correo electrónico y demás datos de contacto.
  - Suministrar en todo momento información cierta, fidedigna, suficiente, clara y actualizada respecto de los productos que ofrezcan. En especial, deberán indicar sus

[57] Disponible en http://www.oecd.org/sti/consumer/34023784.pdf

características y propiedades tales como el tamaño, el peso, la medida, el material del que está fabricado, su naturaleza, el origen, el modo de fabricación, los componentes, los usos, la forma de empleo, las propiedades, la calidad, la idoneidad, la cantidad, o cualquier otro factor pertinente, independientemente que se acompañen de imágenes, de tal forma que el consumidor pueda hacerse una representación lo más aproximada a la realidad del producto.

- Informar, en el medio de comercio electrónico utilizado, los medios de que disponen para realizar los pagos, el tiempo de entrega del bien o la prestación del servicio, el derecho de retracto que le asiste al consumidor y el procedimiento para ejercerlo, y cualquier otra información relevante para que el consumidor pueda adoptar una decisión de compra libremente y sin ser inducido en error.
- La aceptación de la transacción por parte del consumidor deberá ser expresa, inequívoca y verificable por la autoridad competente. El consumidor debe tener el derecho de cancelar la transacción hasta antes de concluirla.
- Concluida la transacción, el proveedor y expendedor deberá remitir, a más tardar el día calendario siguiente de efectuado el pedido, un acuse de recibo del mismo, con información precisa del tiempo de entrega, precio exacto, incluyendo los impuestos, gastos de envío y la forma en que se realizó el pago.
- Queda prohibida cualquier disposición contractual en la que se presuma la voluntad del consumidor o que su silencio se considere como consentimiento, cuando de esta se deriven erogaciones u obligaciones a su cargo.
- Mantener en mecanismos de soporte duradero la prueba de la relación comercial, en especial de la identidad plena del consumidor, su voluntad expresa de contratar, de la forma en que se realizó el pago y la entrega real y efectiva de los bienes o servicios

adquiridos, de tal forma que garantice la integridad y autenticidad de la información y que sea verificable por la autoridad competente, por el mismo tiempo que se deben guardar los documentos de comercio.

- Adoptar mecanismos de seguridad apropiados y confiables que garanticen la protección de la información personal del consumidor y de la transacción misma. El proveedor será responsable por las fallas en la seguridad de las transacciones realizadas por los medios por él dispuestos, sean propios o ajenos.
- Disponer en el mismo medio en que realiza comercio electrónico, de mecanismos para que el consumidor pueda radicar sus peticiones, quejas o reclamos, de tal forma que le quede constancia de la fecha y hora de la radicación, incluyendo un mecanismo para su posterior seguimiento.

V. Conclusiones

A continuación se presentan las conclusiones en relación con lo expuesto en el presente trabajo a la luz del caso hipotético propuesto:

- Que en el ordenamiento jurídico colombiano es posible evidenciar que es posible hacer uso de distintos tipos de mecanismos de firmas electrónicas, siempre y cuando estos den cumplimiento a lo dispuesto en el Decreto 2364 de 2012, especialmente a lo que se refiere a los atributos jurídicos de “confiable” y “apropiado”.
- Que una firma electrónica sería simplemente cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita. En este concepto amplio y tecnológicamente indefinido de firma,

tendrían cabida técnicas tan simples como un nombre u otro elemento identificativo, incluido al final de un mensaje electrónico, pero que en cualquier caso debe procurar su valor probatorio a efectos de garantizar la autenticación, así como la integridad del mensaje. Así por ejemplo, la firma del propio sujeto escaneada e incorporada a un documento electrónico es una firma electrónica, y como tal ha de ser tenida, pero no ofrece ninguna seguridad o fiabilidad sobre la identidad e integridad del texto cuando exista controversia sobre tales extremos.

- Ello pone de manifiesto una primera realidad, como es que existen distintas clases de electrónica, si bien con distintos niveles o grados de seguridad, lo que se traduce jurídicamente en una distinta eficacia probatoria de las distintas firmas electrónicas que aunque en principio son válidos jurídicamente todos los mecanismos de firmas electrónicas, desde que cumplan lo dispuesto en el Decreto 2364 de 2012, siendo así que todos pueden ser catalogados como equivalentes de una firma manuscrita, no obstante, la firma digital tiene una bondades o ventajas desde el punto de vista jurídico que la hacen ser mucho más robusta jurídicamente que los demás tipos de firmas electrónicas, lo cual se debe a las presunciones legales de autenticidad y no repudio.
- Que el ordenamiento jurídico colombiano consagra mecanismos robustos de autenticación electrónica y de firmas electrónicas, siendo así que a algunos de estos los ha dotado de robustez jurídica, como es el caso de la firma digital. Sin embargo, darles el carácter de mayor o menor robustez desde el punto de vista técnico, depende necesariamente no solo de las propiedades del mecanismo de firma electrónica, sino también de la combinación de factores de autenticación que convertirán a una solución en algo más o menos seguro desde el punto de vista electrónico.

- Que la firma biométrica a través de la huella con la participación de la Registraduría Nacional del estado Civil, podría catalogarse como el segundo tipo de firma electrónica más robusto, después de la firma digital, toda vez que llevar a cabo una repudiación de la misma resultaría muy difícil, pues se la validación de identidad se realiza contra la base de datos biográfica y biométrica más confiable de Colombia que es la de la Registraduría Nacional del Estado Civil, que se actualiza en tiempo real al nutrirse de otras bases de datos.
- Que si bien las claves como mecanismos de firma también pueden ser seguras, no obstante, no gozan de las presunciones de legales de autenticidad y no repudio, y además no necesariamente conllevan la participación de terceros como entidades de certificación digital y centrales de riesgos, toda vez que pueden ser directamente generadas por la misma compañía, que no está obligada a cumplir unos estándares técnicos altos exigidos por una autoridad competente. por lo que podrían ser quebrantadas fácilmente. De igual forma, se podrían en duda que la compañía puede obrar como juez y parte en la emisión de la firma.
- Que la participación de terceros como las entidades de certificación digital o la misma Registraduría Nacional del Estado Civil, puede hacer que los mecanismos de firmas electrónicas sean más seguros, pues cuentan con el respaldo de tercero que se encuentran soportados o fundamentados en un normativa y en una vigilancia y control.

Bibliografía

Doctrina

CASTRO, Marcela. Fundamentos de derecho de los negocios para no abogados: Capítulo VII Comercio Electrónico,
Nelson Remolina Angarita. Bogotá: Editorial Temis, 2013.

RINCÓN CÁRDENAS, Erick. Derecho del Comercio Electrónico y de Internet. Segunda Edición. Bogotá: Editorial Legis, 2015.

TRIVELLI GONZÁLEZ, María Paz. El Principio de Neutralidad Tecnológica en la Ley No 19.799. Disponible en http://www.derechoinformatico.uchile.cl/index.php/RCHDI/article/viewFile/10675/10953

PEÑA VALENZUELA, Daniel. De la firma manuscrita a las firmas electrónica y digital. Derecho Internacional de los Negocios Tomo V. Universidad Externado de Colombia. Bogotá: 2015.

Diccionario de la Lengua Española. Real Academia Española, Vigésima segunda edición, Madrid, 2001.

Jurisprudencia:

Corte Constitucional, Sentencia C- 831 de 2001, M.P Alvaro Tafur Gálvis.

Corte Constitucional, Sentencia C – 662 de 2000, M.P. Fabio Morón Díaz.

Sentencia de casación, Sala de Casación Civil, septiembre 4 de 2000, rad. 5565, M. P.: Jaramillo, C. I. Citada sentencia del 27 de agosto de 2003 (proceso 20166) de la Corte Suprema de Justicia (CSJ), M. P.: Pulido de Barón, M.

Normas:

Ley 527 de 1999

Decreto ley 019 de 2012

Decreto 2364 de 2012

Decreto 333 de 2014

Decreto 1074 de 2015

Recursos Electrónicos:

Objetivos de Desarrollo Sostenible. Disponible en https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

OECD, Recommendation of the Council on Government Strategies, Public Governance and Territorial Development Directorate. 15th July 2014. Disponible en http://www.oecd.org/gov/public-innovation/Recommendation-digital-government-strategies.pdf

OECD, Recommendation of the Council on Government Strategies. Disponible en https://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf

Ley Modelo de la CNUDMI sobre Firmas Electrónicas de 2001, página 8. Disponible en http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf

Ley Modelo de la CNUDMI sobre Comercio Electrónico de 1996, p 17. Disponible en https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional en su documento de "fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas". Disponible en https://www.uncitral.org/pdf/spanish/texts/electcom/08-55701_Ebook.pdf

Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, p 16. Disponible en https://www.boe.es/doue/2014/257/L00073-00114.pdf

Organismo Nacional de Acreditación de Colombia (ONAC), Directorio de Acreditación. Disponible en https://onac.org.co/directorio-de-acreditacion-buscador

Entidades de Certificación Digital, ficha técnica del esquema. ONAC, Disponible en https://onac.org.co/certificacion-de-firmas-digitales

Certificación 16-ECD-001 de la compañía Gestión de Seguridad Electrónica GSE S.A. proferida por el Organismo Nacional de Acreditación de Colombia (ONAC). Disponible en https://onac.org.co/certificados/16-ECD-001.pdf

Guía No. 3 Cero papel en la Administración Pública, Documento electrónico. Ministerio de Tecnologías de la Información y las Comunicaciones. Disponible en https://docplayer.es/3613313-Guia-no-3-cero-papel-en-la-administracion-publica-documentos-electronicos.html

Biometría: conveniente y segura. Edición 1138, Semana Económica, 2018. Asobancaria. Disponible en https://www.asobancaria.com/wp-content/uploads/1138-C-28-05-2018.pdf

Operadores biométricos habilitados por la Registraduría Nacional del Estado Civil. Disponible en https://wsp.registraduria.gov.co/biometria/operadores/listar/

Clave Virtual, Cámara de Comercio de Bogotá https://linea.ccb.org.co/clavevirtual/portalconsulta/default.aspx y https://www.ccb.org.co/Inscripciones-y-renovaciones/Registro-Unico-de-Proponentes/Clave-virtual

Entrevistas:

Entrevista a Camilo Reyes, Director de Factura Electrónica, Certicámara S.A.

Entrevista a Tatiana Hernández, Directora de Identidad Digital, Firmas y Componentes, Certicámara S.A.