"Los servicios de estampado cronológico y archivo confiable a cargo de las entidades de certificación satisfacen la necesidad de no repudio en las comunicaciones y transacciones electrónicas, y complementan los servicios de certificación digital propios de este tipo de entidades"

Estampado cronológico, archivo y conservación de mensajes de datos como medidas de seguridad jurídica preventiva

Erick Rincón Cárdenas[1]

RESUMEN

Dentro de la habilitación legal de las entidades de certificación digital para el comercio electrónico se encuentran algunos servicios que tienen tanta o mayor importancia que las firmas y los certificados digitales. Se trata del *estampado cronológico* y el archivo de documentos. Estos servicios prestados a través de terceros de confianza se fundamentan en la idea de que el documento electrónico —asimilado jurídicamente al documento en soporte papel— es único y original. Es la única evidencia legal autentica e íntegra que acredita la relación, el acto, el contrato, la manifestación etc. Es por ello que no se nos escapa la trascendencia jurídica que tiene asegurar la conservación, el archivo y la recuperación del documento que es evidencia legal.

ABSTRACT

Within the legal rating of the certification authorities for electronic commerce are some services that have so much or greater importance than digital signatures and

1 Abogado de la Universidad del Rosario. Especializado en Derecho Financiero y Derecho Contractual de la Universidad del Rosario. D.E.A. en Derecho Mercantil de la Universidad Alfonso X de España. Candidato a Doctor en Derecho. Profesor de la cátedra de Comercio Electrónico en la Universidad del Rosario. En la actualidad es Asesor de la Vicepresidencia Jurídica de la Cámara de Comercio de Bogotá.

Las ideas expuestas en este documento son opiniones personales, de exclusiva responsabilidad del autor y no comprometen la posición oficial de cualquier entidad respecto de los temas aquí tratados.

digital certificates. I am talking about time stamping and trusted archive. These services offered through third parties of confidence are based on the idea that the electronic document (legally assimilated to the document in paper) is unique and original. It is the only authentic and complete legal evidence that credits reports, acts, contracts, manifestations etc. That is why we recognize that to assure the conservation, file and recovery of the document —which is legal evidence— is of great legal transcendence.

KEYWORDS: *Estampado cronológico*, entidad de certificación, *archivo confiable*. Time stamping, certification authorities, trusted archive service.

Introducción

Tras más de cinco años de aplicación de la ley 527 de 1999, el mencionado instrumento normativo se ha mostrado como determinante al momento de calificar la seguridad jurídica de un mensaje de datos empleado en cualquier tipo de comunicación electrónica. Ello por cuanto estableció un mecanismo técnico con atributos que hacen posible presumir la confiabilidad de un mensaje de datos, esto es la firma digital —una de las especies de la firma electrónica.[2]

Dentro del contexto de seguridad jurídica en entornos electrónicos y de conformidad con el marco legal vigente, es fundamental la intervención de los prestadores de servicios de certificación digital, entendiendo por estos aquellas personas que, autorizadas conforme a las disposiciones legales, están facultadas para emitir certificados en relación con las firmas digitales de las personas. La obligación general del prestador de servicios de certificación consiste en utilizar sistemas, procedimientos y recursos humanos adecuadamente confiables y actuar de conformidad con las declaraciones que haga respecto a las políticas de certificación contenidas en la Declaración de Prácticas de Certificación (DPC). Deben actuar, además, con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el certificado expedido, sean exactas y cabales.

Hoy, con casi seis años de vigencia de la ley, se reconoce el importante papel de dichas entidades en garantizar la seguridad —tanto técnica como jurídica— de las diferentes comunicaciones por medios electrónicos. Además, se ha asociado su intervención a la generación y verificación de firmas y certificados digitales, pues son los productos y servicios tradicionales que prestan las mencionadas entidades.[3]

---

2 De conformidad con la ley, se entiende firma digital como un valor numérico que se adhiere a un mensaje de datos y que utiliza un procedimiento matemático vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de afectada la transformación.

3 Un ejemplo de ello lo constituye la aplicación de la firma digital en diferentes trámites y procedimientos a través de las siguientes normas:

1. La Resolución No.643 de 2004 de la Superintendencia de Notariado y Registro - Por la cual se definen las reglas para el envío electrónico de las copias de las escrituras públicas sujetas a registro en las Cámaras de Comercio, y en la que se fijan las condiciones para la remisión de documentos de origen notarial desde las Notarías Colombianas a las Cámaras de Comercio utilizando firmas digitales.
2. Las Circulares No. 011, 012, 013 y 014 de 2004, de la Superintendencia de Salud, que habilitan el uso de firmas digitales certificadas para el envío de reportes de información financiera y general por parte de las instituciones prestadoras de servicios privadas, las entidades promotoras de salud, las empresas licoreras, las loterías y en general, los obligados a reportar a la Superintendencia.

Sin embargo, es importante recordar que dentro de la habilitación legal de las entidades de certificación se encuentran otros servicios que tienen tanta o mayor importancia que las firmas y los certificados digitales y que también podrían estar asociados a estos. Se trata del *estampado cronológico* y el archivo de documentos.[4] El presente artículo pretende profundizar en las posibilidades jurídicas de estos dos servicios a cargo de las entidades de certificación digital que, a pesar de su importancia, aún no han sido analizados jurídicamente.[5]

---

3. La Circular 27 de 2004 de la Superintendencia Bancaria que posibilitó la comunicación entre la superintendencia y sus vigiladas utilizando firmas digitales.
4. La Circular externa 07 de 2005 de la Superintendencia de Sociedades, en la que se habilita el envío electrónico —utilizando firma digital— de la información financiera requerida a las sociedades comerciales vigiladas y controladas, sucursales de sociedades extranjeras y empresas unipersonales vigiladas y controladas.
5. Las Circulares externas 06 y 09 de 2005 de la Superintendencia de Valores en las que se establecieron el uso de la firma digital en la presentación de los reportes de envío de información de fondos de inversión de capital extranjero y las sociedades administradoras de fondos de valores y de inversión relacionados con los títulos que componen cada portafolio, junto con sus estados financieros. De manera precedente la Circular 11 de 2003 de la Superintendencia de Valores habilitó el uso de firmas digitales certificadas para el envío de reportes por los vigilados de esa entidad
6. Las Circulares externas 038 y 057 de 2005 del Ministerio de Comercio, Industria y Turismo en las que se establece el uso de la firma digital para la utilización de la Ventanilla Única de Comercio Exterior (VUCE).

4 La ley 527 de 1999, da el siguiente tratamiento al tema:

"Articulo 30. actividades de las entidades de certificación. Las entidades de certificación autorizadas por la Superintendencia de Industria y Comercio para prestar sus servicios en el país, podrán realizar, entre otras, las siguientes actividades:

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

"2. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos.

"3. Emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la presente ley.

"4. Ofrecer o facilitar los servicios de creación de firmas digitales certificadas.

"5. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.

"6. Ofrecer los servicios de archivo y conservación de mensajes de datos." (Resaltado fuera del texto original)

5 El decreto No. 1747 de septiembre 11 de 2000, por el cual se reglamenta parcialmente la ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales, define así el servicio: "Estampado cronológico: mensaje de datos firmado por una entidad de certificación que sirve para verificar que otro mensaje de datos no ha cambiado en un período que comienza en la fecha y hora en que se presta el servicio y termina en la fecha en que la firma del mensaje de datos generado por el prestador del servicio de estampado, pierde validez."

Con el objetivo de emprender este análisis, el artículo tendrá la siguiente estructura: (i) Se introducirá al lector en el importante papel que cumplen las entidades de certificación en la seguridad de las comunicaciones electrónicas; (ii) se definirá ampliamente el concepto de *estampado cronológico* y se analizará la forma en la que las entidades de certificación intervienen en la prestación del servicio; (iii) se analizarán las posibilidades normativas del *estampado cronológico*— de conformidad con nuestro ordenamiento jurídico vigente —en entornos electrónicos o con ocasión de la utilización de mensajes de datos; (iv) se expondrá el concepto de *archivo confiable* de mensajes de datos; y finalmente (v) se expondrá el fundamento normativo para la aplicación del servicio de *archivo confiable* de conformidad con nuestro ordenamiento jurídico vigente.

1. Las entidades de certificación

Las entidades de certificación digital son terceros de confianza que se dedican a la prestación de servicios de certificación digital, a través de un sistema del mismo tipo. Los servicios de certificación digital brindan seguridad a las comunicaciones que se realizan en redes abiertas —como por ejemplo en Internet— mediante la expedición de certificados digitales en los que ofrecen información a los usuarios sobre la persona con la que se están comunicando.

Legalmente, una entidad de certificación digital se define como toda persona jurídica, pública o privada, nacional o extranjera, cámara de comercio o notario que, previa autorización estatal, está facultada para emitir certificados digitales, ofrecer o facilitar los servicios de *estampado cronológico* de mensajes de datos y cualquier otra función relativa a las comunicaciones basadas en las firmas digitales.[6]

La ley 527 de 1999 divide las entidades de certificación en entidades cerradas y abiertas.[7] Las entidades cerradas pueden ofrecer sus servicios sólo para el intercambio

6 En sentencia C-662 de 2000 se cuestionó el texto íntegro de la ley 527 de 1999 y, en especial, sus artículos 10, 11, 12, 13, 14, 15, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 y 45, por estimar que violan el artículo 131 de la Carta Política, así como los artículos 152 y 153. Afirma la citada providencia que, en consecuencia, las entidades de certificación serán "las encargadas entre otras cosas, de facilitar y garantizar las transacciones comerciales por medios electrónicos o medios diferentes a los estipulados en papel e implican un alto 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." (Corte Constitucional, sentencia C-662 de 2000).

7 Para la elaboración del decreto reglamentario de la ley 527 de 1999 se establecieron cuatro grupos temáticos integrados por representantes de distintas entidades públicas, privadas y académicas quienes se encargaron de estudiar de manera técnica y detallada la ley para determinar cuáles de sus apartes deberían ser objeto de reglamentación. Los grupos integrados y coordinados por el Ministerio de Comercio, analizaron los siguientes temas: Archivo y

de mensajes entre la entidad de certificación y el suscriptor, sin exigir remuneración por ello. Por oposición, las entidades de certificación abiertas pueden ofrecer sus servicios para el intercambio de mensajes sin limitación y reciben remuneración por ello. Significa lo anterior que una entidad de certificación cerrada puede emitir certificados digitales: (i) Útiles sólo para firmar digitalmente los mensajes de datos que intercambien la entidad y los titulares (suscriptores) de los certificados y (ii) no puede recibir remuneración alguna por el servicio.

Por su parte, los certificados de una entidad de certificación abierta pueden ser usados para firmar digitalmente mensajes de datos enviados por el firmante a cualquier persona. Además, la entidad puede cobrar por este servicio. En general, los certificados digitales son "documentos electrónicos" expedidos por una entidad de certificación que identifican al suscriptor y le permiten firmar digitalmente mensajes de datos.

La principal ventaja jurídica de las firmas digitales es que permiten presumir que quien las impuso en un mensaje de datos tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo. Este es el efecto jurídico de la propiedad de *no repudiación de mensajes de datos* que tiene la certificación digital.

Esta presunción, garantiza que quien observe una firma digital en un mensaje de datos puede suponer válidamente y de manera inequívoca, que el firmante es quien dice ser y que se vincula con el contenido del mensaje.

Sin embargo, los certificados digitales emitidos por una entidad de certificación cerrada no pueden, de manera directa, aplicar esta presunción a las firmas digitales que se imponen en los mensajes intercambiados entre la entidad de certificación cerrada y el suscriptor del servicio. En caso de controversia (usualmente causada por repudiación judicial o administrativa del mensaje) se hace necesario que la entidad demuestre, entre otros, que la firma ha estado bajo el control exclusivo de la persona que la usa de manera permanente. Por el contrario, los certificados digitales emitidos por una entidad de certificación abierta si pueden tener este efecto de manera universal.

Para emitir los certificados digitales las entidades de certificación digital utilizan lo que se conoce como la *Infraestructura de Clave Pública* (PKI, por sus siglas en inglés), es decir el conjunto de elementos tecnológicos que, mediante la utilización de un par de llaves criptográficas almacenadas en el certificado digital (una llave de conocimiento público y la otra de uso privado), logran:

---

conservación de documentos, bajo la coordinación del Ministerio de Justicia y del Derecho; Documentos electrónicos, bajo la coordinación de la DIAN; El Contrato de Transporte de Mercancías, bajo la coordinación del Ministerio de Transporte y Entidades de Certificación y Firma Digital, bajo la coordinación de la Superintendencia de Industria y Comercio. El análisis determinó que únicamente el tema de Entidades de Certificación y Firma Digital debería ser objeto de reglamentación por parte del Gobierno Nacional.Ver: http://www.mincomercio.gov.co/VBeContent/NewsDetail.asp?ID=937&IDCompany=4:

1. Identificar a quien se envía una comunicación.
2. Impedir que terceras personas puedan observar los mensajes que se envían a través de medios electrónicos.
3. Impedir que un tercero pueda alterar la información que es enviada a través de medios electrónicos.
4. Evitar que el suscriptor del servicio de certificación digital que envió un mensaje electrónico pueda después negar dicho envío.

Sobre este último atributo (No repudio), los servicios de *estampado cronológico* y archivo de mensajes de datos tienen una especial relevancia, como lo veremos a continuación.

2. *El* estampado cronológico

El aumento de uso de documentos electrónicos y la necesidad de establecer relaciones entre un documento y su tiempo de generación, modificación y firma, trae como consecuencia la necesidad de crear evidencias de la posesión de esos datos en un momento determinado. La solución consiste en introducir —más en el contenido que en el continente— señales de tiempo, relacionadas con el momento de creación y modificación de un documento. Ello mediante el uso del servicio de *estampado cronológico*, cuya única finalidad es probar que un determinado instante, todos los agentes involucrados declararon disponer o disponían de un documento.

El servicio de *estampado cronológico* —en inglés, *time stamping*— o fechado digital como se le conoce en otros países, parte de una premisa fundamental y es que el tiempo ha sido, es y seguirá siendo una de las variables más importantes en el desarrollo de cualquier actividad humana y por tanto, referencia básica de la mayor parte de los procedimientos y trámites que tienen lugar entre el sector público y privado. Tradicionalmente, la constancia expresa de la fecha y hora de la realización de un acto se efectúa sobre soporte papel, circunstancia que inevitablemente se ve modificada con la utilización generalizada de las nuevas tecnologías de la información.

El actual entorno precisa de la utilización del servicio de sellado de tiempo, con el objetivo de brindarle confianza a la comunidad. En estos momentos existen distintas líneas de trabajo y tendencias en cuanto a los protocolos que deben aplicarse para garantizar la seguridad de tales servicios de fechado digital, la fuente de tiempos a utilizar y los mecanismos de sincronización.[8]

8 Sobre este tema se puede consultarse el siguiente vinculo:

http://64.233.187.104/search?q=cache:Njk0KWKP8PIJ:wotan.liu.edu/dois/data/Papers/juledslbl7425.html+%22fechado+digital%22+%2B+%22firma+digital%22+&hl=es

Los servicios de fechado digital, comienzan a tener relevancia cuando se tienen en cuenta hechos cotidianos que no pocas veces generan conflictos, como son: (i) La constancia de fecha y hora de las transacciones; (ii) ¿cuándo se emitió una factura? y (iii) ¿si se presentó a tiempo una reclamación?.

Cuando se realizan operaciones en plataformas tecnológicas, el conocimiento del tiempo es importante y solicitar a un tercero que de constancia de ello, es fundamental al momento de aportar pruebas.[9] Por ello, la ley 527 de 1999 contempló esa posibilidad en la prestación de servicios del tercero de confianza del comercio electrónico: las entidades de certificación digital. En el contexto arriba descrito, a un documento electrónico es posible agregarle *estampado cronológico* con el propósito de dejar evidencia de que desde una fecha y hora ciertas, el documento no ha sido modificado. El estampado (en inglés, *Timestamping*) es un mecanismo *on-line* que permite demostrar que una serie de datos han existido y no han sido alterados, desde un instante específico en el tiempo. Allí, la entidad de certificación digital actúa como tercera parte de confianza, testificando la existencia de dichos datos electrónicos en una fecha y hora concretos.[10]

De acuerdo con la normatividad vigente[11] un *estampado cronológico* es un mensaje de datos firmado digitalmente por una entidad de certificación que sirve para verificar que dicho mensaje no ha cambiado en un período determinado; período que comienza en la fecha y hora en que se presta el servicio de *estampado cronológico* y que termina en la fecha en que la firma del mensaje de datos generado por la entidad de certificación pierde validez. El "estampado" puede también acompañar un mensaje de datos firmado digitalmente por el suscriptor de un certificado digital, para evidenciar de manera inequívoca e inviolable, incluso para el firmante, el momento en que ese mensaje de datos fue o se encontraba firmado digitalmente.

Concluyendo sobre el concepto, se puede decir que el *estampado cronológico* es el método idóneo para proporcionar certidumbre probatoria del instante de tiempo en que un documento electrónico es generado, enviado o recibido. Es decir el "estampado" es un archivo informático que vincula la información a una fecha y una hora específica. Esta vinculación se produce a través de un sistema seguro de tiempo sincronizado con la *Escala de Tiempo Universal* (UTC).

9 Agenda de Conectividad, "Pagos en Línea y firma electrónica, para fin de año en Colombia", publicado originalmente el 03/29/2004, en http://www.agenda.gov.co/BulletinBoard/view_one.cfm?MenuID=3&ID=116

10 Sobre la actuación de una entidad de certificación, se puede profundizar en: http://www.ancert.com/?do=products&group=timestamping&option=timestamping

11 Artículo 1, numeral 8° del decreto 1747 de 2000.

2.1. La necesidad del servicio[12]

El tiempo es un hecho irreversible que afecta globalmente todas las actividades humanas y es un componente clave para las relaciones causales entre procesos. Las relaciones de dependencia entre unos hechos y otros son función del orden en el que se realizan cada uno de ellos y suelen ser manifestación de las relaciones causales que los unen. La precisión en el tiempo y los contenidos de las transacciones resultan de gran importancia en el comercio electrónico. Sin embargo, las transacciones actuales se realizan usando fuentes de tiempo de los propios computadores de compradores o vendedores. Por tanto, el tiempo no es confiable y puede ser fácilmente manipulado y repudiado. Así mismo, los contenidos de los pedidos, facturas u otros documentos implicados en transacciones *on-line*, son susceptibles de ser alterados. Estos problemas diezman la confianza de la gente en el comercio electrónico y entorpecen su desarrollo.

Al aplicar *estampas cronológicas* en los documentos electrónicos, se garantiza que las transacciones ocurren en un momento particular y que sus contenidos no han sido alterados desde entonces. Al integrar un servicio de *estampa cronológica* se puede prevenir efectivamente el fraude y la repudiación. Compradores y vendedores pueden operar, por lo tanto, en un entorno fiable y tener mayor confianza en el comercio electrónico.

Ejemplificando las necesidades de este servicio en particular, uno de los casos más interesantes es el de un Concurso Público de Ofertas. En este caso, varias compañías exponen sus opciones como respuesta a un mismo pliego y presentan sus ofertas con el objetivo de ganar el concurso. Actualmente sus propuestas, convenientemente firmadas por sus representantes legales, se introducen en sobres que se cierran y sellan para, posteriormente, ser entregados en depósito ante el organismo titular del concurso. Cuando han sido presentadas todas las propuestas dentro de un mismo plazo de tiempo marcado por las normas del concurso, se reúnen en un acto público todas las partes involucradas para verificar el estado inalterado de los sellos y luego, abrir los sobres haciendo público su contenido.

Si alguien pudiese abrir los sobres antes de que se termine el plazo de presentación de ofertas, el trasgresor podría conocer información privilegiada que le permitiría ganar fraudulentamente el concurso. Además, si alguien pudiese sustituir o modificar una oferta previa, incluyendo algo nuevo después de que haya terminado el plazo de presentaciones, también dispondría de información privilegiada que posiblemente se habría filtrado desde sus oponentes, ya que éstos se encuentran más relajados al creer que nada puede hacerse ya para modificar las opciones presentadas.

12 Sobre el particular se puede consultar en siguiente vínculo: http://tirnanog.ls.fi.upm.es/CriptoLab/Proyectos/TicTac/TicTac.html

En este caso, lo mejor sería no tener que entregar, en modo alguno, las propuestas antes de que deban ser abiertas y hechas públicas. Para poder hacerlo así, tan sólo es necesario que exista un mecanismo confiable que pruebe la existencia de cada una de las propuestas con anterioridad a la finalización del plazo de presentación, de modo que nadie pueda modificarlas con posterioridad y antes de hacerlas públicas, resolviendo automáticamente el concurso.

Está fuera de discusión que el entorno físico —por oposición al virtual, si se permite dicha asociación— está bastante bien adaptado al paso del tiempo. La sociedad ha desarrollado figuras y procedimientos sociales que lo consolidan de forma vinculante para las partes. En efecto, se encuentran figuras como la de los notarios que dan fe de la fecha y hora de un acto.

En el entorno virtual el tiempo pasa de otra forma, si es que tan siquiera pasa. Así por ejemplo, el reloj de un computador es fácilmente manipulable, los documentos son sencillamente editables, entre otras cosas. Pero si se intenta hacer del comercio electrónico una realidad y digitalizar buena parte de la actividad humana, se debe encontrar el remedio de aquella seguridad física a la que nos hemos acostumbrado y en la que hemos basado nuestras leyes. Es en este punto donde aparecen los sistemas de fechado digital que intentan correlacionar la existencia de los *bits* a los eventos humanos de referencia, en general y en particular, al convenio de tiempo absoluto.[13]

2.2. Problemas que puede solucionar el *estampado cronológico*

Del análisis de la figura es relevante destacar los problemas que pretende solucionar —partiendo de los que conjura la propia certificación digital— a saber:

(i) El primero de los problemas —que no está directamente asociado al *estampado cronológico*— lo constituye la verificación de la autenticidad del origen de la información. Es decir, cómo saber si realmente la información que llega es de quien dice ser el remitente y si la transacción gestionada es realmente la que se solicitó. Sin embargo, más que un problema asociado al fechado digital, podría decirse que se trata de un problema común que puede ser resulto a través de la firma digital (éste último instrumento también puede solventar otros problemas comunes a las transacciones electrónicas como son la integridad y la confidencialidad).

(ii) En segundo lugar, pero no por ello menos importante, se encuentra el *no repudio*. En general, los certificados digitales son "documentos electrónicos" expe-

13 Sobre el particular, consultar en siguiente vínculo: http://www.eurologic.es/conceptos/fechadodigital.htm

didos por una entidad de certificación que identifica al suscriptor y le permite firmar digitalmente mensajes de datos. La ventaja jurídica de las firmas digitales es que permiten presumir que quien las impuso en un mensaje de datos tenía la intención de "acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo."[14] Este es el efecto jurídico de la propiedad de *no repudio* de mensajes de datos que tiene la certificación digital. Dicha presunción garantiza que quien observe una firma digital en un mensaje de datos puede suponer válidamente y de manera inequívoca, que el firmante es quien dice ser y que se vincula con el contenido del mensaje.

Desde el punto de vista jurídico, el problema más destacado parece ser el *no repudio* ya que trae como consecuencia, desde el punto de vista probatorio, que el remitente de un mensaje de datos no niegue ser autor de ciertos actos. El *no repudio,* que se resuelve con la firma digital, puede complementarse con un esquema de *estampado cronológico* Es por ello que es necesario hacer alusión a las formas en las que se podría implementar dicho servicio:

a. A través de las entidades de certificación digital. Ello teniendo en cuenta que en la legislación colombiana dichas entidades son terceros de confianza que pueden contar con la habilitación legal para asumir estas funciones, intervenir en la generación de firmas y certificados digitales y garantizar la seguridad de una comunicación electrónica, tanto técnica como jurídicamente.

b. De forma independiente a través de entidades constituidas únicamente para estos efectos, como son las denominadas *Autoridades de Fechado Digital*, más conocidas por su sigla en inglés como TSA (*Time Stamping Authorities*).[15] Las autoridades de fechado digital vinculan un instante de tiempo a un documento electrónico, avalándolo con su firma y resolviendo, en consecuencia, el problema de la exactitud temporal de los documentos electrónicos. Estas autoridades pueden constituirse como entes individuales o como una entidad multipropósito (En el caso colombiano y conforme a la habilitación legal de la ley 527 de 1999, éste último parece ser el caso de las entidades de certificación digital).

Sin embargo, en este esquema de autoridades independientes también es superlativa la configuración de un esquema en el que se utilice la firma digital, pues puede resultar demasiado endeble para el sistema de encriptación asimétrica confiar en que el individuo velará diligentemente por la administración de su clave secreta. Es decir, es posible que exista una mala administración de la clave secreta por parte del usuario

14 Artículo 28, ley 527 de 1999.

15 Sobre el particular, consultar el siguiente vínculo: http://www.htmlweb.net/seguridad/varios/software_seguridad.html

provocando así la quiebra del sistema. Ante esta posible quiebra, se podría argumentar que el individuo cambia frecuentemente de clave, pero si lo hace la infraestructura de clave pública podría verse viciada por la transmisión, entre las distintas autoridades, de distintos ficheros de claves que no están actualizados.

> Dicho problema está adquiriendo importancia en los Estados Unidos de América.[16] De ahí que se estén implementando soluciones como: (i) Los repositorios o listas de revocación de certificados por extravío o robo de claves privadas, (ii) que las autoridades de fechado digital hagan uso de la firma digital, permitiendo al verificador determinar fehacientemente si la firma digital fue ejecutada dentro del período de validez del certificado, previniendo fechados fraudulentos antes o después de la fecha consignada e impidiendo alterar el contenido del documento posteriormente al instante de firma.

2.3. Definición de estampado cronológico e intervención de la entidad de certificación.

Se puede deducir entonces que el *estampado cronológico* es un sistema que permite certificar la fecha y la hora en que se ha realizado una transacción electrónica. Por lo tanto, es un proceso esencial para cualquier transacción en línea que permite evitar confusiones e imprecisiones. Lo mejor es hacer que el *estampado cronológico* dependa de una tercera parte de confianza en lugar de una parte implicada.[17] Este sistema toma el resumen (*hash*) de un documento, lo vincula con información de la fecha y hora —con la precisión que corresponda a la calidad del servicio, indicando en todo caso la zona horaria en que se trabaja para lograr una interpretación universal— y firma digitalmente el resultado o conjunto.[18]

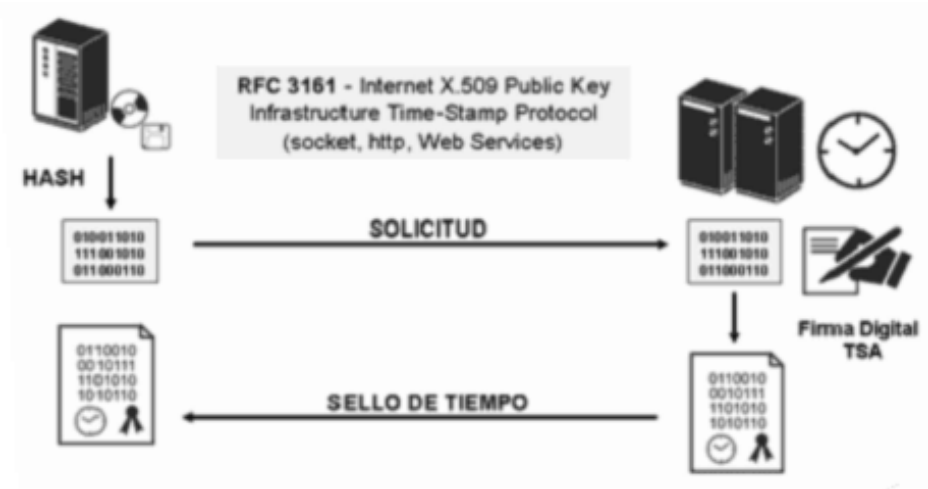
Evidentemente no sirve que cualquiera lo firme, ya que la parte interesada podría firmar hoy y repetir la firma pasado mañana, realizando pequeños cambios sobre el documento pero dejando la fecha igual (postdatado). Como se advirtió en el aparte precedente, en el proceso del *estampado cronológico* aparece una tercera parte que avala el procedimiento con su autoridad, firma con la fecha y hora actuales y se compromete a tener un reloj razonablemente en hora y a no fechar sino con la fecha y hora real.

16 Sobre el particular, consultar el siguiente vínculo: http://premium.vlex.com/doctrina/REDI_Revista_Electronica_Derecho_Informatico/Firma_Digital/2100-107123,01.html

17 Tomado de: https://www.camaragipuzkoa.com/certificaciondigital/biblioteca/Glosario.htm

18 Por ello, el legislador colombiano y no de manera caprichosa, ubicó la prestación de este tipo de servicios en las entidades de certificación digital.

En principio el servicio de *estampado cronológico* no certifica la propiedad de la información, ni tan siquiera a la de la información en sí. La entidad de certificación no comprueba el contenido del documento, ni la identidad del sujeto que lo somete a estampado, más allá de la identificación necesaria para poder cobrar y mantener un registro digno de actividad. En ese orden de ideas y con el propósito de ofrecer realmente *seguridad jurídica*, éste servicio en nuestro país se ha asociado a las actividades



propias de las entidades de certificación digital. El servicio se puede explicar gráficamente de la siguiente manera:

Grafico 1. Elaborado por Agencia Notarial de Certificación, (ANCERT) Madrid, España.[19]

Esto se explica de la siguiente manera: (i) Un usuario quiere obtener un sello de tiempo para un documento electrónico que él posee, (ii) un resumen digital (técnicamente un *hash*) se genera para el documento en el computador del usuario; (iii) este resumen forma la solicitud que se envía a la entidad de certificación que presta el servicio de *estampado cronológico;* (iv) la entidad de certificación que presta el servicio de *estampado cronológico* genera un sello de tiempo (o estampa cronológica) con esta huella, la fecha y hora obtenida de una fuente fiable y la firma digital. De esta manera, al estampar cronológicamente esta representación resumida del documento, lo que realmente se está haciendo es sellar el documento original; (v) el sello de tiempo se envía de vuelta al usuario; y (vi) la entidad de certificación que presta los servicios de *estampado cronológico* mantiene un registro de los sellos emitidos para su futura verificación.

19 Grafico tomado de: http://www.ancert.com/?do=products&group=timestamping&option=timestamping

Esta función contiene la llave privada[20] del certificado digital del suscriptor —en este caso, el de la entidad de certificación— así como las propiedades del mensaje de datos firmado digitalmente:

- Nombre del mensaje de datos
- Tamaño del mensaje de datos
- Fecha de generación del mensaje de datos
- *Hash* (algoritmo de encriptación)[21]

El procedimiento para estampar cronológicamente un documento confidencial, puede ser el siguiente: (a) obtener una huella digital del documento usando una función de *hash* segura y (b) enviar la huella digital del documento al servicio de fechado digital.

De esta forma sólo el autor conoce el documento original. Una vez recibe el sello de fechado digital tiene los elementos que avalan la autoría de su documento. Así, un documento electrónico que de cuenta de una relación contractual digital, debe tener su sello de *estampado cronológico* y cada uno de los firmantes, debe tener una copia del sello para poder demostrar la validez del contrato.[22]

Aquí es importante advertir que todos los certificados digitales tienen fecha de expiración; en promedio son válidos por uno o dos años. En el caso colombiano se ha utilizado tradicionalmente un período de vigencia de un año. Una vez un certificado digital ha caducado, no es apto para autenticar un documento. Para verificar y autenticar documentos cuyo período de validez es muy amplio, se requiere un sello de *estampado cronológico* expedido por una entidad de certificación que preste dicho servicio.

En ese orden de ideas, el *estampado cronológico* está formado por el documento original, la fecha y hora en la cual es registrado y la firma digital de la autoridad de fechado. Un sello de tiempo, valida una firma digital aún cuando el certificado digital respectivo del firmante haya caducado.

Dado que la naturaleza exacta del objeto no afecta su existencia, los documentos (objetos) que pueden ser estampados cronológicamente no están sujetos a una estructura fija. Con esta libertad de formato, el servicio estampado puede emitir sellos para elementos tan dispares como: una transacción electrónica bancaria, un documento

20 El decreto 1747 de 2000, define en el artículo 1°, lo siguiente: "Clave Privada: Valor o valores numéricos que, utilizados conjuntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos."

21 El "resumen" o "valor hash" representa al documento, a todos los efectos, de forma unívoca ya que la probabilidad de que dos documentos distintos tengan el mismo "resumen" es del orden de (1/2)^128 para una función hash de 128 bits.

22 Sobre el particular, consultar el siguiente vínculo: http://business.fortunecity.com/bren/126/comer1.htm

de patente o de su solicitud, obras intelectuales de todo tipo (escritos, imágenes, registros sonoros, software, etc.), entre otros. La finalidad de este servicio es, fundamentalmente, agilizar y facilitar al usuario final los trámites de la presentación de ciertos documentos haciéndolo de forma electrónica.

Para que este sistema funcione, es necesario contar con varios elementos fundamentales para el proceso de estampado, sin los cuales el servicio no sería fiable en cuanto al tiempo que marca:

- Los satélites de posición GPS (*Global Positioning System*) como fuente de tiempo UTC (Unidad de Tiempo Universal) que utilizamos para emitir sellos que estén sincronizados con todos los demás eventos que ocurren en nuestro mundo.
- El servicio de Hora por protocolo (*Network Time Protocol*, NTP). El uso de este protocolo permite sincronizar el reloj con otro que, supuestamente, es fiable o está conectado a una fuente horaria casi perfecta. Por lo general, esta fuente suele ser un reloj atómico o estar alimentado por sistemas GPS.
- El reloj del servicio de *estampado cronológico* ya que es el que, sincronizado con los relojes atómicos de los satélites GPS, o el servicio NTP, nos permite fabricar los sellos cuando llegan las solicitudes de los clientes.

Adicionalmente y desde el punto de vista técnico, existen tres protocolos criptográficos disponibles para facilitar un servicio de fechado digital:

- Protocolo básico, es aquel en el que la entidad de certificación prestadora de servicios de *estampado cronológico* se limita a recoger el resumen, concatenarlo con la fecha y hora y firmar el conjunto digitalmente.
- Protocolo vinculado, además de insertar la fecha y hora, serializa los actos de firma. Cada vez que se fecha un documento se incluye entre lo firmado el resumen *hash* del certificado de tiempo anterior y una referencia al próximo certificado de tiempo que se vaya a emitir. El certificado queda doblemente vinculado, atrapado en el tiempo en términos relativos: después de y antes de.
- Protocolo distribuido, consiste en no usar un fechador, sino muchos. Lo que hace el usuario es dirigirse a un conjunto de fechadores para que fechen por separado, usando el conjunto de fechados singulares como certificado confiable. El *estampado cronológico* individual pudiera ser básico o vinculado. La confianza deriva de la acumulación de evidencias.[23]

23 Sobre el particular, consultar el siguiente vínculo: http://www.lasasesorias.com/es/profesional/direccprofesional/altapc/fechado.html

2.4. El servicio de *estampado cronológico* en el caso colombiano

En Colombia se entiende el servicio de *estampado cronológico* como un servicio complementario, opcional y separado del servicio de emisión de certificados digitales para firma digital, por el cual una entidad de certificación digital suministra, de manera electrónica y a solicitud de una persona, verificar que otro mensaje de datos generado, transmitido o recibido por el propio suscriptor no ha cambiado desde la fecha y el tiempo del día en que el suscriptor hace la solicitud.

El *estampado cronológico* suministrado por una entidad de certificación es solicitado por el usuario de manera electrónica a través de los canales seguros dispuestos por la entidad para ese propósito, y en el instante cronológico en que efectivamente se genera, transmite o recibe digitalmente un mensaje de datos firmado digitalmente por el usuario.

El servicio de *estampado cronológico* es suministrado por una entidad de certificación en un formato electrónico seguro y adecuado de modo que se incorpora al mensaje de datos generado, transmitido o recibido por el usuario impidiendo su posterior alteración. El *estampado cronológico* de un mensaje de datos es único y no puede ser incorporado a otro u otros mensajes de datos diferentes.

El *estampado cronológico* contiene, además, la información correspondiente al tiempo del día y la fecha en que el usuario solicita el servicio de *estampado cronológico* para un mensaje de datos. La información del estampado proporciona tres datos:

> (i) Tiempo del día: Expresado en hora, minuto y segundo (hh; mm; ss) de acuerdo con el Sistema Internacional de Medidas (SI) adoptado en la República de Colombia para la medición del tiempo.[24] Entendiéndose para los efectos de interpretación que la hora puede tener un valor numérico que diariamente asciende desde cero (00) hasta veinticuatro (24), el minuto un valor numérico que cada hora asciende desde cero (0) hasta cincuenta y nueve (59) y el segundo, un valor numérico que cada minuto asciende desde cero (00) hasta cincuenta y nueve (59).
>
> (ii) Fecha: Expresada en día, mes y año (dd; mm; aaaa) de acuerdo con el calendario Juliano[25] que es el generalmente aceptado en la República de

24 El Consejo Nacional de Normas y Calidad en 1995 declaró obligatorio el uso del Sistema Internacional de Unidades SI en Colombia, estableciendo como Unidades SI la hora, minuto y segundo.

25 El Calendario Juliano hace referencia al sistema moderno utilizado desde el año 46 A.C. Cada año esta compuesto por 365 días, divididos en doce (12) meses, que pueden ser de 30 o 31 días, a excepción del segundo mes (febrero) que tiene 28 días. Cada cuatro (4) años habrá un año compuesto por 366 días, denominado Año Bisiesto, en el cual el mes de febrero tiene un día adicional.

Colombia. Entendiéndose que el día tendrá un valor numérico que asciende mensualmente de uno (01) a treinta y uno (31), el mes un valor numérico que asciende anualmente desde uno (01) a doce (12); el año un valor que asciende partiendo del número dos mil seis (2006) hasta el número tres mil (3000).

(iii) Firma de los datos i) y ii) realizada con el certificado de la entidad de certificación.

La entidad de certificación que preste los servicios de *estampado cronológico* deberá tener en cuenta los valores asignados al tiempo del día y la fecha con base en la hora legal de la República de Colombia,[26] tomada directamente de los patrones de referencia del laboratorio de tiempo y frecuencia de la Superintendencia de Industria y Comercio, de acuerdo con lo establecido en el numeral 5 del artículo 20 del decreto 2153 de 1992, en el cual se faculta a la Superintendencia para mantener, coordinar y dar la hora legal de la República de Colombia.[27]

Los valores asignados al tiempo del día y la fecha no tienen en cuenta ni aplican en ningún caso los valores que el sistema informático del solicitante del servicio de "estampado cronológico certificado" señale. Ni el solicitante del servicio de *estampado cronológico*, ni ningún tercero podrá cambiar o solicitar la aplicación de valores distintos de tiempo del día y fecha. Al contar con la hora legal de la República de Colombia, el *estampado cronológico* constituye prueba inequívoca del instante de tiempo en que un documento electrónico es creado, enviado o recibido.

En ese contexto el servicio de *estampado cronológico* sólo podrá utilizar la hora legal de la República de Colombia, por lo tanto, no reconoce la localización geográfica ni la zona de tiempo en que se encuentre el solicitante/usuario que pida el servicio.

En Colombia será necesario tener en cuenta que las entidades de certificación podrán ofrecer el servicio de *estampado cronológico,* siempre y cuando el usuario[28] del servicio:

---

26 La hora legal de la República de Colombia, según el decreto 2707 de 1982, corresponde al Tiempo Universal Coordinado (UTC) disminuido en 5 horas.

27 El laboratorio de tiempo y frecuencia de la Superintendencia de Industria y Comercio, para dar cumplimiento a sus funciones, opera el patrón de tiempo de la República de Colombia con base en la señal emitida por un Reloj Atómico de Rubidio localizado en las instalaciones de la propia Superintendencia. Este reloj es sincronizado con la señal de referencia internacional emitida por el Observatorio Naval de los Estados Unidos (USNO) que corresponde a la escala de Tiempo Universal Coordinado (UTC-USNO).

28 El usuario del servicio de estampado cronológico adicionalmente deberá utilizar medios y servicios de telecomunicación idóneos y compatibles con el servicio, tales como equipos de cómputo, software, proveedor de servicio de Internet, entre otros. El suscriptor del servicio será responsable por la calidad, agilidad y seguridad del servicio.

i) Le haya sido activado y se encuentre vigente el servicio de estampado.

ii) Se encuentre adecuada y continuamente conectado al canal proporcionado por la entidad de certificación para el efecto

iii) Tenga previamente preparado el mensaje de datos que requiere estampar cronológicamente.

En ese orden de ideas, es importante que el usuario del servicio de *estampado cronológico* se asegure de no requerir cambios o de iniciar el proceso definitivo de firmado digital del mensaje de datos que requiere sellar o estampar. Posterior a la solicitud del servicio de estampado de un mensaje de datos, ningún cambio podrá efectuarse sobre éste, sin que se pierda o altere la estampa cronológica.

Sobre el procedimiento para obtener la hora legal, será necesario que la Superintendencia de Industria y Comercio transmita la hora legal colombiana a la entidad de certificación a través de una señal de ondas de radio con una frecuencia de 141.275 Mhz. Esta señal será recibida por la entidad de certificación mediante dispositivos de recepción y monitoreo. Una vez capturada la señal, ésta será a su vez trasladada a un servidor NTP (*Network Time Protocol*), el cual la deja disponible para el servidor de *estampado cronológico* al que tiene acceso el usuario del servicio, ya sea a través de Internet o de los canales especiales que la entidad de certificación ponga a su disposición.

De otro lado, el usuario del servicio de *estampado cronológico* deberá tomar todas las precauciones y medidas conducentes para efectuar la solicitud del servicio de estampado de un mensaje de datos, en particular, deberá tener en consideración que el término de fijación de cada *estampado cronológico* dependerá de las condiciones de calidad, agilidad y seguridad de los medios y servicios de telecomunicación dispuestos por el suscriptor para efectuar la solicitud del a la entidad de certificación y recibir la respuesta correspondiente.

No esta de más decir que el usuario deberá dar el uso debido y legítimo al servicio. El usuario no podrá utilizarlo con fines ilegales o contrarios a la seguridad y estabilidad de éste u otros servicios que ofrezca la entidad de certificación. Incluso la concurrencia de esa circunstancia será causal de revocación de todos los servicios que la entidad de certificación digital preste al usuario. Allí, sobre la responsabilidad de la entidad de certificación en el proceso de estampado para todos los efectos legales, el usuario será el único responsable de la imposición de un *estampado cronológico* en un mensaje de datos y no se entenderá que, por la prestación del servicio, la entidad de certificación digital conoce o hace parte de los actos o negocios jurídicos a que pueda asociarse el mensaje de datos al que se imponga un estampado.

En lo que tiene que ver con las partes confiantes del servicio de *estampado cronológico,* se debe considerar como parte confiante cualquier persona que reciba, conozca o desee dar efecto a un mensaje de datos que ostente un *estampado cronológico*. También

es importante tener en cuenta que cualquier parte confiante conocerá, aceptará y se vinculará jurídicamente a las condiciones del servicio, ofrecidas por la entidad de certificación digital.

De conformidad con las disposiciones legales vigentes, la responsabilidad de la entidad de certificación digital en la prestación del servicio de *estampado cronológico* estará dada por la implementación y mantenimiento de los sistemas de seguridad que resulten razonables en función del servicio prestado y en general, por la infraestructura necesaria para la prestación adecuada del servicio.[29]

3. Aplicación del estampado cronológico

Para efectos de la aplicación del *estampado cronológico* será necesario tener en cuenta que en el ordenamiento jurídico colombiano existen disposiciones que se refieren a la necesidad de dar certeza sobre el tiempo de una determinada actuación o la realización de un trámite. Entre esas normas se encuentran las siguientes:

- Ley 80 de 1993, artículo 8 sobre la constancia escrita de la fecha y hora exacta de la presentación de las propuestas, indicando de manera clara y precisa el nombre o razón social del proponente y el de la persona que en nombre, o por cuenta de éste, ha efectuado materialmente el acto de presentación.
- Decreto 679 de 1994, por el cual se reglamenta parcialmente la ley 80 de 1993.
- Decreto 1968 de 2001 por el cual se reglamenta el capítulo V de la ley 643 de 2001 sobre el régimen de rifas.
- Decreto 2002 de 2002, por el cual se adoptan medidas para el control del orden público y se definen las zonas de rehabilitación y consolidación.

29 De acuerdo a lo anterior, la entidad de certificación digital prestará de manera continúa e ininterrumpida el servicio de estampado cronológico, excepto en los siguientes casos:

- Caso fortuito o fuerza mayor: Se entenderán como fuerza mayor o caso fortuito, pero sin limitarse exclusivamente a ellos, los siguientes acontecimientos: terremoto, inundación, incendio, corte masivo de electricidad, tormenta, actos de terrorismo, agresión extranjera, sismo, virus, falla o vicio informático o en todo caso cualquier otro hecho imprevisible e irresistible.
- Corte programado del servicio: Certicámara cuenta con un plazo permitido de interrupción programada del servicio. Cualquier evento de interrupción será comunicado previamente a los usuarios del servicio con la anticipación que señalen las normas aplicables, el cual en todo caso no será inferior a cinco (5) días hábiles.
- Interrupción, cambio o restricción de la competencia legal, la capacidad técnica, administrativa o financiera, y en general la disponibilidad de la Superintendencia de Industria y Comercio o de la entidad pública o privada, nacional o extranjera designada o que corresponda para suministrar la hora legal de la República de Colombia

- Decreto 2170 de 2002, por el cual se reglamenta la ley 80 de 1993, se modifica el decreto 855 de 1994 y se dictan otras disposiciones en aplicación de la ley 527 de 1999.
- Decreto 875 de 2005, por el cual se reglamenta el parágrafo del artículo 36 de la ley 845 de 2003, que establece los procedimientos para la toma de muestras, recolección, análisis, expedición de resultados y demás aspectos relacionados con el programa de control al dopaje.
- Resolución 000102 de 2005, por medio de la cual se establecen pautas para el manejo de las comunicaciones oficiales en el Servicio Nacional de Aprendizaje (Sena) y se dictan otras disposiciones relacionadas con la gestión documental.
- Decreto 2831 de 2005 por el cual se reglamentan el inciso 2° del artículo 3° y el numeral 6° del artículo 7° de la ley 91 de 1989, y el artículo 56 de la ley 962 de 2005, y se dictan otras disposiciones.
- Resolución 1012 de 2005, por la cual se reglamenta el trámite interno del Derecho de Petición y quejas ante la honorable Cámara de Representantes.
- Decreto 2900 de 2005, por el cual se reglamenta el decreto-ley 790 de 2005 —Vinculación a los empleos de carrera.
- Ley 962 de 2005, por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.

4. *Autoridad de* archivo confiable

Durante la preparación de la ley modelo de la Comisión de las Naciones Unidas para el desarrollo del Derecho Mercantil (CNUDMI) se prestó particular atención a las funciones que tradicionalmente desempeñan diversos tipos de "escritos" consignados sobre papel. En las discusiones de la ley modelo se enunciaron las principales razones por las que en el derecho interno se hacía necesario requerir la presentación de un "escrito": 1) Dejar una prueba tangible de la existencia y la naturaleza de la intención de las partes de comprometerse; 2) alertar a las partes ante la gravedad de las consecuencias de concluir un contrato; 3) proporcionar un documento que sea legible para todos; 4) proporcionar un documento inalterable que permita dejar constancia permanente de la operación; 5) facilitar la reproducción de un documento de manera que cada una de las partes pueda disponer de un ejemplar de un mismo texto; 6) permitir la autenticación mediante la firma del documento de los datos en él consignados; 7) proporcionar un documento presentable ante las autoridades públicas y los tribunales; 8) dar expresión definitiva a la intención del autor del "escrito" y dejar constancia de dicha intención; 9) proporcionar un soporte material que faci-

lite la conservación de los datos en forma visible; 10) facilitar las tareas de control o de verificación ulterior para fines contables, fiscales o reglamentarios; y 11) determinar el nacimiento de todo derecho o de toda obligación jurídica cuya validez dependa de un escrito.[30]

Como se puede advertir de la lectura de las razones anteriormente señaladas, la conservación juega un papel bastante importante. La obligación de la conservación de la documentación no sólo esta establecida en distintas disposiciones comerciales y tributarias, sino también en las específicas sobre patrimonio cultural y sobre archivos. Y en el caso que nos ocupa, la aceptación plena del documento electrónico (asimilado en sus efectos jurídicos al soporte papel), en el cumplimiento del requisito de conservación.[31]

A manera de ejemplo, en el derecho colombiano uno de los deberes que la ley ha impuesto a los comerciantes es el de llevar contabilidad de sus asuntos y negocios, al igual que la información y documentos relacionados con los mismos, previendo la obligación complementaria de que la contabilidad, así como los libros, registros contables en general, inventarios y estados financieros, deban ajustarse a las disposiciones del Código de Comercio y demás normas sobre la materia, como imperativamente lo señala el artículo 48 del mismo código.

Sin embargo, las normas reglamentarias no establecen específicamente qué libros debe llevar el comerciante, limitándose a indicar la necesidad de llevar aquellos libros que la ley determine como obligatorios, como es el caso de los libros de registro de accionistas o de socios y los de actas de asambleas o juntas directivas, al igual que los auxiliares necesarios para el adecuado entendimiento de los mismos, constituyendo éstos en su conjunto, lo que en el artículo 49 del estatuto mercantil denomina libros de comercio.

El artículo 48 del Código de Comercio, en concordancia con el articulo 19 numeral 3º, exigió que la contabilidad, así como la documentación e información del comerciante, se llevara de conformidad con las disposiciones legales, e indicó que dichas normas podrían autorizar "el uso de sistemas que como la microfilmación, faciliten la guarda de su archivo y correspondencia." A la vez, permitió la utilización de "otros procedimientos de reconocido valor técnico-contable, con el fin de asentar sus operaciones, siempre que facilite el conocimiento y

30 Ver: Guía para la incorporación en el Derecho Interno de la Ley Modelo de la CNUDMI para el Comercio Electrónico.

31 El informe repartido en la II Reunión Plenaria de la Comisión de Asuntos Americanos de la Comisión de Informática y Seguridad Jurídica de la Unión Internacional del Notariado Latino, explica que el archivo y conservación del documento electrónico ofrece la posibilidad a las partes de presentar en juicio una copia certificada compulsada por el notario, que conserva el original, con la misma fuerza probatoria del original mismo, indudablemente permitirá atribuir mayor confidencialidad a documentos que son, en muchos aspectos, incorporales.

prueba de la historia clara, completa y fidedigna de los asientos individuales y el estado general de los negocios."

Por lo anterior, se puede concluir que los libros llevados de manera manual o impresa para documentar los registros, datos o informaciones contables, no son la única forma que el citado código en principio concibió para el manejo o documentación de la contabilidad. Sí es la que legalmente autoriza hasta ahora, por la mayor confianza y seguridad que tradicionalmente este sistema genera y por el alcance de algunos textos legales.[32]

Adicionalmente, se debe tener en cuenta los establecido en la ley 527 de 1.999 y recientemente en la ley 962 de 2005, normas que directamente aluden a la conservación de los mensajes de datos y documentos (artículo 12) y a la racionalización de la conservación de libros y papeles del comerciante (artículo 28).[33]

Por todo lo anterior, la conservación de los libros del comerciante por medios electrónicos es posible. El problema estriba en que técnicamente es muy discutida la perdurabilidad del documento en soporte electrónico y parece que no hay acuerdo sobre los sistemas de homologación o validación técnica del soporte electrónico que garanticen su perdurabilidad más allá de unos años. La mayoría de las soluciones informáticas ofrecidas en el mercado van desde equipos para procesamiento, envió y transmisión de información, hasta aplicativos y sistemas que integran cualquier tipo de documentos permitiendo al usuario una gestión homogénea y transparente, independiente de su origen. Igualmente se presentan soluciones adaptables a diferentes plataformas de bases de datos y con absoluta independencia de los diferentes elementos hardware y software con los que se deben integrar.[34]

4.1. Concepto y características

Antes de iniciar el análisis de la habilitación legal dada en la ley 527 de 1999, en cuanto al archivo y conservación de mensajes de datos, es importante hacerse las siguientes preguntas:

- ¿Existen documentos electrónicos que se deban archivar de manera confiable por un requerimiento legal o reglamentario?

32 Concepto 220-069768 del 6 de diciembre de 2005 de la Superintendencia de Sociedades

33 Con la ley 962 del año en curso y por virtud de lo dispuesto en su artículo 28, fue derogado el artículo 60 del Código citado y con éste el artículo 134 del decreto 2649 de 1993, en la medida en que se modificó el término durante el cual el comerciante debe conservar su información comercial y contable, reduciendo éste de veinte a diez años, con la posibilidad de utilizar para el efecto a elección del comerciante su conservación en papel o en cualquier medio técnico o electrónico que garantice su reproducción.

34 Ver: http://www.archivogeneral.gov.co/version2/htm/tablas/sem/gesdocu.htm

- ¿Es necesario evitar la impresión y almacenamiento de montañas de documentos en papel, para reducir costos?
- ¿Se requiere tener una constancia de un mensaje de datos en un servidor independiente de su infraestructura tecnológica?
- ¿Se requiere tener un respaldo de la información digital para garantizar su integridad durante el tiempo de almacenamiento?

En todos los contextos de documentos, la conservación desempeña un papel importante. Esta tiene asociados varios aspectos, entre los que se deben resaltar la duración y accesibilidad, en función de la naturaleza del documento. Es decir, el documento debe ser susceptible de ser conservado por cierto tiempo (siendo posible su eventual destrucción después de un tiempo) y el acceso al mismo debe garantizarse sea que se trata de un documento público o restringido.

Es en el entorno antes descrito que un servicio especializado juega un papel importante para la conservación de documentos electrónicos. Este servicio deberá garantizar la existencia, integridad y autenticidad del documento electrónico sobre cualquier período del tiempo. Además, asegurar la responsabilidad de crear y almacenar evidencia y/o de recibir y almacenar datos para garantizar su integridad y para mantener su accesibilidad. Por lo anterior, nos referiremos al servicio de *archivo confiable* (prestado por las entidades de *archivo confiable* TAA —*Trusted Archive Authority*. En el caso colombiano puede ser prestado por las entidades de certificación digital).

El proceso de sustituir el papel por documentos con un soporte diferente —esto es, por mensajes de datos digitales— se conoce como "desmaterialización", proceso que en todo caso debe tener en cuenta los requisitos para la estabilidad de los documentos a largo plazo. Puesto que la conservación de los documentos creados por una empresa o entidad es absolutamente necesaria, el acervo documental se puede presentar ante el servicio de *archivo confiable,* Este servicio busca que un tercero de confianza, a saber una entidad de certificación digital, garantice la incorporación de ciertos atributos de *seguridad jurídica* al documento electrónico. En consecuencia, la función principal del servicio de *archivo confiable* será proveer integridad y autenticidad para la existencia archivada de los datos en períodos largos de tiempo.

La información almacenada en el archivo puede ser de cualquier naturaleza, es decir, cualquier mensaje de datos digital. Este mensaje de datos será firmado y *estampado cronológicamente* al momento de entrar al repositorio, para garantizar, de esta manera, la integridad de la información durante el almacenamiento.

Los documentos susceptibles de utilizar los servicios de *archivo confiable* están principalmente relacionados con el proceso de conservación de información que tenga como característica un requerimiento legal de archivo. Tal información normalmente cumple propósitos legales especiales o eventualmente, tiene por objeto demostrar la validez de una firma digital. En este último caso —con el fin de aumentar

las garantías de los documentos firmados digitalmente— se definen los servicios de *archivo confiables* (Trusted Archival Services -TAS). Es importante advertir entonces que las firmas digitales pueden ser archivadas localmente y verificadas años después, pues éstas puedan necesitarse para ser utilizadas como evidencias después de ser creadas.

En el mismo sentido en el que se definen los TAS por parte del EESSI[35], la IETF[36] (en el ámbito de PKIX[37]) publicó recientemente el primer borrador (http://www.ietf.org/internetdrafts/draft-ietf-pkix-tap-00.txt) sobre "*Trusted Archive Protocol* - TAP". En este se define el servicio de *archivo confiable* como un servicio que garantiza el "no repudio" en periodos largos, mediante el mantenimiento de una infraestructura segura de almacenamiento.[38]

En este orden de ideas, el *archivo confiable* hace posible que el tercero —las entidades de certificación digital— e responsabilicen de "guardar con cuidado y vigilancia"[39] el documento y permitir, posteriormente, su recuperación con determinados efectos legales.

Un servicio de *archivo confiable* de documentos electrónicos debe cubrir las siguientes necesidades:

- Archivo de todo tipo de documentos.
- *Estampado cronológico* de los documentos.
- Garantizar que el documento custodiado no sea modificado durante su permanencia en el archivo, y consecuentemente, mantener el valor legal que tenía al momento de ser archivado.

Por otra parte, la legislación exige una alta confidencialidad en determinados documentos. En este caso y como se ha advertido preliminarmente, el *archivo confiable* podría plantearse vinculado con la firma digital, suficiente para presentar como prueba de la existencia del documento.

Nuevos aspectos aparecen al valorar los periodos de archivo y conservación de los documentos electrónicos. Desde el punto de vista del soporte clásico en papel, el único problema es su posible degradación con el tiempo. El soporte electrónico añade, por ejemplo —y en el caso de que el documento sea firmado digitalmente— la

35 EESSI, corresponde a las siglas en inglés de European Electronic Signature Standardization Initiative.

36 IETF, corresponde a las siglas en inglés de Internet Engineering Task Force

37 PKIX, corresponde a las siglas en inglés de Public Key Infraestructure X — 509

38 TAP es una especificación que define: (i) Las estructuras de datos para la representación de datos almacenados (ii) Transacciones para interactuar con el TAA (Trusted Archive Authority). Estas transacciones incluyen el envío de información para almacenar, la recuperación de los datos o evidencia y el borrado de la información almacenada.

39 Definición de la palabra "custodiar" de la Real Academia Española de la Lengua.

necesidad de plantearse problemas tales como los cambios de formatos y la validez temporal de los certificados digitales con los que se firman los documentos.

Allí será importante tener en cuenta que los plazos de archivo y conservación —de conformidad con los requerimientos legales— determinan qué tecnologías y soportes deben usarse para llevarla a cabo. La conservación a corto y mediano plazo podrá afrontarse con relativa facilidad.

Por el contrario, la conservación a largo plazo plantea la necesidad de fijar con claridad qué formatos de documentos se aceptan en custodia y qué estrategia de mantenimiento de los mismos debe plantearse (migración de formatos o emulación de formatos antiguos). En caso de archivo a muy largo plazo, debe estudiarse o bien las mismas soluciones, pero mejoradas o incluso el paso de los documentos a sistemas de muy larga duración, como por ejemplo el microfilm.

De otro lado —y en lo que tiene que ver con el archivo de la firma digital— debe definirse una estrategia de "refresco" de las firmas. El servicios de *archivo confiable* cuando se ocupa del problema de las firmas electrónicas o digitales unidas a los documentos, debe tener en cuenta que normalmente el período de validez de éstas es bastante limitado (En Colombia tiene un promedio de un (1) año).

4.2. Fundamento legal

Teniendo en cuenta que la información almacenada a través del proceso de digitalización, se puede circunscribir dentro del concepto del mensaje de datos que trae la ley 527 de 1999, se exponen a continuación los apartes normativos que sustentarían la posibilidad de que este tipo de sistemas sean completamente validos y efectivos en lo referente a la conservación y almacenamiento de la información.

La ley 527 de 1999, establece en su artículo 2º la definición del *Mensaje de Datos* en los siguientes términos:

> *"Mensaje de Datos. La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónicos de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.*

Igualmente, consagra el artículo 6º de la mencionada ley que cuando una norma requiera que la información conste por escrito, este requisito quedará satisfecho con un mensaje de datos, si la información que contiene es accesible para su posterior consulta. En este sentido establece el citado artículo: *"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."*

Siguiendo el texto de la ley 527, también se encuentra que el artículo 8º consagra frente a la posibilidad de que una norma requiera que la información sea presentada

y conservada en su forma original, que dicho requisito quedare satisfecho con un mensaje de datos, si se presentan las siguientes condiciones:

> *"Artículo 8º. Original. Cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, sí:*
>
> a. "Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma.
>
> b. "De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar.
>
> *"Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que la información no sea presentada o conservada en su forma original."*

Respecto de la conservación de los mensajes de datos y documentos, la ley 527 claramente establece en su artículo 12º[40] 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:[41]

---

40 Concepto 05054043 del 12 de octubre de 2005, proferido por la Superintendencia de Industria y Comercio:"…a partir de la entrada en vigencia de la Ley 962 de 2005 y en concordancia con lo señalado en el artículo 12 de la Ley 527 de 1999, los libros y papeles del comerciante únicamente deben ser conservados por un período de diez (10) años contados a partir de la fecha del último asiento, documento, o comprobante, pudiéndose utilizar para el efecto, a elección del comerciante, su conservación en papel o en cualquier medio técnico, magnético o electrónico que garantice su reproducción exacta. Al respecto, se debe aclarar que en caso de que se utilice un medio electrónico para la conservación de tales documentos, el mismo deberá reunir los requisitos establecidos en el artículo 12 de la Ley 527 de 1999 y en dicho caso, no será necesaria la conservación física (en papel) de los libros y papeles del comerciante. En este evento, una vez se garantice la reproducción exacta de los libros y papeles, a través del citado medio electrónico, el comerciante está en posibilidad de destruir directamente dichos documentos, encontrándose obligado, únicamente, a conservarlos por un período de diez (10) años en el medio electrónico en el que se hubieren reproducido."

41 El tema tiene un extenso tratamiento en la normatividad internacional y ha sido preocupación de las legislaciones sobre la materia en la comunidad andina de naciones, a saber:

- **Ecuador - Ley de Comercio Electrónico**

  Artículo 8.- Conservación de los mensajes de datos.- Toda información sometida a esta Ley, podrá ser conservada; este requisito quedará cumplido mediante el archivo del mensaje de datos, siempre que se reúnan las siguientes condiciones:

  a. que la información que contenga sea accesible para su posterior consulta;

  b. que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formatoque sea demostrable que reproduce con exactitud la información generada, enviada o recibida;

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. que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado; y,

d. Que se garantice su integridad por el tiempo que se establezca en el Reglamento a esta Ley.

Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones mencionadas en este artículo.

Para la información que tenga por única finalidad facilitar el envío o recepción del mensaje de datos, no será obligatorio el cumplimiento de lo establecido en los literales anteriores.

- **Perú - Reglamento de la ley nº 27269 de firmas y certificados digitales. Decreto supremo no. 019-2002-JUS**

Artículo 10 - Conservación de documentos electrónicos. Cuando el usuario lo solicite o la legislación exija que los documentos, registros o informaciones requieran de una formalidad adicional para la conservación de mensajes de datos o documentos electrónicos firmados electrónicamente, deberá cumplirse con lo siguiente:

a) Que sean accesibles para su posterior consulta.

b) Que sean conservados con su formato original de generación, envío, recepción u otro formato que reproduzca en forma demostrable la exactitud e integridad del contenido digital o electrónico.

c) Que sea conservado todo dato que permita determinar el origen, destino, fecha y hora del envío y recepción, en concordancia con lo establecido en el Decreto Legislativo No. 681 y sus normas complementarias.

Cuando los documentos y mensajes de datos firmados electrónicamente sean conservados mediante microformatos y almacenados en microarchivos, se sujetarán a lo dispuesto por el Decreto Legislativo N. 681 y sus normas modificatorias y reglamentarias. El notario o federatario responsable, que cuente con certificado o diploma de idoneidad técnica, certifica el cumplimiento de los requisitos establecidos en el presente artículo.

- **Venezuela- decreto 1.024. ley sobre mensajes de datos y firmas electrónicas 10 de febrero de 2001**

Artículo 8 - Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con relación a un Mensaje de Datos, si la información que éste contiene es accesible para su ulterior consulta. Cuando la ley requiera que ciertos actos o negocios jurídicos consten por escrito y su soporte deba permanecer accesible, conservado o archivado por un período determinado o en forma permanente, estos requisitos quedarán satisfechos mediante la conservación de los Mensajes de Datos, siempre que se cumplan las siguientes condiciones:

Que la información que contengan pueda ser consultada posteriormente.

Que conserven el formato en que se generó, archivó o recibió o en algún formato que sea demostrable que reproduce con exactitud la información generada o recibida.

Que se conserve todo dato que permita determinar el origen y el destino del Mensaje de Datos, la fecha y la hora en que fue enviado o recibido.

Toda persona podrá recurrir a los servicios de un tercero para dar cumplimiento a los requisitos señalados en este artículo.

c. La conservación de la información debe permitir determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o reproducido el documento.[42]

El inciso final expresamente establece: *"Los libros y papeles del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta".*

Este artículo tiene la finalidad de fijar las condiciones para que se cumpla la obligación de conservar mensajes de datos. Lo que hace la ley es reproducir las condiciones enunciadas en el artículo 6º para que un mensaje de datos satisfaga la regla que exige la presentación de un escrito.[43]

Posteriormente, se pone de relieve que no es preciso conservar el mensaje sin modificaciones, a condición de que la información archivada reproduzca con exactitud el mensaje de datos en la forma recibida. No sería apropiado exigir que la información se conserve sin modificaciones, ya que por regla general los mensajes son descodificados, comprimidos o convertidos antes de ser archivados.

Adicionalmente, se hace referencia en el artículo a toda la información que debe archivarse, que incluye, aparte del mensaje propiamente dicho, cierta información sobre la transmisión que puede resultar necesaria para identificarlo, entre ella la fecha y hora en la que fue enviado o recibido. Esto enfatiza la necesidad de contar con el servicio de *estampado cronológico.* Dicha norma se constituye en una disposición de mayor exigencia que la mayoría de las normas nacionales vigentes sobre conservación de comunicaciones consignadas sobre papel.

En la práctica, la conservación de información —especialmente de la relativa a la transmisión— puede estar a cargo muchas veces de alguien que no es ni el iniciador, ni el destinatario, como es el caso de un intermediario. No obstante, la intención consiste en que la persona obligada a conservar cierta información, relativa a la transmisión, no pueda aducir para no cumplirla, por ejemplo, que el sistema de comunicaciones que utiliza la otra persona no conserva la información necesaria. Con ello se pretende desalentar las malas prácticas o las conductas dolosas. Es por ello, que las entidades de certificación digital —entendidas como terceros de confianza para el comercio electrónico— son las llamadas a prestar este tipo de servicios.[44]

---

42 Vease Código de Comercio, artículo 60; Código de Procedimiento Civil, artículo 268; Circular Externa 007 de 1996 Superintendência Bancaria, Título I Cap. XI Num. 4.1.

43 Con respecto a la conservación de los mensajes de datos, el artículo 10 de la ley modelo de la CNUDMI reproducido por la legislación colombiana, establece un conjunto de nuevas reglas con respecto a los requisitos de conservación de la información (por ejemplo, a efectos contables o fiscales) a fin de evitar que esos requisitos obstaculicen el desarrollo comercial moderno.

44 Ver: Guía para la incorporación al Derecho Interno de la Ley Modelo CNUDMI de Comercio electrónico. Adicionalmente se podrán ver los siguientes documentos de la Comisión:

A la luz del artículo 9º de la ley 527 se considera que la información consignada en un mensaje de datos es íntegra. Esto siempre y cuando haya permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso. Sin embargo, es importante recordar la denominada presunción de confiabilidad de las firmas digitales emitidas por una entidad de certificación abierta,[45] en la medida que permiten presumir que quien las impuso en un mensaje de datos tenía la intención de "acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo."[46] Este es el efecto jurídico de la propiedad de *no repudio* de mensajes de datos que tiene la certificación digital. Dicha presunción garantiza que quien observe una firma digital en un mensaje de datos puede suponer válidamente y de manera inequívoca, que el firmante es quien dice ser y que se vincula con el contenido del mensaje.

Sobre la conservación de mensajes de datos y archivo de documentos a través de terceros, la ley 527 en su artículo 13 establece que el cumplimiento de la obligación de conservar documentos, registros o informaciones en mensajes de datos, se podrá realizar directamente o a través de terceros, siempre y cuando se cumplan las condiciones enunciadas en el artículo 12 de la misma ley.

Finalmente, en este punto el artículo 30 de la ley 527 señala la posibilidad que tienen las entidades de certificación de ofrecer los servicios de archivo y conservación de mensajes de datos.

4.3. Aplicación del *archivo confiable*, a partir de la normatividad colombiana sobre la materia

Para efectos de la aplicación del *archivo confiable* de mensajes de datos será necesario tener en cuenta que en el ordenamiento jurídico colombiano existen disposiciones que se refieren a la necesidad de conservar documentos, además de las disposiciones comerciales o tributarias.

- A/51/17, párrs. 185 a 187;
- A/50/17, párrs. 264 a 270 (artículo 9);
- A/CN.9/407, párrs. 82 a 84;
- A/CN.9/406, párrs. 59 a 72;
- A/CN.9/WG.IV/WP.60 artículo 14;
- A/CN.9/387, párrs. 164 a 168;
- A/CN.9/WG.IV/WP.57, artículo 14;
- A/CN.9/373, párrs. 123 a 125;
- A/CN.9/WG.IV/WP.55, párr. 94.

45 A la luz del artículo 28 de la ley 527 de 1999 y del artículo 15 del decreto 1747 de 2000.

46 Artículo 28, ley 527 de 1999.

Por ejemplo, es necesario mencionar el decreto 2150 de 1995 —por medio del cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios, existentes en la Administración Pública— que dispuso en su artículo 26 que las entidades de la administración pública deberían habilitar sistemas de transmisión electrónica de datos para que los usuarios envíen o reciban la información requerida en sus actuaciones frente a la administración y que en ningún caso las entidades públicas podrían limitar el uso de tecnologías para el archivo documental por parte de los particulares, sin perjuicio de sus estándares tecnológicos. Recordemos, como elemento interesante, en el tema de los documentos electrónicos que son considerados como pruebas a la luz de la ley 527 de 1999.[47]

Adicionalmente se pueden observar, entre otras, las siguientes normas que requieren la conservación de documentos o le dan especial valor a ciertas formas de conservación:

- Decreto 2527 de 1950 - Presidencia de la República, microfilmación y valor probatorio de copias fotostáticas.
- Decreto 3354 de 1954 - Presidencia de la República, microfilmación y valor probatorio de copias fotostáticas.
- Decreto 410 de 1971 - Código de Comercio colombiano.
- Ley 23 de 1981, capítulo III - Historias Clínicas.
- Acuerdo 07 de 1994 - Archivo General de la Nación, Comité de Archivo, artículo 19.
- Acuerdo 11 de 1996 - Archivo General de la Nación, criterios de conservación y organización de material gráfico.
- Circular 2 de 1997 - Archivo General de la Nación, parámetros para implementar nuevas tecnologías en archivos públicos.
- Acuerdo 46 de 2000 - Archivo General de la Nación, por el cual se establecen los procedimientos para la eliminación.
- Acuerdo 48 de 2000 - Archivo General de la Nación, por el cual se desarrolla el artículo 59 del capítulo 7 -Conservación de documentos.
- Acuerdo 50 de 2000 - Archivo General de la Nación, por el cual se desarrolla el artículo 64 del Título VII, Conservación de Documento.
- Acuerdo 57 de 2000 - Archivo General de la Nación, por el cual se establecen los procedimientos para la entrega de documentos y archivos de las entidades en proceso de liquidación, fusión o privatización y se dictan otras disposiciones.

47 VV.AA. Evidencia Digital: contexto, situación e implicaciones nacionales, en Revista de Derecho, Comunicaciones y Nuevas Tecnologías, Número 1, Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática, Universidad de los Andes, Bogotá, 2005.

- Acuerdo 60 de 2001 - Archivo General de la Nación, administración de comunicaciones oficiales.
- Acuerdo 56 de 2000 - Archivo General de la Nación, acceso a documentos de archivo para historiadores.
- Resolución 400 de 2000 - Contaduría General de la Nación, Plan General de Contabilidad Pública.
- Acuerdo 37 de 2002 - Archivo General de la Nación, requisitos para la contratar depósito, custodia, organización, reprografía y conservación de documentos de archivo.
- Resolución de 1995 de 1999 - Ministerio de Salud, manejo de Historias Clínicas.
- Circular 4 de 2003 - Departamento Administrativo de la Función Publica y Archivo General de la Nación, Organización Historias Laborales.
- Ley 962 de 2005 - Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.

5. Conclusiones

El *estampado cronológico* y el archivo y la conservación de documentos electrónicos a través de terceros de confianza, se fundamenta en la idea de que el documento electrónico —asimilado jurídicamente al documento en soporte papel— es único y original. Es la única evidencia legal autentica e íntegra que acredita la relación, el acto, el contrato, la manifestación etc. Es por ello que no se nos escapa la trascendencia jurídica que tiene asegurar la conservación, el archivo y la recuperación del documento que es evidencia legal.

Para avanzar en la discusión de estas figuras es importante tener en cuenta la adopción de un conjunto de medidas en el campo de la denominada seguridad jurídica preventiva; medidas que perfectamente podrían estar en la línea con las funciones asignadas a las entidades de certificación digital por la regulación colombiana

En cuanto a la seguridad, básicamente se deben definir políticas generales de seguridad de información, particularmente en el manejo de los documentos para que realmente puedan fluir electrónicamente. Para ello dichos documentos deben:

- Ser confidenciales. Es decir, sólo los deben ver las partes autorizadas.
- Ser auténticos. Es decir, haber sido creados por quien dice generarlos.
- Ser fácilmente recuperables. Es decir, en el momento en que los medios de información y los medios de almacenamiento cambien, la información deberá trasladarse a esos nuevos medios.

- Ser íntegros. Es decir, que se debe garantizar el almacenamiento tal cual se produjo en el momento en que se genero el documento.[48]

En la búsqueda de los anteriores requerimientos, la intervención de las entidades de certificación digital como terceros de confianza, resulta para el comercio electrónico fundamental, siendo esenciales para complementar la seguridad jurídica que puede proveer la firma digital de un documento electrónico, los servicios de *estampado cronológico* y de archivo y conservación de mensajes de datos. Incluso, sin necesidad de que el documento electrónico esté firmado digitalmente, los servicios de *estampado cronológico y archivo confiable* a cargo de las entidades de certificación, pueden responder adecuadamente a la necesidad de *no repudio* en las comunicaciones y transacciones electrónicas.

Bibliografia

Documentos y legislación:

- Circular Externa 007 de 1996 Superintendencia Bancaria; Título I Cap. XI Num. 4.1
- Código de Comercio
- Código de Procedimiento Civil
- Decreto Número 1747 de septiembre 11 de 2000, por el cual se reglamenta parcialmente la ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales
- Documento CNUDMI A/50/17, párrs. 264 a 270 (artículo 9)
- Documento CNUDMI A/51/17, párrs. 185 a 187
- Documento CNUDMI A/CN.9/373, párrs. 123 a 125
- Documento CNUDMI A/CN.9/387, párrs. 164 a 168
- Documento CNUDMI A/CN.9/406, párrs. 59 a 72
- Documento CNUDMI A/CN.9/407, párrs. 82 a 84
- Documento CNUDMI A/CN.9/WG.IV/WP.55, párr. 94.
- Documento CNUDMI A/CN.9/WG.IV/WP.57, artículo 14
- Documento CNUDMI A/CN.9/WG.IV/WP.60 artículo 14
- Guía para la incorporación en el Derecho Interno de la Ley Modelo de la CNUDMI para el Comercio Electrónico.
- Informe de la Comisión de Asuntos Americanos de la Comisión de Informática y Seguridad Jurídica de la Unión Internacional del Notariado Latino,

48 http://www.archivogeneral.gov.co/version2/htm/tablas/sem/docele.htm

- Sentencia C-662 de 2000 de la Corte Constitucional

- VV.AA. Evidencia Digital: contexto, situación e implicaciones nacionales, en Revista de Derecho, Comunicaciones y Nuevas Tecnologías, Número 1, Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática, Universidad de los Andes, Bogotá, 2005.

Páginas web:

- http://www.archivogeneral.gov.co/version2/htm/tablas/sem/gesdocu.htm

- http://64.233.187.104/search?q=cache:Njk0KWKP8PIJ:wotan.liu.edu/dois/data/Papers/juledslbl7425.html+%22fechado+digital%22+%2B+%22firma+digital%22+&hl=es

- http://business.fortunecity.com/bren/126/comer1.htm

- http://premium.vlex.com/doctrina/REDI_Revista_Electronica_Derecho_Informatico/Firma_Digital/2100-107123,01.html

- http://tirnanog.ls.fi.upm.es/CriptoLab/Proyectos/TicTac/TicTac.html

- http://www.agenda.gov.co/BulletinBoard/view_one.cfm?MenuID=3&ID=116

- http://www.ancert.com/?do=products&group=timestamping&option=timestamping

- http://www.archivogeneral.gov.co/version2/htm/tablas/sem/dispole.htm

- http://www.archivogeneral.gov.co/version2/htm/tablas/sem/docele.htm

- http://www.eurologic.es/conceptos/fechadodigital.htm

- http://www.htmlweb.net/seguridad/varios/software_seguridad.html

- http://www.lasasesorias.com/es/profesional/direccprofesional/altapc/fechado.html

- http://www.mincomercio.gov.co/VBeContent/NewsDetail.asp?ID=937&IDCompany=4

- https://www.camaragipuzkoa.com/certificaciondigital/biblioteca/Glosario.htm