ALCANCE DE LAS FIRMAS DIGITALES

LAURA DANIELA GARCÍA REY
PAULA NARANJO URREA

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE DERECHO
VILLAVICENCIO
2019

ALCANCE DE LAS FIRMAS DIGITALES

LAURA DANIELA GARCÍA REY
PAULA NARANJO URREA

Trabajo de grado presentado como requisito para optar al título de abogado

Asesor
MG. RODRIGO CORTÉS BORRERO
Magister en derecho contractual público y privado

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE DERECHO
VILLAVICENCIO
2019

Autoridades Académicas

P. José Gabriel MESA ANGULO, O. P.
Rector General

P. Eduardo GONZÁLEZ GIL, O. P.
Vicerrector Académico General

P. José Arturo RESTREPO RESTREPO O.P.
Rector Sede Villavicencio

P. Rodrigo GARCÍA JARA, O.P.
Vicerrector Académico Sede Villavicencio

Adm. JULIETH ANDREA SIERRA TOBÓN
Secretaria de División Sede Villavicencio

Doc. SONIA PATRICIA CORTES ZAMBRANO
Decano de la Facultad de Derecho

Contenido

Pág.

Resumen

La herramienta tecnológica de nuestro tema de investigación es la firma digital. Con base en las respuestas de los derechos de petición radicados en entidades públicas, privadas y mixtas de Villavicencio se ve reflejado el desconocimiento y por ende la falta de aplicación de la firma digital, arrojando resultados de preocupación e interés para todos como por ejemplo la comisión de delitos informáticos; concluyendo así la necesidad de que se implemente la firma digital, y poder así gozar de un progreso tecnológico en la comunidad Villavicense y así estar a la vanguardia de la nueva era tecnológica con seguridad y confianza.

*Palabras claves***:** Herramienta tecnológica, firma digital y desconocimiento.

Abstract

The technological tool of our research topic is the digital signature. Based on the responses of the petition rights filed in public, private and mixed entities of Villavicencio, the lack of knowledge and therefore the lack of application of the digital signature is reflected, yielding results of concern and interest for all, such as the commission of computer crimes; thus concluding the need to implement the digital signature, and thus be able to enjoy technological progress in the community of Villavicencio and thus be at the forefront of the new technological era with security and confidence.

Key words: Technological tool, digital signature and ignorance.

Introducción

1.1. Contexto de las firmas digitales.

Con la llegada de importantes y trascendentes tiempos como lo fue el término del siglo XX y el arrasador siglo XXI vemos incorporados en ellos la solución a muchos problemas, aun no solucionados del todo, en los que se veía un país como Colombia con los temas de las Comunicaciones y las Tecnologías, que de forma considerable han dado un giro de 180 grados en la forma en como no solo la administración ve la necesidad de funcionar, desarrollar e interactuar con las demás entidades y los administrados, sino como los privados y de forma general personas del común han hecho de estos avances actos de cotidianidad.

Otro acontecimiento que dio cabida al uso de la firma digital como herramienta tecnológica fue el innovador comercio electrónico, este surge de la combinación entre la informática y los medios de comunicación, esto claramente demostrando el alcance de la ciencia en la cotidianidad de la vida de todas las personas.

1.2. Importancia del recorrido de mensaje de datos.

En el marco del desarrollo de las comunicaciones y las tecnologías se habla ahora de una información que plasmada en un medio tecnológico pasara a llamarse un mensaje de datos contenido ahora en un documento electrónico que debe gozar de seguridad, autenticidad y si el usuario lo desea también de disponibilidad, es de esta forma como se recurre a la internet**,** (Herrera Pérez, 2005):

En el mundo moderno la información se maneja en forma de datos, es decir, la información que se procesa y almacena en los sistemas de cómputo y que normalmente se relaciona con números, símbolos y texto. La generación y el procesamiento de los datos se realizan por medio de los sistemas de cómputo, y es lo que se conoce como informática. El transporte de esos datos para el intercambio de información se efectúa a través de las redes de transmisión de datos y en lo que se conoce como tele informática. Si bien la primera disciplina puede funcionar por sí sola, cuando se trata de compartir con otras entidades la información y el resultado el procesamiento de esta, es imprescindible el apoyo de la segunda disciplina.

Ahora bien, hablando de aquel mensaje de datos que requiere de seguridad, confidencialidad, autenticidad y no repudio es necesario la intervención de una herramienta que brinde todos estos componentes para la confiabilidad a la hora de necesitar intercambiar ese mensaje de datos con otra persona, esa herramienta es la firma digital.

Las firmas digitales, como se habló anteriormente es una herramienta útil y eficaz que se ha venido implementando debido a los avances del siglo xxi para realizar comunicaciones, efectuar transacciones, crear documentos electrónicos o cualquier otra actividad mediante el uso del intercambio electrónico de datos y su importancia para el desarrollo del comercio y la producción, permitiendo la realización y concreción de múltiples negocios de trascendental importancia, tanto para el sector público como para el sector privado.

Claramente debe existir un manejo y vigilancia para contrarrestar cualquier tipo de amenaza al mensaje de datos que se va enviar, para ello es necesario un proceso de identificación y autenticación, en donde el usuario deberá ingresar un Nombre o cualquier otra cosa que lo determine y sumando a esto una contraseña que asegure que es en realidad la persona que dice ser.

1.3. **Uso de las firmas digitales Colombia.**

Ahora bien, con la llegada de la Ley 527 de 1999 a Colombia, el estado se ve en la necesidad de transformar y agregar al ordenamiento jurídico para estar a la vanguardia de los nuevos avances tecnológicos en materia comercial y de las comunicaciones, algo que facilitase la nueva manera de hace más fácil el intercambio de información, de adquirir productos y servicios de forma rápida y segura y en general de las relaciones internacionales tanto del sector público como del privado.

Como cualquier acontecimiento, las firmas digitales trajeron consigo la posibilidad de que con la más alta seguridad se mantuviese a salvo información que requiere de esta estricta característica, para ello según la historia de Certicámara S.A (Certicámara - Líderes en certificación digital en Colombia 2017) dice:

En el año 2001, la Cámara de Comercio de Bogotá, en asocio con las Cámaras de Comercio de Medellín, Cali, Bucaramanga, Cúcuta, Aburrá Sur y la Confederación de Cámaras de Comercio, Confecámaras crearon la Sociedad Cameral de Certificación Digital, CERTICÁMARA S.A., entidad de certificación digital abierta, constituida con el propósito de asegurar jurídica y técnicamente las transacciones, comunicaciones, aplicaciones y en

general cualquier proceso de administración de información digital de conformidad con la Ley 527 de 1999 y los estándares técnicos internacionales. Los servicios de Certificación Digital de nuestra entidad están soportados gracias a la mundialmente y reconocida tecnología PKI, de origen europeo, para el envío, recepción, archivo y procesamiento de la información electrónica.” Fue así, con la ayuda de las principales Cámara de Comercio del País y Confecámaras se crea esta sociedad para que sea en el caso de las firmas digitales aquella entidad que participaría como un tercero de confianza para la expedición de los certificados digitales o también llamados claves públicas en el proceso de envío de mensaje de datos o documentos electrónicos de entidades públicas y también del sector privado.

Pero es importante atender a la problemática que como grupo nos surge, que es la de por qué si Villavicencio siendo una ciudad capital, en donde se concentra en su mayoría la mayor parte de recursos que a esta ciudad entran, por su avance económico, y estructural, ¿no se le hará necesario implementar un recurso tecnológico para el mejoramiento de la administración en cuanto a seguridad, pues por supuesto no somos ajenos a distintos delitos de corrupción, falsificación de documentos y entre otros que podrían ser evitados con la implementación de esta herramienta y no solo en la administración sino en el comercio a cargo de los particulares, cuyos negocios se han podido ver afectados por artimañas de terceros para delitos de estafa, hurto entre otros? y es que en Villavicencio, el uso de esta herramienta útil como lo es la firma digital tanto en las entidades públicas como privadas no es habitual, y el desconocimiento sobre todo aun en los administrados y personas en general.

2. Marco Teórico

En el artículo 2 de la Ley 527 de 1999 encontramos la definición de firma digital, como un procedimiento matemático conocido vinculado a la clave del iniciador y al texto del mensaje; que garantiza dos atributos propios de las comunicaciones electrónicas: la autenticidad y la integridad, que a su vez derivan en un tercero que tiene también gran trascendencia jurídica: el no repudio de acuerdo al Decreto 2364 de 2012, el mecanismo que garantiza autenticidad e integridad.

A inicios del siglo XXI, el desarrollo de las nuevas tecnologías de la información vincula das a la revolución de las te le comunicaciones ha plantea do nuevos desafíos para el derecho. El advenimiento del mundo digital provoca la aparición de circunstancias totalmente

nuevas que impiden en ocasiones tanto la aplicación de instrumentos jurídicos tradicionales como su adaptación al nuevo me dio; exigiendo, en consecuencia, nuevas formulaciones específicas por parte del orden jurídico. (Ortega Martínez, 2004)[1]

La firma digital es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, posibilitando que éstos gocen de una característica que únicamente era propia de los documentos en papel, es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje. Algunos de los atributos más representativos de la firma digital son: es única, es verificable, está bajo control exclusivo del iniciador, está ligada a la información del mensaje y está de acuerdo con la reglamentación. (Rojas López, Suarez Botero, Meneses Durango & D, 2011)

2.1 Funcionamiento.

La firma digital de un mensaje electrónico está asociado a un proceso coordinado, organizado y secuencial para permitir que sea seguro, para ello se tiene que:

1. El emisor crea un mensaje determinado
2. El emisor aplica al mensaje una función hash y así obtiene un resumen del mensaje
3. El emisor cifra el mensaje utilizando su clave privada
4. El emisor le envía al receptor un correo electrónico con los siguientes elementos:

4.1 El cuerpo del mensaje (sin cifrar o cifrado, por medio de la clave pública del receptor)

4.2 La firma del mensaje, que se compone de:

4.2.1 El hash o mensaje cifrado con la clave privada del emisor

4.2.2 El certificado digital del emisor con todos sus datos y que está cifrado con la clave privada del Prestador de Servicios de certificación.

(Rojas López, Suarez Botero, Meneses Durango & D, 2011)[2]

1 Las tecnologías de la información y las comunicaciones están engendrando un nuevo sistema económico y social donde la producción, procesamiento y distribución de conocimiento e información constituyen la fuente fundamental de productividad, bienestar y poder. Esto ha de terminado que se califique a las sociedades modernas como “sociedades de la información”, caracterizadas como un tipo de sociedad que está surgiendo por el creciente papel de las telecomunicaciones como elemento fundamental de la vida cotidiana, lo que ha llevado a afirmar que, como con secuencia de la profunda transformación operada en el sector de las comunicaciones, y concretamente de las nuevas tecnologías de la información, estemos en presencia de una nueva revolución científica y tecnológica, la llamada “economía digital”.

2.2 Requisitos para la firma digital.

1. La firma digital debe ser válida. Para ello una entidad de certificación en la que confíe el sistema operativo debe firmar el certificado digital en el que se basa la firma digital.
2. El certificado asociado a la firma digital no debe a ver caducado.
3. La persona o la organización que firma (conocida como el publicador) es de confianza para el destinatario.
4. El certificado asociado a la firma digital ha sido emitido para el publicador firmante por una entidad de certificación acreditada.

El proceso que se lleva a cabo para realizar la firma digital es el siguiente: Se emplean 2 algoritmos de cifrado de clave asimétrica (o pública), estos algoritmos funcionan mediante el uso de 2 claves, una pública y una privada que van a pertenecer a un mismo sujeto, esas claves se obtienen mediante un algoritmo y empleando un algoritmo concreto. Un mensaje cifrado con la clave pública de un sujeto solo podrá ser descifrado con la clave privada del mismo y nunca con la pública, la clave pública está al alcance de cualquiera, mientras que la clave privada debe ser custodiada únicamente por el propietario del par de claves.

Entonces al momento de recibir el correo electrónico el receptor descifra el certificado digital del emisor que está en el correo electrónico usando la clave pública del prestador de servicios de certificación que ha expedido el certificado , ahora esa clave pública se encuentra en la página web del prestador de servicios de certificación , posteriormente una vez descifrado el certificado el receptor accede a la clave pública del emisor y con esta clave descifrara el hash creado por el emisor para ello el receptor aplicara al cuerpo del mensaje la misma función has que utilizo el emisor con anterioridad para obtener un mensaje , en el caso en el que el cuerpo del mensaje también este cifrado para garantizar una mayor seguridad , el receptor deberá descifrarlo utilizando su propia clave privada .

Después el receptor comparara el hash que tienen que coincidir y de esta manera se asegurara de que el mensaje no haya sido alterado durante su envió, de esta manera se garantiza que el

2 La implementación del comercio electrónico requiere de una tecnología que permita soportar los procesos del negocio financiero, sin poner en riesgo la integridad de la información del cliente. El comercio electrónico y el sistema de firma digital requieren infraestructura tecnológica de comunicaciones, equipo de cómputo y aplicaciones que permitan el intercambio de información con empresas y otras entidades. Estos cambios tecnológicos pueden representar problemas como son: seguridad de las transacciones, y la implantación y administración de plataformas que permitan realizar transacciones seguras; es decir en general la administración segura de la información. La seguridad requiere de equipo y software adicional para minimizar el riesgo de un ataque.

mensaje cifrado por el receptor con la clave pública no ha sido cifrada con la clave privada del emisor y por tanto proviene de este. (Rojas López, Suarez Botero, Meneses Durango & D, 2011)

3. Antecedentes y desarrollo legal de la firma digital.

La evolución tecnológica de los últimos años en el campo electrónico y digital, ha transformado la industria, el comercio, el sector servicios, domestico, entre otros. Jijena Leiva, Palazzi & Téllez Valdés, 2003.

En lo que respecta al derecho, el encuentro con esta sociedad e Internet es inevitable, ya "que donde hay sociedad hay derecho" (ubi societas ibi ius) y esta sociedad de la información no puede constituir una excepción. Ahora que el grado de tele informatización de la sociedad ha llegado a puntos insoslayablemente álgidos, la intervención del derecho se convierte en imperioso menester, a través del surgimiento de un cuerpo de normas jurídicas que rigen de manera efectiva estas nuevas situaciones, dentro de las cuales y sin pretender ser exhaustivos, tenemos a Internet, los nombres dominios, el comercio electrónico Y las firmas digitales, como sólo algunos ejemplos representativos.

En 1976 el concepto de firma digital fue introducido por Diffie y Hellman y decía que la firma digital era un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje.

En 1978 R. Riveros, A Shamir y L. Adleman, del MIT proponen el hasta hoy más usado método firma digital, denominado RSA, ese método en principio obedece a los mismos principios que la firma autógrafa.

En 1985 se publica la tesis (A Public Key Cryptosystem and Siganture Scheme Based Discrete Logarithms) con la que posteriormente se construyó la base de algoritmos de la firma digital, adoptando por el instituto Nacional de Estándares y Tecnológico como el estándar de firmas digitales.

1991 Ub algoritmo propuesto por el instituto nacional de normas y tecnología de los estados unidos para su uso en su estándar de firma digital (DSS) ese algoritmo como su nombre lo indica, sirve para firmas y para cifrar información.

1995 La primera ley en materia de firma digital en el mundo fue la denominada “Utah Digital signature Act” publicada en mayo de 1995 en el Estado de UTAH, en Estados Unidos.

3.1. Marco legal

Aunque el tema de firmas digitales aparentemente se podría decir que ha tenido poca regulación, a continuación se presenta la normatividad de la cual la gente tiene poco conocimiento pero que es de necesario aprendizaje.

Ley 527 de 1999

Esta desarrolla varios temas de datos pero en concreto respecto a la firma digital, nos da una pequeña definición de esta y en un capítulo dedicado a este tema, expresa los atributos de la firma digital y equipara esta con la firma escrita, siempre y cuando cumpla con ciertos requisitos allí previstos. Así pues la Corte Constitucional explica el porqué de la necesidad de esta ley:

Los antecedentes de la Ley 527 de 1999

Ley 1564 de 2012**:** comúnmente conocido como código general del proceso y que reemplaza al antiguo código de procedimiento civil o DECRETO 1400 DE 1970 y sus posteriores modificaciones. A diferencia del antiguo código que en los temas de poderes especiales solo podían ser conferidos mediante escritura pública o memorial dirigido al juez, en el nuevo código general del proceso promueve el uso de la firma digital, haciendo uso de esta para conferir poderes especiales. (Ley 1564 de 2012, por la cual se expide el Código General del Proceso, de 12 de julio de 2012 Diario Oficial No. 48.489)

Ley 962 de 2005: conocida como ley anti tramites, en sus primeros artículos se refiere al tema de la firma digital, haciendo un énfasis de hacer uso de las nuevas tecnologías con el fin de cumplir principios tales como economía, celeridad, entre otros y ya en el tema específico, hace alusión de que en caso de la sustanciación de actuaciones y actos administrativos, la firma escrita puede ser reemplazada por la firma digital, siempre y cuando esta cumpla sus requisitos legales. Es importante aclarar que todo el tema del uso de tecnologías y entre estas esta la firma digital, podrán ser usados si la entidad de la administración pública dispone de las herramientas necesarias para el uso de estos avances tecnológicos. (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. Versión original publicada en el Diario Oficial No. 45.963 de 08 de julio de 2005)

Ley 1150 de 2007: que regula temas de contratación estatal, añade el uso de los medios tecnológicos entre ellos la firma digital, para todo lo relacionado a actos administrativos, contratos o actos derivados en la etapa contractual o pre-contractual entre otros temas, el uso de estos medios está regulado por ley 527 de 1999. (Ley 1150 de 2007, Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos, Diario Oficial No. 46.691 de 16 de julio de 2007)

Decreto Ley 019 de 2012: modificó unos artículos de la Ley 527 de 1999 en lo relacionado a las entidades de certificación. En el presente decreto ley el artículo 160 dispuso necesario y obligatorio que las entidades de certificación debían estar acreditadas ante la ONAC. Derogó este decreto ley en su artículo 176 también artículos de la ley 527 de 1999 como lo son el 41 y 42. (Decreto [con fuerza de ley] 019 de 2012. Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública. Diario Oficial No. 48.308 de 10 de enero de 2012)

Decreto 333 de 2014: este decreto es el encargado de reglamentar el artículo 160 del decreto ley 019 de 2012, de lo que resulta la reglamentación de las entidades de certificación y la renovación del artículo 29 de la Ley 527 de 1999. Por ende el haber este decreto reglamentado el artículo 160 del decreto ley 019 de 2012 con respecto a la acreditación de las entidades de certificación seguido a esto entraría a agregar o complementar los artículos 29, 30, literal (h) del 32 y el 34 de la ley 527 de 1999. (Decreto 333 de 2014. Por el cual se reglamenta el artículo 160 del Decreto-ley 19 de 2012, febrero de 2014)

Sentencia C-662-2000: es la respuesta de la Corte Constitucional a La ciudadana Olga Lucia Toro Pérez, en ejercicio de la acción pública de inconstitucionalidad consagrada en la Constitución Política de 1991, pide a la Corte declarar inexequibles los 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 de la Ley 527 de 1999.A lo que la corte responde declarando exequible todos y cada uno de estos artículos,

además aclarando a la accionante cual había sido modo groso el porqué de la expedición de la ley, y esto fue lo que aclaro:

La exposición de motivo del proyecto presentado al Congreso de la República por los Ministros de Justicia y del Derecho, de Desarrollo, de Comercio Exterior y de Transporte, que culminó en la expedición de la Ley 527 de 1999, ilustró las exigencias que el cambio tecnológico planteaba en términos de la actualización de la legislación nacional para ponerla a tono con las nuevas realidades de comunicación e interacción imperantes y para darle fundamento jurídico a las transacciones comerciales efectuadas por medios electrónicos y fuerza probatoria a los mensajes de datos, en los siguientes términos :
"...

El desarrollo tecnológico que se viene logrando en los países industrializados, permite agilizar y hacer mucho más operante la prestación de los servicios y el intercambio de bienes tangibles o intangibles, lo cual hace importante que nuestro país incorpore dentro de su estructura legal, normas que faciliten las condiciones para acceder a canales eficientes de derecho mercantil internacional, en virtud a los obstáculos que para éste encarna una deficiente y obsoleta regulación al respecto"

Claro está, tomando también en cuenta directrices u observaciones hechas por la Comisión de las Naciones Unidas para el desarrollo del Derecho Mercantil Internacional y la expedición de la Ley Modelo sobre comercio electrónico.

Sentencia C-831-2001: es la respuesta de la Corte Constitucional ante la acción pública de inconstitucionalidad presentada por el ciudadano Daniel Peña Valenzuela que demandó el artículo 6 de la Ley 527 de 1999 que se encuentra en el Capítulo 2 y habla sobre la Aplicación de los requisitos jurídicos de los mensajes de datos, pues cree que vulnera los articulo 28 y 152 de la constitución política, ya que el artículo se refiere a que cualquier norma que exija información por escrito quedara satisfecho aun cuando esta se haya hecho por un mensaje de datos y que luego pueda volverse a consultar, pero el ciudadano cree que vulnera el Artículo 28 de C.P que trata sobre la libertad personal, adherido a esto como un derecho fundamental, y que una tema como este de derecho fundamental ha debido ser tratado por una ley estatutaria y no por una ley ordinaria como lo es la ley 527 de 1999, a lo que la corte respondió que la ley hacia énfasis al comercio electrónico de bienes y servicios, y

por tanto no debía ser entendido por el ciudadano desde ese punto de vista el artículo 6 de la ley 527 de 1999, así que la Corte declaro exequible el artículo de la presente.

La Circular No.643 de 2004: de la Superintendencia de Notariado y Registro:
En esta circular fijan las condiciones para enviar documentos que nazcan de las Notarías a las Cámaras de Comercio utilizando firmas digitales certificadas. (Rincón Cárdenas, 2006)

La Circular 012 de 2004: La Supersalud exige que el envío de reportes de información financiera y general de las ESE (Empresas Sociales del Estado) se haga con el uso de las firmas digitales certificadas. (Rincón Cárdenas, 2006)

La Circular 013 de 2004: La Supersalud exige que el envío de reportes de información sobre IVA cedido al Sector Salud por parte de las gobernaciones, secretarias de hacienda, secretarias de salud, productores de licores entre otros. (Rincón Cárdenas ,2006)

La Circular externa 50 de 2003: Ministerio de Industria y Comercio, establece la posibilidad del registro de importación a través de Internet (VUCE Ventanilla única de Comercio Exterior). Este trámite puede hacerse de forma remota firmado digitalmente y de ese modo reducir el trámite que se piensa racionalizar por este medio.
Esta circular crea la posibilidad de que se pueda hacer el registro de importación a través de Internet, y este trámite se podrá hacer de forma rápida firmado digitalmente y así crear rapidez para este procedimiento. (Rincón Cárdenas,2006)

Circular de Supersociedades: Dirigida a todas las sociedades mercantiles vigiladas y controladas por la superintendencia para el envío de información financiera y contable a través del sistema SIREM el Sistema de Información y Riesgo Empresarial un sistema vía Web que permite entregar todos los reportes e informes por esta vía con el uso de certificados digitales. (Rincón Cárdenas, 2006)

La Circular 011 de 2004: La Supersalud exige que el envío de reportes de información financiera y general de las IPS se haga con el uso de las firmas digitales certificadas. (Rincón Cárdenas, 2006)

Directiva Presidencial N° 4 del 03 de Abril de 2012 Consiste en el reemplazo del papeleo por soportes y medios electrónicos, que se fundamentan en la implementación de Tecnologías de la Información y las Telecomunicaciones. Claro que esto tiene aspectos más favorables que el descongestionamiento en la administración, también ayuda a la mejora y protección del medio ambiente. El propósito de seguir adelante con la Política de Eficiencia Administrativa y Cero Papel en la Administración Publica, los organismos y entidades a las que va destinada esta directiva tienen el deber de organizar, racionalizar, disminuir todo los tramites y procesos internos para una eficiente y rápida prestación del servicio por parte de estas entidades. (Eficiencia administrativa y lineamientos de la política cero papel en la administración pública 2012)

3.2 ¿Cómo sé que el certificado descargado es real y no se ha generado de forma fraudulenta?

Allí aparecen las Autoridades de Certificación (CA), que son organismos directamente encargados de generar certificados digitales de cualquier tipo, desde firma digital hasta certificados de servidor SSL , estas serán entidades autorizadas que generan certificados como anteriormente las nombrábamos ,en cada uno de los certificados SSL (en base del protocolo x.509) se establece un emisor que es la entidad (persona, asociación, empresa etc.) que ha generado el certificado , verificando el emisor , así como los certificados involucrados se puede asegurar si el certificado lo ha emitido dicha entidad y de este modo se puede clasificar en base a la confianza que se deposita en dicha entidad . Esta validación queda reflejada en el diagrama de funcionamiento de SSL.

Las Autoridades de Certificación disponen de un certificado conocido como Certificado Raíz (Root CA), y como su nombre indica es el certificado que validará todos y cada uno de los certificados emitidos por la CA; sin embargo, este certificado no es el que firmará los certificados de suscriptor (o certificados finales), sino se empleará únicamente para firmar los denominados Certificados Subordinados (Sub-CA), y estos últimos firmarán los certificados de suscriptor (o finales) pero en Colombia aún no se ve esta jerarquía. (Cutanda, 2014).

3.3 ¿Cómo sé que el certificado que firma el anterior es válido?

El modelo de cadena de confianza este modelo establece una relación entre certificados, el Root CA que validara todos los certificados, pero solo firmara los certificados subordinados y los certificados subordinados firmaran los certificados finales, es decir los del suscriptor, el motivo de esta jerarquía es para proteger al certificado raíz ya que si un tercero consiguiera la clave privada de un certificado raíz emitiría certificados de CA debido a ello los certificados finales no están firmados con esta clave , un certificados de suscriptor firmado por el raíz no sería de suscriptor sino subordinado, lo que conllevaría dar esa clave a un usuario , por este motivo la clave privada del certificado de raíz se encuentra en offline , en un dispositivo de seguridad cifrado. De modo que, para validar un certificado de un suscriptor, se deberá comprobar la firma para toda la cadena de confianza de la CA emisora, quedando así clara la procedencia del mismo. (Cutanda, 2014)

4. La firma digital como método de seguridad informática

Mediante derecho de petición con radicado 20170020009602 el día 16 de enero de 2017 se pidió información acerca de los delitos informáticos que se presentan en la zona del departamento del Meta, a cuya petición contestó DIANA MILENA BACCA DUARTE, Profesional de Gestión III, Dirección Seccional Meta. Fiscalía General de la Nación, quien arrojó el siguiente resultado:

Tabla 1. Alcance de firmas digitales

Año	Delito	Cant.
2012	Acceso abusivo a un sistema informático art 269a ley 273 de 2009	11
	Acceso abusivo a un sistema informático art 269a ley 273 de 2009, agravado por realizarse sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros art. 269h n1	2
	Acceso abusivo a un sistema informático. Art. 195 c.p.	2
	Hurto por medios informáticos y semejantes art. 269i ley 273 de 2009	110
	Interceptación de datos informáticos, art 269c ley 273 de 2009	1
	Suplantación de sitios web para capturar datos personales art 269g ley 273 de 2009	1
	Transferencia no consentida de activos valiéndose de alguna manipulación informática o artificio semejante art. 269j ley 273 de 2009	2

Tabla 1. Continuación

2013	Acceso abusivo a un sistema informático art 269a ley 273 de 2009	2
	Hurto por medios informáticos y semejantes art. 269i ley 273 de 2009	123
	Interceptación de datos informáticos art 269c ley 273 de 2009 agravado por obtener provecho para sí o para un tercero. Art. 269h n5	1
	Interceptación de datos informáticos, art 269c ley 273 de 2009	1
	Suplantación de sitios web para capturar datos personales art 269g ley 273 de 2009	1
	Transferencia no consentida de activos valiéndose de alguna manipulación informática o artificio semejante art. 269j ley 273 de 2009	3
2014	Acceso abusivo a un sistema informático art 269a ley 273 de 2009	10
	Acceso abusivo a un sistema informático. Art. 195 c.p.	2
	Hurto por medios informáticos y semejantes art. 269i ley 273 de 2009	114
	Interceptación de datos informáticos, art 269c ley 273 de 2009	1
	Suplantación de sitios web para capturar datos personales art 269g ley 273 de 2009	5
	Suplantación de sitios web para capturar datos personales art 269g ley 273 de 2009, agravado por obtener provecho para sí o para un tercero. Art. 269h n5	1
	Transferencia no consentida de activos valiéndose de alguna manipulación informática o artificio semejante art. 269j ley 273 de 2009	2
2015	Acceso abusivo a un sistema informático art 269a ley 273 de 2009	17
	Hurto por medios informáticos y semejantes art. 269i ley 273 de 2009	120
	Interceptación de datos informáticos, art 269c ley 273 de 2009	2
	Transferencia no consentida de activos valiéndose de alguna manipulación informática o artificio semejante art. 269j ley 273 de 2009	1
2016	Acceso abusivo a un sistema informático art 269a ley 273 de 2009	13
	Hurto por medios informáticos y semejantes art. 269i ley 273 de 2009	140
	Suplantación de sitios web para capturar datos personales art 269g ley 273 de 2009	2
	Suplantación de sitios web para capturar datos personales art 269g ley 273 de 2009, agravado por aprovecharse de la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este. art. 269h n3	1
	Transferencia no consentida de activos valiéndose de alguna manipulación informática o artificio semejante art. 269j ley 273 de 2009	4
2017	Acceso abusivo a un sistema informático art 269a ley 273 de 2009	6
	Hurto por medios informáticos y semejantes art. 269i ley 273 de 2009	12
TOTAL		**713**

Nota: delitos informáticos que se presentan en la zona del departamento del Meta. Aportado por DIANA MILENA BACCA DUARTE, Profesional de Gestión III, Dirección Seccional Meta. Fiscalía General de la Nación, por Naranjo & García, 2017.

De lo anterior se puede inferir que la sociedad se encuentra en la necesidad de incorporar una herramienta tecnológica en su cotidiano vivir para disminuir las delitos informáticos.

5. Metodología

La investigación manifiesta en este artículo es de carácter cualitativo, pues para la realización de tal se necesitó la caracterización de un tema y se partió de algo ya conocido y no de simples teorías, determinar sus cualidades y alcances en un determinado territorio, el uso de entrevista como medio de recolección de datos característico de esta metodología llevo a una correcta dirección de nuestro escrito, además de otros medios como algunos libros. Además, se implementó un método descriptivo y analítico de las firmas digitales, abarcando una amplia manifestación del legislador que aparentemente no había pero que se logró manifestar en el reciente escrito.

Conclusiones

El uso de herramientas tecnológicas a lo largo de la historia ha provocado que las mismas se hagan trascendentales para el desarrollo de las sociedades, desarrollo necesario para no quedar en el olvido, o sin importancia para otros países.

Para nadie es un secreto que con la revolución digital ha traído consigo determinantemente el ingreso de nuevas tecnologías, consecuente a esto unas problemáticas que a lo largo de su desarrollo (de las tecnologías) también se han ido incrementando los problemas. Con ello hago alusión a las inseguridades que se generan con el uso de medios electrónicos para la comunicación, realización, finalización o dirección de negocios internacionales de índole público o privado.

Ahora bien, en el marco de una seguridad en los documentos electrónicos, manera por la cual se hacen posible las comunicaciones de sujetos que se encuentran muchas veces al otro lado del mundo, se ha visto necesario que a estos (documentos electrónicos) se les adhiera una herramienta para imposibilitar a un tercero ajeno de dicha relación a intervenir de forma negativa en ello, en otras palabras, evitar delitos informáticos, tales como: acceso abusivo a un sistema informático, hurto por medios informáticos y semejantes, suplantación de sitios web para capturar datos personales, interceptación de datos informáticos, entre otros,

que, sin una herramienta como la firma digital, para asegurar esa información, sea o no trascendental para los sujetos de dichas relaciones, puede ser fácilmente hurtada, modificada, plagiada o en pocas palabras hackeada.

Es por ello, que uno de los factores implementados con el apogeo de la globalización, especialmente la llegada directa de las TIC'S, es la necesidad en la que se encuentran los estados de regular aquellas acciones y sus consecuencias, donde trascendentalmente y sin querer dejarlo a un lado, es por orden internacional que aquellas figuras han debido regularse.

En el caso concreto, como Colombia, ha hecho caso a aquellas directrices de la ONU, en principio, de legislar sobre ello; sin embargo aunque su marco legal es amplio y especifico, aun no se ha podido llegar a la creencia fundamental que se pretende con el implemento de estas nuevas herramientas, que es la de prevenir los delitos, que como se dijo antes, se suscitan en dichos temas, pues para nadie es un secreto que actualmente existen personas que dedican a la tarea de sustraer información no pertinente de manera ilícita, irregular o ilegal, ello, gracias al avance exponencial y no controlado de materiales tecnológicos que está al alcance fácilmente para cualquier persona; pero ahora es aún más necesario que estas herramientas que el legislador ha dispuesto, sean usadas idóneamente por los demás entes descentralizados para que exista armonía, integridad y buena práctica de aquellas herramientas.

Referencias Bibliográficas

Cert Superior, 2016,¿Qué es un Certificado SSL?, Recuperado: https://www.certsuperior.com/

Areitio,J, (2008), *Seguridad de la información*. 1. Madrid: Paraninfo Cengage Learning.

Baca, G, (2016), *Introducción a la seguridad informática*. Distrito Federal: Grupo Editorial Patria.

Bennasar, A, (2010), *La validez del documento electrónico y su eficacia en sede procesal*. 1. Valladolid: Lex Nova.

Bolivar,L. Comercio Electrónico B2c: *La Protección De Los Consumidores En Colombia*, (2002). . P. 8-10. Recuperado de: file:///C:/Users/prof-biblioteca2/Downloads/2162-Texto%20del%20art%C3%ADculo-7385-1-10-20101028.pdf

Cortéz, J. & Cardona, D, (2015), *Gobierno electrónico en América Latina.* 1. Bogotá: Editorial Universidad del Rosario.

Cutanda, D, (2013), *Fundamentos sobre certificados digitales* - Security Art Work. Security Art Work . Recuperado: https://www.securityartwork.es/2013/05/13/fundamentos-sobre-certificados-digitales/

Cutanda, D, (2014), *Fundamentos sobre certificados digitales – Declaración de Prácticas de Certificación*. Available from: https://www.securityartwork.es/2014/02/07/fundamentos-sobre-certificados-digitales-declaracion-de-practicas-de-certificacion/

Díaz, G; Castro, M; Alzorris, A & Sancristobal, E, (2014), *Procesos y herramientas para la seguridad de redes.*

Firtman, S, (2005), *Seguridad informática*. 1. Buenos Aires: MP Ediciones.

Flórez, G, (2014), *La validez jurídica de los documentos electrónicos en Colombia a partir de sus evolución legislativa y jurisprudencial*. Verba Iuris. Available from:

http://www.unilibre.edu.co/verbaiuris/31/la-validez-juridica-de-los-documentos-electronicos-en-colombia-a-partir-de-su-evolucion-legislativa-y-jurisprudencial.pdf

García, M; Francisco, J & and Arredondo, F (2015), *El documento electrónico. Un reto a la seguridad jurídica.* 1. Madrid: Dykinson.

Gómez, A, (2011), *Enciclopedia de la seguridad informática*. 2. Madrid: Ra-Ma.

González, L & Fuentes, JM, (2014), *Sistemas seguros de acceso y transmisión de datos. 1. Antequera,* Málaga: IC Editorial.

Gutiérrez, J & Tena, J, (2003), *Protocolos criptográficos y seguridad en redes.* 1. Santander: Servicio de Publicaciones de la Universidad de Cantabria.

Herrera, E, (2005), *Tecnologías y redes de transmisión de datos*. México: Limusa.

Huidobro, M, Blanco, J & Calero, J (2006), *Redes de area local [recurso electrónico]*. 2. México: International Cengage Editores Spain Paraninfo, S.A.

Error509. Introducción a los certificados digitales. Certificados Digitales. Recuperado de : https://www.error509.com/2018/09/introduccion-a-los-certificados-digitales/

Leiva, J, Renato, J, Palazzi, Pablo, A & Téllez,J, (2003), *El derecho y la sociedad de la información. México, D.F.: Miguel Ángel Porrúa.*

Ley 527. (1999), Por la cual se expiden algunas disposiciones en materia de firma digital. Diario Oficial No 43.673. Obtenido de: https://www.mintic.gov.co/portal/604/articles-3679_documento.pdf

Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno 2001, 2002, 1. Nueva York: Naciones Unidas.

Maza, I, (2002) *Derecho y tecnologías de la información. 1. Chile*: Fundación Fernando Fueyo Laneri.

Ortiz, R; Paez, A & Angel, E (2017), 10. *Innovación, burocracia y gobierno electrónico en la administración pública. Hologramtica* Available from: http://www.cienciared.com.ar/ra/usr/3/895/hologramatica_n12vol2pp25_42.pdf

Quintero, J; (2006), *Firma digital basada en redes*. *Revista Científica, 2006-08-00 nro: 8* Available from: https://revistas.udistrital.edu.co/ojs/index.php/revcie/article/view/336/499

Ramos, B & Rigaborda, A (2004), *Avances en criptología y seguridad de la información.* Madrid: Ediciones Díaz de Santos.

Rincón, E & Vergara, C, (2017), *Administración pública electrónica: hacia el procedimiento administrativo electrónico*. 1. Bogotá: Editorial Universidad del Rosario.

Rincón, E, (2006), *Manual de derecho de comercio electrónico y de Internet*. Bogotá: Centro Ed. Rosarista.

Rojas, D; Suarez, M; Meneses, N. (2011). *Firma digital: instrumento de transmisión de información a entidades financieras.* Revista Avances en Sistemas e Informática. Vol 8 (num 1),pag 7-14 . Disponible en:<http://www.redalyc.org/articulo.oa?id=133117278002> ISSN 1657-7663

San Martin, E, (2014), *Salvaguarda y seguridad de los datos*. Antequera, Málaga: IC Editorial.

Sarubi, P, (2008), *Seguridad informática – Técnicas de defensa comunes bajo variantes del sistema operativo Unix*. Buenos Aires. Available from: https://es.scribd.com/document/7103092/Seguridad-Informatica-Tecnicas-de-defensa-comunes-bajo-variantes-del-sistema-operativo-Unix

Seguridad De La Información, (2014). 1. Guatemala: Segunda Cohorte del Doctorado en Seguridad.

What is an SSL certificate?. Recuperado de: https://www.globalsign.com/en/ssl-information-center/what-is-an-ssl-certificate/

Stallings, W, (2004), *Fundamentos De Seguridad En Redes*. 2. Madrid: Pearson Educación de México, SA de CV.

Torres, H, (2005), *El Sistema de Seguridad Jurídica en el comercio electrónico*-Peru. Available from: https://books.google.com.co/books?id=lXnlrIO09yUC&pg=PA115&dq=seguridad+de+las+firmas+digitales+revistas&hl=es-

419&sa=X&ved=0ahUKEwjFwpD4ueXaAhVQzFMKHSdOBaMQ6AEIPTAF#v=onepage&q=seguridad%2

Torres, H, (2005), *El sistema de seguridad jurídica en el comercio electrónico.* 1. Lima: Pontificia Universidad Católica del Perú - Fondo Ed.

Vega, F, (2012), Puerto Rico*: Comentarios a la Ley de Firmas digitales de... Portal de e-governo, inclusão digital e sociedade do conhecimento*. Available from: http://www.egov.ufsc.br/portal/conteudo/comentarios-la-ley-de-firmas-digitales-de-puerto-rico

Zambrano, F, *Elementos legales de validez jurídica de los actos administrativos emitidos a través de medios electrónicos de acuerdo a la ley 1437 de 2011*. Available from: http://repository.usta.edu.co/handle/11634/572