FACULTAD DE DERECHO Y GOBERNABILIDAD

Título del trabajo:

“Estándares internacionales de la firma electrónica y sus principios generales, propuesta de mejoramiento periodo 2020 – 2021”

Carrera:

Derecho con énfasis en Legislación Empresarial y Tributaria

Autor:

Gilson Andrés Córdova Marcillo

Tutor (a):

Ab. Mercedes Coronel Gómez, Mgtr.

Samborondón-Ecuador

2020

DEDICATORIA

Dedico esta tesis a mi papá, Wilson Córdova Toainga, por siempre estar para mí con las palabras correctas de apoyo, por ayudarme a alcanzar mis metas y a mi mamá, Petita Marcillo Alay, por ser mi apoyo incondicional, por brindarme ese amor de madre y dándome siempre sus bendiciones, sin ellos esto no hubiese sido posible, ellos son un gran ejemplo en mi vida, a pesar de la distancia física, siempre estuvieron cerca motivándome para ser mejor cada día, por su apoyo constante, por llenar mi vida con sus valiosos consejos.

AGRADECIMIENTOS

Quiero expresar mi gratitud a Dios, quien con su bendición llena siempre mi vida y a toda mi familia, por estar siempre presentes, por mantener a mi familia siempre unida ya que el amor de Dios es grande.

A mis padres, Wilson y Petita por ser mi pilar fundamental y haberme apoyado incondicionalmente, quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño, este sueño no es solo mío, ya que también es el de mis padres en verme como profesional.

Agradezco a los docentes de la Facultad de Derecho y Gobernabilidad, por haber compartido sus conocimientos a lo largo de la preparación de nuestra profesión.

RESUMEN

Este proyecto de investigación se analizó los Estándares internacionales de la firma electrónica y sus principios generales, propuesta de mejoramiento periodo 2020-2021, tuvo como problemática la necesidad existente de analizar lo concerniente a las firmas electrónicas en el Ecuador surge la necesidad de partir de las definiciones técnicas como de la criptografía, claves públicas y privadas , considerándose que dentro de los países que tiene más desarrollado el tema de las firmas están Argentina y España, en sus respectivas legislaciones regulan a la firma digital, sin quitarle el valor a otras firmas que empleen distintos tipos de tecnología, en Ecuador se denomina como firma electrónica, donde se contradice el principio de neutralidad tecnológica, que esta descrito y protegido por la Ley Modelo de la Comisión de Naciones Unidad para el Derecho Mercantil Internacional, es por esto que la firma digital es el equivalente funcional de la firma manuscrita, porque garantiza la identificación del firmante, por esto es necesaria una reforma legal y tuvo como objetivo general de esta investigación fue comparar la normativa de la legislación ecuatoriana acerca de las firmas electrónicas, sus entandares internacionales y su regulación con los principios generales.

Para este trabajo se emplearon métodos de investigación propios de la ciencia del Derecho, tales como las normativas de otros países ya mencionados anteriormente, y como muestra, se obtuvo la opinión de expertos como al Ab. Fabrizio García Bacigalupo. LL.M. MSc., Ab. Francisco Cedeño Díaz y al Ab. Shafick Juez Cabezas, quienes poseen aproximadamente con 10 años de experiencia, y finalmente, de acuerdo a lo analizado en el marco teórico, y en las entrevistas es necesaria una reforma para que se pueda mejorar los protocolos de seguridad con la firma digital.

Palabras claves: firma electrónica, certificado electrónico, firma digital.

ASTRACT

This research project analyzed the International Standards for Electronic Signatures and their general principles, proposed for improvement in the period 2020-2021, and had as a problem the need to analyze what concerns the electronic signatures in Ecuador. It is necessary to start from the technical definitions such as cryptography, public and private keys, considering that within the countries that have more developed the issue of signatures are Argentina and Spain, in their respective legislations regulate the digital signature, without taking away the value of other signatures that use different types of technology, In Ecuador it is called an electronic signature, which contradicts the principle of technological neutrality, which is described and protected by the Model Law of the United Nations Commission on International Trade Law, which is why the digital signature is the functional equivalent of the handwritten signature, because it guarantees the identification of the signatory, so a legal reform is necessary and the general objective of this research was to compare the rules of Ecuadorian law on electronic signatures, their international standards and their regulation with general principles.

For this work, research methods were used that are typical of the science of law, such as the regulations of other countries already mentioned above, and as a sample, the opinion of experts such as Ab. Fabrizio Garcia Bacigalupo was obtained. Francisco Cedeño Díaz and Shafick Juez Cabezas, who have approximately 10 years of experience, and finally, according to what was analyzed in the theoretical framework and in the interviews, a reform is necessary so that the security protocols can be improved with the digital signature.

Keywords: electronic signature, electronic certificate, digital signature.

CERTIFICACION DE REVISION FINAL

QUE EL PRESENTE PROYECTO DE INVESTIGACIÓN O EXAMEN COMPLEXIVO TITULADO: “ESTÁNDARES INTERNACIONALES DE LA FIRMA ELECTRÓNICA Y SUS PRINCIPIOS GENERALES, PROPUESTA DE MEJORAMIENTO PERIODO 2020-2021“, FUE REVISADO, SIENDO SU CONTENIDO ORIGINAL EN SU TOTALIDAD, ASÍ COMO EL CUMPLIMIENTO DE LOS REQUERIMIENTOS QUE SE DICTAN EN LA GUÍA DE ELABORACIÓN DEL TRABAJO DE TITULACIÓN, POR LO QUE SE AUTORIZA A: **GILSON ANDRÉS CÓRDOVA MARCILLO,** QUE PROCEDA A SU PRESENTACION.

Samborondón, 11-06-2020

Mgtr. Mercedes Coronel Gómez

TUTOR

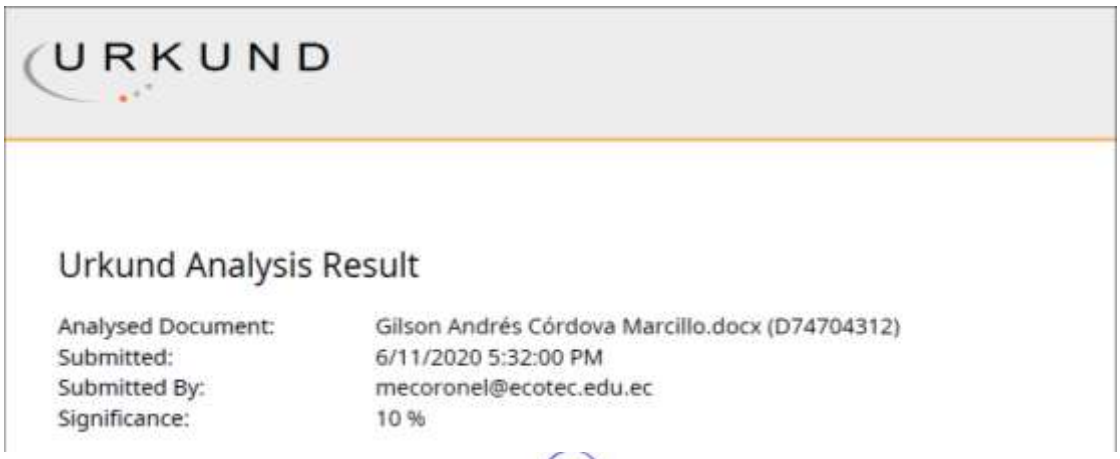
CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS

Habiendo sido nombrado Mgtr. Mercedes Coronel Gómez, tutor del trabajo de titulación "Estándares internacionales de firma electrónica y sus principios generales, propuesta de mejoramiento 2020-2012" elaborado por Gilson Andrés Córdova Marcillo**,** con mi respectiva supervisión como requerimiento parcial para la obtención del título de Abogado de los Tribunales y Juzgados de la República del Ecuador.

Se informa que el mismo ha resultado tener un porcentaje de coincidencias 10 % mismo que se puede verificar en el siguiente link:

https://secure.urkund.com/old/view/72028472-980481-220066#FY1LCgIxEETvknUh3UknPZmriAsZVGbhbGYp3t0noWh49cmnvM+yXk0ut5Q71ytqqKM/m/JKonIbfsNvgQbCb4s84AELOgEPWId1sp2tTq7/GRsJT7I5VUWBfKRoxFQf4pnGVCpN2ZXjpnLur2N/7tv92B5ltYvNzMX4whe2rMX3Bw==

Adicional se adjunta print de pantalla de dicho resultado.


URKUND

Urkund Analysis Result

Analysed Document:	Gilson Andrés Córdova Marcillo.docx (D74704312)
Submitted:	6/11/2020 5:32:00 PM
Submitted By:	mecoronel@ecotec.edu.ec
Significance:	10 %

Mgtr. Mercedes Coronel Gómez

TUTOR

Tabla de contenido

INTRODUCCIÓN

En nuestro tiempo las nuevas tecnologías de información y comunicación han transformado con su aplicación, casi todas las actividades que el ser humano realiza en este siglo XXI.

Este trabajo se desarrolla en cinco capítulos, se pretende determinar que la normativa que regula la firma electrónica en el Ecuador, específicamente en la Ley de Comercio Electrónico y Firmas Electrónicas y Mensajes de Datos, debe de tener por objeto una actualización para tener tendencias actuales sobre las firmas electrónicas y digitales, analizar con detalle la doctrina y la normativa de Argentina, España, de otros organismos como la Unión Europea y la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDIM), conocida por sus siglas en inglés como UNCITRAL.

En el primer capítulo se revisará lo concerniente a los objetivos y problemática, justificación de la investigación, y este capítulo se titula Diseño de la Investigación

En el Segundo capítulo se analizara la Firma Electrónica, partiendo de definiciones técnicas como las de criptografías, claves públicas y privadas, el análisis de la firma electrónica y firma digital, considerándose la importancia entre otros temas y análisis de la normativa internacional sobre las firmas electrónicas, además, contiene el análisis de los certificados de Firmas Electrónicas y de las entidades de certificación de información, en el caso de Ecuador se denominan Entidades de Certificación de Información, también se considera el período de validez del certificado de Firma Electrónica, que involucra, la duración, extinción y suspensión del mismo.

El tercer capítulo tratará respecto del Marco Metodológico de la investigación y los métodos empleados tales como el empírico, exegético, documental entre otros.

En el cuarto capítulo se realizarán unas entrevistas a un grupo de expertos para tener como base su conocimiento respecto de las firmas electrónicas en Ecuador.

El quinto capítulo versa netamente referente de la propuesta del proyecto la cual se va a efectuar referente a una reforma a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, para finalizar con conclusiones y recomendaciones.

La finalidad es determinar de qué se tratan estos certificados y entidades de certificación en la normativa internacional, así como se encuentran en la normativa ecuatoriana.

En todas las legislaciones se regula la firma digital, donde se analizó la Ley Modelo de la Comisión de Naciones Unidad para el Derecho Mercantil Internacional. Además, se estudió el cuerpo normativo vigente en el Ecuador. También, se analizaron los principios y estándares internacionales de la forma digital, donde nos centramos en demostrar que la normativa que regula la firma electrónica en Ecuador requiere de una actualización. En lo cual se propone de una nueva ley exclusivamente sobre firmas digitales.

CAPÍTULO I

DISEÑO DE LA INVESTIGACIÓN

En el presente capítulo se va a diseñar la problemática de la investigación, objetivos y su justificación.

Tema

Estándares internacionales de la firma electrónica y sus principios generales, propuesta de mejoramiento periodo 2020 – 2021

Planteamiento del problema científico

La necesidad existente de analizar lo concerniente a las firmas electrónicas en el Ecuador surge de la necesidad de partir de las definiciones técnicas como las de criptografías, claves públicas y privadas, considerándose también la importancia de la normativa internacional, y verificar si el Derecho Electrónico ecuatoriano se encuentra acorde a la normativa internacional existente, la regulación y control de las entidades de certificación, así como de sus funciones.

Para llegar a una situación óptima de debe realizar un estudio que dé como finalidad el planteamiento de que si se necesita una reforma comparando con los países de Argentina y España; además de conocer el tiempo de validez del certificado de forma electrónica, que involucra la duración, extinción y suspensión del mismo. Lo descrito con la finalidad de determinar que se tratan estos certificados y entidades de certificación en la normativa internacional, y como se encuentran concebidos en la normativa ecuatoriana.

Pregunta problemática

¿Es suficiente la normativa existente sobre las firmas electrónicas en el Ecuador en relación al cumplimiento de los estándares internacionales y sus principios generales?

Objetivos

Objetivo general

Comparar la normativa de la legislación ecuatoriana acerca de las firmas electrónicas, sus estándares internacionales y su relación con los principios generales.

Objetivos específicos

- Conocer el procedimiento del uso de las firmas electrónicas en el Ecuador respecto de sus principios generales.
- Determinar países específicos donde se use la firma electrónica.
- Proponer una reforma al cuerpo normativo ecuatoriano, para que este pueda satisfacer no solo los parámetros internacionales, sino también la realidad nacional y así fomentar el uso de la firma electrónica y digital.

Justificación

Es importante poder realizar este tema en el Ecuador en el sentido del derecho electrónico es nuevo, no existe mayor regulación salvo Ley de Comercio Electrónico, Firmas Electrónicas y mensajes de Datos, existe además el Reglamento General a la Ley de Comercio Electrónico, firmas Electrónicas y Mensajes de Datos, pero se regula a manera general puesto que esta ley fue promulgada en el año 2002, en derecho el tema de las firmas electrónicas es completamente nuevo y con el auge del internet de que todo es digital y por la coyuntura que está pasando el país que se está implemento el teletrabajo, es necesario abordar este tema de investigar a fondo para poder tener claro muchos aspectos y ofrecer este estudio a la sociedad.

Este nuevo tipo de soporte no pretende alterar el significado jurídico de los actos comerciales y es por esto que, el simple motivo de estar en soporte electrónico, no debería ser

justificación para cambiar el derecho existente al momento sobre las transacciones comerciales. El objetivo principal es que el hecho de que se necesiten nuevas normas para aplicar los aspectos electrónicos de comercio, no significa que se deban cambiar completamente las regulaciones sobre las relaciones comerciales.

Novedad o aspecto innovador

El aspecto innovador o novedoso del presente proyecto de investigación jurídico versa en torno a que este tema es poco estudiado en el país y aun no se le brinda la atención ni la importancia debida, cabe recalcar que el potencial que posee las firmas electrónicas no se ha explotado todavía en el Ecuador, y bien este también es uno de los factores por el cual se ha escogido este tema de estudios.

CAPÍTULO II

MARCO TEÓRICO

1.1. Marco teórico

1.1.1. Antecedentes

Desde la era del internet en la década de los 90s la comunicación entre las personas comenzó a cambiar, llegando a que la comunicación es casi instantáneas y eficaz, a pasar de los años el internet a logrado encajar en el comercio y en el derecho, a más del internet, que la informática, la globalización y la tecnología han cambiado mucho el aspecto de nuestras vidas a medida de gran escala.

El internet, es una red abierta en las cuales confluyen una gran cantidad de personas con la posibilidad de interceptar con diversas finalidades las transacciones electrónicas, generando riesgos e incertidumbres en las rutinas comerciales, para esto la seguridad informática consiste en "que el acceso a la información allí contenida, así como su modificación, solo sea posible a las personas que se encuentren acreditadas y dentro de los limites autorizado". (Costas, 2010, pág. 19)

Existe una clara tendencia hacia la interoperabilidad e interconectividad ofrecida por las redes, debido a esto, la seguridad de la información se ha vuelto crucial en el desarrollo de la sociedad. (Bertolín, 2008, pág. 2) Las redes brindan un sistema amplio de almacenamiento de información, así como envió y recepción de la misma; por la seguridad de esta información y por lo tanto, los mecanismos que la sustentan, se han vuelto un tema de suma importancia, especialmente para el Derecho.

En el Derecho Civil, la voluntad o el consentimiento son parte fundamental para la celebración de todo tipo de contratos, acuerdos, actas, etc. La expresión de la palabra voluntad de una persona se manifiesta a través de su firma, cuando apareció el internet la tradicional firma manuscrita quedo relegada, y es aquí cuando aparece la firma electrónica adaptándose a las necesidades actuales.

Según Bernardo Carlino, la tecnología avanza a un ritmo muy acelerado, mucho más rápido de lo que avanza el derecho, en lo absoluto para la sociedad debería que ambas partes avanzara a un mismo ritmo.

Las firmas cumplen una función, primero que nada de Identificación y determina la personalidad, Podemos señalar que las firmas electrónicas fueron creadas con fines de seguridad informática, por el cual se acopla a la contratación electrónica y demás figuras del Derecho moderno, que deben ofrecer a sus usuarios la misma seguridad jurídica en el intercambio de información, al poder dar de esta manera una mayor certeza en cuanto a la integridad, autenticación y no repudio en él envió de un mensaje de datos, en el transcurso de este capítulo, se tratará de demostrar si es correcto que la legislación del Ecuador norme como Firma Electrónica, o firma digital, y si su régimen de aplicación se encuentra acorde a la normativa internacional.

1.1.2. La firma manuscrita

El vocablo firma proviene del latín *firmare* que significa, afirmar, dar fuerza y por otra parte el vocablo autógrafa significa grabar o escribir por sí mismo y se emplea al escrito de mano de su propio autor. Al ser Según el diccionario de la Real Academia Española: la firma es el nombre y apellido escritos por una persona de su propia mano en un documento, con o sin rubrica, para darle autenticidad o mostrar la aprobación de su contenido.

La tradicional firma manuscrita aporta autenticidad ya que cumple la función de identificar a la persona, que involucra a la persona que participa con el contenido del documento, el uso de las firmas electrónicas nos permite cubrir algunos aspectos funcionales de la firma autógrafa y más si hablamos de la firma electrónica avanzada, que sería la confidencialidad, no repudiación, autenticidad e integridad. Las características mencionadas

que posee una firma autógrafa y gracias a ellas se pueden ahorrar controversias y tener la seguridad jurídica que se necesita.

La **firma Autógrafa,** cumple con la función específica señalada anteriormente, es el medio de Identificación del documento, de Declaración con la asunción del contenido del documento por el autor de la firma teniendo la voluntad de obligarse, también tiene un carácter Probatorio que permite identificar si el autor de la firma es efectivamente aquel el dueño de la propia firma.

la firma autógrafa es utilizada para expresar el consentimiento de las partes sobre un contrato en particular, de hecho, su uso no se encuentra regulado en ninguna legislación, la utilización de la firma autógrafa se ha venido dando a lo largo de los años.

En el título segundo de la ley trata el tema de las firmas electrónicas en el artículo 13 se define como "Son los datos en formas electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos". (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, art. 13). En la Ley Modelo de la CNUDMI, "la firma electrónica aspira abarcar todos los usos tradicionales de una firma manuscrita con consecuencias jurídicas, siendo la identificación del firmante y la intención de firmar solo el mínimo común denominador de los diversos criterios relativos a la firma que se hallan en los diversos ordenamientos jurídicos".

1.1.3. Principios Internacionales de la Firma Electrónica

1.1.3.1. Principio de la Firma Digital

Para Lorenzetti un principio "es un enunciado amplio que permite solucionar un problema y orienta un comportamiento […] se trata de normas prima facie" (Lorenzetti, 2001, pág. 47) esto quiere decir que dichas normas son flexibles y se pueden cambiar o

completar, por no tener una determinación acabada. Son normas de aplicación general, no especifica, que pretende brindar un soporte al momento de solucionar un problema o dictar un comportamiento. Son bases que permiten simplificar la labor del legislador así como el fruto de la misma que son las leyes.

Esto lo respalda Ana Yazmín Torres al decir que:

> "los principios generales del derecho son los enunciados normativos más generales que, sin haber integrado al ordenamiento jurídico en virtud de procedimientos formales, forman parte de él, porque le sirven de fundamento a otros enunciados normativos particulares o recogen de manera abstracta el contenido de un grupo de ellos".

Con esta característica de ser generales, es que funcionan como una herramienta para la homogenización de las legislaciones de distintos países, resultan entonces, no sólo normas generales, sino también como guías para la elaboración de leyes y que están puedan ser reconocidas por otros Estados, esto sirve para que no exista una contradicción mayor entre las mismas.

La firma digital, cuenta con distintos principios creados para la facilidad de la interpretación, la homogenización y la aplicación de normas que traten sobre este tema. En estos principios se encuentra el de equivalencia funcional y el de neutralidad tecnológica. Aquellos principios fueron plasmados en la Ley Modelo de la CNUDMI sobre el Comercio Electrónico y en la Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico.

1.1.3.2. Equivalencia funcional

Este principio de equivalencia funcional es aquel mediante el cual los medios electrónicos adquieren la misma validez que los documentos que cuentan con un soporte de

papel. En el artículo 5 de la Ley Modelo de la Comisión de las Naciones Unidas para el Desarrollo Mercantil Internacional esta hace un referencia al dicho principio, al establecer que "No se negara efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que este en forma de mensaje de datos" (Ley Modelo de la CNUDMI, art. 5). De hecho, dichos mensajes de datos deben cumplir con los requisitos de forma de un documento con soporte en papel como lo son: la fiabilidad, rastreabilidas, inalterabilidad, la posibilidad de una posterior consulta del mismo, la autenticacion del mismo a tráves de la firma, la legalidad, entre otros, como lo mensiona la guía de la Ley modelo de la CNUDMI. (pág. 21 parrafo 16 y 17)

Siguiendo esta línea, el Reglamento General a la Ley de Comercio Electrónico, Firma Electrónicas y Mensajes de Datos, en su artículo tercero establece que" Cumplidos los requisitos de accesibilidad, el mensaje de datos tiene iguales efectos jurídicos que los documentos que constan por escrito" (art. 3) En este mismo artículo se determina dos requisitos para que un documento se conciba como accesible en su posterioridad, estos son:

a) ha sido generada y puede ser almacenada en un lenguaje electrónico/informático y formato entendibles por las partes involucradas en el intercambio de información y sus respectivos sistemas de informáticos de procesamiento de la información, pudiéndose recuperar su contenido y el de los remitidos o anexos correspondientes en cualquier momento empleados los mecanismos previstos y reconocidos para el efecto; y,
b) se puede recuperar o se puede acceder a la información empleando los mecanismos provistos al momento de recibido y almacenado, y que deberán detallarse y proporcionarse independientemente del mensaje de datos a fin de garantizar el posterior acceso al mismo" (Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, 2002, art. 3)

En la Guía para la incorporación al derecho interno de la Ley Modelo CNUDMI sobre el Comercio Electrónico, se menciona que la Ley Modelo reconoce el principal problema para el desarrollo interno de medios modernos de comunicación son “los requisitos legales que prescriben en el empleo de la documentación tradicional con soporte de papel” (pág. 20, párrafo 15). Es por esto que el principio de equivalencia funcional resulta ser uno de los principios más importantes del comercio electrónico, esto facilita la aplicación y el desarrollo del comercio electrónico, al brindar una herramienta que permita adaptar la legislación existente a los instrumentos electrónicos necesarios en el ámbito del comercio electrónico.

Al formar parte de una organización en la cual se establece que los países miembros deberán suscribir todos los tratados existentes como requisito previo, al momento de legislar también se debe de tomar en cuenta, la Ley Modelo de la CNUDMI. Se podría decir que crear un modelo de ley específico sería algo ineficaz. Por todo lo señalado en este último párrafo cabe recalcar que el principio de equivalencia funcional es la base del éxito de la aplicación de la firma digital, puesto con este principio se evita que el Estado tenga que cambiar cada una de sus legislaciones ya sean leyes o reglamentos.

1.1.3.3. Neutralidad tecnología

El principio de neutralidad es aquel mediante el cual se asegura la no discriminación a otras tecnologías, ya sean nuevas o existentes, especialmente en lo que concierne a la legislación de temas como el comercio electrónico. A través de este principio se asegura que el Estado no imponga sus preferencias a favor o en contra de otras tecnologías.

La neutralidad tecnológica es una garantía de independencia, soberanía y construcción democrática de las infraestructuras informáticas, en este principio se logra garantizar que los medios electrónicos gocen de la independencia necesaria para su evolución.

El principio fundamental como lo es el de neutralidad tecnología, es sumamente importantes. Con el uso adecuado, se pueden solventar situaciones que se presenten en un futuro, para las cuales no exista el cuerpo normativo adecuado, y de esta manera prevenir cualquier tipo de daños que esto pueda llegar a ocasionar, y se supone que además de ser una garantía, es una forma eficaz para la mitigación de daños que se puedan generar a futuro.

El principio de neutralidad tecnológica no solo protege al usuario, sino también al sector privado dedicado al desarrollo de las tecnologías. Al estar esta parte del mercado en constante evolución resulta altamente rentable y esto le favorece al sector privado.

En la Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, al hablar sobre crear un equivalente funcional para los distintos tipos de firmas, se aclara que "cualquier esfuerzo por elaborar reglas sobre las normas y procedimientos que deberían utilizarse como sustitutos en casos especiales de firmas, podría crear el riesgo de vincular irremisiblemente el régimen de la Ley Modelo a una determinada etapa del desarrollo técnico". (Art, 7 párrafo 55). En resumen, este principio resulta fundamente puesto que, aparte de evitar favoritismos que acarrean privilegios económicos, y si en algún momento se llegare a vincular la legislación a un tipo de tecnología determinado, la innovación también se vería perjudicada y por ende el sector privado, que resulta ser la matriz productiva de un país, al limitar la productividad del sector privado limitando la capacidad de innovación para la misma, se correría el riesgo de generar monopolios dentro del sistema y eso afectaría no solo al gran empresario, sino también al mediano.

1.1.3.4. Principios de comercio electrónico aplicable a la firma digital

Existen principios del comercio electrónicos que son aplicables a la firma digital; Lorenzetti expone algunos de ellos:

1. El de libertad de comercio, "implica la autorregulación de las partes y con ello una mínima intervención estatal que se limita a lo necesario para el funcionamiento institucional del mercado". (Lorenzetti, pág. 49) Bajo este principio se crea el concepto de que el contrato es ley para las partes. Esto quiere decir lo que se acuerde en un contrato, esta tendrá fuerza de ley y sus disposiciones serán las que valga, antes a lo que está estipulado en la ley, siempre y cuando no se incurra en un ilícito con las mismas.
2. La protección a la privacidad, que resulta importante en la re por la cantidad masiva de almacenamiento de información y el fácil acceso a la misma que esta ofrece. Al ser la privacidad un tema muy delicado y el tratamiento de la información, que constituye parte fundamental de la privacidad, aún más. Por esto que el acceso a la información debe ser limitado o por lo menos debe de existir un control que permita garantizar la protección a la privacidad de la persona y la información que la misma desee mantener confidencial. (Lorenzetti, 2001, págs. 50-51)
3. En el carácter internacional, este principio se basa en la notable tendencia a la homogenización de las legislaciones (Lorenzetti, 2001, pág. 52), en la Ley Modelo de la CNUDMI. Los principios en general resultan aplicables y deben ser considerados por las legislaciones internas de cada país al momento de redactar y anunciar sus leyes.

   En el comercio electrónico, la confianza es un tema delicado y es importante, puesto que por las posibilidades que brinda el mismo, las partes pueden no conocerse y no haber formado una relación de confianza como sucede en el mundo físico del comercio. Para que en el ámbito del comercio y una de las

formas de hacerlo es que el principio de buena fe sea imperativamente exigido para luego ser reconocido y aplicado en su totalidad.

1.2. Marco conceptual

1.2.1. Concepto de firma electrónica

La Firma Electrónica es una herramienta para hacer efectivo el comercio electrónico, y en sentido amplio es toda transacción realizada a través de redes electrónicas de información conocidas como el Internet, en la doctrina positivista, encontramos la siguiente definición: "Trazado gráfico, conteniendo habitualmente el nombre, apellido y rubrica de una persona, con él se suscriben los documentos para darles autoría y obligarse con lo que en ellos se dice".

El Doctor Juan Pérez Rivadeneira, lo define: "Cualquier método o símbolo basado en medios electrónicos utilizados o adoptados por una parte con la intensión actual de vincularse o autenticar un documento, cumpliendo todas o alguna de las funciones de las firmas electrónicas". La firma electrónica igual tendrá valides y se lo reconocerá con los mismos efectos jurídicos que a una firma manuscrita en documentos escritos.

Existen muchas definiciones de firmas electrónicas, pero se considera que la más completa es la establecida en el artículo 2, por la UNCITRAL:

Por "firma electrónica" se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos.

Conceptualizando un poco más dentro de la firma electrónica encontramos lo siguiente: Es la transformación de un mensaje utilizando un sistema de cifrado asimétrico de

manera que la persona que posee el mensaje original y la clave pública del firmante, pueda establecer de forma segura, que dicha transformación se efectuó utilizando la clave privada correspondiente a la clave pública del firmante, y si el mensaje es original o fue alterado desde su concepción.

Para poder entender este concepto hay que aclarar que la clave pública de la forma electrónica de una determinada persona puede ser conocida por cualquier otra persona, de ahí su denominación "publica", por el contrario, la clave privada debe ser suspicazmente guardada por el titular de la firma electrónica, para que no pueda ser mal usada por terceros, sin embargo, ambas claves tienen una correlación algorítmica entre sí, esto se da con las firmas electrónicas que utilizan claves asimétricas.

1.2.2. La criptografía

Criptografía es la ciencia de la seguridad de la información que muchos la llaman como "Arte de escribir con clave secreta o de un modo enigmático", en ella se puede almacenar o transmitir información que solo permite ser revelada por aquellos que solo deben verla. La palabra viene del griego kryptos que esto significa "oculto" y graphia, que significa "escritura".

La criptografía originada del año 2000 A.C., el primer método de criptografía era conocido como Escítala, el segundo criptosistema que se conoce fue documentado por el historiador griego Polibio: un sistema basado en la posición de las letras en una tabla. También los romanos usaron el sistema de criptografía moderna siendo el método actualmente conocido como Cesar, porque supuestamente Julio Cesar lo empleo donde el no confiaba en sus mensajeros cuando se comunicaba con los gobernadores y oficiales. El método criptográfico utilizado por los griegos fue la escítala, un método de trasposición basado en un cilindro que servía como clave que se enrolaba el mensaje para poder cifrarlo.

En Europa en la edad media, el primer libro europeo escrito en el siglo XIII por el monje franciscano Roger Bacon, describe el uso de la criptografía, titulado La Epístola sobre las obras de arte secretas y la nulidad de la magia, que describe siete métodos distintos para mantener los mensajes en secretos. En el año 1379 Gabriele de Lavinde escribió el primer manual sobre la criptografía.

A principios del siglo XIX Thomas Jefferson invento una máquina que constituía por 10 cilindros montados en un mismo eje de forma independiente, donde se colocaba el alfabeto y al girar los cilindros quedaba cifrado el mensaje, en ese mismo siglo Kerckhoffs estableció los principios de la criptografía moderna, los algoritmos modernos que usan una clave para controlar el cifrado y descifrar el mensaje, Kerckhoffs establece que la seguridad del cifrado debe residir en el secreto de la clave y no en el mecanismo del cifrado.

El americano Samuel F. B. Morse en 1832, desarrollo el Código Morse, aunque no es propiamente un código como los otros, esto es otra forma de cifrar las letras del alfabeto dentro de sonidos largos y cortos, Morse en el año 1844 trasmitió el primer mensaje telegráfico entre dos ciudades llamada Baltimore y Boston, demostrando al mundo que se pueden mandar mensajes a largas distancias, cuyo uso se prolongó hasta la segunda Guerra Mundial.

La criptografía moderna lleva dos hechos significativos que marcan un punto de inflexión en el mundo de la criptografía, el primero, los estudios por Claude Shannon (1948), la criptología deja de ser considerada como un arte, para ser tratada como una rama más de las matemáticas, el segundo hecho, es una publicación que realizo Whitfiel Diffie y Martin Hellman (1976), proponen un nuevo método de cifrado, creando criptosistemas de clave públicas.

En tiempos modernos, la criptología ha llegado ser tan importante para el sistema computarizado, de tener la habilidad de poder almacenar de manera segura, el internet ha permitido que todas estas herramientas sean mercadeadas, como la tecnología y técnicas de criptografía, la mayoría de los sistemas criptográficos avanzados se encuentran ya en el dominio público de cada país.

Volviendo al tema principal, la firma digital viene a constituirse en una especie de Firma Electrónica, que se expresa: “la criptografía también puede emplearse para crear firmas digitales, para autenticar mensajes electrónicos y para verificar su integridad (esto es: los mensajes se recibieron en la misma forma en que se enviaron y provienen de la fuente indicada) lo que en el contexto de los negocios electrónicos resulta de vital importancia". (Hance, 1997, pág. 180) Existen dos tipos de criptografía, la simétrica de una sola clave, y la asimetría o de clave pública, que se maneja con dos claves diferentes pero matemáticamente relacionadas entre sí, lo anterior en base a grandes números producidos utilizando una serie de fórmulas matemáticas aplicadas a números primos, sin embargo, la criptología de clave pública no precisamente podría utilizar algoritmos, de hecho en la actualidad se están utilizando o desarrollando otras técnicas matemáticas, para brindar un alto grado de seguridad mediante el empleo de longitudes de clave notablemente reducidas, estas técnicas ofrecen más seguridad a las claves y por ende a la forma digital.

La criptología simétrica como lo manifiesta Miguel Dávara es aquella en la que: “se utiliza la misma clave para cifrar que para descifrar los datos, con lo que ambas partes, emisor y receptor, deben conocer la clave (uno para cifrar y otro para descifrar), teniendo que basar sus relaciones en cuestiones de total y absoluta confianza, ya que, para que exista seguridad, la clave debe permanecer secreta y uno debe confiar que en el otro no la da a conocer a nadie y viceversa.” Como se explica, las dos partes u operadores comparten una clave secreta por medio de la cual es posible cifrar y descifrar el mensaje.

La criptografía asimétrica, se basa en que cada uno de los operadores tiene dos claves; una privada que sólo él la conoce, y una publica que conocen o pueden conocer todos los que intervienen en el trafico electrónico, clave que incluso puede constar en un directorio público, para poder comprender mejor lo anotado, citemos a Rafael Mateu De Ros que revela: "Cuando el operador A quiere un mensaje electrónico aplica al mismo su clave privada y el mensaje así cifrado se envía a B, que al recibir el mensaje le aplica la clave pública de A para obtener el mensaje descifrado.". Este último sistema tiene una gran ventaja de generar confidencialidad en él envió de mensajes a través de canales inseguros como son las redes abiertas Internet, así como también, permite crear las firmas digitales, dotando a los mensajes de datos de autenticidad integridad y no rechazo de origen, que son las condiciones básicas de las firmas digitales.

Como establece la Firma Electrónica en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Registro Oficial No. 557, de 17 de abril del 2002), hay que tener presente la criptografía asimétrica, ya que cumple un papel muy importante en nuestra normativa, a futuro podrían presentarse nuevas especies de Firmas Electrónicas donde el articulo 10 el Reglamento a la Ley contempla neutralidad tecnología.

1.2.3. Claves públicas y claves privadas

La criptografía asimétrica en la que se basa la PKI (Public Key Infraestructure) o Infraestructura de Clave Pública, emplea un par de claves, esto podrían ser dos pares de claves, solo se puede descifrar con la otra y viceversa, una de esas claves se la denomina pública y se la incluye en el certificado electrónico, la otra se la denomina probada y únicamente conocida por el titular del certificado.

En correlación a las claves, las describe como: "las claves complementarias utilizadas para las firmas digitales se denominan como claves privadas, que se utiliza para firmar

digitalmente, mediante un dispositivo de creación de firma digital en un criptosistema asimétrico seguro, y la clave pública, que de ordinario conocen más personas y se utiliza para que el tercero que actúa confiando en el certificado pueda verificar la firma digital". (Devoto, 2001, pág. 169)

1.2.4. Diferencias entre la firma electrónica y la firma digital

1.2.4.1. Firma Electrónica

Se entiende por Firma Electrónica, como un mecanismo electrónico mediante el cual se añaden ciertos códigos a un archivo electrónico para asegurarlo, estas transacciones electrónicas deben de garantizar a los usuarios seguridad y confianza, ya que estas caracterizas son propias de las firmas manuscritas. Mauricio Devoto (2001) define: "El termino Firma Electrónica sería un término genérico y tecnológicamente neutro, y haría referencia al universo de métodos por los que se podrían firmar un documento electrónico. Estas firmas podrían tomar diversas formas y ser creadas por medio de diferentes tecnologías, por ejemplo, el nombre de una persona colocada al final de un correo electrónico, la imagen digitalizada de una firma manuscrita agregada a un documento electrónico, un código secreto o PIN, un identificador basado en un mecanismo biométrico, y finalmente una firma digital creada por medio del uso de criptografía de clave pública."

La firma electrónica como se encuentra definida en la mayor parte de las normativas del mundo es un término genérico, también se la contempla dentro de esta a la firma digital, esto quiere decir cuando de la define a la Firma Electrónica esta hace en un sentido de neutralidad tecnológica, en esta permite anticiparse al avance de la tecnología, donde se podría presentar otro tipo de firma que no sean la firma digital o de clave pública.

1.2.4.2. Firma Digital

Juan Carlos Riofrío comenta sobre la firma digital: "Si la definición de firma de por si envuelve muchas complicaciones, la de firma digital todavía más", la firma digital se basa en el uso de la criptografía asimétrica que es una especie de Firma Electrónica caracterizada por complementar elementos de seguridad que la Firma Electrónica no posee.

José Manuel Villar expresa: "Ello es así porque la firma digital cumple, en relación con los documentos electrónicos, las principales funciones que se atribuyen a la firma manuscrita sobre un documento en papel; a saber, permite identificar al autor del escrito, autenticación y constatar que el mensaje no ha sido alterado después de su firma integral".

Una característica importante de la firma digital es que da lugar al no rechazo o no repudio, es decir, que las partes que intervienen no pueden negar su actuación y, es garantía de confidencialidad; esto está contemplado en las normativas sobre el tema y que protegen los datos al acceso de terceros no autorizados, esto se refiere al certificado de Firma Electrónica y entidades de certificación que se encuentran regulados en la Ley de Comercio Electrónico.

Analizando la Firma Electrónica y la Firma Digita, son distintas, son dos tipos de firmas que Ricardo Lorenzetti comenta: *"La gran diferencia estriba en que cuando se utilice la firma digital, se aplican presunciones juris tatum sobre la identidad del firmante y la identidad del documento que suscriba."*. Para finalizar podemos decir que los autores consideran que la firma digital basada en la criptografía asimétrica, por el constituye el sistema más seguro y un paso fundamental para el comercio electrónico.

1.2.5. Integridad, No Repudio y Firma Digital

Un documento cuenta con integridad cuando no ha sido alterado y esto permite que el mismo no ha sido manipulado de ninguna manera, esta correcta implementación de este

requerimiento, una vez que se compruebe que el mensaje o el documento no ha sido alterado de ninguna manera se puede proceder a la autenticación del mismo. Podemos exponer que primero se hiciera la autenticación y resulte que el mensaje o documento se ha manipulado, entonces la identificación del emisor resulta irrelevante, por esto la confidencialidad es primordial, ya que es el primer paso para poder asegurar la integridad del mensaje o documento.

La diferencia entre la autenticación y el no repudio de un mensaje de datos, Costas explica que el no repudio "es un servicio de seguridad estrechamente relacionado con la autenticación y permite probar la participación de las partes en una comunicación. La diferencia con la autenticación es que la primera se produce entre las partes que establecen la comunicación y el servicio de no repudio se produce frente a un tercero" (Costas, pág. 28).

La autenticación se produce entre las partes que participan en el envío y recepción del mensaje o el documento, mientras que, el no repudio se aplica en el caso en el que exista un conflicto con respecto a la identificación del emisor y su vinculación con el contenido ante un tercero que resolverá dicho conflicto. Costas sustenta que la autenticación recae sobre el autor del documento y su destinatario, mientras que el no repudio prueba él envió y la recepción del mismo (Costas, pág. 29).

El no repudio es un tipo de garantía sobre la identidad del emisor y su vinculación con el contenido, donde no puede negar su participación. En este principio se presume que el emisor es quien dice ser y el que envió del mensaje o documento fue voluntario. Esto se produce cuando el receptor recibe una prueba donde el emisor es el legítimo del mensaje, si en caso de que se inicie un juicio al respecto, la prueba recaería sobre el emisor y no del receptor debido al no repudio.

Podemos hablar sobre dos posibilidades de no repudio, la primera, que recae sobre el emisor y se denomina no repudio en origen y la segunda que recae sobre el receptor, no repudio en destino. Esta última explica que el receptor no puede negar la recepción del mensaje o documento, ya que el emisor tiene pruebas de la recepción del mismo. En el servicio de no repudio en destino, suprime la posibilidad de que le receptor niegue la recepción del mensaje o documento y así su vinculación al mismo. (Costas, 2010, pág. 29)

Devoto afirma que la verificación de la firma digital no solo ayuda con la identificación del mensaje, sino con la comprobación de la integridad del mismo, este procedimiento de verificación consiste en que el emisor prepara un digesto del mensaje, ya que es un resumen del mismo, mediante la utilización de un algoritmo de control seguro, ese resumen es enviado también al receptor, en el cual al recibir el mensaje completo debe realizar otro digesto del mismo mensaje. El acto seguido se compara los dos resúmenes y si coinciden a la perfección, entonces se asegura que el mensaje no ha sido alterado y así se cumple con el requerimiento de integridad.

1.2.6. Firma Digital

La firma es un mecanismo de protección de los mensajes de datos, la firma digital es esencial en cualquier ámbito en que se empleen documentos electrónicos, donde esto provee de autenticidad, veracidad, confidencialidad y no repudio al mensaje de datos.

Al ser una red tan amplia e impersonal es necesario contar con un mecanismo de identificación seguro y es por estas razones que la firma digital adquiere la importancia que posee.

La firma digital produce los mismos efectos que la manuscrita, como lo explica Jesús Ignacio Fernández que la firma “es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje”. Es necesario que la firma

cumpla con ciertos requisitos para que sea considerada como el equivalente a una firma manuscrita, como sería el poder vincular el mensaje de datos al firmante, esto se lo designa como identidad; la integridad, que exista la certeza de que el mensaje no fue alterado; para no repudiar, se explica que el firmante no puede negar su firma ni el vínculo existente con el mensaje de datos y la confidencialidad, explicada como la seguridad de que el mensaje no pueda ser leído por terceros no autorizados.

La Ley Modelo de la Comisión de Naciones Unidas para el Derecho Mercantil Internacional, en el artículo 7, en numera las características que debe reunir la firma, y las establece como tales, la identificación de la persona y el vínculo aprobatorio que esta tiene con el mensaje de datos y la fiabilidad del método empleado para la creación de la firma. (Ley Modelo de la CNUDMI, art. 7)

La firma digital esta basada en los sistemas de criptografía de clave pública. Esta firma la que se utiliza generalmente y que se almacena en soportes de hardware y sofware, mientras que la firma electrónica es almacenada en soporte de hardware (Costas, 2010, pág. 253). La firma electrónica es un conjunto de datos ordenados lógicamente que sirve para vincular a una persona al contenido del mensaje de datos y asegurar la identidad del mismo, siempre y cuando cumpla con los requisitos ya mencionados, utilizando el sistema de criptografía asimétrica. Es por esto que se logra llegar a una equivalencia funcional óptima con la firma manuscrita, debido a que se cumplen con los requisitos preestablecidos para otorgar seguridad jurídica a las mismas.

1.2.7. Proceso de firma digital

La criptografía asimétrica asegura la confidencialidad y la integridad, pero no la autenticación y el no repudio, la firma digital se utiliza para estos fines, como lo explica costas, que el emisor decide escribir un mensaje al receptor, pero para que este compruebe la

identidad del emisor, este debe firmarlo. Para esto el emisor resume el mensaje, lo que se denomina una función hash. Para Devoto:

> "esta función consiste en un proceso matemático, basado en un algoritmo que crea una representación digital o forma comprimida del mensaje, a menudo conocida con el nombre de "digesto de mensaje" o "huella digital" del mensaje, en forma de un 2valor control" o "resultado control" de una longitud estándar que suele ser mucho menor que la del mensaje, pero que es no obstante esencialmente única al mismo." (Devoto, 2001, págs. 169-170)

Dicho en otras palabras, es una función que permite resumir un texto, mediante algoritmos en una presentación alfanumérica y así se puede comprobar que el texto recibido es el mismo que fue enviado. Después se la utilización de la función hash, se produce a cifrar el resultado con su clave privada, para que esta manera, obtener su firma digital. Se procede a enviar el mensaje firmado al receptor, quien descifra el resumen utilizado la clave pública del emisor; aplica la función hash al mismo mensaje y si los resúmenes coinciden, entonces el receptor puede estar seguro de que en efecto fue el emisor quien envío el mensaje. El mensaje que se envía se cifra con la clave pública del emisor para que el mismo lo descifre con su clave privada, de esta manera se asegura la confidencialidad, la integridad, la autenticación y el no repudio.

1.3. Marco legal

1.3.1. Duración de la Firma Electrónica

En la Ley de Comercio Electrónico en el artículo 18, establece: "Las firmas electrónicas tendrán duración indefinida. Podrán ser revocadas, anuladas o suspendidas de conformidad con lo que el reglamento a esta ley señale." En el Ecuador la firma electrónica tiene un periodo de valides indefinida o indeterminado, esto quiere decir que durara hasta la

muerte del titular, ya que la firma electrónica de la manera como está creada en la normativa ecuatoriana tiene los mismo efectos jurídicos que la firma manuscrita.

En el artículo anteriormente mencionado habla de la revocación, anulación o suspensión de las firmas electrónicas, donde el ecuatoriano Efraín Torres Chávez da su punto de vista: "Revocar, es dejar sin efecto una declaración de voluntad o un acto jurídico en que unilateralmente se tenga tal potestad. La anulación es levantar la validez y quitarle todo valor a un acto o contrato. Suspensión, es detención de un acto, interrupción de un oficio o beneficio, es una sanción administrativa donde se le priva a alguien de las operaciones." En el reglamento a esta ley, no dice nada referente a la revocación anulación y suspensión de la firma electrónica. En lo ya mencionado no se debe de confundir con la extinción, suspensión y revocación del Certificado de Firmas Electrónicas, artículo 24, 25, y 26 de la Ley de Comercio Electrónico, adicional con el artículo 13 del Reglamento General a la Ley de Comercio Electrónico.

1.3.2. Extinción de la Firma Electrónica

El artículo 19, de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, señala las causas porque la firma electrónica se extingue, esto significa la terminación de la responsabilidad del titular de éste con la firma electrónica, en el inciso final del artículo, debemos aclarar que la extinción de la firma electrónica no exime a su titular de las obligaciones que contrajo antes de la extinción y que haya sido derivadas de su uso, detallaremos las causas de la extinción:

a) voluntad de su titular; en esta causa el titular debe comunicar y presentar tal decisión a la entidad del certificado, el motivo de dejar sin efecto el certificado de Firma Electrónica.

b) Fallecimiento o incapacidad de su titular; en este caso para la extinción sea afectiva se debe de presentar la partida de defunción; y en caso de discapacidad del titular de la firma, esta tiene concordancia con el Código Civil, donde se habría que determinar el hecho de la incapacidad, si es absoluta o relativa.

c) Disolución o liquidación de la persona jurídica, titular de la firma; en este literal es donde se reconoce a la persona jurídica como titular de la firma electrónica, en materia societaria, para una disolución o liquidación de una compañía, ésta debe ser considerada por la Junta de Accionistas, y aprobada por resolución de la Superintendencia de Compañías, luego debe de ser inscrita en el Registro Mercantil, es aquí donde surte efectos, este procedimiento toma tiempo por lo cual mientras tanto la firma electrónica estaría vigente. Debe de reformarse la Ley en este sentido, haciendo referencia a la Ley de Compañías.

d) Por causa judicialmente declarada; como lo explica Efraín Torres Chávez: "no es otra que la expresada en la Ley y a petición de parte, en materia de infracciones informáticas o administrativas, el juez podrá, según sus facultades legales, de oficio, dar por extinguida una firma electrónica. En estas circunstancia, el bien jurídico protegido es la propiedad del titular."

1.3.3. Obligaciones del Titular de la Firma Electrónica

La firma electrónica tiene una equivalencia a la firma manuscrita, genera obligaciones para su titular, el artículo 17 de la Ley 67 señala como obligaciones del titular de una firma electrónica las siguientes:

1) Cumplir con las obligaciones derivadas del uso de la firma electrónica;

2) Actuar con la debida diligencia y tomar las medidas de seguridad necesarias, para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada;
3) Notificar por cualquier medio a las personas vinculadas, cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y utilización indebidamente;
4) Verificar la exactitud de sus declaraciones;
5) Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el destinatario conociere de la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia;
6) Notificar al a entidad de certificación de información los riesgos sobre su firma y solicitar oportunamente la cancelación de los certificados; y,
7) Las demás señaladas en la Ley y sus reglamentos.

1.3.4. Certificado de Firma Electrónica

1.3.4.1. Concepto y clases de certificados

Como parte del sistema de la Firma Electrónica tenemos al certificado de ésta, que Ángel García la define como: "La certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad", y Xavier Ribas en complemento a lo aludido define al certificado que es: "Documento digital que identifica a la autoridad certificadora que lo ha emitido, identifica al firmante del mensaje o transacción, contiene la clave pública del firmante, y contiene a su vez la firma digital de la autoridad certificadora que lo ha emitido." (Ribas, 1997)

Los certificados son emitidos por una entidad certificadora, como parte de su trabajo identifica a las partes, Aranzazu Calvo-Sotelo y Manuel Lobo también lo define: "El empleo

de la Firma Electrónica basada en un sistema de clave pública o asimétrica tiene su punto débil en la identificación de las partes. Este punto débil ha sido solventado mediante la expedición, por terceros de confianza, (presentadores de servicios de certificación), de certificados que garantizan la distribución segura de claves públicas o datos de verificación de firma y que vincula, de forma indisoluble, el par de claves (públicas y privadas) a una persona determinada". En el artículo 20 de la Ley de Comercio Electrónico, firmas Electrónicas y Mensajes de Datos define al certificado de Firma Electrónica como: "es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad". De todo lo anterior un certificado es un mensaje de datos que confirma la vinculación firma/persona, pero esta no se determina al tipo de persona, ya que en nuestras leyes pueden ser naturales o jurídicas, en la emisión de un certificado se lo realiza a través de un proceso de comprobación, del que la normativa ecuatoriana carece y que habrá que reglamentarlo. En los artículos 20 y 21 Ley de Comercio Electrónico son concordantes, ya que el ultimo se refiere al uso del certificado, donde se emplea para acreditar la identidad del titular de una firma electrónica.

En el articulo 20, de la ley, guarda concordancia con la definición de la disposicion general, novena de la Ley que expresa: "Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que pueden ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes: documentos electrónicos, registros electrónicos, correos electrónicos, servicios web, telegrama, télex, fax e intercambio electrónico de datos.", una vez más confirma la existencia en la en la normativa nacional de la concepción de neutralidad tecnológica, que se ha señalado en la definición firma

electrónica, dejando a futuro la posibilidad de que puedan existir otros tipos de firmas electrónicas.

la normativa ecuatoriana referente a la definición de certificado de Firma Electrónica, se concluye que se encuentra acorde a la normativa internacional, esta vincula una clave pública con la persona determinada, pero hace falta reglamentar el procedimiento de comprobación que confirma la identidad del titular del certificado, así la normativa internacional ha establecido un procedimiento para la generación y emosión de los certificados. En el siguiente título se propone un modelo de procedimiento de comprobación.

1.3.4.2. Generación y emisión del certificado

Señalábamos que todo tramita de expedición de certificados necesita un procedimiento del que carece la legislación del Ecuador sobre la firma electrónica, a continuación ilustraremos un mecanismo que ayudaría a la aplicación para la expedición de certificados en la legislación, explicando antes, que en la normativa internacional cada entidad de certificación tiene sus propias políticas al respecto. El procedimiento tendría las siguientes fases:

a) Solicitud y registro del solicitante.- Para este trámite necesariamente debe iniciar con la solicitud de emisión de certificado, punto de partida y del que acata todo lo subsiguiente, Mauricio Devoto en reseña a este paso comenta: *"La solicitud de un certificado de clave pública para firmar digitalmente constituye el punto de partida en la regulación usuario-certificador de clave pública. Recordemos que el certificado de clave pública es el documento digital firmado digitalmente por un certificador de clave pública, que asocia una clave pública con su suscriptor durante el período de vigencia del certificado"* (Devoto, pág. 210). La solicitud o aplicación contiene inmerso el consentimiento del suscriptor, hecho con el que

debe darse es con la firma manuscrita del mismo. El registro se confirmaría, y registraría al solicitante cuando entre cierta información adicional, que la misma registra y que incluso puede ser incluida en el certificado dependiendo de la finalidad de este.

b) Comprobación de la solicitud.- Esta fase es trascendental, ya que de esta depende el buen funcionamiento del sistema de certificados, como también las responsabilidades que se general para la autoridad de certificación, en otras palabras, la solicitud y el registro son datos mínimos que deben ser confirmados. Estos hechos deben de ser comprobados obligatoriamente, como lo es la autenticación del sujeto, en donde se confirma la identidad del solicitante y que corresponda a la clave pública contenida en el certificado; esta identidad se comprueba con el uso de técnicas de confirmación que pueden cambiar en función de una política determinada de certificados o de una clase de certificados, como son: la presencia del solicitante, documentos acreditativos, confirmación de datos personales por una tercera parte; esta verificación tiene una importancia ya que ha sido exigida en las diferentes regulación sobre la materia, también sería la razón de que esta sea considerado en la normativa ecuatoriana, otro elemento sujeto a verificación obligatoria tiene relación con la posesión legitima de una clave privada apta y válida con la correspondiente clave pública, que esta comprueba que el solicitante tenga la clave privada correspondiente a la clave pública del sujeto del certificado.

c) Firma y emisión del certificado.- Confirmado que la información entregada por el solicitante es real, la entidad certificadora firma digitalmente el certificado utilizando la clave privada de la que es titular; haciendo un razonamiento lógico cuando se emita un certificado por una autoridad de certificación, ésta genera el

certificado y la firma digital del mismo, se garantiza de esta maneta la autenticidad del documento y la integridad de su contenido “certificado de firma electrónica”, de hecho, el certificado debe contener otros requisitos que se requerirían de acuerdo a la normativa del país.

d) El envío de una copia del certificado y aceptación del mismo por parte del solicitante.- Esto corresponde a una fase que se presenta como consecuencia de los anteriores literales, en la cual la entidad de certificación envía una copia del certificado al suscriptor, se lo debe revisar y si esa de acuerdo a sus intereses aceptarlo. Esto es una fase que depende del certificador.

e) Publicación y archivo del certificado.- La publicación puede ser relacionada como un servicio que presta la entidad de certificación en un directorio de certificados, también, la publicación implicaría indirectamente que el suscriptor ha aceptado el certificado y su contenido; una copia del certificado debe ser archivada, por ejemplo a futuro en caso de pérdida. En concluyente, la publicación es importante porque de esta manera los usuarios pueden verificar la Firma Electrónica.

   Para finalizar, en el hecho de que cada entidad de certificación fija sus políticas referentes a la generación y emisión de los certificados, es importante que en la normativa del Ecuador se contemple un procedimiento para tal efecto, ya que se está garantizando las actuaciones del titular del certificado de Firma Electrónica y de la entidad de certificación que debe estar supervisado por la Superintendencia de Telecomunicaciones en calidad de ente de control.

1.3.4.3. Certificados de la Firma Electrónica y entidades de certificación de información

En el desarrollo de este trabajo, es elemental tener presente a la criptografía especialmente la asimétrica, por la utilización de las claves públicas y las claves privadas

para la firma digital; ya que en ciertas normativas como en la comunidad Europea se identifica a lo que es la firma electrónica avanzada.

La criptografía asimétrica o de clave pública como se la denomina, y las firmas digitales proveen seguridad al comercio electrónico, para que esto funcione es necesaria la utilización de los denominados certificados de Firma Electrónica, que asocian la clave pública a una persona determinada, y que deben de ser emitidos por las entidades de certificación de información.

En el desarrollo de este capítulo se tratarán estos temas, revisando la normativa del Ecuador, su reglamentación, así también refiriéndonos a la normativa internacional.

1.3.4.4. Requisitos del certificado de la Firma Electrónica

En concordancia con lo presentado en el literal b) del título anterior, la Ley de Comercio Electrónico del Ecuador en el artículo 22, determina cuáles son los requisitos mínimos obligatorios del certificado de Firma Electrónica para ser considerado válido y son:

a) Identificación de la entidad de certificación de información; vendría a ser el nombre o razón social de la entidad, incluso correo electrónico y de ser el caso página web.
b) Domicilio legal de la entidad de certificación de información; está contemplando dentro del literal anterior.
c) Los datos del titular del certificado que permitan su ubicación e identificación; en la normativa española se dice signatario; datos en donde pueden ser nombres y apellidos, si se actúa en representación, deberá acreditar poder; podemos señalar que estos datos sólo se utilizarán para los fines pertinente al certificado, esto siendo un requisito importante, no debe ser muy detallado, como lo ha sido recomendando por la UNCITRAL.

d) El método de verificación de la firma del titular del certificado;

e) Las fechas de emisión y expiración del certificado; en este literal solo se habla de fechas, no de horas, a mi criterio debería insertarse la hora, puesto que en el sistema de los computadores y de las redes de información siempre está presente esta información, en el comercio electrónico el horario de trabajo no existe, en la legislación española se habla de certificados reconocidos, en el artículo 12, en el literal a) del Real Decreto Ley sobre la Firma Electrónica, obliga a los prestadores de servicios de certificación que expidan este tipo de certificados el en indicar la fecha y hora en las que se expidió o se dejó sin efecto un certificado.

f) El numero único de serie que identifica el certificado; número que puede ser el referente dentro del listado de certificados revocados y que no se repiten dentro de una misma entidad de certificación.

g) La firma electrónica de la entidad de certificación de información; como en el caso de la normativa española en lo que respecta a certificados reconocidos se exige la Firma Electrónica avanzada, que es la firma digital.

h) Las limitaciones o restricciones para los usos del certificado; los objetivos para los cuales se emitió el certificado imponen ciertas limitaciones de responsabilidades a la entidad de certificación y el valor de las transacciones para las que el certificado es apto; este último guarda concordancia con el artículo 31, de la Ley de Comercio Electrónico, esta parte obliga a que tenga un límite de uso el certificado, y el importe de las transacciones que deben constar como cláusulas en los contratos con los usuarios.

i) Los demás señalados en esta ley y los reglamentos; revisada la documentación, nada dice al respecto la normativa del país respecto de este punto, por lo que se necesita emisión de nuevos reglamentos que normen estos vacíos legales.

> Del análisis hecho en relación con la normativa española se desprende que nuestro certificado ante tal normativa no sería un certificado reconocido, no cumplía todos los requisitos para serlo, nuestra Ley de Comercio Electrónico define los requisitos como certificados de Firma Electrónica, pero no como certificado reconocido como lo contempla la otra normativa, situación que debe ser aclarada en el sentido de definir cuáles son los certificados reconocidos y cuáles pueden ser considerados simplemente como certificado.

1.3.4.5. Duración del certificado de Firma Electrónica

Todos los certificados de Firma Electrónica tienen un periodo de validez, la razón de esto es porque en un sistema bien tratado de emisión de certificados el juego de claves (públicas y privadas) está también debería tener una vida limitada.

En la Ley de Comercio Electrónico del Ecuador, la duración del certificado de Firma Electrónica se encuentra en el artículo 23, éste artículo contempla dos situaciones: la primera, nos da a entender un acuerdo contractual para el período de validez entre el titular de la Firma Electrónica y la entidad de certificación, es decir, en este caso quedaría al libre albedrío, de las partes, esto no sería tan seguro para el sistema y ni para los usuarios, ya que no sería un régimen uniforme; la segunda, se presenta de una forma determínate, y es cuando no se llega a un acuerdo, el plazo de validez de los certificados de Firma Electrónica será establecido por el Reglamento.

Si revisamos al Reglamento a la Ley, específicamente al artículo 11, éste hace mención a que de no existir acuerdo entre las partes el certificado de Firma Electrónica se emitiría con una validez de dos años a partir de su expedición, pero hace un excepción al tratarse de certificados emitidos con relación al ejercicios de cargos públicos o privados,

donde esto podría tener una duración superior a dos años, sin que exceda el tiempo de duración del cargo o prorroga de acuerdo a la Ley.

1.3.4.6. Extinción del certificado de Firma Electrónica

En el artículo 24, de la Ley de Comercio Electrónico se refiere a la extinción de la Firma Electrónica, para analizar se lo dividirá en dos partes: la primera, estarían contenidas las causas por las cuales se extinguen el certificado de la Firma Electrónica; y la segunda, que corresponde al segundo inciso del artículo, que norma el hecho o momento de la extinción:

Las causas para la extinción del certificado son:

a) Solicitud de su titular; compartimos el criterio de Efraín Torres Cháves que al respecto argumenta: "requisito que debe constar en un Reglamento, pues es norma de la aplicación."
b) Extinción de la Firma Electrónica de conformidad con lo establecido en el artículo 19, de esta ley; voluntad de su titular, fallecimiento o incapacidad de su titular, disolución o liquidación de la persona jurídica y por causa judicialmente declarada.
c) La expiración del plazo de validez del certificado de Firma Electrónica; es una causal demasiado entendible, como lo argumenta Apol Lonia Martínez cuando dice: "En cualquier caso, finalizado el período de vida del certificado, cabe entender que cesan también las obligaciones y responsabilidades de la autoridad y del suscriptor", el vínculo entre la clave pública y el sujeto del certificado no sería ya valido, y por lo tanto, no debe confiarse en el certificado.

   El segundo inciso del artículo 24, de la Ley, esta regula el momento en que se extingue el certificado, haciéndose efectivo este hecho desde la comunicación a la entidad de certificación de información, excepto en el caso de fallecimiento del titular de la Firma Electrónica en este caso se extingue a partir de que sucede el

fallecimiento, se habría que determinar qué tipo de comunicación, que podría ser un mensaje de datos o de acuerdo a derecho conforme al proceso de emisión.

1.3.4.7. Suspensión del certificado de Firma Electrónica

Al emitirse el certificado el suscriptor estima que se lo va a utilizar por el tiempo de validez para el cual se emitió, pero se pueden presentar circunstancias que dejen sin validez a dichos instrumentos antes de cumplir el período operacional para el cual se lo emitió.

La suspensión de un certificado se traduce en hacer al certificado operativo; inoperatividad que es temporal y reversible, por lo que ninguno de los usuarios puede fundamentarse en el contenido de tal, suspensión que incluye e involucra también a la clave pública y privada del suscriptor.

La Ley de Comercio Electrónico del Ecuador no define la suspensión del certificado de la Firma Electrónica, indicando únicamente en el artículo 25, las causas por las que la entidad de certificación de información podrá suspender temporalmente el certificado, estas causas son:

a) Que sea dispuesto por el CONATEL, de conformidad con lo previsto en esta ley;
b) Se compruebe por parte de la entidad de certificación de información, falsedad en los datos consignados por el titular del certificado; y,
c) Se produzca el incumplimiento del contrato celebrado entre la entidad de certificación de información y el titular de la Firma Electrónica."

El mencionado literal a), tiene concordancia con el literal b) del artículo 37, de la misma Ley, el que determina que el CONATEL en su calidad de organismo de autorización, registro y regulación de las entidades de certificación podrá suspender los certificados cuando los haya emitido, sin haber cumplido las formalidades legales, esto previo informe motivado de la Superintendencia de Telecomunicación.

Otro punto importante del segundo inciso del mismo artículo 25 de la Ley, se previene la situación de que una vez ocurrida la suspensión de un certificado de Firma Electrónica, es necesaria la inmediata notificación por parte de la entidad de certificación y al organismo de control, de conformidad con el artículo 14, del Reglamento de la Ley, se realizara a la dirección electrónica y a la dirección física que hubiese señalado en el contrato, debiéndose también señalar las causas de la suspensión.

1.3.5. Regulación Jurídica de la Firma Digital

El desarrollo de las Tecnologías de la Información y la Comunicación (TIC), deben desarrollarse otros ámbitos de la vida como: los estudios, el trabajo, las empresas y las estrategias de un país, como las regulaciones que permiten crear una base para las mismas. La evolución digital lleva a las empresas locales que participen a nivel mundial en las actividades de comercio, esto lleva a un nivel superior de actividades, donde la reproducción crece. Para que funcione correctamente, no solo el desarrollo de la tecnología, sino también una legislación que ayude a controlar, supervisar y regular las actividades correspondientes.

En la Ley Modelo sobre el Comercio Electrónico de la CNUDMI se alude que unas de las razones por la creación de esta ley llevan a que el número de transacciones realizadas por medios electrónicos, han crecido sustancialmente en el ámbito del comercio internacional. Además, en todos los países, y en especial en los países en desarrollo, mostraban un gran interés en el desarrollo y progreso amplio del derecho mercantil internacional.

La firma digital cumple con los requerimientos de seguridad necesarios, y esto al ser la firma en general el método utilizado para vincular a la persona con un mensaje o documento y por lo tanto para manifestar la voluntad de obligarse conforme a lo que se establezca, resulta indispensable la creación de un método equivalente para el comercio electrónico, ya que adquirido cada vez mayor fuerza. Cuando hablamos de la firma, esta sirve

para garantizar la autoría, las personas, usualmente se hacen la idea de la firma manuscrita, pero con las nuevas tecnologías y los nuevos modos de transaccionar electrónicamente ya que la firma manuscrita no se pueden usar en este ámbito, y se aplica la firma digital.

1.3.6. Iniciativa de Regulación

1.3.6.1. Ley Modelo de la CNUDMI

En la Asamblea General de las Naciones Unidas, el 17 de diciembre de 1966, en la resolución 2205 (XXI), se establece la Comisión de las Naciones Unidad para el Desarrollo Mercantil Internacional y se encargó a fomentar la armonización y unificación del derecho mercantil internacional. En 1984 se inició el proceso de elaboración de la Ley Modelo realizado por el secretario general de la ONU sobre un informe llamado "Aspectos jurídicos del procedo automático de datos". En esta comisión se redactó la Ley Modelo sobre el Comercio Electrónico al observar que iba aumentando el número de las transacciones comerciales por vías electrónicas.

Esta Ley fue aprobada el 16 de diciembre de 1996, en la Octava sesión plenaria de la CNUDMI. La finalidad de esta ley es para que los países puedan tener una guía para la elaboración de sus legislaciones respectivas que traten sobre este tema. En la Ley Modelo y en la Guía de la misma, se establecen directrices generales para que otros países miembros puedan adaptar su legislación conforme a las disposiciones que están establecidas por la Ley Modelo y Guía mencionadas. En su artículo cuarto establece que "Las cuestiones relativas a materias que se rijan por la presente Ley y que no estén expresamente resueltas en ella serán dirimidas de conformidad con los principios generales en que se inspiran." (Ley Modelo de la CNUDMI, art. 4)

Existen otros principios, como el de proteccion a la privacidad, libertdad del comercio, libertad de informa y auteodeterminacion, entre otros. Estos principios mencionados los explicaremos.

En el artículo 7 de la Ley Modelo de la CNUDMI se establecen los requisitos que se debe de cumplir la firma en relacion a un mensaje de datos; el primero se trata sobre la identificacion y vinculacion del firmante con el texto, se debe de identificar a la persona de manera precisa y se debe de vincular al emisor con el texto, de esta manera se debe de entender que el acuerdo con lo enviado. El segundo requisito explica que el metodo debe de ser fiable para todas las circunstancia. Estos dos requisitos deben de ser cumplidos por la firma digital, al proveer confidencialidad, integridad, autenticación, el requisito de no repudio y disponibilidad (Ley Modelo de la CNUDMI, art. 7). debido a la generalidad que caracteriza a la Ley Modelo, con este artículo inclusive con una firma escaneada podria tener validez, esto depende de al acuerdo al que lleguen las partes.

En la Guía para la incorporacion al derecho interno de la Ley Modelo de la CNUDMI sobre el Comercio Electrónico se recomienda a los Estados miembros que desarrollen equivalentes funcionales para los tipos de firmas manuscritas ya existentes (Ley Modelo de la CNUDMI, art. 7). Posteriormente se establecen ciertos facotres que se pueden tener en cuenta para determinar si el método seleccionado es el indicado:

> "1) la percción técnica del equipo utilizado por cada una de las partes; 2) la naturaleza de su actividad comercial; 3) la frecuencia de sus relaciones comerciales; 4) el tipo y magnitud de la operación; 5) la función de los requisitos de firma con arreglo a la norma legal o reglamentaria aplicable; 6) la capacidad de los sistemas de comunicaión; 7) la observancia de los procedimientos de autenticación establecidos por intermediarios; 8) la gama de procedimientos de autenticación que ofrecen los

> intermediarios; 9) la observancia de los usos y prácticas comerciales; 10) la existencia de mecanismos de aseguramiento contra el riesgo de mensajes no autorizados; 11) la importancia y el valor de la información contenida en el mensaje de datos; 12) la disponibilidad de otros métodos de identificación y el costo de su aplicación; 13) el grado de aceptación o no aceptación del método de identificación en la industria o esfera pertinente, tanto en el momento cuando se acordó el método como cuando se comunicó el mensaje de datos; 14) cualquier otro factor pertinente." (Ley Modelo de la CNUDMI, art.7)

Lo ya mensionado hasta el momento es pertinente señalar que la firma digital puede solvertar mucho, todos los factores mencionados asegurando la identificación y vinculación al mensaje de datos por parte del emisor. Podemos resaltar que en la Ley Modelo nose utiliza el termino "electrónica" para describir a la firma.

1.3.7. Normativa Internacional

1.3.7.1. Regulación de la firma digital en Argentina

En Argentina la firma digital y la forma electrónica no son lo mismo, a pesar de que se reconoce dos tipos de firmas (ley 25.506, art, 1). La firma electrónica es aquella que no cumple con todos los requisitos para ser necesarios para ser considerada firma digital, como lo establece el artículo 5 de la Ley 25.506, promulgada el 11 de diciembre de 20001. Por otro lado, la firma digital la podemos definir como el "resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose esta bajo su absoluto control." (Ley 25.506, art. 2).

En el articulo tercero de la Ley mencionada se trata del principio de equivalancia funcional, quiere decir que la exigencia de requerir una firma manuscrita se podra cumplir con el uso de una forma digital (Ley 25.506., art, 3). Para que una firma digital pase ser

considerada válida debe de reunir los requisitos del artículo 9, primero, la firma digital tiene que ser creada durante el periodo de vigencia que tenga el certificado digital emitido, segundo, trata sobre la verificación de los datos plasmados en el certificado y vayan acorde a los datos presentados por el titular y su firma, y tercero, el certificado haya sido emitido por una entidad certificadora licenciada (Ley 25.506, art. 9).

Mencionaremos dos atribuciones adicionales que se le da al a firma en la Ley Argentina son; cuando un documento esté firmado digitalmente o se encuentre reproducido de uno que si se encuentre firmado, será este considerado como documento original y de esta manera obtiene un valor probatorio (Ley 25.506 art. 11). La otra atribución trata sobre la conservación, que está unido con el requerimeinto de seguridad de la disponibilidad, cuando se requiera la conservación de algún tipo de documento físico, el documento digital permitirá cumplir esta disposición siempre y cuando esté firmado digitalmente y se pueda acceder al mismo posteriormente. Además de estar disponible, debe ser posible verificar la hora de creación, el destino y origen del mensaje, así como el moennto de envió o recepción (Ley 25.506, art, 12).

En el artículo 7 establece un principio que resulta importante, para apoyar el requerimiento de seguridad denominado no repudio, y este es el principio de presunción de autoría. Esto quiere decir que sepresume que el firmante es el dueño legítimo de la firma digital y por esto se respalda el requerimiento de no repudio de la misma, a menos que exista prueba en contrario, situación en la cual se deduce que la carga probatoria reace sobre quien niega la validez de la firma, es decir, el dueño de la misma (Ley 25.506, art. 7).

Se complementa esto con la presunción trascrita en el artículo 10 que explica que "Cuando un documento digital sea enviado en forma automática por un dispositivo programado y lleve la firma digital del remitente se presumirá, salvo prueba en contrario,

que eldocumento firmado proviene del remiente" (Ley 25.506, art. 10) Es decir, en caso de que exista un programa de respuesta automática y esta consteste un mensaje de datos enviado, entonces se presumirá que proviene del remiente del mensaje, siempre y cuando esté firmado digitalmente.

Podemos mencionar también la presunción de integridad de un mensaje, esta presunción revela que en caso de que un mensaje haya sido verificado así como la firma digital, entonces esta se presumirá que el mensjae no ha sufrido alteraciones desde que se firmó (Ley 25.506, art. 8).

Los certificados de firmas, la ley Argentina contiene disposiciones que hablan sobre el plazo de los mismo, el reconocimiento de los certificados emitidos en el extranjero y los requisitos que deben cumplir, es importante mencionar que antes de enumerar los datos mínimos que deben contener los certificados, establece que deberán cumplirse aquellos requisitos que vayan conforme a los estándares internacionales y deben ser emitidos por una entidad de certificación licenciada. Los datos que deben contener un certificado son aquellos que permitan la correcta identificscion del firmante y toda la información relevante del mismo, así como el plazo de vigencia (Ley 25.506, art. 14).

En Argentina se crea una Comisión Asesora para la infraestructura de firma digital, que tiene como función emitir recomendaciones sobre:

a) Estándares tecnológicos;
b) Sistemas de registro de toda la información relativa a la emisión de certificados digitales;
c) Requisitos mínimos de información que se debe suministrar a los potenciales titulares de certificados digitales de los términos de la política de certificación;
d) Metodologia y requerimiento del resguardo físico de la información;

e) Otros que le sean requeridos por la autoridad de aplicación. (Ley 25.506, art. 36)

Así lo explica el artículo 36 de la Ley 25.506, esta comisión tiene el deber de consultar con los usuarios, las cámaras de comercio, entre otros, sobre los temas referentes a la firma digital y esto se hará saber los resultados de dichas consultas a la autoridad encargada de la aplicación (Ley 25.506, art. 35).

1.3.7.2. Regulación de la firma en España

En España, el 19 de diciembre de 2003, se aprobó la Ley 59/2003 de Firma Electrónica. Esta Ley tiene como antecedente el Real Decreto Ley 14/1999, que fue aprobada el 17 de septiembre de 1999, la legislación española describe tres tipos de firma: la electrónica, la electrónica avanzada y la electrónica reconocida. La primera es dada por la Ley Modelo CNUDMI, la segunda es la que permite la identificación del firmante al igual que la comprobación de que no ha existido alteración al mensaje de datos, así como lo logra hacer la firma digital y por último esta la firma electrónica reconocida. La única diferencia entre la firma avanzada y la firma reconocida es que esta última cuenta con un certificado reconocido y es generada por un sistema considerado como seguro. Esta última firma es reconocida se considera como la firma manuscrita, ya que consta con las seguridades necesarias para serlo. Sin embargo, no se le quitará efectos jurídicos a una firma electrónica con respecto al mensaje de datos en la que fue usada, por lo que no cumpla con todos los requisitos necesarios para ser considerada una firma electrónica reconocida (Ley 59/200, art. 3).

La legislacion de españa, al igual que en la argentina y en la ecuatoriana, como se vera posteriormente, el sistema idóneo para permitir validez a la firma es el certificado otorgado por una netidad certificadora de informacion. Sin ambargo, en lo que se direfencia esta legislacion con las otras ya mencionadas, es que en esta se reconoce el certificado

electrónico, ya que es un mensaje de datos firmado electrónicamente por una entidad certificada en la cual se presentan los datos que vinculan al firmante con su respectiva forma y el certificado electrónico reconocido. (Ley 59/2003, art.6). Este último es aquel que es emitido por una entidad certificadora que cumple con todos los requisitos que se establece en la ley, principalmente en los temas que tratensobre la autenticación, las condiciones establecidas por las partes, y por último, a la garantias que brindan la entidad y sufiabilidad. Este contenido es el mismo establecido enla legislación ecuatoriana, que se tratara más adelante.

En el artículo 24 de la Ley 24/2003 trata el tema de los dispositivos de creación de la firma electrónica; los datos de creación de firma son los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica, un dispositovo de creación de firma es un programa o sistema informátivo que sirve para aplicar los datos de creación de la firma, y por ultimo, un disposotivo seguro de creación de firma es un dispositvo de creación de firma que ofrece, al menos, las siguientes garantías:

a) Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.
b) Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.
c) Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.
d) Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma. (Ley 59/2003, art. 24)

Como se regula el dispositivo de creación de la firma, también se regula el dispositivo de verificación de la misma en el artículo siguiente. Los datos que se utilizan para verificar la firma electronica son códigos o claves públicas, este dispositvo, al igual al otro, es un programa o sistema informativo que sirve para emplear los datos descritos como anterioridad. Entre las garantias ue deben cumplir un sistema de verificaicon de firma electrónica se encuentran: la fiabilidad de la verificación, que aparte de todo, se verifique tambien el certificado, referente a la autenticidad y validez del mismo, que también exista la posibilidad de verificar la integridad del mensaje, que se deba mostrar la identidad del firmante, entre otros más técnicos. (Ley 59/2003, art. 25)

Podemos mencionar que en la legislación española se integra la firma electrónica avanzada a un docuemnto de identidad que tiene como nombre documento naional de identidad o DNI. Este documento certifica de forma electrónica la identidad del titular, con este documento se puede firmar documentos puúblicos y privados, tambien se acredita la identidad y todos los datos personales del titular y firmante así como la integridad de los documentos que se firmen utilizando este medio. (Ley 59/2003, art. 15)

Para finalizar, la firma electrónica avanzada es el equivalente funcional para la firma manuscrita, acorde a lo establecido en la legislación española. La firma electrónica avanzada sirve para identificar al firmante, otorgarle integridad y autenticidad al mensaje y asegurar el no repudio del mismo. Podriamos decir, que la firma electrpónica avanzada cumple la misma función y brinda la misma seguridad que la firma digital, y la única diferencia recae en el nombre otorgado a estas.

CAPÍTULO III

MARCO METODOLÓGICO

3.1. Tipo de investigación

Para el presente proyecto se implementó la investigación jurídica en la cual "se describe no sólo cómo se ha de proceder de hecho, sino que plantea también la cuestión sobre el valor, sobre el posible éxito de ciertos métodos. No procede en esto tan solo 'descriptivamente', sino también normativamente." (Larenz, 2010)

3.2. Enfoque

El enfoque de la investigación es cualitativo debida a que se van a estudiar las características y normas acerca de las firmas electrónicas en el Ecuador, debido a que no existen mayores investigaciones respecto al tema en mención ya que es una materia relativamente nueva.

3.3. Población y muestra

Para definir la población y muestra del presente proyecto de investigación jurídica se utilizó la entrevista al comité de expertos, por medio de la cual se pudo obtener entrevistas del Abg. Fabrizio Andrés García Bacigalupo, Abg. Francisco Oliverio Cedeño Díaz y Abg. Shafick Junther Juez Cabezas, con experiencia en la materia y en el ejercicio profesional entre 10 y 15 años.

3.4. Métodos de investigación jurídica

3.4.1. Método empírico

El método empírico se utiliza por lo general en las investigaciones jurídicas con enfoque cualitativo debido a que no se tienen mayores datos cuantitativos sino más bien se realiza un análisis teórico; este método permite la implementación de una entrevista a un comité de 3 expertos con experiencia en el área o materia de la cual versa determinada investigación. (Larenz, 2010)

3.4.2. Método documental

El método documental se empleó al momento de realizar un análisis a la diferente doctrina que se tuvo al alcance ya se en físico o digital.

3.4.3. Método jurídico comparado

Este método se utilizó al momento de realizar un análisis comparado con los países de Argentina y España.

CAPÍTULO IV

ANÁLISIS DE RESULTADOS

En el presente capítulo se revisarán los resultados de las encuestas aplicadas al grupo de expertos.

4.1. Análisis de entrevistas

Experto entrevistado 1

Nombres y Apellidos: Fabrizio Andrés García Bacigalupo

Años de experiencia laboral: 15 años

Cargos ocupados: Abogado litigante en libre ejercicio, docente y capacitador en materias de derecho.

1. ¿Que conoce usted acerca de las firmas electrónicas?

Todo lo pertinente para su correcta aplicación y uso.

2. ¿Usted ha empleado firmas electrónicas, ha tenido casos en los cuales se hayan empleado esto?

Si, hace más de dos años la utilizo para comunicaciones dirigidas a ciertas entidades públicas como el Banco Central del Ecuador, Ministerio de Finanzas, Instituto Ecuatoriano de Seguridad Social, comunicaciones cursadas generalmente a través del Quipux.

Durante la pandemia, me ha sido útil para impulso procesal, mediante la suscripción electrónica de escritos, presentados por la ventanilla virtual, ante la Corte Provincial de Justicia del Guayas, Santa Elena y Corte Nacional de Justicia.

3. ¿En su opinión usted que tan avanzado cree que el Ecuador está en cuestiones de firmas electrónicas?

En los últimos años ha existido un avance importante, especialmente para la ejecución de trámites públicos. Sin embargo, considero que todavía existe un desconocimiento generalizado

por parte de la ciudadanía en general, lo que hace que el sistema aún funcione de forma muy limitada.

4. ¿En la Región de América Latina que país usted cree que tiene una correcta regulación de firma electrónica?

De lo que conozco en México se utilizan mucho y por ende su regulación se encontraría acorde.

5. ¿Qué mecanismo usted emplearía para mejorar la calidad de firma electrónica en el Ecuador?

Su masificación, al punto de que todas las entidades y personas, sean naturales o jurídicas, la utilicen y acepten como válida.

6. ¿Que se podría implementar en las firmas electrónicas que no estén implementadas en el Ecuador?

Desde el punto de vista técnico creo que las firmas electrónicas en Ecuador, constan con todos los protocolos de seguridad necesarios. Lo que se debe mejorar, es su difusión pública.

7. ¿Qué opina sobre la normativa internacional sobre la firma electrónica, y que debería mejorar en la normativa en el Ecuador?

Considero que la normativa en Ecuador y en el mundo, es clara; empresas como GLOVO, UBER EATS por ejemplo, utilizan en su máximo potencial las firmas electrónicas, para entenderse con sus socios, empleados y clientes. Esto es un buen ejemplo de transnacionales, utilizando la legislación local, para adaptar sus modelos de negocios originalmente diseñados en otros países. La normativa local, tendría armonía con la internacional.

Experto entrevistado 2

Nombres y Apellidos: Francisco Oliverio Cedeño Díaz

Años de experiencia laboral: 10 años

Cargos ocupados: Director de Gestión Social Municipal, Registrador (e) de la Propiedad y Mercantil del cantón Naranjal, libre ejercicio profesional.

1. ¿Que conoce usted acerca de las firmas electrónicas?

La firma electrónica se viene utilizando desde hace varios años atrás, todo encaminado a avanzar de manera paralela a la modernidad y a los avances tecnológicos, pues ahora es muy común transferir documentos que no llevan una firma auténtica sino un documento digitalizado que es susceptible a alguna manipulación. Para eliminar definitivamente los fraudes por suplantación de identidad.

Con la firma electrónica regulada por la Ley de Comercio Electrónico publicada en el Registro Oficial el 17 de abril del 2002.

2. ¿Usted ha empleado firmas electrónicas, ha tenido casos en los cuales se hayan empleado esto?

Como funcionario público, esto es como Registrador Encargado de la Propiedad y Mercantil del cantón Naranjal utilice firma electrónica por medio de un token que se adquirió para ese efecto.

3. ¿En su opinión usted que tan avanzado cree que el Ecuador está en cuestiones de firmas electrónicas?

En los últimos años el Ecuador ha venido realizando un avance tecnológico sostenido en lo que a telecomunicaciones se refiere, con la instalación de fibra óptica, y por la prestación de servicios de empresas privadas es ahora muy común que un gran porcentaje de la ciudadanía tenga acceso a internet el cual cada día ofrece mejor calidad.

El uso de la firma electrónica por estar regulado por Ley lo vuelve seguro en su uso porque obtener la firma electrónica para personas naturales o representantes legales de personas jurídicas y funcionarios públicos es posible, sin mayores complicaciones pero por medio de entidades debidamente autorizadas como lo son:

El Banco Central Del Ecuador, Registro Civil, Security Data Seguridad en Datos y Firma Digital S.A., Consejo De La Judicatura, ANFAC Autoridad de Certificación Ecuador C.A.

4. ¿En la Región de América Latina que país usted cree que tiene una correcta regulación de firma electrónica?

En Colombia, se viene implementado la firma electrónica, con certificación en la nube, firma biométrica, verificación de huellas etc. es uno de los países más avanzado en el uso de la era digital.

5. ¿Qué mecanismo usted emplearía para mejorar la calidad de firma electrónica en el Ecuador?

Mejorar la calidad implica hacer más accesible este sistema a mayor cantidad de ciudadanos con múltiples ocupaciones por lo que se deberá extender el servicio a teléfonos móviles, tablets, etc. con el aval suficiente para su uso internacional que permita el flujo de documentos electrónicos, para disminuir el uso del papel.

6. ¿Qué se podría implementar en las firmas electrónicas que no estén implementadas en el Ecuador?

Normar el uso de la firma electrónica para uso financiero o bancario con reglas aplicables que sean claras y que faciliten su uso en esas instituciones.

7. ¿Qué opina sobre la normativa internacional sobre la firma electrónica, y que debería mejorar en la normativa en el Ecuador?

A nivel mundial el uso de la firma electrónica es algo que se realiza de la manera común, habiendo generado la confianza en su uso por lo versátil de su realización la que puede hacerse de manera remota sin la necesidad de la comparecencia de las partes para realizar transacciones de toda índole.

Experto entrevistado 3

Nombres y Apellidos: Ab. Shafick Junther Juez Cabezas

Años de experiencia laboral: 10 años

Cargos ocupados: Trabajo en la universidad Ecotec, Consorcio Jurídico ARGUE

1. ¿Que conoce usted acerca de las firmas electrónicas?

Conozco que las emitía en banco central y el registro civil para realizar procesos respectos a temas aduaneros y la firma de gestión documental del gobierno del ecuador.

2. ¿Usted ha empleado firmas electrónicas, ha tenido casos en los cuales se hayan empleado esto?

Si, cuando ejercía un cargo en el gobierno por el sistema Quipux.

3. ¿En su opinión usted que tan avanzado cree que el Ecuador está en cuestiones de firmas electrónicas?

Un 50 por ciento.

4. ¿En la Región de América Latina que país usted cree que tiene una correcta regulación de firma electrónica?

En Brasil.

5. ¿Qué mecanismo usted emplearía para mejorar la calidad de firma electrónica en el Ecuador?

Primero socialización oportuna y segundo que se la emplee para no solo cosas gubernamentales.

6. ¿Que se podría implementar en las firmas electrónicas que no estén implementadas en el Ecuador?

El Ecuador cuenta con un sistema de seguridad referente a Firmas Electrónicas, pero lo que se debe mejorar es que todos tengan el conocimiento de ella.

7. ¿Qué opina sobre la normativa internacional sobre la firma electrónica, y que debería mejorar en la normativa en el Ecuador?

La normativa ecuatoriana está diseñada acorde a la normativa internacional.

Análisis de entrevista a expertos

Como los expertos de la entrevista manifiestan que deberían tener el acceso a obtener la firma electrónica las personas naturales y jurídicas, no solo la parte gubernamental, ya que en otros países si cuentan con ese acceso en obtener una firma electrónica, además, la normativa ecuatoriana tiene armonía con la normativa internacional ya que sirve como Ley Modelo para todos los Estados Miembros.

CAPÍTULO V

PROPUESTA

5.1. Justificación de la propuesta

La Ley de Comercio Electrónico, Firma Electrónica y Mensajes de Datos cuenta con disposiciones que pueden resultar ser demasiado básicas en lo que a firmas se refiere. Al analizar la Ley Modelo de la CNUDMI y la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y compararlas, se pueden notar un afín extremo, casi igual entre estos cuerpos legales. La Comisión de Naciones Unidas sobre el Desarrollo Mercantil Internacional (CNUDMI) redactó dicha Ley Modelo para que los Estados Miembros puedan utilizar como guía y para que las disposiciones escritas en esta, sean acogidas por los mismos.

Sin embargo, de que este texto sea aplicable como modelo, no quiere decir que no se puedan añadir disposiciones que favorezcan e impulsen su uso, en Argentina y España crearon leyes que regulan la firma digital. La Ley Modelo es intencionalmente general respecto a los aspectos que regula, esto es para que los Estados Miembros puedan ajustar sus leyes a dicho texto y tengan capacidad para regular otras situaciones que consideren necesarios.

En la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, y en el Reglamento se habla de la firma electrónica como el semejante funcional de la firma manuscrita (art.14). La firma digital puede brindar todas las garantías necesarias para que los requerimientos de seguridad queden satisfechos.

La firma electrónica discrimina otros tipos de tecnologías, y no cumplen con todos los estándares internacionales descritos anteriormente. El Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos establece que no se discriminara a ningún tipo de firma electrónica (art10). Pero al referirse a lo electrónico se discrimina los otros tipos de tecnología y como lo hemos mencionado en este trabajo, la firma digital no es

un tipo de firma electrónica, estas firmas no tienen una relación género-especie, por lo tanto, se discrimina a la firma digital, puesto que no es una firma electrónica.

El éxito del comercio electrónico está basado en la confianza de los usuarios, es indispensable contar con una herramienta que promete la mayor confianza posible, una herramienta que garantice la autoría, integridad, la confidencialidad y el no repudio de la información contenida en el mensaje y de la misma firma, en lo que a no repudio se refiere.

La firma digital es una de las herramientas eficaces para promover la confianza necesaria en el comercio electrónico, porque además de cumplir con los estándares internacionales brindan una solución efectiva a cada requerimiento de seguridad de la información, esta cumple con lis mínimos requisitos establecidos, que son el de identificación y vinculación.

El comercio electrónico ha tomado fuerza con el paso del tiempo, es por eso que es necesario contar con un cuerpo normativo que respalde y brinde tanto una guía como un apoyo para las nuevas situaciones que se generen. Y lo que es más necesario, contar con un cuerpo normativo que vaya conforme a los estándares y principios internacionales. Sin violar ningunos de esos principios como acontece ahora con el uso del término tecnología versus el principio de neutralidad tecnología, principio adoptado y reconocido globalmente. Las leyes y los Reglamentos deben evolucionar acorde a las necesidades de las personas y es el caso donde existen elementos que deben ser actualizados.

Para empezar por la actualización del término “electrónico” a “digital” respecto a las firmas. Al exponer que la firma electrónica es discriminatoria frente a otros tipos de tecnologías y al ser el Ecuador miembro de las Naciones Unidas, no puede violentar el principio de neutralidad tecnológica. En el Reglamento a la Ley de Comercio Electrónico,

Firmas Electrónicas y Mensajes de Datos reconoce expresadamente este principio, pero al referirse a firma electrónica se lo desvalida.

La firma digital es el tipo de firma que brinda más seguridad, y esta debería ser promovida por el Estado. Los participantes del comercio electrónico deben poder contar con el debido respaldo por parte de las leyes por las cuales si rigen los actos de comercio, y deben de poder confiar en que las leyes los respaldan conforme a los parámetros internacionales, para que las disposiciones que sujeten puedan ser aceptadas por leyes de otros países con los que se quiere interactuar comercialmente a través de personas de ese Estado.

La firma digital es una parte fundamental del comercio electrónico, mediante la utilización de la misma se pueden suplir todos los requerimientos de seguridad de la información, para así poder generar la confianza en el tan amplio campo de la red. Se necesita un cuerpo normativo que regule todos los aspectos esenciales de la firma digital, en este caso, es necesario que en este cuerpo legal se establezcan todos los aspectos referentes a las garantías y la validez de la firma digital.

5.2. Propuesta de reforma a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

Como se ha expuesto el tema de la no violación al principio de la neutralidad tecnológica, se deberían reconocer otros tipos de firmas como la digital, ya que sería la principal por la seguridad que esta brinda. Resulta interesante como otros países han evolucionado más con este tema.

Al ser la firma digital un elemento primordial para el comercio electrónico, sería sensato darle la importancia que se merece al crear una ley que se base en este tema y los aspectos que este conlleva. La firma digital no debe de ser tratada de manera básica ya que la firma digital no es sencilla. Tiene un mecanismo complejo que debe ser regulado de acuerdo

al mismo, para poder sacar el mayor provecho de esta tan útil herramienta. En resumen, la propuesta es la reforma a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos en el siguiente artículo.

Articulo actual

Art. 13 Firma Electrónica.- Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que pueden ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e identificar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.

Articulo reformado

En tal sentido el contenido del artículo 13 de la Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos, podría ser el siguiente: *"Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que pueden ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e identificar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.*

1. *Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley.*
2. *Y para todo lo concerniente respecto de los procedimientos a la firma digital serían los mismos procedimientos de la firma electrónica."*

CONCLUSIONES

- La firma digital surge como una solución técnica que compensa todos los requerimientos de seguridad de la información, a excepción de la disponibilidad, donde se necesita un programa de almacenamiento donde se complementa con el empleo de la firma digital, esta firma digital desde el punto de vista teórico internacional, es una firma electrónica avanzada, si tenemos una firma digital que está en un token, al momento de introducir el token en el ordenador pide una clave, y cuando se cumple dos criterios de autenticación ya se tiene la firma digital, pero para tener una firma mucho más segura, se vincula tres cosas, el token tiene un lector de huella digital, que se asocia al dueño del token y la clave, y al vincular las tres cosas ya tenemos una firma mucho más segura.
- En el transcurso del tiempo se ha establecido una clara tendencia a regular sobre la firma digital, por todos los beneficios que esta conlleva, por esto la ley Argentina se norma la firma digital. En la legislación española se habla sobre la firma avanzada que es el parecido a la firma digital, este tipo de firma no es solamente una herramienta del comercio electrónico y por esto no debería estar directamente vinculado con este como se hace en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. La firma digital brinda la seguridad necesaria para que las personas puedan confiar en su sistema. Los beneficios que conlleva el uso de la firma digital, es contar con un cuerpo normativo que vaya acorde para así explotar su uso y beneficios posibles.
- Para finalizar, la firma digital es el tipo de firma para ser regulado, ya que cumple con todos los requerimientos de seguridad, con los estándares internacionales y esta no contradice con ningún principio, en tal sentido se realizó la propuesta de reforma a la

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos para insertar la firma digital en Ecuador.

RECOMENDACIONES

- Se recomienda realizar mayores estudios sobre el tema investigado, puesto que en el Ecuador no ha existido mayor avance en esta área. Ya que la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos fue redactada en el año 2002 y desde su publicación no ha sido revisada, y más aún en lo que se refiere al tema de firmas electrónicas.
- Adicionalmente se recomienda trabajar en un proyecto de ley que pueda ser tratado en las Universidades, ya que con la que cuenta el Ecuador no cumple con las exigencias del mundo actual. Se necesita de una actualización en lo que se refiere a firmas digitales, para que las personas puedan sacar el mayor provecho posible. Este trabajo tiene una finalidad de proponer una actualización a la normativa que regula a la firma electrónica en el Ecuador.

Bibliografía

Bertolín, J. A. (2008). *Seguridad de la Información. Redes, informática y sistemas de información.* Madrid, España: Paraninfo. Recuperado el 01 de 06 de 2020, de https://books.google.com.ec/books?id=_z2GcBD3deYC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q=firma%20electronica&f=false

Costas, J. (2010). *Seguridad Informática.* Madrid, España: RA-MA. Recuperado el 22 de Mayo de 2020

Devoto, M. (2001). *Comercio Electrónico y Firma Digital.* Buenos Aires: La Ley S.A.

Hance, O. (1997). *Leyes y Negocios en Internet.* México: Mc Graw - Hill. Recuperado el 04 de 05 de 2020

Larenz, K. (2010). *Metodología de la ciencia del derecho.* Barcelona: Ariel Derecho.

Ley 25.506. (11 de Diciembre de 2001). InfoLEG. En M. d. Nación (Ed.). Argentina. Recuperado el 21 de Mayo de 2020, de Informacion Legislativa: http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

Ley 59/2003. (2003). *Ley 59/ de diciembre, de la firma electrónica.* Recuperado el 27 de Mayo de 2020, de https://www.boe.es/buscar/pdf/2003/BOE-A-2003-23399-consolidado.pdf

Ley de Comercio Electrónico, firmas Electrónicas y Mensajes de Datos. (2002). Ecuador. Recuperado el 03 de Junio de 2020

Ley Modelo de la CNUDMI. (s.f.). Recuperado el 26 de Mayo de 2020, de https://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf

Ley Modelo de la CNUDMI. (1998). *Sobre Comercio Electrónico con la Guia para su incorporación al derecho interno 1996.* Naciones Unidad. Recuperado el 26 de Mayo de 2020, de https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf

Lorenzetti, R. L. (2001). *Comercio Electrónico.* Buenos Aires, Argentina: Abeledo-Perrot. Recuperado el 05 de 06 de 2020, de https://books.google.com.ec/books/about/Comercio_electr%C3%B3nico.html?id=qu_PAAAACAAJ&redir_esc=y

Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. (2002). Ecuador. Recuperado el 05 de 06 de 2020

Ribas, X. (Enero de 1997). *Contract-Soft onnet*. Obtenido de http://www.onnet.es/06041002.htm