

**UNIVERSIDAD DE EL SALVADOR
FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES ESCUELA
DE CIENCIAS JURÍDICAS.**



**RETOS EN LA IMPLEMENTACIÓN DE LA FIRMA ELECTRÓNICA EN
EL SALVADOR EN EL PERIODO 2016-2020**

**TRABAJO DE GRADO PARA OBTENER EL TÍTULO DE LICENCIADOS
EN CIENCIAS JURÍDICAS**

PRESENTADO POR:

**PAREDES RIVAS, DAVID ALEXANDER
PÉREZ JIMÉNEZ, KRISCIA DAMARIS
VÁSQUEZ BAUTISTA, MARÍA JOSÉ**

DOCENTE ASESOR:

DRA. ALICIA ZELAYA QUINTANILLA

CIUDAD UNIVERSITARIA, SAN SALVADOR, AGOSTO DE 2021

TRIBUNAL CALIFICADOR

**DR. RUTILIO ANTONIO DÍAZ MARTÍNEZ.
PRESIDENTE**

**MCS. WILMER HUMBERTO MARÍN SÁNCHEZ.
SECRETARIO**

**DRA. ALICIA ZELAYA QUINTANILLA.
VOCAL**

UNIVERSIDAD DE EL SALVADOR

Msc. Roger Armando Arias Alvarado
RECTOR

Dr. Raúl Ernesto Azcúnaga López
VICERRECTOR ACADEMICO

Ing. Juan Rosa Quintanilla Quintanilla
VICERRECTOR ADMINISTRATIVO

Msc. Francisco Antonio Alarcón Sandoval
SECRETARIO GENERAL

Lic. Rafael Humberto Peña Marín
FISCAL GENERAL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

Dra. Evelyn Beatriz Farfán Mata
DECANA

Dr. Edgardo Herrera Pacheco
VICEDECANO

Licda. Digna Reina Contreras de Cornejo
SECRETARIA

Lic. René Mauricio Mejía Méndez
DIRECTOR DE ESCUELA DE CIENCIAS JURÍDICAS.

Licda. Digna Reina Contreras de Cornejo
DIRECTORA GENERAL DE PROCESOS DE GRADUACIÓN

Lic. Enmanuel Román Funes
**COORDINADOR DE PROCESO DE GRADUACIÓN
DE LA ESCUELA DE CIENCIAS JURÍDICAS.**

AGRADECIMIENTOS

A mis papás, por estar siempre comprometidos con mi educación, por apoyarme en todo momento y enseñarme que todo esfuerzo siempre tendrá su recompensa.

A mi hermana Eva, porque a pesar de ser menor que yo, me enseñó que podemos vivir momentos o situaciones difíciles, pero siempre debemos de ser perseverantes y seguir adelante porque todo lo malo pasa.

A mis abuelos, por ser parte fundamental y esencial de mi vida, por darme la oportunidad de aprender de su experiencia a lo largo del tiempo

A mis compañeros de trabajo de grado, porque son amigos para toda la vida, me siento agradecida por encontrarme con excelentes personas a lo largo de la carrera.

A mi asesora, por estar comprometida con nuestro trabajo de grado en cada una de sus fases hasta su finalización, por ser una excelente catedrática en el área mercantil y bancario.

María José Vásquez Bautista.

AGRADECIMIENTOS

Agradezco a Dios en primer lugar por darme la sabiduría necesaria y ayudarme a poder salir adelante durante toda la carrera para culminarla de la mejor forma.

A mis padres, por el cariño y apoyo incondicional que me dieron desde un inicio en mis estudios y a lo largo de la carrera, por darme todo lo necesario y estar conmigo siempre, quienes siempre me animaron a cumplir esta meta en común.

A mis compañeras de trabajo de grado, con quienes pudimos lograr estos objetivos juntos, por el apoyo y ayuda mutua que nos dimos luego de mucho trabajo a lo largo de la carrera y durante esta investigación.

A nuestra asesora de trabajo de grado, por estar con nosotros durante todas las fases de la investigación, por apoyarnos e instruirnos en cada asesoría y poder culminar nuestra carrera.

David Alexander Paredes Rivas.

AGRADECIMIENTOS

Agradezco a Dios y a la Virgencita por iluminar mi mente, llenarme de sabiduría, acompañarme en todo momento y por proveerme todo lo necesario para alcanzar mi sueño.

A mis papás, por su apoyo y amor incondicional, consejos constantes y por brindarme todo su apoyo para alentarme a seguir adelante en mi carrera y estar conmigo siempre que los necesitara.

A mi hermana, por inspirarme a ser mejor profesional, por guiarme con su ejemplo y por extender su mano en momentos agotadores, gracias sobre todo a no darme por vencida.

Y finalmente a mis compañeros de trabajo de grado; porque la vida nos hizo ser los mejores amigos incondicionales, por apoyarnos a culminar nuestra carrera y alcanzar nuestro éxito profesional.

A mi asesora de Trabajo de Grado, por estar pendiente en cada fase de esta investigación, por brindarnos su apoyo y alentarnos a ser mejores profesionales.

Kriscia Damaris Pérez Jiménez.

ÍNDICE DE CONTENIDOS

RESUMEN.....	I
SIGLAS Y ABREVIATURAS	II
INTRODUCCIÓN.....	III
CAPÍTULO I:	1
GENERALIDADES DE LA FIRMA ELECTRÓNICA Y SU EVOLUCIÓN NACIONAL E INTERNACIONAL	1
1.1 La Firma.....	1
1.2 Clases de Firma	2
1.2.1 Firma Autógrafa	2
1.2.2. Firma Mecánica	2
1.2.3 Firma Digital-Firma Electrónica.....	3
1.3 Características de la Firma.....	5
1.3.1 Según el modo en que se emplea la firma	5
1.3.2 Según el fin de la firma	6
1.4 Elementos de la Firma	6
1.4.1 Elementos Formales	6
1.4.2 Elementos Funcionales.....	7
1.5. Evolución Nacional e Internacional de la Firma Electrónica.....	7
1.5.1. Primeros países en implementar la Firma Electrónica	7
1.5.2 La Firma Electrónica en El Salvador	18
1.6 Principios de la Firma Electrónica	19
1.6.1 Principio de Autenticidad.....	19
1.6.2 Principio de Integridad	19
1.6.3 Principio de Confidencialidad.....	20
1.6.4 Principio de equivalencia funcional	21
1.6.5 Principio de No Repudio o No Repudiación	21
1.6.6 Principio de Neutralidad Tecnológica.....	22
1.6.7 Principio de Seguridad.....	22
1.7 Ventajas y Desventajas de la Firma Electrónica.....	22

1.7.1 Ventajas de la Firma Electrónica.....	22
1.7.2 Desventajas de la Firma Electrónica.....	24
CAPÍTULO II:	25
FUNCIONAMIENTO Y USO DE LA FIRMA ELECTRÓNICA.....	25
2.1 Criptografía	25
2.2. Tipos de Cifrado Criptográfico.....	26
2.2.1. Criptografía de llave privada o simétrica	26
2.2.2. Criptografía de llave pública o asimétrica.....	28
2.3. Certificados Digitales.....	29
2.4. Los Entes Certificadores	30
2.4.1. Funciones de los Entes Certificadores	31
2.4.2. Tipos de Entes Certificadores	32
2.5. Formas en que se custodia un Certificado Digital.....	35
2.6. Ámbito de aplicación de la Firma Electrónica	36
2.6.1. Comercio Electrónico.....	36
2.6.2. Gobierno Electrónico	38
2.7. Validez de la Firma Electrónica	39
CAPÍTULO III:	41
PREÁMBULO DEL COMERCIO ELECTRÓNICO Y SU DESARROLLO A NIVEL NACIONAL E INTERNACIONAL.....	41
3.1. Comercio Electrónico (E-Commerce)	41
3.2 Ventajas y Desventajas del Comercio Electrónico.....	42
3.2.1 Ventajas del Comercio Electrónico	42
3.2.2 Desventajas del Comercio Electrónico.....	44
3.3 Características del Comercio Electrónico	45
3.4 Elementos del Comercio Electrónico.....	46
3.5 Principios del Comercio Electrónico	49
3.5.1 Principio de equivalencia funcional	49
3.5.2 Principio de neutralidad tecnológica.....	49
3.5.3 Principio de no repudiación.....	49
3.6. Clasificación del Comercio Electrónico.....	49
3.6.1. Según el medio de comunicación empleado.....	50
3.6.2. Según la actividad desarrollada	50

3.6.3. Según el grado de seguridad	50
3.6.4. Según los sujetos participantes.....	51
3.7. Desarrollo del Comercio Electrónico en El Salvador.....	53
3.8. Desarrollo del Comercio Electrónico en el ámbito Internacional	55
CAPÍTULO IV:	58
INTRODUCCIÓN A LA PROTECCIÓN DE DATOS PERSONALES Y SU IMPLEMENTACIÓN EN EL SALVADOR	58
4.1. Protección de Datos Personales	58
4.2. Sujetos y objeto de la Protección de Datos Personales.....	59
4.2.1. Sujetos de los datos personales	59
4.2.2 Objeto de la protección de datos personales	60
4.3. Principios de la Protección de Datos Personales.....	61
4.3.1. Principios Internacionales	61
4.3.2. Principios Nacionales.....	62
4.4 Clasificación de los Datos Personales.....	63
4.5. Categoría de los Datos Personales	64
4.6. Derechos Protegidos.....	65
4.6.1. Derecho al Honor.....	65
4.6.2. Derecho a la Intimidad	65
4.6.3. Derecho a la Privacidad.....	66
4.6.4. Derecho a la Autodeterminación Informativa.....	67
4.6.5. Derecho a la Seguridad Jurídica	67
4.6.6. Derecho a la protección de Datos Personales	68
4.7. La Protección de los Datos Personales en El Salvador	68
CAPÍTULO V:	71
RETOS EN LA APLICACIÓN DE LA FIRMA ELECTRÓNICA EN EL SALVADOR	71
5.1. Avances y Obstáculos de la Ley de Firma Electrónica	71
5.2. Relación normativa de la Ley de Firma Electrónica.....	73
5.2.1. Principios en común entre las leyes tratadas	73
5.2.2. Aspectos o puntos en común entre las leyes tratadas	76
5.3. Retos a superar para potenciar y dar aplicación a la Firma Electrónica en El Salvador.....	81

5.3.1 Potenciar el Gobierno Electrónico en El Salvador	81
5.3.2 Sancionar el Decreto N° 875 de la Ley de Protección de Datos Personales en El Salvador.....	82
5.3.3 Autorizar a las certificadoras digitales y certificadoras de almacenamiento electrónico	83
5.3.4 Implementar la Ley de Comercio Electrónico con el correcto funcionamiento de la Firma Electrónica en El Salvador	84
5.3.5 Destacar el rol del notario ante el uso de la Firma Electrónica.....	85
5.3.6 Detallar puntos básicos para crear y operar las páginas web	86
CONCLUSIONES.....	87
RECOMENDACIONES.....	90
BIBLIOGRAFÍA.....	92

RESUMEN

La firma, en general, es el medio por el cual damos nuestro consentimiento ante un acto jurídico, teniendo en cuenta el desarrollo tecnológico, al momento de firmar ya no solo se realiza de forma manuscrita, hoy en día se realiza por medios electrónicos, el término adecuado a ello es “firma electrónica”, por medio de ella garantizamos la integridad y consentimiento de los documentos realizados por medios electrónicos.

La firma electrónica marca un avance en nuestro país, desde el punto de vista de tres ámbitos, legal, electrónico y comercial. Al hacer uso de ella, se desglosa un abanico de opciones de contratación a nivel mundial, sin tener que desplazarnos a otros países. Por esa razón es necesario tener una sólida regulación de los medios electrónicos y la protección de los datos que se ven envueltos.

Se debe tener en cuenta la Constitución, que da cabida a la regulación de estos temas, para ello tenemos el art. 101 inc. 2 de la Cn. en lo relativo al desarrollo económico y el art. 2 de la misma, acerca de derechos fundamentales como lo son seguridad, honor e intimidad. Por esta razón es necesario tener en cuenta tres normas bases para desarrollar la firma electrónica, en primer lugar la Ley de Firma Electrónica que regula lo relativo a su uso, los entes certificadores, obligaciones y sanciones de los proveedores autorizados, que están bajo la supervisión de la Unidad de Firma Electrónica del MINEC, en segundo lugar la Ley de Comercio Electrónico, que ayudará a dar un mayor uso y campo de aplicación a la firma electrónica y por último, la Ley de Protección de Datos Personales, con la cual se busca resguardar todos los datos colocados de manera electrónica en la red al realizar contrataciones y transacciones en línea.

SIGLAS Y ABREVIATURAS

SIGLAS:

AFC	Acuerdo de Facilitación de Comercio
CSJ	Corte Suprema de Justicia
DL	Decreto Legislativo
FCE	Ley de Comercio Electrónico
LFE	Ley de Firma Electrónica
LPDP	Ley de Protección de Datos Personales
MINEC	Ministerio de Economía
RAE	Real Academia Española
OEA	Organización de los Estados Americanos
OMC	Organización Mundial de Comercio
TLC-CAFTA	Tratado de Libre Comercio entre República Dominicana, Centroamérica y Estados Unidos
UFE	Unidad de Firma Electrónica
UE	Unión Europea

ABREVIATURAS:

Art.	Artículo
Ed.	Edición
Edit.	Editorial
Cn.	Constitución
Inc.	Inciso
Lit.	Literal
Ord.	Ordinal
Num.	Numeral
Ppio.	Principio

INTRODUCCIÓN

A lo largo del tiempo se han venido dando diversos avances y retrocesos a nivel social, político, económico y tecnológico, estos puntos siempre van teniendo relación unos con otros, ellos nos ayudan a medir cómo se encuentran los índices de desarrollo en un país, es por ello que se necesitan regular los avances que se dan en una sociedad, para determinar y limitar cómo se desenvuelve; en cuanto al ámbito económico y tecnológico es imprescindible normar ciertos aspectos para el pleno desarrollo de los países, junto con el comercio y en este caso de la mano con la tecnología.

En la búsqueda de unificar diversos aspectos relacionados en el párrafo anterior; en el trabajo de investigación se abarcó temas legales, comerciales y tecnológicos, por esa razón el tema sobre el cual versa la investigación es “Retos en la Implementación de la Firma Electrónica en El Salvador en el período 2016-2020”, teniendo como eje central el problema de investigación que es el siguiente, “Para aplicar efectivamente la Ley de Firma Electrónica en el periodo 2016-2020, ¿En qué medida será necesaria la implementación de la Ley de Comercio Electrónico y la Ley de Protección de Datos Personales?”. Al conocer las bases del trabajo de grado, se hará mención de cada uno de los capítulos tratados y su contenido.

El presente trabajo está compuesto por cinco capítulos, en donde el Capítulo I se denomina “Generalidades de la Firma Electrónica y su evolución Nacional e Internacional”, el cual trata acerca de aspectos generales de la firma, como su definición, clases, características, elementos y dentro de él, cómo se ha venido evolucionando la Firma Electrónica en diferentes países a nivel mundial, realizando para ello un cuadro resumen de la normativas de cada uno de los países tomados en cuenta, si aún sigue vigente la ley o leyes y algunos datos importantes

acerca de ella, así como principios de la firma electrónica y las ventajas y desventajas del mismo.

En el Capítulo II titulado, “Funcionamiento y uso de la Firma Electrónica”, trata temas referidos al manejo y uso de la firma electrónica desde el punto de vista criptográfico, es decir, desde temas referidos a sistemas, tocando puntos como la llave privada o simétrica y la llave pública o asimétrica, también desarrollando los certificados digitales y los entes certificadores, que son lo que le dan vida y distribuyen las firmas electrónicas a los usuarios, a su vez la forma en que se custodian dichos certificados, el ámbito de aplicación que posee la firma electrónica y la validez de la que goza en nuestro marco jurídico.

Pasando al Capítulo III nombrado, “Preámbulo del Comercio Electrónico y su desarrollo a nivel Nacional e Internacional”, en el cual se desarrolla el comercio electrónico desde su definición, pasando por la ventajas y desventajas que se muestran con esta modalidad de realizar un intercambio comercial, los elementos, sus principios y la clasificación que se presentan en él, así como el desarrollo que ha tenido en nuestro país y a nivel internacional a lo largo del tiempo, buscando tener un enlace con la firma electrónica y el potenciamiento del comercio electrónico y las diversas transacciones en línea.

En cuanto al Capítulo IV citado como “Introducción a la protección de datos personales y su implementación en El Salvador”, trata temas como el mismo capítulo lo nombra, temas de acuerdo a la protección de datos personales como los sujetos y objeto de protección, definición, principios, clasificación, categorías y los derechos que se ven protegidos al darle cumplimiento por medio de una ley a este derecho en El Salvador.

Y en el último apartado, el Capítulo V llamado, “Retos para la correcta aplicación y desarrollo de la Firma Electrónica en El Salvador”, este capítulo se encuentra dividido en tres partes, en la primera parte se muestra los

avances realizados en relación a los cuerpos normativos tomados en cuenta, siendo la Ley de Firma Electrónica que entró en vigencia en el año 2015, la Ley de Comercio Electrónico que entra en vigencia en el año 2021 y el Decreto N° 875 de la Ley de Protección de Datos Personales, también todos los avances dados hasta la fecha en cuanto a la firma electrónica y la importancia que tiene en el desarrollo del comercio nacional e internacional y aspectos legales que aún no han sido regulados. En la segunda parte se realizó una relación entre las tres leyes, teniendo en cuenta los principios y puntos que tienen en común, con el fin de realizar un análisis conjunto. En la tercera parte, se establecen los retos a superar para el desarrollo e implementación de la firma electrónica en El Salvador, desafíos que se esperan se puedan solventar a corto plazo para la implementación de nuevas modalidades técnico-legales.

Para realizar la investigación, la metodología aplicada es de tipo explicativa, con ella se buscó encontrar, qué factores hacen que no se aplique la Ley de Firma Electrónica, también es una investigación documental, debido a que nos apoyamos en el conocimiento de especialistas en la materia y en datos bibliográficos, abordando los temas desde diversos puntos, con el fin de aumentar el conocimiento teórico-doctrinal que ya ha obtenido en estos temas.

Lo que se pretende con el presente trabajo de graduación, es demostrar que la Ley de Firma Electrónica necesita la implementación de la Ley de Comercio Electrónico y la Ley de Protección de Datos Personales para su efectiva aplicación, dar un óptimo e integral desarrollo y puesta en marcha de la firma electrónica, porque hasta el momento no ha sido aplicable su ley ni la firma como tal, por esa razón hemos propuesto que se acompañe de otras temas como el comercio electrónico y la protección de datos personales, para darle un mayor ámbito de aplicación, a la vez dar seguridad a todas las transacciones por medio de la firma electrónica y la

protección de los datos estipulados en los procesos realizados de manera virtual

CAPÍTULO I:

GENERALIDADES DE LA FIRMA ELECTRÓNICA Y SU EVOLUCIÓN NACIONAL E INTERNACIONAL

Como capítulo número uno se desarrollará y explicaran, en primer lugar, la clasificación de firma y la importancia de ella, así como también los elementos, características que contiene y como al día de hoy se tiene una firma electrónica a su vez, la evolución internacional que tiene la misma, con la finalidad de conocer sobre los aspectos generales y la posición en la que se encuentra en el país en este tema.

1.1 La Firma

La palabra firma se abordará, en un primer momento desde su origen etimológico, “firma viene del verbo firmar, y este procede del latín firmare (volver firme, sólido y seguro, asegurar) y este del adjetivo firmus (sólido, fuerte, que no se mueve), pues la palabra de uno es sólida, pero más sólida es su firma. Es decir, una vez firmado no lo puede retirar”.¹

Según la Real Academia Española (RAE), firma es, “Nombre o apellidos escritos por una persona de su propia mano en un documento, con o sin rúbrica, para darle autenticidad o mostrar la aprobación de su contenido”.²

Para Cabanellas firma es, “Nombre y apellido, o título, que se pone al pie de un escrito, para acreditar que procede de quien lo suscribe, para autorizar lo ahí manifestado o para obligarse a lo declarado. Conjunto de

¹ Joan Corominas, *Breve Diccionario Etimológico de la Lengua Castellana*, (Editorial Gredos, Madrid, tercera edición muy revisada y mejorada, 1987), 274

² Real Academia Española, *Diccionario de la Real Academia Española RAE*, (vigésimo tercera edición, 2014), definición de firma

expedientes u otros documentos que se someten a la autorización escrita de un jefe, y acto en el cual se verifica. COMERCIAL. Nombre o denominación que se adopta para ejercer el comercio y firmar los actos y contratos de tráfico mercantil. EN BLANCO. La que se da o estampa antes de llenarse un escrito; ya totalmente, por no contar en la hoja o pliego sino la firma; o bien parcialmente, por huecos dejados para rellenar con cantidades, fechas, nombres y datos o indicaciones diversos. ENTERA. La compuesta por el nombre y apellido”.³

1.2 Clases de Firma

1.2.1 Firma Autógrafa

La Ley de Firma de Electrónica en su artículo 3 proporciona algunas definiciones, dentro de estas, está la de Firma Autógrafa, siendo toda “marca o signo, que una persona escribe de su propia mano en un instrumento o documento para asegurar o autenticar la identidad de una persona como prueba del consentimiento y verificación de la información contenida en dicho instrumento”.

Con respecto a la Firma Autógrafa, además de lo dicho anteriormente, se puede decir que es el “conjunto de signos plasmados por el puño y letra del emisor o que es el conjunto de caracteres que una persona utiliza para dar consentimiento, en algunas ocasiones hay personas que solo escriben su nombre y otras que tienen firmas complejas”.⁴

1.2.2. Firma Mecánica

Esta firma es la que se realiza por medios mecánicos. Y son los siguientes:

³ Guillermo Cabanellas de Torres, *Diccionario Jurídico Elemental Nueva Edición Actualizada por Guillermo Cabanellas de las Cuevas*, (Editorial Heliasta S.R.L. undécima edición, 1993), 138

⁴ Ale Ortega, Tipos de Firma Electrónica: Conoce los tipos de firmas y encuentra la mejor opción para tu negocio (Blog) de Mifiel 2019, <https://blog.mifiel.com/comparacion-tipos-de-firmas/>

Facsímile: etimológicamente significa imitación o semejanza, es la reproducción de la firma en sellos que se estampa en algún escrito o documento, los sellos contienen la copia en relieve de la firma autógrafa, los sellos pueden ser metálicos, de goma o de plástico. Se ocupan para estampar copias de la correspondencia (el original va firmado), se recurre a este método para ahorrar tiempo.⁵

Máquina de firma: su verdadero nombre es pantógrafo, son máquinas que, con un engranaje y palancas, acciona una serie de plumas que siguen el trazo original y estampan en varios documentos a la vez la firma autógrafa, haciéndolo como la escribe la persona que la usa. En el país esta máquina no se conoce mucho y no se utilizó.⁶

1.2.3 Firma Digital-Firma Electrónica

A) Firma Digital: La Firma Digital “es un mecanismo criptográfico que permite verificar la autenticidad e integridad de ciertos datos, permite al receptor determinar la entidad originadora de dicho mensaje, aplicando la autenticación y no repudio.”⁷

Otra definición sobre Firma Digital, es una técnica matemática utilizada para validar la autenticidad e integridad de un mensaje, software o documento digital, esta consta de dos claves o secuencias de carácter separadas; consiste en aplicar mecanismos criptográficos al contenido de un mensaje o documento, con el objeto de demostrar al receptor del mensaje que el emisor es real (autenticación), este no puede negar que

⁵ Sarbelio Enrique López Flores, “La Firma Electrónica, Tecnología del Siglo XXI en la Legislación Salvadoreña”, (tesis de grado, optando al título de Licenciatura en Ciencias Jurídicas, Universidad de El Salvador, 2007), 76.

⁶ *Ibíd.* 77

⁷ Andrea Verenice Basante Andrade, Mónica Cecilia Gallegos Varela, Cathy Pamela Guevara Vega, y otros, *Comercio Electrónico*, (Imprenta Universitaria, Universidad Técnica del Norte, Ibarra, Ecuador, 2016), 114-115

envió el mensaje (no repudio) y que el mensaje no ha sido alterado desde su emisión (integridad).⁸

B) Firma Electrónica: La página del Ministerio de Economía de preguntas y respuestas sobre la firma electrónica da una definición de ella, La Firma Electrónica “es una herramienta tecnológica que permite garantizar la autoría íntegra de los documentos electrónicos, posibilitando que estos gocen de una característica que únicamente era propia de los documentos en papel. También, una Firma Electrónica es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje.”⁹

Según el artículo 3 relativo a las definiciones del Reglamento (UE) N° 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, conocido como Reglamento eIDAS, la Firma Electrónica son “los datos en formato electrónico anexos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar”.

Una última definición de Firma Electrónica es la que se encuentra en la Ley E-SIGN Federal de los Estados Unidos, definiéndolo “como un sonido, símbolo o proceso electrónico adjunto a un contrato u otro registro, o lógicamente asociado a este, y ejecutado o adoptado por una persona con la intención de firmar el registro”. Cabe destacar los usos que tiene la firma electrónica, como lo son, contratos, firmar ofertas, autorizaciones, renunciaciones, documentos financieros, etc, estos son legalmente vinculantes

⁸ Leyre Leyre Soto, ¿Qué es una firma digital?, (Blog) Signaturit 18 de agosto de 2020, <https://blog.signaturit.com/es/que-es-una-firma-digital>

⁹ Ministerio de Economía de El Salvador, Preguntas y Respuestas, ¿Qué es la Firma Electrónica?, acceso el 26 de octubre de 2020, <https://firmaelectronica.minec.gob.sv/about/faqs/>

en la gran mayoría de transacciones ya sean personales o empresariales en prácticamente todos los países.¹⁰

La Firma Electrónica se clasifica en dos tipos, Firma Electrónica Simple y Certificada, que la Ley de Firma Electrónica en su artículo 3 las define así.

Firma Electrónica Simple: “Son los datos en forma electrónica, consignados en un mensaje de datos o lógicamente asociados al mismo, que pueden 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.”

Firma Electrónica Certificada: “Son datos en forma electrónica, consignadas en un mensaje de datos o lógicamente asociados al mismo, que permiten la identificación del signatario, y que los datos de creación de la firma se encuentran en exclusivo control del signatario, lo que permite que sea detectable cualquier modificación ulterior al contenido del mensaje de datos.”

1.3 Características de la Firma

1.3.1 Según el modo en que se emplea la firma

- a. **Identificativa:** sirve para identificar quién es el autor del documento, esto se hace a través de la firma que la persona estampa.
- b. **Declarativa:** es la elevación del contenido del documento por el autor de la firma, se trata más que todo de la conclusión de un contrato. La firma representa la voluntad de obligarse.
- c. **Probatoria:** se puede identificar si el autor de la firma es la persona que ha sido identificada en el acto de la propia.

¹⁰ Ley ESIGN, (Estados Unidos de América: Congreso de los Estados Unidos, 2000)

1.3.2 Según el fin de la firma

- a. **Consentimiento:** con la firma se expresa el consentimiento de lo que se plasma en el documento y la intención que se tiene de asignarle efectos jurídicos.
- b. **Solemnidad:** requisitos que exige la ley para ciertos actos y que estos tengan validez jurídica.
- c. **Prueba:** la firma sirve como medio de prueba de que se han realizado ciertos actos jurídicos y si se da algún litigio sirva como medio probatorio, el cual está establecido en la legislación salvadoreña.
- d. **Forma:** sirve como requisitos de la exteriorización de la voluntad a través de la firma.¹¹

1.4 Elementos de la Firma

1.4.1 Elementos Formales

Los elementos formales son elementos materiales de la firma, estos están relacionados con los procedimientos utilizados para firmar y el diseño mismo de la firma.

- a) **La firma como signo personal:** la firma es presentada como un signo muy distintivo y personal, esto se debe a que se pone por el propio puño y letra del firmante, individualizando a cada sujeto con ella.
- b) **El animus signandi:** se refiere al elemento intencional o intelectual de la firma, es la voluntad de asumir el contenido de un documento, (no es igual a la voluntad de contratar), es decir, la firma es el resultado de la expresión de voluntad de una persona.

¹¹ Apollonio Martínez Nadal, *Comercio Electrónico, firma digital y autoridades de Certificación*, (Editorial Civitas, 3era ed. Madrid, España, 2001), 368-369

1.4.2 Elementos Funcionales

Teniendo en cuenta la noción de la firma como el signo o conjunto de signos se pueden distinguir dos funciones.

- a) **Identificadora:** con la firma se asegura la relación jurídica entre el acto firmado y la persona que lo ha firmado, se expresa la identidad, aceptación y autoría del firmante.
- b) **Autenticación:** el autor de la firma expresa el consentimiento y hace propio el mensaje dándole autoría al documento.

1.5. Evolución Nacional e Internacional de la Firma Electrónica

1.5.1. Primeros países en implementar la Firma Electrónica

En este punto se abordarán los países más importantes en cada región o continente en implementar la Firma Electrónica, detallando el país, la o las leyes emitidas, fecha de publicación y datos relevantes o importantes acerca de la ley o del país respecto a la Firma Electrónica.

Primero se tomarán en consideración al continente de América, debido a que es el que mejor se conoce por pertenecer a él.

América			
País	Ley o leyes	Publicación	Datos importantes
Estados Unidos	Uniform Electronic Transactions Act.	Aprobada el 23-30/07/1999, desde esta fecha se recomienda su sanción en	Denominada la Ley Uniforme de Transacciones Electrónicas, que fue vista en la Conferencia Nacional de Comisiones sobre Leyes Estatales Uniformes. ¹²

¹² Uniform Electronic Transactions Act. (Estados Unidos de América: Congreso de los Estados Unidos, 1999)

		todos los estados.	
	Electronic Signatures in Global and National Commerce Act. o Ley ESIGN.	Publicada el 30/06/2000.	Forma parte del Código de los Estados Unidos y es la Ley de Firma Electrónica en el Comercio Nacional y Mundial, la parte importantes es el título 15 del comercio, capítulo 96, Firma Electrónica en el Comercio Nacional y Mundial, arts. 7001-7031. ¹³
	Electronic Code of Federal Regulations.	Datos actualizados hasta 05/11/2020.	El Código Electrónico de Regulaciones Federales, el título 17, Bolsa de Comercio y Mercado de Valores, capítulo I, Comisión de Comercio en futuros sobre mercancías, parte 1, Reglamentación General de la Bolsa de Comercio, art. 1.4, firmas electrónicas, reconocimientos y verificaciones.
México	Código de Comercio.	Publicado del 7-13/10/1889. Última reforma publicada 28/03/2018.	Se encuentra en el libro segundo, del comercio en general, título segundo, de comercio electrónico, cap. I, de los mensajes de datos,

¹³ Ley ESIGN, (Estados Unidos de América: Congreso de los Estados Unidos, 2000)

			capítulo I Bis, de la digitalización, cap. II, de las firmas, cap. III, de los prestadores de servicios de certificación.
	Ley de Firma Electrónica Avanzada.	Sancionada el 24/11/2011. Promulgada 06/01/2012. Publicada el 11/01/2012.	Se pasa de la Firma Electrónica Simple que estaba regulada en el Código de Comercio a la Firma Electrónica Avanzada con esta nueva ley. ¹⁴
	Reglamento de la Ley de Firma Electrónica Avanzada.	Sancionada el 19/03/2014. Publicada el 21/03/2014.	Con este reglamento se establecen las normas para el uso de la firma electrónica avanzada, los servicios de ella y su homologación con otras firmas avanzadas. ¹⁵
El Salvador	Ley de Firma Electrónica.	Emitida el 26/10/2015. Entrada en vigencia, 180 días después de publicada en el Diario Oficial.	Esta Ley fue la primera en el país en relación a la Firma Electrónica, aunque no ha tenido mucha importancia hasta el momento porque no se cuenta con certificadoras nacionales. ¹⁶
	Reglamento de	Emitida el	Tal como lo establece la ley,

¹⁴ Ley de Firma Electrónica Avanzada, (México: Congreso General de México, 2011)

¹⁵ Reglamento de la Ley de Firma Electrónica Avanzada, (México: Congreso General de México, 2014)

¹⁶ Ley de Firma Electrónica, (El Salvador: Asamblea Legislativa de El Salvador, 2015)

	la Ley de Firma Electrónica.	24/10/2016. Entra en vigencia, 8 días después de ser publicada en el Diario Oficial.	se creó un reglamento para que pudiera regular instituciones y a las certificadoras. ¹⁷
Costa Rica	Ley 8454, Ley de Certificados, Firmas Digitales y Documentos Electrónicos.	Emitida el 22/08/2005. Publicada el 13/10/2005.	Se da la ley gracias a que se presenta el 29/02/2002 un Proyecto de Ley ante la Asamblea Legislativa, se tramitó como expediente 14.276.
	Reglamento de la Ley 8454, Reglamento de la Ley de Certificados, Firmas Digitales y Documentos Electrónicos.	Emitida el 20/03/2006 Publicado el 21/04/2006.	En la ley en su art. 33 hace referencia a la creación del Reglamento. Se tocan puntos como las jerarquías de la certificación nacional, lineamientos técnicos que deben cumplir los certificadoros. ¹⁸
Panamá	Ley N° 51.	Del 22/07/2008. Publicada el jueves 24/07/2008.	Esta ley es concerniente a la materia de comercio electrónico y almacenamiento

¹⁷ Reglamento de la Ley de Firma Electrónica, (El Salvador: Asamblea Legislativa de El Salvador, 2016)

¹⁸ Ley 8454, Ley de Certificados, Firmas Digitales y Documentos Electrónicos, (Costa Rica: Asamblea Legislativa de Costa Rica, 2005)

			tecnológico de documentos. ¹⁹
	Ley N° 82.	Aprobada el 29/10/2012. Publicada el 09/11/2012	Con ella se otorga al Registro Público de Panamá atribuciones de autoridad registradora y certificadora raíz de firma electrónica. ²⁰
	Decreto Ejecutivo 684.	Del 18/10/2013. Publicado el 23/10/2013.	Reglamenta la Ley N° 51 y la Ley N° 82, será aplicado y obligatorio para particulares, servidores públicos, prestadores de servicios de certificación y la Dirección Nacional de Firma Electrónica del Registro Público de Panamá.
	Resolución N° DG-125-2013.	Del 06/11/2013. Publicada el 12/11/2013.	Es el Reglamento Técnico N° 1 de la Dirección Nacional de Firma Electrónica, lo deben cumplir los prestadores de servicios de certificación con el Gobierno Central, Autónomas, Semiautónomas, municipios y notarias.
Colombia	Ley N° 527.	Sancionada y promulgada 21/08/1999.	En ella se define y reglamenta el acceso y el uso de los mensajes de datos, del

¹⁹ Ley N° 51, (Panamá: Asamblea Nacional de Panamá, 2008)

²⁰ Ley N° 82, (Panamá: Asamblea Nacional de Panamá, 2012)

		Publicada el 21/08/1999.	comercio electrónico y de las firmas digitales, también se establecen las entidades de certificación. ²¹
	Decreto N° 2364.	Sancionado 22/10/2012.	En el decreto se reglamenta el artículo 7 de la Ley N°527 de 1999, sobre la firma electrónica y se dictan otras disposiciones. ²²
Argentina	Ley de Firma Digital 25.506	Sancionada el 14/11/2001. Promulgada de hecho el 11/12/2001. Entró en vigor en 2007.	Argentina fue de los primeros países en Latinoamérica en tener Ley de Firma Electrónica. En su art. 48 dice que le da un plazo máximo de años desde su vigencia para que se aplique la ley, la firma electrónica en todas las normativas del art. 8 de la Ley 24.156, además esta ley sigue el modelo de la CNUDMI sobre Firmas Electrónicas. ²³
	Decisiones Administrativas 927/2014. Certificaciones	Aprobada el 03/11/2014.	En 2014 se amplía el uso de la firma electrónica por esta decisión administrativa y se le va a dar una mayor

²¹ Ley N° 527, (Colombia: Congreso de la República de Colombia, 1999)

²² Ley N° 2364, ((Colombia: Congreso de la República de Colombia, 2012)

²³ Ley de Firma Digital 25.506, (Argentina: Congreso de la Nación Argentina, 2001)

	Digitales. Políticas, contenidos, requisitos y formularios.		aplicación, se puede usar para actividades privadas, se reglamenta el sello de tiempo, certificados de competencia y de aplicaciones.
	Sección 1197 del Código Civil Argentino.	Promulgación, el 29/09/1869. En vigor, 01/01/1871. Derogación del Código Civil por el Código Civil y Comercial de la Nación, aprobado por ley 26.994, Promulgado según decreto 1795/2014, del 2015.	Dice que “cuando las partes están de acuerdo en que aceptarán firmas electrónicas como válidas y que no van a cuestionar su validez, el acuerdo que tomen es legalmente vinculante.
	Decreto 892/2017.	El decreto fue creado el 01/11/2017. Sancionado el 02/11/2017.	Con este decreto se regula la Firma Digital Remota. ²⁴

El segundo continente a tomar en cuenta será Europa, acá es donde ha tenido un mayor impacto, regulación y avance.

²⁴ Decreto 892/2017, (Argentina: Congreso de la Nación Argentina, 2017)

Europa			
País	Ley o leyes	Publicación	Datos importantes
Alemania	German Signature Law of 2001.	Del 2001.	Cambiada en el año de 2005. ²⁵
España	Ley 59/2003, de 19 de diciembre, de Firma Electrónica.	Publicación, 20/12/2003. Entra en vigor el 20/03/2004.	Su última actualización es del 23/09/2020. ²⁶
	Real Decreto N° 1553/2005	Realizado el 23/12/2005. Publicado el 24/12/2005	Su última modificación fue el 30/05/2015, en él se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
Reino Unido de Gran Bretaña e Irlanda del Norte	Electronic Communications Act 2000	Publicada el 25/05/2000	Esta ley tiene disposiciones para regular la prestación de servicios criptográficos en el Reino Unido y le da legalidad a la Firma Electrónica; se actualizó en enero de 2016. ²⁷
	Statutory Instruments 2002 N° 318 o	Se hace el 13/02/2002. Se presenta	La última actualización que se hizo fue en octubre de 2015 y se derogó el

²⁵ German Signature Law of 2001, (Alemania: Bundesrat, 2001)

²⁶ Ley 59/2003, de 19 de diciembre, de firma electrónica, (España: Congreso de los Diputados, 2003)

²⁷ Electronic Communications Act. 2000, (Reino Unido: Parlamento de Westminster, 2000)

	The Electronic Signatures Regulations 2002	ante el Parlamento el 14/02/2002. Entra en vigor el 08/03/2002	22/07/2016.
--	--	---	-------------

Pasando a otro continente se encuentra Asia, un continente con países muy desarrollados y potencias en el campo tecnológico.

Asia			
País	Ley o leyes	Publicación	Datos importantes
China	Ley de Firma Electrónica.	Aprobada en agosto de 2004. Entra en vigencia el 01/04/2005	Su creación se dio durante la onceava reunión del Comité Permanente de la Asamblea Popular de China. Tendrá la misma validez que la firma manuscrita y será avalada por un certificador. ²⁸
Japón	La Concerning Electronic Signatures and Certification Services.	Creada el 24/05/2000. Publicada el 01/04/2001.	Con la ley se busca el uso de métodos electrónicos y el uso de la firma electrónica en diferentes áreas, para el desarrollo del país. ²⁹

Tomando en consideración a Oceanía, se tendrá dos de los países más desarrollados de esa región para ponerse como referencia.

²⁸ Ley de Firma Electrónica, (China: Congreso Nacional del Pueblo, 2004)

²⁹ Concerning Electronic Signatures and Certification Services, (Japón: La Cámara de Representantes, 2000)

Oceanía			
País	Ley o leyes	Publicación	Datos importantes
Australia	Ley de Transacciones Electrónicas.	Del año 1999.	Con la ley se da paso a la modernización y uso de recursos electrónicos en el país. ³⁰

Para finalizar con los continentes, está África, con un país como referencia, siendo Sudáfrica el más desarrollado de la región.

África			
País	Ley o leyes	Publicación	Datos importantes
Sudáfrica	Electronic Communications and Transactions Act, 2002.	Creada el 31/07/2002.	Con la ley se busca regular las transacciones y comunicaciones electrónicas e implementar el uso de gobierno electrónico. ³¹

Como punto extra están dos Organizaciones muy importantes a nivel Internacional como lo son las Naciones Unidas y la Unión Europea.

Organizaciones			
Organizaciones	Ley o Leyes	Publicación	Datos importantes
Naciones Unidas	Ley Modelo de la CNUDMI sobre	Aprobada el 12/12/2001.	Dada por la comisión de las Naciones Unidas para el

³⁰ Ley de Transacciones Electrónicas, (Australia: Parlamento de Australia, 1999)

³¹ Electronic Communications and Transactions Act. 2002, (Sudáfrica: Parlamento de Sudáfrica, 2002)

	Firmas Electrónicas con la Guía para su incorporación al derecho interno, 2001.	Publicación, New York, 2002.	Derecho Mercantil Internacional.
	Ley Modelo de la CNUDMI sobre las Firmas Electrónicas. 2001, (Situación Actual).	Adoptada el 05/07/2001.	Busca hacer posible y fácil el uso de la firma electrónica, dando criterios de fiabilidad técnicos.
	Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales.	New York 2007.	Con el Convenio se busca la comunicación electrónica entre las partes contratantes de distintos Estados.
Unión Europea	Directiva 1999/93/CE	Del 13/10/1999.	El fin que busca la Directiva es darle un uso a la firma electrónica y que sea reconocida jurídicamente. Fue derogada el 01/07/2016.
	Directiva N° 2006/123/CE.	Es del 12/12/2006	La Directiva trata sobre los prestadores de servicios en lo relativo a la firma electrónic.

	Decisión de la Comisión N° 2011/130/UE.	Del 25/02/2011.	Se busca que entre los Estados miembros pueda haber un tráfico de documentos firmados electrónicamente.
	Reglamento (UE) N° 910/2014.	Del 23/07/2014. Publicado el 28/08/2014.	Este Reglamento deroga a la Directiva 1999/93/CE. En él se ve la identificación electrónica y los servicios de confianza para transacciones electrónicas en el mercado interior.

1.5.2 La Firma Electrónica en El Salvador

En El Salvador hasta hace unos años ha cobrado relevancia e impacto la firma electrónica, no fue hasta el 2015, para ser más exactos el 1 de octubre de ese año la Asamblea Legislativa aprueba la Ley de Firma Electrónica, la ley es adoptada luego de siete años de haber presentado la primera idea para que se creara.

El Salvador se estaba quedando muy atrás en los avances tecnológico-legales, nuestro país era el único en la región Centroamericana, y de los siete países que restaban en toda Latinoamérica y el Caribe en no contar con la regulación en este tema.

Algo muy importante que se debe resaltar, es que desde el momento en que se aprueba la ley se ha visto poco avance en la implementación de la firma electrónica, si bien es cierto ya existía la ley y luego se crearía un reglamento al siguiente año (2016), pero seguía sin existir más que lo

teórico, hasta el momento no hay certificadoras de documentos ni de almacenamiento, esto repercute en que no se puede dar paso a implementar, también que en el país no se cuenta aún no con una ley de Protección de Datos Personales, con ella se podría dar una mayor seguridad a las transacciones y brindar seguridad jurídica a los usuarios.

Es por ello que los retos a superar son la creación e implementación de esas leyes, darle la total facultad a la Unidad de Firma Electrónica, mayor presupuesto, capacitación técnica y legal, definir a los entes certificadores si serán público, privados o de ambos sectores para brindar el servicio de firma electrónica.

1.6 Principios de la Firma Electrónica

Los Principios Generales de la Firma Electrónica se encuentran establecidos en el artículo 4 de nuestra Ley de Firma Electrónica, estos son:

1.6.1 Principio de Autenticidad

Este principio garantiza que el mensaje es confiable y que va a perdurar en el tiempo.

Para dar cumplimiento a este principio la ley de Firma Electrónica, en el artículo 14 brinda las garantías mínimas que debe de cumplir el Sistema de Almacenamiento de Documentos Electrónicos para que los mensajes sean confiables y perduren en el tiempo. Manifiesta que el almacenamiento debe de ser nítido, seguro y con absoluta fidelidad de igual forma garantiza que el documento o mensaje puede ser recuperado en cualquier momento.

1.6.2 Principio de Integridad

Con él se le da certeza a los datos que se reciben por los diferentes medios electrónicos y que estos no se han modificado en su trayecto, desde el

iniciador (quien envía el mensaje de datos) hasta el destinatario (quien recibe el mensaje de datos).

En primer lugar, el destinatario debe verificar que el mensaje ha sido enviado por el iniciador o por su representante con la respectiva firma electrónica certificada, es importante mencionar que este mensaje debe de ser enviado por medio de un sistema de información debidamente autorizado por el iniciador. Artículo 19 Ley de Firma Electrónica.

Otra forma de dar certeza a los datos tanto enviados como recibidos es el acuse de recibo, este debe de ser solicitado por el iniciador o acordado entre el iniciador y el destinatario, se deberá acordar una forma o método para efectuarlo. Artículo 22 Ley de Firma Electrónica.

1.6.3 Principio de Confidencialidad

Con este principio se le da garantía a quien envía el mensaje (iniciador) y a quien lo recibe (destinatario) que el o los mensajes electrónicos enviados no se conocerán por terceras personas sin que ellos lo autoricen de forma expresa.

Este principio es una total responsabilidad y obligación de los prestadores de servicios de certificación y de los prestadores de servicios de almacenamientos, específicamente del que realice el registro de los datos y todas aquellas personas que intervengan en el proceso, incluso esta obligación persiste después de haber terminado las relaciones con el responsable del registro de datos, artículo 5 literal c) de la Ley de Firma Electrónica.

1.6.4 Principio de equivalencia funcional

Los documentos archivados y los comunicados que se hacen de forma electrónica los verifican, para determinar si cumplen con los requisitos que se exigen en los documentos que se presentan en papel y por escrito, con la finalidad de establecer si satisface los objetivos y funciones estipuladas con ellos.

La equivalencia funcional es una forma de agilizar el manejo de documentos que tienen validez jurídica, debemos destacar que para aplicar este principio el mensaje de datos al ser enviado debe de tener una firma electrónica certificada.

En palabras sencillas, los documentos enviados electrónicamente por medio de un sistema de datos con su respectiva firma certificada, tendrán la misma validez jurídica que aquellos que han sido emitidos de la manera común, es decir, físicamente. Artículo 7 Ley de Firma Electrónica. A toda regla general le existe una excepción, no podrá realizarse el procedimiento anterior con todos aquellos documentos que por exigencia de ley deban contener en ellos solemnidades.

1.6.5 Principio de No Repudio o No Repudiación

Con este principio se garantiza que, al suscribirse un mensaje con firma electrónica certificada, el mensaje no podrá ser repudiado, es decir, no se puede repudiar su autoría por quien envió el mensaje o el iniciador.

Al momento de adquirir una firma electrónica, el prestador de servicios está en la obligación de brindar al usuario un certificado electrónico, con los requisitos establecidos en el artículo 58 de la Ley de firma electrónica, ya que con dicho certificado se garantiza la autoría de la firma electrónica certificada, así como también la autenticidad, integridad, confidencialidad y la no repudiación del documento electrónico enviado, es decir que el

iniciador no puede en ningún alegar que el mensaje no fue enviado por él.
Artículo 57 ley de firma electrónica.

1.6.6 Principio de Neutralidad Tecnológica

Este principio hace referencia a que no se van a discriminar a las diferentes tecnologías, siempre y cuando estas sean seguras y se pueda transferir mensajes a través de ellas con el cumplimiento de las leyes y los estándares establecidos de la firma electrónica.

1.6.7 Principio de Seguridad

Gracias a este principio se puede dar certeza y legalidad que la persona que firma (firmante) y que está debidamente acreditada, se ha podido identificar correctamente, pudiendo así garantizar la integridad, disponibilidad, autenticación, confidencialidad, no repudio y el buen uso de la información que se encuentra en un sistema informático muy seguro.

Este último principio hace relación a todos los anteriores, garantizando a su vez una integridad en los principios y seguridad en los sistemas informáticos, que son la base para la firma electrónica y su buen funcionamiento para el traslado o tráfico de datos a través de los usuarios.³²

1.7 Ventajas y Desventajas de la Firma Electrónica

1.7.1 Ventajas de la Firma Electrónica

Ahorro en tiempo y costes: En este sentido como se puede reflejar en la firma electrónica es que existen dos puntos de vista y uno de los principales beneficios que trae consigo es la optimización de tiempo ya que no es necesario archivar papeles o documentar archivos, el proceso es inmediato, por lo que antes un proceso podría demorar días ahora el

³² Ley de Firma Electrónica (El Salvador, Asamblea Legislativa de El Salvador, 2015) artículo 4

procedimiento online tarda unos cuantos minutos siendo de forma rápida al usuario y como segundo punto e importante también es en el ahorro de gastos, además de ser mínimos, se compensan rápidamente. Es por ello que estas dos características fundamentales e interesantes que trae la firma electrónica lo llevan a ser innovadora en la implementación de empresas.

Se evitan posibles errores: Este beneficio es muy importante para la firma electrónica porque está diseñada para que en la automatización del proceso y en su transcurso este tenga una garantía en la cual no se producirá ningún fallo en ningún momento por lo que hay una gran mejora en el nivel de servicio que este presenta, mejorando también el nivel de satisfacción. Habitualmente estos fallos o inconvenientes se generan en los procesos de forma manual pero, en este caso, la firma electrónica tiene una ventaja sobresaliente para que el usuario sienta seguridad de que no habrá falla alguna al momento de la implementación.

Mejora nuestra imagen: De los usuarios que ya usan la firma electrónica denotan que están actualizados y que se han incorporado al ritmo de la tecnología e innovación de la misma. Para los empresarios este es un punto que deben tomar en cuenta en sus empresas para estar al ritmo con las nuevas tecnologías para generar un mayor impacto.

Disponibilidad inmediata: La accesibilidad y compatibilidad que tiene la firma electrónica es impresionante porque se puede acceder desde cualquier dispositivo de forma que se puede utilizar en cualquier momento y lugar utilizándose así de manera instantánea e inmediata.

Ecológica: Con el tema de la sostenibilidad la firma electrónica aporta su granito de arena al planeta aportando a reducir el consumo de papel y a reducir la contaminación producida por los desplazamientos in situ.

Se facilita la autenticación: Y como último punto que se valora sobre la

firma electrónica es la facilitación de la autenticación, esto afecta positivamente a la profesión y también al usuario.³³

1.7.2 Desventajas de la Firma Electrónica

Puede ser hackeada: Como podría llegar a suceder, en el ámbito tecnológico puede existir un riesgo a que la plataforma sea hackeada; pero la probabilidad es el mínimo si de igual forma los usuarios son responsables, la posibilidad sería muy baja ante este riesgo, por lo que tenemos que asegurarnos siempre que los Certificados que se reciben tienen que ser enviados por un organismo confiable y seguro y sobre todo que las claves de seguridad estén convenientemente bien guardadas. Teniendo en cuenta este factor realmente importante, la plataforma se encontrará segura y así mismo se evitarán problemas a futuro.³⁴

Como se ha mostrado a lo largo del capítulo, se puede desarrollar, conceptualizar y conocer la historia de la firma electrónica, junto con sus clasificaciones, principios, ventajas y desventajas, etc. hasta llegar a la era digital, pasando por grandes avances tecnológicos, es por ello, que en el siguiente capítulo se desarrollará el funcionamiento y uso de la firma electrónica, adentrándonos en temas referidos más al ámbito informático o de sistemas, con el fin de comprender y guiar al manejo de la firma electrónica.

³³ Elizabeth Urrego, Maribel Vargas Aguirre, Verónica Chica Echavarría, "Propuesta de Implementación de la Firma Digital para la Cooperativa CCOPSERP", (tesis de grado, para optar a la licenciatura en Ciencias Económicas y Administrativas, Universidad de Medellín, 2011), 46

³⁴ *Ibíd.*

CAPÍTULO II:

FUNCIONAMIENTO Y USO DE LA FIRMA ELECTRÓNICA

En el presente capítulo, se abordarán los diferentes mecanismos criptográficos en cuanto al uso y funcionamiento de la firma electrónica, junto con los principios y las ventajas y desventajas que ésta pueda llegar a tener, con el propósito de conocer su validez jurídica y ámbito de aplicación.

2.1 Criptografía

En este acápite se desarrollarán diversas definiciones de la criptografía, para familiarizar, cómo la criptografía y sus clasificaciones influyen en el uso y funcionamiento de la firma electrónica.

La criptografía se define como, “técnica utilizada para cifrar mensajes que contienen información, la palabra proviene del griego “Kryptos y Graphein”, que significa “escondido y escritura”, denominado también, escritura secreta, ya que el cifrado supone un grado de secretitud para evitar el descifrado por personas ajenas a los receptores originales del mensaje.

La criptografía es parte de la criptología (del griego Kryptos = oculto y Logos = ciencia o estudio); la otra parte de la criptografía es el criptoanálisis, que tiene como objeto el descifrado de la información procesada por algún criptosistema, es decir, que se encuentre cifrada”.³⁵

Criptografía se puede decir que “es el arte de escribir algo que no se puede entender, a menos que tenga una palabra clave. También se puede decir que es, el mensaje cifrado, en sí, está a la vista. Se puede leer, pero su

³⁵ Johnny Antonio Pabón Cadavid, “La Criptografía y la Protección a la Información Digital”, Revista la Propiedad Inmaterial, n. 14 (2010): 59

significado está oculto. La criptografía se usa en la computación para mandar secretos de una computadora a otra, algunos de los componentes básicos de ella son, mensaje en claro, clave, algoritmo, cifrar, mensaje cifrado y descifrar”.³⁶

Según la Real Academia Española (RAE), Criptografía es el “arte de escribir con clave secreta o de un modo enigmático”.³⁷

“La Criptografía, como arte de enviar mensajes en clave secreta o de modo enigmático, históricamente ha consistido en sustituir las letras por guarismos, a los que se le asigna un orden o valor convencional, sustituir las letras por otras letras, alterando su valor, sustituir las letras por signos (musicales, algebraicos, etc.), sustituir las letras por signos arbitrarios, sustituir las letras de un idioma por caracteres propios de otra, o sustituir las letras sencillas por grupos de letras. O alterar el orden de los signos o letras que componen el mensaje. Actualmente son complejos algoritmos matemáticos implementados en la más sofisticada tecnología.”³⁸

2.2. Tipos de Cifrado Criptográfico

2.2.1. Criptografía de llave privada o simétrica

“Se refiere al conjunto de métodos que permiten tener una comunicación segura entre emisor y receptor, siempre y cuando con anticipación se hayan intercambiado la clave que es llamada clave simétrica.

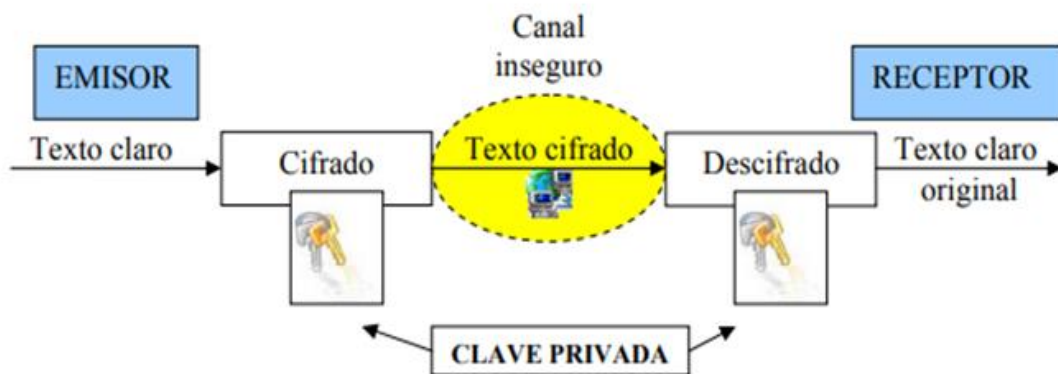
³⁶ Joan Corominas, *Breve Diccionario Etimológico de la Lengua Castellana*, (Editorial Gredos, Madrid, tercera edición muy revisada y mejorada, 1987), 179

³⁷ Real Academia Española, *Diccionario de la Real Academia Española* RAE, (vigésimo tercera edición, 2014), definición de criptografía

³⁸ Andrea Verence Basantes Andrade, Mónica Cecilia Gallegos Varela, Cathy Pamela Guevara Vega, Alexandra Elizabeth Jácome Ortega, *Comercio Electrónico*, (Ibarra - Ecuador: Imprenta Universitaria, 2016), 114

Es denominado cifrado simétrico, porque utiliza la misma clave para cifrar y descifrar un mensaje. Se conoce también como cifrado de clave privada.”³⁹

A continuación, se presenta el siguiente esquema detallando cómo se envía y cifra un mensaje utilizando la llave privada o simétrica:



Dentro de las características que se pueden tomar en cuenta en las llaves privadas o simétricas serían:

- Existe solo una llave privada por individuo o usuario, quiere decir que es única, por ello debe cuidarse, recordarla o no extraviarla.
- Su uso es únicamente por parte del propietario, lo recomendable es que solo el propietario de la llave la use, excepcionalmente la puede usar otra persona, esto se da con la debida autorización cuando son empresas, que un apoderado tiene el uso de la llave.
- La llave es secreta, dependiendo del tipo de llave que sea, estas son secretas y por esa razón solo el propietario debe saberla y utilizarla.

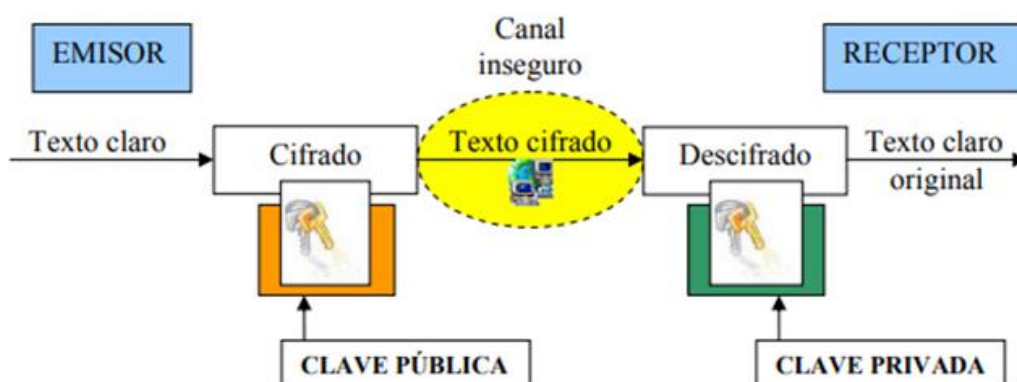
³⁹ Constanza Alejandra Rioseco San Martín, “Introducción a la Criptografía”, (memoria para optar al título de profesor de enseñanza media en educación matemática, Universidad del Bío-Bío, 2016), 59

- Su uso es poder descifrar la información enviada y generar de esa forma firmas.⁴⁰

2.2.2. Criptografía de llave pública o asimétrica

“Este cifrado se caracteriza por utilizar dos claves diferentes para el emisor y receptor, entonces para cifrar el mensaje se necesita una clave pública y para descifrar mensajes una clave privada. Nace con la finalidad de buscar métodos más prácticos para intercambiar claves simétricas”.⁴¹

A continuación, se presenta el siguiente esquema detallando cómo se envía y cifra un mensaje utilizando la llave pública o asimétrica:



Las características a destacar del sistema criptográfico de llave pública o asimétrica son las siguientes:

- El usuario solo puede poseer una llave pública.
- Su uso es encriptar la información que se desea y con ella poder generar firmas electrónicas certificadas, pasar a su vez del papel a otro método más seguro de resguardo, ahorro y cuidado del medio ambiente.

⁴⁰ Sarbelio Enrique López Flores, “La Firma Electrónica, Tecnología del Siglo XXI en la Legislación Salvadoreña”, (tesis de grado, optando al título de Licenciatura en Ciencias Jurídicas, Universidad de El Salvador, 2007), 88.

⁴¹ Constanza Alejandra Rioseco San Martín, “Introducción a la Criptografía”, (memoria para optar al título de profesor de enseñanza media en educación matemática, Universidad del Bío-Bío, 2016), 62

- La llave se pone a disposición de todos los usuarios, con el fin que todos puedan acceder a ella.
- La llave privada es de uso único y exclusivo del usuario.⁴²

2.3. Certificados Digitales

Antes de hablar de los Entes Certificadores hay que establecer qué es un Certificado Digital y así entender la importancia y función de las Certificadoras, “un Certificado Digital es un archivo electrónico que tiene un tamaño máximo de 2 Kilobytes y que contiene los datos de identificación personal de A (emisor del mensaje), la clave pública de A y la firma privada del propio Prestador de Servicios de Certificación. Ese archivo electrónico es cifrado por la entidad Prestadora de Servicios de Certificación con la clave privada de ésta”.⁴³

Destacar también que es un Certificado de Firma Electrónica, “es un documento digital mediante el cual la autoridad de certificación asegura la vinculación entre la identidad del usuario, su clave pública y privada”.⁴⁴

Luego de tener una noción de lo que es un certificado digital estableceremos qué información va a contener, siendo datos personales y propios del certificado a emitir, los cuales son:

- Nombre completo y DUI del propietario.
- Clave pública del certificado.
- Número de serie del certificado.
- Fecha de emisión y expiración.
- La Autoridad de Certificación que lo emite.

⁴² Sarbelio Enrique López Flores, “La Firma Electrónica, Tecnología del Siglo XXI en la Legislación Salvadoreña”, (tesis de grado, optando al título de Licenciatura en Ciencias Jurídicas, Universidad de El Salvador, 2007), 94.

⁴³ Jesús Ignacio Fernández Domingo, *La firma electrónica: aspectos de la ley 59/2003, de 19 de diciembre*, (Editorial Reus, Madrid, 2006) 58

⁴⁴ Ley de Firma Electrónica, (El Salvador: Asamblea Legislativa de El Salvador, 2015) art. 3

- Referencia a las políticas asociadas al certificado.
- A quién pertenece (empresa, persona natural o empleado público).

Es de hacer notar, que tal como lo menciona el artículo 59 de la Ley de Firma Electrónica, el certificado tiene un plazo de vigencia, el cual será estipulado entre las partes por mutuo acuerdo, regularmente es de un año de vigencia, pero esto puede variar según la forma en que se custodia el certificado digital.

En cuanto al precio del certificado digital, queda igualmente a discreción de las partes debido a que actualmente en la ley no se encuentra tasado, como parte de la investigación de campo realizada en la Unidad de Firma Electrónica, específicamente el encargado legal de la unidad manifestó que “aún no existe algún proveedor de certificados autoriza”, es por ello que no se puede dar un rango estimado de precio, el único precio que se conoce son las tasas que deben pagar los Proveedores de Certificación y Almacenamiento por la inscripción, la cual tiene un valor de cuatro salarios mínimos mensuales del sector comercio y servicios, en cuanto a la renovación, se cancelarán dos salarios mínimos mensuales del sector comercio y servicios.⁴⁵

2.4. Los Entes Certificadores

Luego de conocer qué son los Certificados Digitales pasaremos a definir qué es una Entidad Certificadora, siendo esta “la encargada de emitir certificados digitales de las solicitudes que cumplan con los requisitos para su obtención. Realiza además funciones de revocación, publicación, almacenamiento y registro de certificados. Se constituye un tercero confiable para las partes involucradas en una transacción electrónica”.⁴⁶

⁴⁵ Ministerio de Economía de El Salvador, Unidad de Firma Electrónica, Tasas de los certificados Digitales, acceso el 10 de febrero <https://firmaelectronica.minec.gob.sv/>

⁴⁶ Jeannie Elizabeth Galán Cortez, Laura Azucena García Mejía, Vilma Verónica Gómez Barahona, “La Firma Digital como medio de seguridad y consentimiento en las

También podemos decir que es, “la persona física o jurídica, pública o privada, que expide, renueva y revoca certificados, pudiendo prestar, además, otros servicios en relación con la firma digital, como la validación de certificados”.⁴⁷

En El Salvador la acreditadora raíz⁴⁸ y el ente competente para controlar, acreditar, registrar, revocar, vigilar, sancionar y multar a los proveedores de certificados electrónicos y de almacenamiento, es la Unidad de Firma Electrónica, luego siguen los entes certificadores que son quienes dan los certificados a los usuarios, esto según la Ley de Firma Electrónica en sus artículos 36 y 37.

2.4.1. Funciones de los Entes Certificadores

- Generan y registran claves, los Entes Certificadores son los encargados de generar y registrar las firmas electrónicas y las claves para los usuarios que requieran a cambio de un pago que será determinado por cada ente.
- Identifican quiénes quieren certificados, los entes necesitan saber quién o quiénes son las personas que van a solicitar o necesitar firma electrónica, sabiendo cómo va avanzando la era tecnológica a nivel mundial y las nuevas herramientas que se necesitan.
- Emiten certificados, al igual que la primera función, los entes Certificadores son los encargados de emitir los certificados digitales

transacciones del Comercio Electrónico”, (tesis de grado, optando al título de Licenciatura en Ciencias Jurídicas, Universidad de El Salvador, 2006), 48

⁴⁷ *Ibíd.* 49

⁴⁸ **Acreditadora raíz:** o también conocida como la Autoridad Certificadora Raíz, es la autoridad de certificación raíz de un país, cuya función principal es habilitar al Prestador de Servicios de Certificación y emitir certificados digitales. (Ministerio de Industria y Comercio, Definición y Acrónimos, 2015, <https://www.acraiz.gov.py/html/preguntFrec-definAcron.html>)

(firmas electrónicas requeridas) por los usuarios, ella dependerá de la función o manejo que le quiera dar el usuario o el rubro para el que quiera ir encaminado, pudiendo ser para documentos como pdf, correos, contratos, etc.

- Mantenimiento de las claves y revocación de las mismas, los entes son los encargados de dar el mantenimiento requerido a los certificados para el flujo constante de datos e información, también ellos pueden revocar los certificados por incumplir la normativa nacional como su normativa interna, llegando a contraer los usuarios sanciones por no dar un uso adecuado a sus certificados.⁴⁹

2.4.2. Tipos de Entes Certificadores

2.4.2.1. Proveedores de Servicios de Certificación Electrónica

Es una persona jurídica autorizada por la autoridad competente, dedicada a emitir certificados electrónicos y demás actividades previstas en la Ley de Firma Electrónica.⁵⁰

Para poder prestar servicios deben cumplir algunos requisitos que están estipulados en el artículo 43 de la Ley de Firma Electrónica, ser personas jurídicas, públicas o privadas, nacionales o extranjeras, debiendo cumplir primero los requisitos para operar en el país y sobre todo, tener la capacidad técnica con la cual se pueda garantizar seguridad y que son fiables los certificados que se emitan, contar a su vez con el personal técnico calificado para solventar alguna falla, contar también con la capacidad estructural (física), equipo adecuado, licencias y estar

⁴⁹ Informática jurídica, La Firma Digital y Entidades de Certificación, acceso el 13 de febrero de 2021, <http://www.informatica-juridica.com/trabajos/la-firma-digital-y-entidades-de-certificacion/#3.1.%20FUNCIONES%20DE%20LAS%20AUTORIDADES%20DE>

⁵⁰ Ministerio de Economía de El Salvador, Definición de los Proveedores de Servicios de Certificación, acceso el 13 de febrero de 2021, <https://firmaelectronica.minec.gob.sv/portfolio-view/video-format/>

financieramente estables para solventar algún imprevisto, además de rendir la fianza establecida por la Unidad de Firma Electrónica en caso de indemnizar a los usuarios por los daños y perjuicios ocasionados. La Unidad de Firma Electrónica evaluará el cumplimiento de los requisitos antes mencionados para poder acreditar o no al proveedor (artículo 15 del Reglamento de la Ley de Firma Electrónica).

Al momento de aprobar los requisitos, el proveedor de servicios de certificación deberá llenar la solicitud para su respectiva acreditación, se le realizará un examen de admisibilidad y de pasar este proceso se dará trámite a su solicitud, la Unidad de Firma Electrónica emitirá el dictamen en relación a la obtención de la acreditación, la resolución de acreditación se publicará y se tendrá un registro de los proveedores autorizados el cual también será publicado en el sitio web del Ministerio de Economía, de esta forma podrá dar inicio a sus actividades, (artículos 18-23 del Reglamento de la Ley de Firma Electrónica).

Resaltar que cumplido todo este proceso los proveedores serán evaluados anualmente para seguir obteniendo su acreditación y seguir funcionando, asimismo, deberán de cumplir con las obligaciones establecidas en el artículo 48 de la Ley de Firma Electrónica, algunas de ellas son,

- Garantizar validez, vigencia, legalidad y seguridad del certificado emitido y las medidas necesarias para que no sea falsificado.
- Verificar la información de sus usuarios, mantener actualizada su información así como de los certificados que se emitan.
- Dar aviso a la Fiscalía General de la República cuando se sospeche o tenga indicios del cometimiento de un delito.
- Renovar la fianza anualmente antes de su vencimiento.

Abonando a los Proveedores de Servicios de Certificados, en el país aún no se cuenta con un Proveedor nacional ni extranjero autorizado, se está a

la espera que en el transcurso del 2021 se comience a autorizar Proveedores nacionales o extranjeros. Algunos proveedores internacionales de certificados digitales son, “e-certchinle, certinet, Seguridata, Uanataca”, entre otras, que pueden llegar a ofrecer sus servicios a nuestro país.

2.4.2.2. Proveedores de Servicios de Almacenamiento de Documentos Electrónicos

Es la persona jurídica autorizada por la autoridad competente que, por la naturaleza de su negocio, brinda servicios de almacenamiento de documentos electrónicos.⁵¹

Al igual que los proveedores de servicios de certificación, los proveedores de servicios de almacenamiento deberán cumplir los requisitos establecidos en el artículo 43 de la Ley de Firma Electrónica, este será evaluado por la Unidad de Firma Electrónica, esto según el artículo 52 de la Ley de Firma Electrónica y el artículo 28 de su respectivo Reglamento. De igual forma que con los prestadores de servicios de certificación se seguirán los mismos pasos para acreditar a los prestadores de servicio de almacenamiento, los cuales están establecidos en los artículos 18 al 23 del Reglamento de la Ley de Firma Electrónica.

Aparte de los requisitos anteriores, deberán cumplir ciertas obligaciones los prestadores de servicios de almacenamiento de documentos electrónicos como, contar con el personal calificado para los servicios de almacenamiento, tener sistemas confiables y protegidos contra cualquier problema, garantizar confianza y protección en la información resguardada,

⁵¹ Ministerio de Economía de El Salvador, Definición de los Proveedores de Servicios de Certificación, acceso el 15 de febrero de 2021, <https://firmaelectronica.minec.gob.sv/portfolio-view/proveedor/>

guardar el documento original por lo menos 10 años y se deberá contar con la declaración de prácticas de almacenamiento de documentos electrónicos que requiere la Ley en su artículo 15 (artículo 54 de la Ley de Firma Electrónica). Se presentan otras obligación, en este caso por parte de los proveedores de almacenamiento electrónico, por mencionar algunas son, cumplir con las políticas, procedimientos de almacenamientos de documentos electrónicos y con lo acordado con los clientes, tener personal capacitado en diferentes áreas (legal, sistemas, informática, administración), informar al cliente de la confidencialidad, límites, responsabilidad y obligaciones que tendrá, garantizar que se preste el servicio de forma ininterrumpida o tener un plan alternativo, tener una línea telefónica para solventar dudas o donde se pueda consultar sobre el servicio prestado (artículo 31 del Reglamento de la Ley de Firma Electrónica).

2.5. Formas en que se custodia un Certificado Digital

El resguardo de cualquier mensaje de datos siempre es de vital importancia para conservarlos y poder acceder a ellos, por esta razón en el campo de la firma electrónica existen diferentes formas de custodiarla, con el fin de tener acceso único y exclusivo, haciendo hincapié en que es necesario custodiarla para que el usuario tenga la seguridad que su documento está protegido y encriptado, de esta forma darle autenticidad e integridad a los mensajes electrónicos, los diferentes medios de custodia son:

a) Token: es un dispositivo criptográfico (en su mayoría de casos tiene forma de una USB y lo posee físicamente el usuario), este resulta ideal para realizar transacciones en las que el usuario por medio de una clave de dígitos como mínimo 8 (PIN Token), con él se puede hacer transacciones en plataformas compatibles según el modelo y versión del sistema operativo. El Token tiene una vigencia de 2 años.

b) Archivo: es un certificado estándar x.509 en formato p12 (significa que puede contener certificados públicos y claves privadas), es perfecto para transacciones masivas, se puede integrar en un servidor o computadora y en cualquier sistema operativo, solo se necesita una clave de acceso y se debe proteger el archivo y las copias que se realicen. Los Archivos tienen una vigencia de 1 año.

c) HSM: según sus siglas es Hardware Security Module, traducido es, Módulo de Seguridad de Hardware. Es un dispositivo criptográfico que genera, almacena y protege claves, siendo ideal para procesar volúmenes altos de transacciones en poco tiempo, un ejemplo puede ser la facturación electrónica. El HSM tiene una vigencia de 3 años.

d) Roaming: Certificado que es almacenado de forma segura en servidores de la ECIBCE, permite realizar operaciones mediante uso de applet que es publicado por ECIBCE o un aplicativo llamado ESP. El Roaming tiene una vigencia de 2 años.⁵²

2.6. Ámbito de aplicación de la Firma Electrónica

2.6.1. Comercio Electrónico

El campo del Comercio Electrónico es el principal nicho para aprovechar todo medio digital o electrónico, en él, las empresas se ven beneficiadas en el rubros económicos, siendo esta una nueva modalidad de percibir ingresos sin muchas dificultades, teniendo horarios mucho más amplios, debido a funcionan las 24 horas del día, casi sin interrupciones, ofreciendo productos, servicios, preventas, ofertas, imágenes y videos detallados de lo que cada empresa realiza, todo esto a costos mucho menores que una

⁵² Certificación Electrónica, Banco Central del Ecuador, Preguntas Frecuentes, acceso el 16 de febrero de 2021, <https://www.eci.bce.ec/preguntas-frecuentes>

tienda física, es por ellos que muchas marcas o empresas buscan posicionarse más en plataformas digitales y ahorrarse el alquiler de un local, de esta forma poder ofrecer más productos y hasta a un mejor precio que su competencia.

Profundizando en otros puntos del Comercio Electrónico, con él se pueden realizar:

- Compra y venta por internet, es lo más común o más conocido que se puede realizar, solo es necesaria una plataforma confiable, un comprador y un vendedor, pactar el artículo a adquirir y pagar el precio, algunos ejemplos son: Amazon, Alibaba, Mercado libre, cualquier comercio que posea una plataforma para realizar o hasta en las redes sociales se puede comercializar.
- Banca electrónica y operaciones en línea, hoy en día la mayoría de bancos (por no decir todos los bancos) tienen plataformas en línea y aplicaciones destinadas a revisar el saldo, realizar pagos de bienes y servicios y a poder hacer transferencias a otras personas, ya sean naturales o jurídicas, sin importar la hora, país y el banco al que se quiera realizar, todo esto por medio de las plataformas de pago online.

Dentro de las plataformas de pago online más importantes y seguras están, PayPal, Google Wallet, Amazon Pay y Dwolla, lo que hacen estas plataformas es conectar a ambas partes de forma online como offline para realizar los pagos y transferencias con mayor seguridad y confianza.

- Factura electrónica, según el art. 6 literal e), de la Ley de Comercio Electrónico, la define así, “es el comprobante electrónico de pago que deberán emitir los proveedores de bienes y servicios usuarios de comercio electrónico a quienes realicen transacciones comerciales con ellos, de conformidad con la legislación pertinente”.

Es un mecanismo que ocupan muchas empresas, les piden el correo a sus clientes para enviarles las facturas, facilitándole la tenencia de facturas, sin necesidad del papel. El sustento legal de la facturación electrónica está en el art. 113 inciso final del Código Tributario y el art. 18 de la Ley de Comercio Electrónico, la factura electrónica tendrá la misma validez contable y tributaria que la factura convencional, cumpliendo con los requisitos y formalidades correspondientes.

En cuanto a la clasificación del comercio electrónico algunas podemos mencionar las siguientes, business to consumers (empresa con consumidores) abreviada B2C, business to business (empresa con empresa) abreviada B2B, business to government (empresa con gobierno) abreviado B2G y consumer to consumer (consumidor con consumidor) abreviada C2C. Estas cuatro son algunas formas en las que se realiza el comercio electrónico a nivel mundial, son de las más conocidas y más usadas, cada una se detallarán con precisión en el siguiente capítulo.

En El Salvador la clasificación que más se usa entre los usuarios para realizar comercio electrónico es de Empresa a Consumidor (Business to Consumer B2C), esta relación se debe a que los consumidores acceden a una plataforma en línea para realizar compras de bienes o servicios.

2.6.2. Gobierno Electrónico

Para entender de lo que estamos hablando, una definición de lo que es Gobierno Electrónico, “El Gobierno Electrónico (e-government) corresponde a todas aquellas iniciativas que implican el uso de las TIC en

la gestión inter-organizacional del Estado e incluye la definición, coordinación, implementación y desarrollo de las políticas públicas”.⁵³

El Gobierno Electrónico implica un gran avance y modernización en un país y en un Gobierno, los ciudadanos pueden realizar todo trámite de forma más fácil, rápida y sencilla, desde la comodidad de sus casas o lugares de trabajo, pueden tener acceso e informarse de los servicios realizados por el Gobierno local y las diferentes instituciones del Estado, velar porque se realice un buen trabajo, un buen manejo de fondos, ver la eficacia, eficiencia y conocer los niveles de transparencia de las instituciones y funcionarios públicos, proyectando así una mayor participación ciudadana y acceso a la información.

Hay que enfatizar las formas en las que se clasifica el Gobierno Electrónico en cuanto a la relación que tiene con los usuarios, estas son cuatro formas, siendo las siguientes, de Gobierno a Ciudadano (Government to Consumer, G2C), de Gobierno a Empresa (Government to Business, G2B), de Gobierno a Empleado (Government to Employee, G2E) y de Gobierno a Gobierno (Government to Government, G2G), cada una de ellas se desarrollaran a fondo en el capítulo siguiente.

2.7. Validez de la Firma Electrónica

La validez de la firma electrónica comienza desde que se aprueba y entra en vigencia la Ley de Firma Electrónica junto con su Reglamento, desde ese momento se dotan de validez jurídica todas las transacciones y actividades de este tipo, dándole así un papel más importante, un mayor desarrollo al comercio electrónico y a la protección de los datos personales.

⁵³ Diego Fernando Cardona Madariaga, *El gobierno electrónico. Una herramienta estratégica de toma de decisiones*, (Univ. Empresa, Bogotá Colombia 2 (3.4.5): 20-45, mayo de 2004), 31

Si bien es cierto, ya existe una Ley de Firma Electrónica y la Ley de Comercio Electrónico, aún falta la aprobación de una ley fundamental (Ley de Protección de Datos Personales) para darle una completa protección a nuestros datos y a las transacciones realizadas de forma electrónica.

Con la entrada en vigencia de la Ley de Firma Electrónica se da paso a otro proceso, en él, se determinan los Entes Certificadores por medio de la Unidad de Firma Electrónica, al estar autorizados los proveedores de servicios de certificación y de almacenamiento podrán crear los certificados digitales, luego seguir con la firma electrónica por medio de los dispositivos de resguardo que el usuario crea más conveniente adquirir.

Cuando los usuarios ya poseen su certificado digital se tendrá que cumplir con ciertos requisitos para que este siga teniendo validez como lo es custodiarlos de forma adecuada, actualizar los datos para darle mayor seguridad, solicitar que se suspenda o revoca su certificado ante alguna vulnerabilidad (artículo 63 Ley de Firma Electrónica), pagar a tiempo el certificado digital para que siga teniendo validez y pueda seguir gozando de las características que posee como seguridad, no repudio, integridad, confidencialidad y autenticidad, entre otras obligaciones de los usuarios.

Con la creación de la Ley de Firma Electrónica se le da validez a la firma de forma electrónica, dando un gran avance, pasando del papel junto con la firma autógrafa a la certificación electrónica de los documentos, proporcionando un ahorro de tiempo y costos, cuidado del medio ambiente, pasar a un gobierno electrónico y dar mayor auge al comercio electrónico, además al crearse una Ley de Protección de Datos Personales poder proteger todos los datos que se resguarden en las diferentes plataformas o cuentas que tengan los usuarios, modernizado así los países y la forma de realizar los trámites a nivel nacional e internacional.

CAPÍTULO III:

PREÁMBULO DEL COMERCIO ELECTRÓNICO Y SU DESARROLLO A NIVEL NACIONAL E INTERNACIONAL

En el desarrollo de este capítulo se expondrá sobre los comienzos del comercio electrónico, adentrándose a la funcionalidad de la firma electrónica en cuanto a los principios, características, ventajas y desventajas, con el fin de conocer los avances que se ha tenido en el país con respecto al ámbito internacional.

3.1. Comercio Electrónico (E-Commerce)

El campo del comercio ha evolucionado desde que llegó el internet, y se ha expandido desde que la mayoría de la población del mundo tiene acceso a él desde su celular. Para entrar más a detalle se define, qué es el “comercio”, etimológicamente, “la palabra comercio viene del latín commercium (compra y venta de mercadería), formada del prefijo con (junto) y la palabra merx (mercancía)”⁵⁴, para la RAE, comercio es la “negociación que se hace comprando y vendiendo o permutando géneros o mercancías”.⁵⁵

Pasando ahora al comercio electrónico, la Oficina de Promoción de la Sociedad de la Información (ISPO) de la Comisión Europea lo define como, “cualquier forma de transacción comercial de bienes y servicios en la cual las partes interactúan de forma electrónica, en lugar de hacerlo a través de intercambios físicos; el comercio electrónico consiste en realizar

⁵⁴ Joan Corominas, *Breve Diccionario Etimológico de la Lengua Castellana*, (Editorial Gredos, Madrid, tercera edición muy revisada y mejorada, 1987), 161

⁵⁵ Real Academia Española, *Diccionario de la Real Academia Española* RAE, (vigésimo tercera edición, 2014), definición de comercio

electrónicamente transacciones comerciales. Está basado en el tratamiento y transmisión electrónica de datos, incluidos textos, imágenes y video”.⁵⁶

A pesar que el comercio electrónico relativamente tiene poco tiempo, ha venido avanzando a grandes pasos, debido a los numerosos avances tecnológicos que se dan, el aumento de usuarios en internet, la facilidad para realizar transacciones de forma online y la necesidad de mantenernos siempre conectados y obtener los productos más nuevos en el mercado, todos estos factores influyen para expandir el mercado en línea y el florecimiento de nuevas empresas y distribuidoras de productos a nivel mundial.

3.2 Ventajas y Desventajas del Comercio Electrónico

3.2.1 Ventajas del Comercio Electrónico

Como hemos visto, el comercio electrónico se puede utilizar en muchos entornos, en las compras, finanzas, industria, etc. Por lo tanto, en el comercio electrónico existen grandes beneficios, siendo algunos: la reducción de trabajo administrativo, transacciones comerciales inmediatas y más precisas y la facilidad en el acceso a la información. A continuación, se presentan las ventajas que proporciona:

Publicidad: en el caso de una página web, permanece como un anuncio constante que ofrece la compañía, en él se tiene fácil acceso mediante la búsqueda del sitio en el navegador y puede actualizarse periódicamente.

Información: provee información actualizada como automatizada de cada producto que se ofrece, incluyendo precios, especificaciones, descripción, fotos, etc. brindando mayor variedad de productos, información completa y garantizada, diferenciándose de los catálogos impresos.

⁵⁶ Andrea Verence Basantes Andrade, Mónica Cecilia Gallegos Varela, Cathy Pamela Guevara Vega, Alexandra Elizabeth Jácome Ortega, Comercio Electrónico, (Ibarra - Ecuador: Imprenta Universitaria, 2016), 19

Marketing: mejora la comercialización del producto, ofreciendo servicios de forma interactiva, las ventas en línea y la empresa proyecta una imagen de vanguardia e innovadora en tecnología, en contraste a las páginas estáticas.

Nuevos Mercados: Da la pauta para abrir nuevas oportunidades a nuevos clientes potenciales a nivel local, nacional e internacional, es decir, dentro del comercio electrónico logra expandir el mercado a nivel global.

Alcance Global: Las nuevas tecnologías permiten que en el comercio electrónico se realicen nuevas transacciones electrónicas, eliminando las fronteras geográficas, ya que el mercado del comercio electrónico, en su mayoría, está conformado por la población a nivel “online”, ofreciendo a los consumidores un nuevo mercado global y brindándole información acorde a sus necesidades, mediante los catálogos de exposición, elaborados con un sistema de acceso para realizar el pedido.

Facilidad de Compra: Permite comprar los artículos desde la comodidad del hogar, trabajo o desde el lugar donde se encuentre, con conexión a internet y recibirlos donde se especifique.

Servicio a Clientes: Todas las dudas, quejas y aclaraciones se verifican y son atendidas de forma efectiva y eficaz, por las plataformas tecnológicas que se pueden incorporar, como, foros, sección de preguntas frecuentes (FAQ), chat en línea (para interactuar con los clientes) y mediante el correo electrónico.

Ventaja Competitiva: los nuevos clientes potenciales comparan más las nuevas y distintas compañías, valorando sus tarjetas de presentación y que esté presente su dirección de Internet. Logrando así una ventaja competitiva por medio de la segmentación de mercados, permitiendo

enfocarse en satisfacer las necesidades de un grupo más selecto de clientes.⁵⁷

3.2.2 Desventajas del Comercio Electrónico

Algunas de las desventajas que presenta el comercio electrónico son:

Reemplazo de la Máquina por el Recurso Humano y el Producto por una Imagen: El trato nunca será el mismo si hablamos de persona a persona, al hablar de persona a máquina, así como la presentación de algún producto, el querer ser atendido y el contacto físico con el artículo, son factores que el cliente pueda sentir diferentes, generen incomodidad y se sienta perdido entre tantos clientes en la plataforma, hasta quizá llegarse a sentir desatendido.

Un medio sin alcance a todo público: Podemos decir que la oportunidad de que una persona, visite, vea, consulte y llegue a comprar en una tienda virtual podría llegar a ser de 2 por cada 10 personas, desafortunadamente en muchos países incluyendo el nuestro, no se cuenta con una estructura económica y ni con la infraestructura tecnológica al alcance de la población, haciéndolo privilegio de pocos y desventaja de muchos; estamos hablando de una herramienta que se encuentra aún en desarrollo y acrecienta la ignorancia entre la gente que no puede ni logra tener la oportunidad de utilizarla, ya que puede verse ajena, desconocida e incluso inalcanzable.

Desconfianza ante los medios electrónicos: Como podemos ver en este caso el número de personas que llega a comprar por internet es aún menor de quien tiene acceso a éste. Esto se debe a que la crisis económica hace dudar del manejo de los hábitos económicos-electrónicos, como el uso de las tarjetas de crédito, para la compra y adquisición de productos y servicios a través de Internet. Muchos potenciales clientes tienen desconfianza de

⁵⁷ *Ibíd*, 27-30

ingresar los dígitos de sus números de tarjeta en alguna página web, en donde se tiene el mito o miedo, que todos pueden llegar a observarlo, provocando que no exista la actividad comercial que reedita los costos de estas aplicaciones.

Las desventajas que podemos observar son en base a la logística comercial y tecnicidades o formas de uso de las diferentes plataformas, en cuanto a lo anterior, se recomienda tener conocimiento previo de lo que se presenta al querer incursionar al comercio electrónico y su respuesta en la gente.⁵⁸

3.3 Características del Comercio Electrónico

Las características principales a destacar del comercio electrónico son:

Difusión: Una de las claves importantes para llegar a los clientes, es primero saber, qué tipo de método utilizar con el tipo de contenido que quieren ver, al tener el objetivo que se pretende alcanzar, se debe buscar el medio idóneo para difundir el contenido o mensaje con que se pretende llegar a los posibles clientes, por las distintas plataformas, canales o medios digitales, es por ello, que también es fundamental tener una buena estrategia de marketing digital.

Espacio Virtual: Este tipo de comercio no necesita de un salón de ventas donde exhibir sus productos, ya que ellos mismos se exhiben en un sitio web, con una cartelera o catálogo virtual, al cual, pueden acceder fácilmente desde un ordenador y conexión a la red; dejando atrás, la renta de un salón.

Alto grado de Automatización: En el campo del comercio electrónico, al momento de utilizar una plataforma, es necesaria la presencia de un

⁵⁸ Víctor Alejandro Zuñiga, "La Actividad Comercial", (tesis de grado, optando al título de Licenciatura en Administración de Empresas, Universidad de las Américas Puebla, México, 2017) 16-17

operador de forma virtual, que actualice los productos, precios, modifique las condiciones de venta, promueva las distintas promociones de compra y realice los envíos. Es por ello que la plataforma cuenta con un alto grado de automatización que genera este tipo de acciones y servicios.

Extensión de los límites geográficos y horarios: Dado que las conexiones de redes electrónicas se encuentran con facilidad y disponibilidad desde el hogar, oficinas, móviles, etc. No es de extrañarse que las compras se efectúen y realicen en cualquier tipo de horario y desde cualquier parte del mundo.⁵⁹

3.4 Elementos del Comercio Electrónico

Los elementos del comercio electrónico son los siguientes:

a) Catálogo de productos-servicios: cuando la tienda virtual tiene un listado de sus productos o servicios, llama la atención del comprador, para llevar a cabo la compra. La lista se presenta en la tienda virtual, la cual debe generar confianza y proyectar profesionalidad hacia sus futuros compradores, esto se puede lograr teniendo la lista en un orden lógico y categórico, que llame la atención por medio de fotografías, videos y explicaciones de los productos y servicios a prestar de una manera clara y precisa.

Una tienda virtual para que sea más llamativa debe de tener un espacio donde los compradores puedan dar su opinión sobre los productos, ayudando a la tienda y que los futuros compradores se guiarán por las opiniones de anteriores clientes y no duden en adquirirlos.

b) Cesta-carrito de la compra: El cesto o carrito ayuda al comprador a crear su propia lista de compras. Al momento de realizar la compra y se

⁵⁹ Andrea Verenice Basante Andrade, Mónica Cecilia Gallegos Varela, Cathy Pamela Guevara Vega, y otros, *Comercio Electrónico*, Características del Comercio Electrónico, (Imprenta Universitaria, Universidad Técnica del Norte, Ibarra, Ecuador, 2016), 25-26

escogen varios productos, el carrito ayuda a ver en forma de lista lo que se va a adquirir, ver el precio, si se debe pagar envío y verificar si agregará o borrará alguno, con la finalidad que el comprador tenga más control de sus compras.

c) Auto-promo y gestión de ofertas: Uno de los elementos fundamentales es hacer visible el precio de los productos o servicios a la hora de realizar la venta, es importante, porque al realizar algún tipo de promoción o descuento, el comprador puede ver cuál era el precio anterior, ver cuál es su descuento y saber cuánto se ahorrará por la promoción. Algo muy importante es ofrecer a los compradores facilidades de pago, por ejemplo, por medio de cuotas con tarjetas de crédito a tasa cero o descuentos con ciertos bancos.

d) Registro de usuarios y panel de control de usuarios: en las tiendas virtuales, antes de realizar la compra se solicita que se llene un registro con datos, como el nombre, correo electrónico, algún documento de identidad, dirección, etc. esto en busca de identificar a los usuarios. El vendedor debe de garantizar al comprador el acceso a sus datos de envío, facturación y el estado de sus pedidos.

e) Proceso de Compra: es importante para el cliente que este procedimiento sea fácil, rápido y nada tedioso, para que no exista la posibilidad de abandonar la compra. Hay que hacerle saber al cliente cuántos pasos debe realizar en su proceso de compra y en cuál se encuentra; la principal información que debe estar en este proceso es, gastos de envío, dirección de entrega, plazos estimados y disponibilidad de productos.

f) Cálculo de costes de envío: el comprador debe tener muy claro cuál será el precio y cómo se calculará, por ejemplo si depende del peso o del volumen, si pagará extra por algún exceso en su paquete.

g) Logística: hay dos tipos de logística, la interna y la externa. Internamente se refiere al procedimiento que realiza la empresa antes de enviar el pedido, como lo es, verificar existencias de productos, emitir facturas o tickets, embalaje etc. y la externa es al momento del envío del pedido, puede ser por medio de una empresa subcontratada.

Agregar también algunos de los sistemas de pago que se presentan:

Terminal de Punto de Venta Virtual (TPV): La mayoría de bancos cuentan con un servicio subcontratando a terceros, es decir, los bancos siempre están atentos a mantener sus medidas de seguridad para cualquier caso de fraude.

Transferencia bancaria: se utiliza para que el vendedor tenga una garantía, por medio del comprobante de la transferencia monetaria brindada por parte del comprador, para realizar con toda seguridad el envío del pedido.

Plataformas para realizar pagos: los pagos se realizan por medio de un tercero o intermediario como PayPal, Google Wallet, Amazon Pay y Dwolla, quienes se encargan de tomar los datos del comprador para hacerlos saber al vendedor, con ellas lo pueden hacer en diferentes comercios para no estar brindando los datos cada vez que se realice una compra.⁶⁰

⁶⁰ Andrea Verence Basantes Andrade, Mónica Cecilia Gallegos Varela, Cathy Pamela Guevara Vega, Alexandra Elizabeth Jácome Ortega, Comercio Electrónico, (Ibarra - Ecuador: Imprenta Universitaria, 2016), 36-41

3.5 Principios del Comercio Electrónico

Según la Ley de Comercio Electrónico en su art. 4 se enumeran los principios del comercio electrónico, que son:

3.5.1 Principio de equivalencia funcional

Hace referencia a que los documentos electrónicos deben cumplir los mismos requisitos y formalidades exigidos a los documentos presentados en forma física.

3.5.2 Principio de neutralidad tecnológica

Hace referencia a que el sistema jurídico tenga la libertad, según la necesidad y la materia, de elegir cuál será el sistema o mecanismo tecnológico a utilizar para que sus operaciones de comercio electrónico sigan siendo eficaces.

3.5.3 Principio de no repudiación

Todos aquellos contratos realizados ya sea por medio de firma electrónica o algún sistema de información que esté de conformidad a la ley, deben de ser aceptados y no rechazados solo por estar en un soporte electrónico.

3.6. Clasificación del Comercio Electrónico

Hay una gran variedad de clasificaciones del comercio electrónico, en este apartado establecemos las más importantes y relevantes, las cuales son:

3.6.1. Según el medio de comunicación empleado

3.6.1.1. Comercio Electrónico Tradicional

Se emplea entre empresas por medio de redes o sistemas cerrados de comunicación, por mencionar algunos: Intranets, Extranet, VPN, entre otras.

3.6.1.2. Comercio Electrónico en Internet

Se desenvuelve en un sistema de comunicación abierto, pudiendo ser en Internet, el cual no se restringe a las relaciones comerciales entre las empresas, debido a que en este sistema cualquier persona puede acceder.

3.6.2. Según la actividad desarrollada

3.6.2.1. Comercio Electrónico Directo

La modalidad consiste en comercializar bienes o servicios intangibles, el pago, pedido, entrega o suministro del producto se ejecuta de manera electrónica o en línea, ejemplo, libros digitales (e-books), servicios de celular, servicios bancarios, software, juegos, aplicaciones, entre otros.

3.6.2.2. Comercio Electrónico Indirecto

El modo en que se comercializan los bienes y servicios es de forma tangible, el pago se efectúa de manera electrónica y la entrega del artículo es de forma física o personal, completándose por los medios típicos de transporte.

3.6.3. Según el grado de seguridad

3.6.3.1. Comercio Electrónico Inseguro

Conocido como, Comercio Electrónico Simple, se caracteriza porque los medios de seguridad electrónica son escasos para proteger las transacciones comerciales, siendo vulnerable para realizar delitos

informáticos, como estafas, un ejemplo de estas páginas web sería Ebay y Deremate.com.

3.6.3.2. Comercio Electrónico Seguro

En este tipo de comercio, las páginas tienen mejores métodos de seguridad electrónica, con el fin de dar confianza a los usuarios en las diferentes transacciones que realicen, algunos ejemplos de estos mecanismos de seguridad son, los certificados digitales, firma electrónica y la criptografía.

3.6.4. Según los sujetos participantes

3.6.4.1. Business to Business (B2B)

En español es, comercio de “Empresa a Empresa”, son las transacciones comerciales de bienes o servicios realizadas entre empresas, este tipo de comercio es uno de los más comunes; entre empresas se pueden dar mejores precios por volumen, productos exclusivos, únicos o intercambios. Ejemplos, Google Ads, Email Marketing y la publicidad en redes sociales.

3.6.4.2. Business to Consumer (B2C)

La relación comercial estipulada es la realizada entre “Empresas y Particulares, Consumidor o Cliente final, siendo este su significado en español, es uno de los más conocido y usados, consiste en que una persona quiere adquirir un bien o servicio de una empresa, acudiendo a la página web (tienda virtual) del establecimiento de su preferencia y compra el o los productos que desea. Algunos ejemplos muy comunes son, Amazon, Alibaba, Netflix, Spotify.

3.6.4.3. Business to Government (B2G)

En español significa de “Empresa a Gobierno”, también se le conoce como Business to Administration (B2A) significa de empresa a administración. Son las transacciones comerciales entre la empresa y el

Gobierno, pasando éstas por procesos establecidos en la ley, para ver qué empresa ofrece en sus plataformas en línea mejores prestaciones, servicios y precios, con el fin de usar adecuadamente el presupuesto, ejemplos de esta relación son, las compras que realiza el Estado en internet a través de concurso o licitación.

3.6.4.4. Consumer to Consumer (C2C)

Que en español es la relación comercial de “Consumidor a Consumidor”, acá los propios consumidores se ofrecen entre ellos los productos o servicios en las plataformas en línea, detallando el precio, forma de pago y la forma de entrega. Ejemplos son, Marketplace, Mercado libre, OLX.

3.6.4.5. Government to Business (G2B)

Su significado es de “Gobierno a Empresa”, conocido por Administration to Business (A2C) o administración a empresa, en esta relación el Gobierno ofrece servicios por medio de sus plataformas digitales a las empresas de una forma más fácil, sin tener que ir a la institución y pasar procesos largos, dentro de los procesos que se pueden realizar son, solicitud y renovación de permisos y licencias, pago de tasas e impuestos, etc.

3.6.4.6. Government to Consumer (G2C)

Traduciendo, es la relación de “Gobierno a Consumidor”, también llamado Administration to Consumer (A2C) o administración a consumidor, es la relación dada del Gobierno a los consumidores, usuarios o ciudadanos en este caso. Se da por medio de las páginas web institucionales, en donde los ciudadanos pueden realizar sus trámites en línea a través de los portales habilitados, como el pago de impuestos, multas, acceder a información pública, agendar citas y solicitar documentos.

3.6.4.7. Government to Government (G2G)

Es la relación de “Gobierno a Gobierno”, conocido como Administration to Administration (A2A) o administración a administración, son las transacciones realizadas por medio electrónico de los datos entre la administración pública, es decir, la información que comparten entre las diferentes instituciones, gobiernos locales, gobierno central y dependencias del Estado

3.6.4.8. Otras Clasificaciones

Hay una gran cantidad de clasificaciones aparte de las ya abordadas, dentro de ellas están, **Business to Employee (B2E)** es la relación de “Empresa a Empleado”, **Business to Investors (B2I)** la relación de “Empresa a Inversor”, **Consumer to Business (C2B)** significa de “Consumidor a Empresa” y **Government to Employee (G2E)** conocido como de “Gobierno a Empleado”.⁶¹

3.7. Desarrollo del Comercio Electrónico en El Salvador

El Salvador como se sabe es un país en vías de desarrollo, haciendo referencia al ámbito tecnológico y en específico al comercio electrónico, en el país se sigue generando cierto temor y desconfianza a la hora de hacer compras o pagos en línea, es por ello que este tema y una ley que lo regule se ha venido retrasando hasta nuestros días.

Ha habido ciertos precedentes sobre regulaciones del comercio electrónico, podemos mencionar al Código de Comercio, la Ley de Bancos, la Ley del CIEX de El Salvador y las reformas realizadas a la Ley de Protección al Consumidor, en donde ya se toman en cuenta algunos puntos referentes al

⁶¹ Andrea Verence Basante Andrade, Mónica Cecilia Gallegos Varela, Cathy Pamela Guevara Vega, y otros, *Comercio Electrónico*, Tipos de Comercio Electrónico, (Imprenta Universitaria, Universidad Técnica del Norte, Ibarra, Ecuador, 2016), 43

comercio electrónico, más recientemente está, la Ley de Firma Electrónica y la Ley de Comercio Electrónico.

Como se dijo, al país aún está explorando esta forma de hacer comercio, la mayoría de transacciones realizadas son de consumo masivo, como la de medicamentos, ropa, electrodomésticos, marketing, aplicaciones y servicios de streaming, muchas de estas actividades se hacen informalmente, por esa razón es necesaria una ley nacional que lo pueda regular y pueda darles seguridad a ambas partes.

Teniendo un apoyo legal se puede resaltar que El Salvador forma parte del Acuerdo de Facilitación de Comercio (AFC), establecido en 2014 por la Organización Mundial del Comercio (OMC), con este acuerdo se busca que apoyen a la disponibilidad de la información en internet, para darle seguridad a las transacciones realizadas por el comercio electrónico, ayudando a países con menos desarrollo, con el fin que puedan potenciar el comercio en línea, a su vez, existen otros acuerdos que buscan impulsarlo, como lo la Asociación con la Unión Europea (Ada-UECA) y el Tratado de Libre Comercio entre República Dominicana Centroamérica y Estados Unidos (TLC-CAFTA). Estos son algunos de los entes y acuerdos que tiene El Salvador para potenciar el comercio electrónico a nivel internacional.⁶²

Con miras a que El Salvador se vuelva un país desarrollado, es indispensable que nuestra legislación vaya avanzando con la tecnología, dándole una mayor relevancia a los procesos y trámites en línea que se realicen con las instituciones públicas (e-government) y trabajar junto con el sector privado para implementar nuevas estrategias, adecuar los procesos e introducirse a la era digital, aprovechando la ayuda internacional, el ejemplo de otros países para fortalecer el comercio

⁶² Centro de Trámites de Importaciones y Exportaciones Banco Central de Reservas, “E-Commerce: Herramienta de facilitación del Comercio Internacional”, INFOCIEX, n. 3 año 19, (julio-septiembre 2017): 3-5

electrónico y darle la seguridad a sus usuarios para que inviertan y se desarrollen en él, siendo otro punto importante para aumentar exportaciones e ingresos al Estado, en busca del desarrollo y apoyo a sectores que más lo necesiten.

3.8. Desarrollo del Comercio Electrónico en el ámbito Internacional

El comercio electrónico o también conocido como e-commerce o e-business, no es nuevo que haya aumentado su progreso a nivel internacional, ni ha tomado por sorpresa a los inversores, desde sus inicios en la década de los 90's, popularizado por la marca International Business Machines (IBM) en el año de 1997, evidenciando más los avances que ha tenido cuando la Organización Mundial de Comercio (OMC) en 1998 comienza a trabajar y a estudiar este tema; en la Segunda Conferencia Ministerial celebrada por la OMC se reconoce su expansión a nivel mundial, y se adopta así la Declaración sobre Comercio Electrónico Mundial, con la que se pretende establecer un plan de trabajo sobre el comercio electrónico, notando así los avances que tiene, los países que se involucran más y los que no cuentan con recursos suficientes para hacer crecer.⁶³

Un detalle a resaltar fue como las grandes empresas comenzaron a invertir en sus páginas web, mostrando sus productos, poniendo ofertas especiales, queriendo incentivar a sus consumidores tradicionales a unirse a la era tecnológica y llamar la atención de las nuevas generaciones por medio de estos sitios, fomentando la difusión del internet en los hogares, hasta convertirse en una necesidad básica y un derecho humano en la actualidad.

Dado el gran impacto y el avance tecnológico que se ha visto en los últimos años, con el aumento de la velocidad del internet, la llegada de los

⁶³ Centro de Trámites de Importaciones y Exportaciones Banco Central de Reservas, "E-Commerce: Herramienta de facilitación del Comercio Internacional", INFOCIEX, n. 3 año 19, (julio-septiembre 2017): 1

smartphones, tabletas, computadoras con más capacidad y las nuevas formas de pago como PayPal, se toma la iniciativa de medir cómo ciertos países o grupo de naciones aportan un mayor consumo al comercio por la vía electrónica. Los datos dados por “Global B2C E-commerce”, posicionando a Europa y a Norteamérica como las regiones que más facturaciones generan, sin dejar atrás el crecimiento presentado por Asia-Pacífico, generando billones de dólares, Latinoamérica no se queda atrás, ha venido evolucionando, teniendo un gran crecimiento, dentro de los países que más compran en línea en la región están, Brasil, Argentina, Colombia, México, entre otros.

Cada vez más son las personas que se introducen a las compras electrónicas, esto se debe a que da una mayor comodidad, agilidad y evita el desplazamiento de los usuarios que pueden comprar a la hora que se deseen.

Conforme a los datos reflejados por “Ecommerce Foundation en 2015”, el comercio internacional se ve en algunos países, en Estados Unidos el 47% de la población realizó compras electrónicas a nivel internacional, en Reino Unido el 38%, China y Hong Kong el 31%, Canadá el 17% de su población, Australia el 16% y en Alemania el 13% de sus habitantes, los números reflejan cómo ciertos países acaparan el mercado y en ellos hay mayor confianza para comprar en línea.⁶⁴ Dentro de todo, las nuevas formas de hacer comercio ayudan a las pequeñas y medianas empresas a expandirse más, beneficiándose de este mercado (en línea) para ofrecer sus productos, sin la necesidad de tener un local físico, con solo crear su página web o una cuenta en alguna red social pueden comenzar a publicar sus

⁶⁴ Romina Gayá, Conexión INTAL, Banco Interamericano de Desarrollo (BID), “El comercio electrónico y la inserción internacional de América Latina y el Caribe”, n. 229, (15 octubre 2015), 11

productos, necesitando solo de un celular y acceso a internet para desarrollarse.⁶⁵

De esta forma es como el comercio electrónico ha venido desarrollándose a nivel internacional, ofreciendo productos en su país y en otros, todo gracias al internet, promoviendo productos y servicios fuera de las fronteras, convirtiéndose en una herramienta indispensable para la expansión de cualquier negocio en la actualidad.

⁶⁵ Secretaría General de la Comunidad Andina, Comunidad Andina, El comercio electrónico en los países en desarrollo: Oportunidades y retos para las pequeñas y medianas empresas, acceso el 10 de marzo de 2021, <http://www.comunidadandina.org/Prensa.aspx?id=3400&accion=detalle&cat=AP&title=el-comercio-electronico-en-los-paises-en-desarrollo-oportunidades-y-retos-para-las-pequenas-y-medianas-empresas>

CAPÍTULO IV:

INTRODUCCIÓN A LA PROTECCIÓN DE DATOS PERSONALES Y SU IMPLEMENTACIÓN EN EL SALVADOR

En cuanto al desarrollo de este capítulo, se explicará la implementación y desarrollo que ha tenido en el transcurso del tiempo la protección a los datos de las personas, tratando temas desde su definición, con el propósito de hacer énfasis en la necesidad de una ley de protección de datos personales.

4.1. Protección de Datos Personales

La protección a los datos es un tema que cada vez da más de qué hablar, debido a la gran conectividad que se tiene con el internet, los smartphones y las redes sociales; los usuarios muchas veces se preguntan, ¿en verdad nuestros datos privados solo nosotros los conocemos? O, si al compartir información con amigos o crear un perfil, ¿terceros puede ver lo que colocamos?, es por ello que para introducirnos a este tema comenzaremos definiendo qué es “Dato Personal”, apoyándonos en el Decreto N° 875 de la Ley de Protección de Datos Personales, en el art. 4 referente a las definiciones, que dice así: “Información concerniente a una persona natural identificada o identificable.

Al conocer el concepto anterior, se define la Protección de Datos Personales, este se encuentra dentro de los Derechos Informáticos, “se trata de la garantía o facultad de control de la propia información frente a su tratamiento automatizado o no, es decir, no solo aquella información albergada en sistemas computacionales, sino en cualquier soporte que permite su utilización, almacenamiento, organización y acceso”. Otra

definición es la de Hondius, “es aquella parte de la legislación que protege el derecho fundamental de la libertad, en particular el derecho individual a la intimidad, respecto del procesamiento manual o automático de datos”.

Destacar que dentro de él se encuentran ligados otros derechos como, la autodeterminación informática, habeas data, la privacidad, entre otros.

4.2. Sujetos y objeto de la Protección de Datos Personales

4.2.1. Sujetos de los datos personales

Para mejor comprensión sobre quién recae la protección de los datos personales se debe saber quiénes son los sujetos obligados de protegerla, ellos son:

a) Titular de la Información: El titular de la información es aquella persona natural o jurídica cuya autonomía genera diferentes tipos de información que recaiga estrictamente sobre su personalidad o sobre las diferentes actividades que realizan.

En relación a lo anterior, y de acuerdo al reconocimiento del derecho de protección de información personal o de la autodeterminación informativa como derecho fundamental, se concluye que toda persona tiene derecho de solicitar el acceso y la protección de su información, asimismo de ejercer el control sobre la misma a través de las distintas acciones que la ley le faculta.

b) Administrador de bases de datos o registros: Pueden ser de diversa índole, ya sea sujetos de derecho público o de derecho privado. La información personal que proporciona cualquier persona obedece a una necesidad o a una obligación. En el primer caso, el sujeto para cubrir una necesidad emergente o para obtener la prestación de un servicio decide acudir ante un particular para obtener su propósito, debiendo de esta

relación, proporcionar información a esta entidad o persona, en el segundo caso, el poder público, para ejercer su actividad, a través de la administración pública del Estado, requiere obligatoriamente información personal.⁶⁶

4.2.2 Objeto de la protección de datos personales

El objeto de protección de datos recae sobre el derecho fundamental de salvaguardar la información e intimidad del usuario, desarrollándolo así:

a) Información Personal: Toda aquella información privada correspondiente a una persona, identificada o identificable, relativa a su nacionalidad, domicilio y patrimonio etc. es decir, aquella que por medio de la cual, la persona es individualizada frente a un grupo social.

b) Información Confidencial: Es lo referente a la ideología, política, religión, origen étnico, situación moral o familiar de una persona, u otra información que pueda afectar su honor, intimidad personal o familiar y la propia imagen.

c) Información Patrimonial: Referente a la información de la situación patrimonial de una persona, a través de ella, se conoce el conjunto de derecho y obligaciones del sujeto respecto al activo y pasivo de bienes.

d) Información Laboral: Es común que los empleadores públicos y privados se interesen en mantener un registro de los trabajadores que laboran, esta información va más allá de su expediente personal, se solicita otro tipo de información, como salud, familiar, social u otra índole, con el fin de realizar un expediente laboral que sirva como parámetro para contratar o mantener en vigencia los contratos laborales. Este tipo de información es

⁶⁶ Javier Armando Zarceño García, Pedro de Jesús Canales Garay, “La Protección de Datos Personales: un Análisis Constitucional de la Ley de Acceso a la Información”, (tesis de grado, optando al título de Licenciatura en Ciencias Jurídicas, Universidad de El Salvador, 2013), 75

la que concierne a los sindicatos, Registro de Trabajadores en el Ministerio de Hacienda, Hospitales de Seguridad Social.

e) Información destinada a terceros: Es otorgada por un sujeto a otro particular, o entidad pública o privada, con el fin que este receptor posteriormente lo comparta con un tercero. Este tipo de información se encuentra en las empresas que suministran a sus clientes, cuando proveen a terceros información sobre solvencia patrimonial y crédito de personas físicas y jurídicas almacenadas en una base de datos computarizada.⁶⁷

4.3. Principios de la Protección de Datos Personales

Los principios presentados en este rubro son variados, para realizar nuestro estudio tomaremos en cuenta los del ámbito internacional y nacional.

4.3.1. Principios Internacionales

Los principios internacionales tomados del “Proyecto de la Ley Modelo de Protección de Datos Personales”, establecida por el Comité Jurídico de la Organización de los Estados Americanos, son 12, siendo los siguientes:

- 1) Propósitos legítimos y justos, seguimiento de los límites legales para el uso de la información.
- 2) Claridad y consentimiento, dar permiso en el uso de los datos.
- 3) Pertinencia y necesidad, congruencia en la información dada.
- 4) Uso limitado y retención, usar solo los datos autorizados.
- 5) Deber de confidencialidad, mantener seguros y en secreto los datos.
- 6) Protección y Seguridad, dar seguridad en el manejo de los datos.
- 7) Fidelidad de la información, mantener íntegra la información.
- 8) Acceso y corrección, actualización y fácil acceso a los datos.
- 9) Información sensible, tener cuidado en el uso de los datos.

⁶⁷ *Ibíd.* 75

- 10) Responsabilidad, diligencia en el manejo de datos
- 11) Flujo transfronterizo de información y responsabilidad, la información corre de un lugar a otro sin límites fronterizos.
- 12) Publicidad de las excepciones, revelar total o parcial información según las necesidades y excepciones que se den.⁶⁸

También el Reglamento (UE) 2016/79 en el art. 5 presenta estos principios:

- a) Licitud, lealtad y transparencia, se debe presentar con el interesado.
- b) Limitación de la finalidad, se siguen fines determinados en el uso de datos, si se cambian el fin por razones importantes, seguirá siendo válido.
- c) Minimización de datos, usar la menor cantidad de datos posibles.
- d) Exactitud, usar exactamente los datos necesarios y actualizados.
- e) Limitación del plazo de conservación, los datos se usan el tiempo necesario, se podrá pasar del tiempo solo si es necesario.
- f) Integridad y confidencialidad, dar seguridad del manejo de datos.
- g) Responsabilidad proactiva, verificar y demostrar que se cumple la normativa de protección a los datos personales.⁶⁹

Agregando otro principio, dado por las directrices de la Organización de las Naciones Unidas para la Regulación de los Archivos de Datos Personales Informatizados, está el “**Principio de no Discriminación**”, establece que no se deben recoger datos que puedan dar origen a algún tipo de discriminación.

4.3.2. Principios Nacionales

Desde un punto de vista nacional, hemos tomado en cuenta el nuevo Decreto N° 875 de la Ley de Protección de Datos Personales, tomando en

⁶⁸ FUSADES – Análisis legal e institucional, “Observaciones a los proyectos de Ley de Protección de Datos Personales, Parte I: Introducción, antecedentes normativos, principios internacionales y derecho comparado”, n. 199 (2019): 5

⁶⁹ *Ibíd.* 6-7

consideración algunos principios internacionales, de los cuales se habló anteriormente, los principios retomados en esta ley se encuentran en el art. 5, los cuales son:

- a) Principio de legalidad: la información se debe procesar de conformidad a esta Ley. Art. 5 lit. a).
- b) Principio de lealtad: quien resguarde los datos debe abstenerse de tratarlos o recabarlos por medios ilegales. Art. 5 lit. b)
- c) Principio de consentimiento y Finalidad: al tratar y recolectar los datos, el titular debe dar su permiso de forma expresa y esclarecer el propósito de ellos y el tiempo de su resguardo. Art. 5 lit. c).
- d) Principio de minimización de datos: al recolectar los datos, estos deben ser específicos con la intención que se busca. Art. 5 lit. d).
- e) Principio de calidad: los datos obtenidos deben ser los indicados para cumplir con el derecho de acceso a ellos. Art. 5 lit. e).
- f) Principio de transparencia: el titular puede verificar sin límite su información y verificar cómo se tratan sus datos. Art. 5 lit. f).
- g) Principio de seguridad de datos: pretende dar integridad y confidencialidad de los datos, para evitar cambios sin autorización la pérdida de los mismos. Art. 5 lit. g).
- h) Principio de privacidad: todos los datos de los titulares deben estar protegidos ante terceras personas que no se les haya permitido su acceso. Art. 5 lit. h).
- i) Principio de Licitud: a los datos debe dársele un tratamiento de acuerdo a la norma actual. Art. 5 lit. i).

4.4 Clasificación de los Datos Personales

A continuación, se desarrolla la clasificación de datos personales:

a) Datos Públicos: Son clasificados como públicos por la ley, es decir, que es estrictamente por mandato de ley. Son datos públicos todos aquellos

que puedan ser consultados por las personas que previamente tengan un interés o estén autorizados para hacerlo, por ejemplo, las sentencias ejecutoriadas que estén autorizadas y que no tengan reserva.

b) Datos Semiprivados: “Es semiprivado el dato que no tiene naturaleza íntima”, es decir, a pesar de tener un solo interés, en un primer plano puede que en el proceso deje solo de ser interés particular y se convierta en un interés de otro individuo o de un grupo de personas o de la sociedad en general.

c) Dato Privado: “Es el dato que únicamente posee naturaleza íntima o reservada”, es decir, a diferencia de los datos semiprivados, este no puede en ningún momento del proceso pasar a ser interés de terceros, solamente del titular, por ejemplo, solo pueden ser de interés del individuo correos electrónicos notificando alguna situación de salud o de carácter laboral.

d) Datos Sensibles: Los datos sensibles son aquellos que afectan de manera directa la intimidad del titular, ya sea por su publicación o uso indebido, con la característica de que dichos datos son de suma importancia y privacidad para el titular. Algunos ejemplos pueden ser, revelar la afiliación a algún partido político, origen étnico, ser miembro de algún movimiento social, entre otros.⁷⁰

4.5. Categoría de los Datos Personales

a. Datos de Salud: Los datos de salud están conformados por: Enfermedades, predisposición a enfermedades o síndromes, riesgo de sufrir accidentes, etc.

⁷⁰ NOVUM JUS, Marcela Rojas Bejarano, Universidad Católica de Colombia, “Evolución del Derecho de Protección de Datos Personales en Colombia respecto a estándares Internacionales”, n. 8, (enero-junio 2014): 128-131

b. Datos de Identidad: Dentro de los datos de identidad se encuentran: Correos electrónicos, números telefónicos, documentos que contengan datos personales (DUI, NIT, Seguro Social, Pasaporte etc.)

c. Datos sobre vida sexual: Los datos sobre la vida sexual se encuentran: el sexo, estado civil y preferencia sexual de la persona.

d. Datos de Hábitos: Dentro de los datos de hábito están los siguientes: Riesgo de sufrir un accidente, Viajes, etc.

e. Datos Ideológicos: Los datos ideológicos pueden ser: políticos, religiosos, o sindicales.⁷¹

4.6. Derechos Protegidos

4.6.1. Derecho al Honor

El derecho al honor está dado en base a la perspectiva que tiene los terceros o la sociedad de la persona, esta perspectiva es en base al actuar de manera socialmente correcta; es generar hacia los demás un reconocimiento de respeto, tenemos como base constitucional el art. 2 inciso 2, “el estado se compromete a garantizar el derecho al honor como derecho individual”⁷².

4.6.2. Derecho a la Intimidad

Es un espacio seguro en el que el individuo puede confiar y sentirse socialmente estable, en la que ningún tercero tiene derecho a invadir su

⁷¹ Laura Nathalie Hernández Rivera, El ABC de la Protección de Datos Personales, Categoría de los datos personales, 25

⁷² Javier Armando Zarceño García, Pedro de Jesús Canales Garay, “La Protección de Datos Personales: un Análisis Constitucional de la Ley de Acceso a la Información”, (tesis de grado, optando al título de Licenciatura en Ciencias Jurídicas, Universidad de El Salvador, 2013), 73

libertad individual, es por ello que nuestra carta Magna le garantiza a la persona este derecho individual. Podemos encontrar su base en el art. 2 inciso 2 de la Constitución de la República de igual forma tenemos el Decreto N° 875 de la Ley de Protección de Datos Personales, en su art. 49 expone sobre los datos sensibles y es un claro ejemplo de la protección al derecho a la intimidad debido a que nadie puede obligar al usuario a proporcionar dichos datos e igualmente se le debe de advertir previamente al usuario que está en todo su derecho a no prestarlos.⁷³

4.6.3. Derecho a la Privacidad

La privacidad del individuo debe de ser respetada por su círculo social y por toda sociedad, a pesar de que estos sepan cuáles son las actividades que este desarrolla en su vida cotidiana, un ejemplo de esto puede ser la dirección de su casa, es un dato personal del conocimiento de las personas cercanas a él, pero nadie tiene derecho a divulgarlo. En el art. 24 inciso 1 de la Constitución tenemos la prohibición a la interferencia y la intervención de las telecomunicaciones, solamente de manera excepcional se podrá autorizar, y debe ser judicialmente cualquier tipo de intervención temporal, con la característica que debe preservarse en todo caso el secreto privado que no tenga relación con el proceso, de igual forma tenemos el Decreto N° 875 de la Ley de Protección de Datos Personales en su art.5 lit. h) menciona que todo lo relacionado con los datos personales del titular será garantizado por el principio de privacidad y especialmente la que sean de naturaleza sensible.⁷⁴

⁷³ Tomas Alberto Amaya Tario, Andrea Karina Avalos Cisneros, Karen Nathaly, Jule Moreno, "Respeto al Derecho de Intimidad en la Estructura de la Ley de Intervenciones de Telecomunicaciones", (tesis de grado, optando al título de Licenciatura en Ciencias Jurídicas, Universidad de El Salvador, 2012), 12

⁷⁴ Javier Armando Zarceño García, Pedro de Jesús Canales Garay, "La Protección de Datos Personales: un Análisis Constitucional de la Ley de Acceso a la Información", (tesis de grado, optando al título de Licenciatura en Ciencias Jurídicas, Universidad de El Salvador, 2013), 70

4.6.4. Derecho a la Autodeterminación Informativa

Este derecho se destaca por resguardar y controlar cualquier tipo de información personal que esté sistematizada, contenida en una base de datos, por ejemplo, las bancas en línea; es importante mencionar el Habeas Data, que significa “tener datos presentes”, el habeas data se resume en el derecho que tienen las personas de conocer toda información personal que se encuentre almacenada en una base de datos informáticos, ya sean públicos o privados. El art. 8 del Decreto N° 875 de la Ley de Protección de Datos Personales es muy claro en este punto, expone el derecho que tiene todo titular a poder acceder a sus datos personales que estén en una base de datos pública o privada, con la característica que debe de ser gratuito, a su vez el art. 9 y 10 menciona que también tienen derecho a la rectificación y supresión de los datos.⁷⁵

4.6.5. Derecho a la Seguridad Jurídica

Según Sentencia Constitucional referencia N° 642-99 “la Seguridad Jurídica es un principio que informa a todo el ordenamiento jurídico en El Salvador” “Por seguridad jurídica se entiende, pues, la certeza que el individuo posee de que su situación jurídica no será modificada más que por procedimientos regulares y autoridades competentes, ambos establecidos previamente” En el art. 1 de la Constitución de la República manifiesta que toda persona humana tiene garantizado el derecho a la seguridad jurídica ya que este es visto como el origen y el fin de la actividad del Estado, también en el Decreto N° 875 de la Ley de Protección de Datos Personales en el art. 5 lit. g) habla sobre la seguridad de los datos, se deben adoptar las medidas necesarias para garantizar a la

⁷⁵ Sala de lo Constitucional, Sentencia de Amparo, Referencias: 934-2007 (El Salvador, Corte Suprema de Justicia, 2011)

persona la seguridad, integridad, disponibilidad y confidencialidad de los datos para evitar cualquier tipo de alteración o pérdida de los datos personales.⁷⁶

4.6.6. Derecho a la protección de Datos Personales

Es garantizar al individuo una protección jurídica en la cual sus datos personales estarán amparados ya sea por el Estado o por una institución privada para evitar en su totalidad la manipulación o utilización errónea de la información este derecho está íntimamente relacionado con el derecho a la autodeterminación informativa. En el art. 6 del Decreto N° 875 de la Ley de Protección de Datos Personales expresa que “toda persona, por sí mismo o por medio de su representante tendrá derecho a saber si están procesando sus datos personales; a conseguir una reproducción inteligible de sus datos; a obtener las rectificaciones; a solicitar su cancelación, referente al derecho de supresión u olvido, esto cuando correspondiere, y a oponerse al tratamiento de sus datos es decir derecho al olvido”

4.7. La Protección de los Datos Personales en El Salvador

En El Salvador el derecho a la Protección de Datos personales no se encuentra explícitamente regulado como tal, en nuestra Constitución se encuentra desde el punto de vista de otros derechos en dos artículos, el art. 2 inciso segundo dice, “Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen”, también, el art. 24 inciso primero y segundo reza así, “La correspondencia de toda clase es inviolable, interceptada no hará fe ni podrá figurar en ninguna actuación, salvo en los

⁷⁶ Sala de lo Constitucional, Sentencia de Amparo, Referencia: 642-99 (El Salvador, Corte Suprema de Justicia, 2000)

casos de concurso y quiebra. Se prohíbe la interferencia y la intervención de las telecomunicaciones...”.

En el siguiente cuadro, se muestran algunas leyes nacionales que hacen referencia a la protección de datos personales en El Salvador.⁷⁷

Ley.	Artículo y Naturaleza.	Regulación.
Ley de Acceso a la Información Pública.	Arts. 31-39; Pública.	Establece derechos que tienen las personas para saber si entidades gubernamentales procesan sus datos, y recoge derechos para tener acceso a ellos.
Ley de Firma Electrónica.	Art. 5; Pública	Fija mecanismos electrónicos para el resguardo de datos personales de carácter electrónico.
Ley de Regulación de Servicios de Información sobre Historial de Créditos de las Personas.	Art. 1; Privada	Avala que se dé un buen manejo de datos de los consumidores o clientes, en relación al historial de créditos.
Ley de Protección al Consumidor.	Art. 18 literal g); Privada	Norma cómo empresas comparten información del consumidor entre los agentes.
Ley General de Telecomunicaciones.	Art. 29; Privada	Cuida la intimidad y datos personales de los usuarios.
Ley Especial Contra los Delitos Informáticos y Conexos.	Arts. 15-26; Pública y Privada	Sanciona de forma penal delitos contra los registros y titulares de datos personales.

⁷⁷ FUSADES – Análisis legal e institucional, “Observaciones a los proyectos de Ley de Protección de Datos Personales, Parte I: Introducción, antecedentes normativos, principios internacionales y derecho comparado”, n. 199 (2019): 3-4

Con respecto a la normativa ya establecida en nuestro país, se puede ver reflejado que hay una dispersión en nuestras leyes, esto no permite que se dé una protección, regulación, ni buen resguardo de los datos personales, es por ello que tres partidos políticos (ARENA, FMLN y GANA) se dieron la tarea de crear proyectos de ley referentes a este tema, para presentar como proyecto final el Decreto N° 875 de la Ley de Protección de Datos Personales.

Aún se encuentra a la espera por parte de casa presidencial que se sancione el proyecto final presentado por la Asamblea Legislativa, para mantener al país a la vanguardia con las leyes y proteger los datos de las personas, no solo de forma física sino de forma electrónica, debido a que hoy en día es necesario introducir ciertos datos personales para mantenerse comunicado, actualizado, hasta para estudiar o trabajar. Se espera que pronto se pueda regular este tema y dar cumplimiento completo a uno de los derechos fundamentales, para dar protección, seguridad y evitar fuga de datos y vulneración a nuestra intimidad.

CAPÍTULO V:

RETOS EN LA APLICACIÓN DE LA FIRMA ELECTRÓNICA EN EL SALVADOR

Como último capítulo, se verá desarrollado los diferentes retos a superar para implementar el desarrollo de la firma electrónica en El Salvador; con la finalidad de hacer una correcta aplicación y funcionamiento de ella.

5.1. Avances y Obstáculos de la Ley de Firma Electrónica

En este capítulo se ve el progreso, impedimentos, relación de cuerpos normativos y los retos a superar para dar un aprovechamiento a los recursos tecnológicos que se van implementando, teniendo como punto central la regulación legal de estos medios, dándole así, protección a los usuarios, comerciantes y demás agentes que intervengan en su desarrollo.

En cuanto a la aplicación de la Firma Electrónica, esta ha tenido muy pocos avances y nula aplicación desde que se creó la Ley de Firma Electrónica, que entró en vigencia en el año 2016, agregando a ellos, en el mismo año se creó el Reglamento de la Ley de Firma Electrónica por mandato de ley. Actualmente en el año 2021 entró en vigencia la Ley de Comercio Electrónico, pero hasta el momento no se está implementando, de igual forma, luego que la Asamblea Legislativa discutió tres proyectos de ley sobre la protección de datos personales presentados por los partidos ARENA, FMLN y GANA, se ha aprobado el Decreto N° 875 de la Ley de Protección de Datos Personales, del cual se está a la espera del sancionamiento por Casa Presidencial. Los avances por escasos que han sido, se han ido prosperando poco a poco, desde el punto de vista económico y en infraestructura digital se han dado gracias al aporte y a la

ayuda de FOMILENIO II, que apoyó para implementar la firma electrónica en El Salvador, si bien es cierto por razones económicas, aún con la inversión, costó dar los primeros pasos y sigue habiendo problemas por resolver.

El hecho que no hay quién pueda acreditar certificados digitales y la falta de personal especializado para brindar información legal y técnica de su funcionamiento, por estas y otras razones se ha venido dilatando el uso y manejo de la firma electrónica en el país.

En el problema de investigación y en el objetivo general, se planteó que para implementar de forma más completa y protegiendo otros derechos, es necesario que existan dos leyes que complementen a la ya existente Ley de Firma Electrónica, en primer lugar una “Ley de Protección de Datos Personales”, para proteger como la misma ley lo dice, los datos de los usuarios de la firma electrónica y todo proceso que se haga en línea o en soporte electrónico, sin dejar atrás la protección de datos en formato físico, teniendo así un sustento legal que salvaguarde y dé seguridad ante un posible hackeo o robo de información, no solo tener como referencia el art. 5 de la Ley de Firma Electrónica que nos habla de cómo tratar los datos personales de los usuarios.

A su vez, también es necesaria la implementación de la “Ley de Comercio Electrónico”, con ella se puede aplicar de forma más amplia la firma electrónica, al momento de realizar contratos entre empresas nacionales e internacionales, todo podría hacerse desde una computadora en el hogar o la oficina, sin necesidad de viajar, reunirse y firmar físicamente un contrato, facilitando y agilizando los procesos de contratación entre las partes, sacando provecho a las tecnologías y dando un mejor aprovechamiento a estas y ahorrando tiempo de las personas.

Tanto la Ley de Firma Electrónica como la Ley de Comercio Electrónico están vigentes, pero se está a la espera que puedan implementarse tanto

de manera individual como en conjunto; los beneficios que se pueden notar al momento de implementar las dos leyes antes relacionadas y la futura Ley de Protección de Datos Personales; en primer lugar, se garantiza la protección y seguridad jurídica de los datos de las personas y dar un mayor campo de aplicación a la firma electrónica, de esta forma avanzar en materia tecnológica, legal y comercial como país, dejar de lado el papel, abonar al cuidado del medio ambiente, dejar atrás procesos extensos y tardados; y dar paso a la innovación institucional en un mundo cada vez más globalizado.

Por esa razón en este capítulo se hace una relación entre estos tres cuerpos normativos ya mencionados, para destacar los puntos que tienen en común y hacer notar otros en los que puede llegarse a profundizar en un futuro, por tal razón dentro del capítulo, se establecen retos para solventar los inconvenientes que ha venido teniendo la Ley de Firma Electrónica en nuestro país.

5.2. Relación normativa de la Ley de Firma Electrónica

En el presente apartado se hará una relación de los principios y puntos en común que se encuentran plasmados en las tres diferentes leyes que hemos tratado en nuestro trabajo de investigación, con el fin de lograr establecer un vínculo entre ellas, al mismo tiempo, ver la integración de los medios tecnológicos en el ámbito legal.

5.2.1. Principios en común entre las leyes tratadas

Confidencialidad: visto como un principio, es el resguardo o la no divulgación de cierta información, en este caso de los datos de las personas sin su previo consentimiento.

La confidencialidad se encuentra regulado como un principio general en tres de las leyes que se han analizado, en primer lugar, en la Ley de Firma

Electrónica aparece en el art. 4 lit. c). En la Ley de Comercio Electrónica lo encontramos en el art. 20 como seguridad y confidencialidad de la información y que en relación a la protección de datos personales se deberá ir a la ley secundaria que la proteja, es por ello que es de importancia la creación de esa ley.

En cuanto al Decreto N° 875 de la Ley de Protección de Datos Personales el art. 5 de los ppios. Generales, trata sobre el ppio. De seguridad de los datos, garantizando la confidencialidad de los datos personales, para evitar alteraciones, pérdidas, consultas o tratamientos sin autorización, para verificar si se desvía información con o sin intención. De igual forma en el art. 9 en el inc. 2, sobre el derecho de rectificación, derecho que tiene todo titular para solicitar y obtener del responsable del cuidado de la base de datos y así poder de manera confidencial, rectificar, actualizar, cancelar o hasta eliminar ciertos datos personales.

Seguridad: Se refiere a un derecho y un principio, que consiste en tomar las medidas de protección necesarias para salvaguardar la privacidad digital, así como también proteger los datos.

La seguridad como primer punto se encuentra regulado en la Ley de Firma Electrónica como principio general en el art. 4 lit. g), que garantiza la integridad, autenticación, confidencialidad y buen uso de la información que resida en un sistema informático. Mientras que en la Ley de Comercio Electrónico en el art. 20 hace referencia específica en cuanto a brindar seguridad y confidencialidad de información personal y crediticia por vía electrónica o por cualquier herramienta tecnológica a los proveedores de bienes y servicios proporcionadas en las diferentes plataformas de comercio electrónico.

En el Decreto N° 875 de la Ley de Protección de Datos Personales en su art. 5 de los ppios. Generales, en el ppio. De seguridad de los datos, busca la seguridad de los datos de todas las personas, para proteger la

información de los usuarios, y en el art. 20 sobre el aviso de privacidad, el cual consiste en un documento en el que se detallan las políticas de privacidad que debe realizar el responsable antes de tratar los datos personales, y así dar seguridad a los usuarios sobre cómo se van a tratar y manejar los datos ante cualquier acción, como el uso de cookies y el uso o custodia de la información.

Equivalencia Funcional: retomado como un principio, en el que todo documento que se encuentra en formato físico se puede realizar en formato electrónico, teniendo la misma validez jurídica y probatoria, es decir, los documentos electrónicos serán homologados a los físicos.

Este concepto lo podemos encontrar tanto en la Ley de Firma Electrónica como en la Ley de Comercio Electrónico como parte de los principios establecidos en estas leyes. En la Ley de Firma Electrónica aparece primero en el art. 2, luego se encuentra en el art. 4 lit. d) como un principio general, por último, se encuentra en los arts. 7 y 8, en este último hay que tener en cuenta en este principio las excepciones que se hacen en la misma ley hacia los documentos que necesiten ciertas formalidades; asimismo lo podemos encontrar en la Ley de Comercio Electrónico dentro de los principios especiales del art. 4 lit. a).

Neutralidad Tecnológica: este principio establece la no discriminación de los medios tecnológicos o los medios físicos en el ámbito legal, ni favorecimiento a uno de los dos, busca un equilibrio.

Presentado en la Ley de Firma Electrónica en el art. 2 y como uno de los principios generales establecidos en el art. 4 lit. f), de igual forma aparece en el art. 4 lit. b) de la Ley de Comercio Electrónico.

No Repudiación: desarrollado como un principio, en que todos los actos que realizan las personas por un medio electrónico no podrán ser rechazada su autoría por estar en soporte electrónico.

En la Ley de Firma Electrónica se puede encontrar en el art. 4 lit. e), como parte de los principios generales, haciendo énfasis a que no se rechazará su autoría al suscribir el acto con firma electrónica certificada, y en la Ley de Comercio Electrónico se ve reflejado en el art. 4 lit. c) también en el apartado de los principios especiales, y que no se podrán negar todos los actos realizados en soporte electrónico, firma electrónica u otro medio previsto en por la ley.

5.2.2. Aspectos o puntos en común entre las leyes tratadas

Tratamiento de Datos Personales: este término aparece definido en el Decreto N° 875 de la Ley de Protección de Datos Personales en el art. 4 de las definiciones, rezando así: "Cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicados a datos personales".

En cuanto a la Ley de Firma Electrónica lo encontramos regulado en el art. 5, prohibiendo la cesión a terceros y requiriendo únicamente los datos necesarios para cualquier trámite de expedición o mantenimiento de los certificados digitales, además, quienes estén a cargo o sean responsables de los datos deberán guardarlos en confidencialidad.

Con respecto al Decreto N° 875 de la Ley de Protección de Datos Personales, para tratar los datos en esta ley se puede ver regulado en diferentes artículos, comenzando con los arts. 24 en relación con el 49, para el tratamiento de los datos sensibles, es necesario obtener el consentimiento del titular o del representante, su consentimiento debe ser libre, específico, informado, expreso e individualizado, además no deben ser obligados para ellos. El procedimiento para tratar los datos personales estará a cargo del responsable, teniendo un informe del acceso, rectificación, cancelación y oposición de los datos, según el art. 38 y el art. 40 hacen alusión, a que el encargado solo puede intervenir en el

tratamiento de la base de datos personales de acuerdo a lo que el contrato haya establecido.

Validez de los contratos: los actos o contratos celebrados por medios digitales serán válidos, produciendo los mismos efectos que los realizados en formato físico, siempre que se cumpla con los requisitos establecidos en la ley.

En la Ley de Firma Electrónica lo podemos encontrar en el art. 31, como validez de actos y contratos, haciendo referencia a que los actos y documentos de las instituciones del Estado que sean instrumentos públicos se pueden suscribir por medio de firma electrónica certificada. Si bien es cierto en la ley solo hace referencia explícita a los actos realizados por el Estado, pero también tendrán validez los actos realizados por particulares. En cuanto a la Ley de Comercio Electrónico se encuentra en el art. 14, representado como, validez y eficacia de los contratos celebrados por vía electrónica, serán válidos todos los actos realizados de forma electrónica siempre que medie previo consentimiento de las partes y los requisitos necesarios para que sea válido (capacidad legal, ausencia de vicios en el consentimiento, objeto lícito y causa lícita). Además, podemos ver al art. 19 del mismo cuerpo normativo, en donde nos dice que serán válidos los contratos realizados por una persona física y un sistema automatizados de mensajes o entre sistemas automatizados de mensajes.

Conservación de mensajes de datos/información: son las medidas que se toman para preservar los datos, documentos, información o mensajes, sin ninguna alteración desde que se resguardan, la información contenida no podrá ser cambiada a solo que el titular lo autorice o él desee hacer un cambio en ella.

Con respecto a la Ley de Firma Electrónica podemos encontrar la conservación en los arts. 11 y 12, haciendo referencia a la conservación de documentos, la información será preservada como se ha emitido el

documento original firmado de forma electrónica; si se desea se podrán conservar los documentos en un soporte diferente en que las partes estipulan, con el fin de conservarlo si es destruido o alterado el documento emitido de forma electrónica. El titular puede conservar el documento por cuenta propia o acudir a un proveedor de servicios de almacenamiento electrónico para que cuide su información. En el art. 34 de la misma ley dispone que las instituciones del Estado pueden conservar registros y archivos de forma electrónica, siempre y cuando tengan competencia para hacerlo, buscando sustituir los documentos en físico, para ellos pueden contratar a prestadores de servicios de almacenamiento de documentos electrónicos o hacerlo ellas mismas.

Pasando a la Ley de Comercio Electrónico, la conservación de mensajes de datos se encuentra regulada en el art. 26, en este caso quienes provean bienes o servicios están obligados a conservar la información por un plazo que se detallará de acuerdo al rubro al que se desempeñan, haciendo un cambio en relación a la Ley de Firma Electrónica ya que en ella no estipula un plazo para conservar la información o se estará dispuesto al contrato realizado con el tercero que los resguarde.

El Decreto N° 875 de la Ley de Protección de Datos Personales, en relación a la conservación de datos de los usuarios, en el art. 41 lit. e) del presente decreto habla sobre las obligaciones del encargado de tratar los datos, él deberá eliminar todo dato personal que tenga en su base de datos luego de terminada la relación jurídica, esto se debe hacer si no existe una excepción legal para seguir conservando los datos personales del titular.

Valor Probatorio: se ve reflejado el valor o fuerza probatoria que tendrán los documentos que, realizados por medios electrónicos, pudiendo hacer uso o no de la firma electrónica certificada.

En relación a la Ley de Firma Electrónica, el art. 10 habla sobre el valor probatorio que tienen los documentos privados electrónicos, si estos

documentos son realizados por firma electrónica certificada, será reconocido como si se hubiera hechos de forma física (en papel). Y en los arts. 6 y 24 nos dice de igual forma que los efectos jurídicos y probatorios que surgen, son como si hubiera sido firmada de forma manuscrita o autógrafa, ya que en los documentos electrónicos se preserva la integridad del documento al estar encriptada la información; mientras que, si son realizados con firma electrónica simple, no tendrá la misma validez probatoria que con la firma electrónica certificada, sino que serán vistos bajo las reglas de la sana crítica.

Basándonos en la Ley de Comercio Electrónico, en el art. 7 trata sobre la información que se da por los medios electrónicos, esta tiene la misma validez, fuerza probatoria y efectos jurídicos que la información que en formato físico, al valorar la fuerza probatoria se tomará en cuenta la facilidad y seguridad en cómo se genera.

Y para culminar, el Decreto N° 875 de la Ley de Protección de Datos Personales, en los arts. 26 y 37 hacen referencia a la carga de la prueba, la cual recae sobre quien resguarde la base de datos, en cualquier caso, siempre protegiendo de terceros no autorizados para que no accedan a los datos personales y hacer ver que el tratamiento o transferencia de ellos se realiza de acuerdo a la ley.

A continuación, sintetizamos por medio de un cuadro resumen las relaciones y aspectos comunes entre las leyes tratadas:

Temas	LFE	LCE	LPDP
Principios en común entre las leyes tratadas.			
Confidencialidad	Art. 4 lit. c)	Art. 20	Arts. 5 lit. g), 9 inc. 2
Seguridad	Art. 4 lit. g)	Art. 20	Arts. 5 lit. g), 20
Equivalencia Funcional.	Arts. 2, 4 lit. d), 7 y 8	Art. 4 lit. a)	
Neutralidad Tecnológica	Arts. 2, 4 lit. f)	Art. 4 lit. b)	
No Repudiación	Art. 4 lit. e)	Art. 4 lit. c)	
Aspectos o puntos en común entre las leyes tratadas.			
Tratamiento de Datos Personales	Art. 5	-	Arts. 24, 38, 40, 43, 49
Validez de los contratos	Art. 31	Arts. 14, 19	
Conservación de mensajes de datos	Arts. 11, 12, 13 , 14, 34	Art. 26	Art. 41 lit. e)
Valor Probatorio	Arts. 10 y 24	Art. 7	Arts. 26, 37

5.3. Retos a superar para potenciar y dar aplicación a la Firma Electrónica en El Salvador

5.3.1 Potenciar el Gobierno Electrónico en El Salvador

Junto con la implementación de la firma electrónica en el país se puede potenciar la innovación, dando paso al Gobierno Electrónico en donde todos los procesos y trámites a realizar entre las instituciones y los usuarios sean por medios digitales, dejando de lado procesos burocráticos y tediosos de los que toda la población se queja.

Teniendo en cuenta que El Salvador forma parte de una Red de Gobiernos Electrónicos de América Latina y el Caribe, llamada “Red GEALC”, siendo una iniciativa presentada por el Gobierno de Chile a la Organización de los Estados Americanos (OEA) en el 2003. La iniciativa buscaba obtener financiamiento para implementar un taller regional de gobierno electrónico, dando a conocer los desafíos, avances y experiencias del Gobierno Chileno a los países de América Latina.⁷⁸

El país al formar parte de la Red GEALC, se comprometió a realizar esfuerzos y darle relevancia al uso de las tecnologías en sus instituciones, con el fin de dar paso a un gobierno electrónico, aumentando de esta forma la eficiencia en los procesos administrativos o de cualquier índole, reflejando este avance con los países de la región. Por esta razón el país se encuentra más comprometido a realizar esfuerzos para hacer grandes cambios en sus instituciones, buscando la agilidad y mejora en los servicios que presta, la implementación de nuevos equipos y soportes electrónicos para estar calificado en el desarrollo y funcionamiento de un sistema electrónico a nivel gubernamental.

⁷⁸ Banco Interamericano de Desarrollo, Red GEALC: *Cinco años de apoyo al E-Gobierno en América Latina y el Caribe*, (México) 2010, 6

5.3.2 Sancionar el Decreto N° 875 de la Ley de Protección de Datos Personales en El Salvador

Es de vital importancia el sancionamiento por parte del Presidente de la República sobre el Decreto N° 875 de la Ley de Protección de Datos Personales, si bien es cierto existen otros cuerpos normativos que buscan regular en cierta forma la protección de datos personales, tal como se abordó en el capítulo 4, planteando también que dicha regulación se encuentra esparcida entre diversos cuerpo normativos, además en ellas no se regula la protección de datos personales desde el punto de vista electrónico, en donde es mucho más fácil invadir la privacidad de las personas, por medio de virus, hackeando correos o redes sociales, es por ellos que es necesario tener una ley marco en donde se centre en protección de este derecho.

Para llegar a crear este decreto se pasó por el trabajo y estudio de tres proyectos de ley, culminando con el Decreto N° 875 de la Ley de Protección de Datos Personales, tomando en consideración puntos de los proyectos previamente presentados, con el fin de unificar las ideas presentadas por el estudio de los partidos políticos.

Un punto muy importante es que se debe tomar en consideración los límites que deben tener las páginas web al momento de acceder a ellas, con respecto a las autorizaciones consciente o inconscientemente que les damos al acceder, como lo son las cookies, asimismo los límites que deben tener las páginas en línea de compras, ya sean de almacenes o intermediarios, con respecto a los datos personales que se introducen, evitando cualquier robo de información o de identidad y con ello el cometimiento de algún ilícito.

Como último punto, también se debe tomar en cuenta la creación del reglamento a este cuerpo normativo, que ya lo establece en su art. 75, en donde se espera se regulen cómo estará conformada la institución

encargada de velar por el cumplimiento de esta ley y porque se protejan los datos de las personas en el país.

5.3.3 Autorizar a las certificadoras digitales y certificadoras de almacenamiento electrónico

Como hemos venido hablando a lo largo del trabajo de investigación, uno de los impedimentos y retos a proponer para solventar el problema que se tiene con el uso de la firma electrónica en el país, se debe a que aún no hay un ente certificador autorizado por la Unidad de Firma Electrónica perteneciente al Ministerio de Economía.

Que no existe aún un ente que emita certificados digitales ni de almacenamiento es un gran problema, ya han pasado más de 5 años desde que entró en vigencia la Ley de Firma Electrónica y hasta el momento no se le ha concedido permisos de emisión a ningún ente nacional o extranjero para que venda los certificados digitales o de almacenamiento, para de esta forma dar uso a la firma electrónica certificada.

La no existencia de entes certificadores dificulta en gran medida la implementación y del uso de la firma electrónica en el país, ya que si no hay quien ofrezca este servicio sin previa autorización es imposible comenzar a tener documentos electrónicos con la validez jurídica que le reviste la Ley de Firma Electrónica, es por ello que es de suma importancia que se dé paso a los trámites previsto en las respectivas leyes para que concursen las empresas que puedan dar tanto servicio de emisión de certificados digitales (firma electrónica) y emisión de certificados de almacenamiento, ambas de tipo electrónico.

Al momento de contar con los entes adecuados se podrá implementar la firma electrónica certificada en el país junto con el resguardo de datos personales de los usuarios de esta, de igual forma se verá involucrado el comercio electrónico, mediando las transacciones hechas por esta vía, brindándole una mayor seguridad y dotándolo de validez ante cualquier

reclamo; por estas razones es imprescindible la pronta autorización de los entes antes expuesto, a su vez llevar al gobierno y al país a una remodelación de los sistemas virtuales y la forma de realizar cualquier gestión dentro de él.

5.3.4 Implementar la Ley de Comercio Electrónico con el correcto funcionamiento de la Firma Electrónica en El Salvador

Para el óptimo desarrollo y funcionamiento de la Ley de Firma Electrónica en nuestro país es importante que se le dé cumplimiento a la Ley de Comercio Electrónico, al implementar esta ley se tendría un mayor campo de aplicación para la firma electrónica en general, generando mayor número de contratos desde la oficina o el hogar, sin necesidad de desplazarse a diferentes puntos de la nación o entre países, optimizando el tiempo de las personas, facilitando y agilizando el desarrollo del intercambio comercial, además modernizando al país al implementarla, y mantener toda relación contractual en dispositivos electrónicos resguardados, realizando reuniones, compra de productos e incorporación de nuevos modelos contractuales, llegando a internacionalizar empresas nacionales y potenciando de esta forma limitaciones que pudieron tener en cuanto a su alcance, debido a la falta de nichos para darse a conocer y desarrollarse.

En la Ley de Comercio Electrónico se busca ofrecer una herramienta legal que regule las relaciones contractuales entre las partes y fijar las pautas en las transacciones con terceros (distribuidores o vendedores) de todos los tratos realizados en línea.

Una particularidad que se pidió en algún momento en esta ley, es que regulará lo concerniente a la protección al consumidor, lo cual ya no era necesario hacer, ya que, con la reforma realizada en el 2019 a la Ley de Protección al Consumidor, se abordó lo referente a las disputas que se

podieran dar en el comercio electrónico, detallando que el ente competente es la Defensoría del Consumidor.

5.3.5 Destacar el rol del notario ante el uso de la Firma Electrónica

Al momento de maximizar el uso de la firma electrónica y dejar de lado la mayoría de contratos hechos en papel, el notario quedaría relegado casi en su totalidad, haciendo uso de él solo cuando el acto o contrato exija indispensablemente solemnidades, tal como lo detallan los arts. 8 y 30 inc. 2 de la Ley de Firma Electrónica.

Al conocer las limitantes que pueda tener el notario ante el uso de la firma electrónica se puede solventar al reformar la Ley del Notariado e implementar la firma electrónica notarial, la cual consiste en, “una firma electrónica avanzada certificada que, previamente dada a conocer a la dirección de notarías, archivo de notarías, Secretaría de Gobierno del Estado, puede ser utilizada por el notario para autorizar instrumentos, enviar telemáticamente actas y escrituras, remitir información a las autoridades administrativas, judiciales y en general para cualquier acto que esté permitido en la ley. La firma electrónica notarial tendrá el mismo valor que la firma autógrafa del notario acompañada de su sello de autorizar”.⁷⁹

El notario al poder tener un papel más protagónico con su propia firma electrónica contribuiría a la formación de un Gobierno Electrónico, entregando todo tipo de documentos públicos o privados de forma electrónica y pudiendo implementar un protocolo electrónico con el mismo valor del protocolo en físico, teniendo siempre las mismas formalidades que la Ley del Notariado ya estipula.

⁷⁹ Carlos Eric Ixtlapale Carmona, “El reto de la firma electrónica notarial: su posible uso para autorizar todos los instrumentos notariales”, Revista IUS, vol. 9, n. 36, jul/dic (2015), 12

5.3.6 Detallar puntos básicos para crear y operar las páginas web

Desde el momento en que se comienza a utilizar el internet para vender productos, muchas tiendas físicas y emprendimientos se animaron a crear páginas en línea en donde puedan ofrecer sus productos, cada una con su personalización y toque único, con el fin de llamar la atención de los clientes, es por ello, que es necesario dar ciertos estándares para crear estos sitios web, que cumplan con requisitos mínimos, como tener carrito de compra para saber qué están adquiriendo los clientes, detallar en qué consiste el producto y añadir ilustraciones que lo representen, así como establecer una sección en donde se detalle el contenido legal de la página como las políticas de privacidad, las cookies, términos y condiciones de los productos y envío del mismo, el establecer estos puntos es necesario, para que la tienda en línea pueda funcionar óptimamente y los usuarios se sientan seguros.

Al momento de operar la página, también se debe ser claro en lo que se ofrece, detallar en su descripción a qué se dedica la tienda, saber con antelación cuáles son las preguntas más frecuentes que puedan realizar los clientes para poder tener preguntas programadas con sus respectivas respuestas, haciendo uso de un chatbot, también otras formas de saber operar bien la página web sería dando facilidades en la forma de pago, utilizando las diferentes instituciones bancarias nacionales y ampliando los métodos de pago para darle facilidades a los clientes.

Todos estos ayudarían a las personas que deseen involucrarse en las ventas en línea y realizar comercio electrónico, dando lineamientos y reglas claras que deben seguir para funcionar de acuerdo a la ley y puedan prosperar en sus negocios.

CONCLUSIONES

En este apartado se desarrollan las conclusiones de la investigación, para poder exponer de una manera clara y concreta cada problemática o avance que se ha dado desde la creación de la Ley de Firma Electrónica, con ello plantear una lista de recomendaciones para poder dar una posible y pronta solución a estos problemas actuales y los posibles que surgirán a futuro.

En el Capítulo Uno; se destaca la firma electrónica, recordando que es el tema que nos atañe en este trabajo, siendo un poco más específicos la firma electrónica certificada, clasificación que nos brinda la LFE; se analizó que es de suma importancia y necesidad, tomando en cuenta dos principios fundamentales que son, el “no repudio” y “la seguridad”, ambos se encuentran en el art. 4 de la misma ley, el no repudio da cabida a que ningún signatario puede rechazar los mensaje enviado, debido al nivel de encriptación que este posee, esto nos lleva a garantizarle al signatario y al usuario la seguridad del proceso electrónico-legal. ¿Por qué es importante y necesaria? Porque analizando la evolución que ha tenido la firma electrónica en los diferentes continentes, nos damos cuenta de que en El Salvador está en un gran retraso en el desarrollo tecnológico-legal, a pesar de tener una Ley de Firma Electrónica, esta no ha podido ser implementada por falta de impulso tecnológico y económico, dando así, la no aplicación de su propia ley.

En el Capítulo Dos también se hace alusión al principio de seguridad, debido a que versa sobre la criptografía, la cual que se puede resumir en “clave de seguridad de datos”, esta que puede ser en llave privada o pública. Analizando el capítulo, concluimos que la Unidad de Firma Electrónica debe hacer un estudio minucioso para autorizar a los diferentes entes certificadores, buscar en ellos que cumpla con los requisitos y obligaciones que establece la LFE, para que esa seguridad, sea garantizada, de igual forma que sea un ente proveedor nacional o

internacional quien emita certificados útiles, legal y económicamente favorables a los usuarios, para sacar al país del retraso tecnológico.

En el Capítulo Tres, se destaca una herramienta fundamental para llevar a cabo el Comercio Electrónico que es “el internet”, hay que destacar, que el proceso del comercio electrónico debe ser claro, seguro y ordenado, para que se puedan realizar una contratos y transacciones con confianza y agilidad, destacando dos principios que la Ley de Comercio Electrónico trata, en primer lugar “el no repudio”, y “la equivalencia funcional”, en la que los documentos tienen la misma validez como estuvieran materialmente o físicamente.

Otro aspecto importante de este capítulo es la conexión que existe entre la firma electrónica y el comercio electrónico, esto se debe a que entre ellos se pueden complementar para realizar contrataciones o transacciones entre las partes, dándole a la firma electrónica un campo amplio de aplicación, proporcionando al mismo tiempo la seguridad y validez necesaria por cualquier conflicto que se llegue a dar, todo esto gracias al cifrado que proporciona.

En el Capítulo Cuatro, se concluye que se necesita de manera urgente la aprobación de una Ley de Datos personales, para que los usuarios a la hora de adquirir un certificado de firma electrónica tengan la seguridad de que estará a salvo su información personales, más la información sensible que uno posee, si bien es cierto, en el Art. 5 de la Ley de la Firma Electrónica manifiesta las reglas para el tratamiento de los datos personales, no menciona en base a qué criterios y a que procedimientos se resolverán las falta de las obligaciones más que sanciones administrativas que la misma LFE estipula.

Para poder garantizar todo lo anterior, se debe basar en los principios generales para la protección de datos, dentro de estos, los dos más importantes son, el “principio de consentimiento”, absolutamente nadie

puede obligar al titular a brindar sus datos personales, siempre debe de existir un consentimiento libre y expreso y como segundo el “principio de seguridad de datos”, es de estricto cumplimiento garantizar la seguridad y confidencialidad de los datos, debido a que su alteración o cualquier tratamiento no autorizado sería un daño grave a los derechos de integridad y honor del titular.

Y con respecto al Capítulo Cinco, el cual se abordan ideas claves para el desarrollo de la firma electrónica, planteando retos que no están alejados de la realidad, los cuales están detallados en este capítulo, se lograría tener un pleno funcionamiento y óptimo avance en la legislación salvadoreña, ya que al implementar el firma electrónica junto con su ley, podemos impulsar nuevas formas de realizar comercio, compartir nuevos proyectos con otros países de la región o a nivel de otros continentes y no quedaríamos relegados en temas tecnológicos.

RECOMENDACIONES

Como se mencionó, uno de los principales retos a superar en esta investigación es, el sancionamiento del decreto N°875 de la Ley de Protección de Datos Personales, se ha identificado que lo idóneo para resolver ese tipo de conflicto es la creación de un ente autónomo, tal como lo establece el capítulo XI del decreto antes mencionado. Al momento de entrar en vigencia la LPDP es necesario que este ente se cree de una forma rápida debido a que sin él caeríamos en la misma falta de un procedimiento idóneo para la protección de datos personales de los usuarios, es decir que a pesar de que se regule en el Art. 5 de la LFE la protección de los datos personales no es suficiente para proteger y amparar la seguridad de los datos de los usuarios.

Con la evolución de una “legislación electrónica” se puede ver el rol del notario un tanto afectado, debido a que se tiene la idea de que el notario solo podrá realizar sus funciones cuando se trate de actos o contratos que exijan solemnidades, pero esta idea podría llegar a cambiar al momento de hacer una renovación y reforma de la legislación judicial con una Ley de Notariado Electrónico, para en un futuro poder llegar a tener un protocolo electrónico, todo esto haciendo uso de una futura firma electrónica notarial, que dota de autenticidad y valor lo que se realice, garantizando la seguridad de los actos o contratos y la integridad de los involucrados.

Aprovechando el auge y desarrollo del comercio electrónico junto con implementación la firma electrónica, una recomendación clave para poder tener una nueva fuente de ingresos para el país, es aplicar los impuestos normales a quienes realicen comercio electrónico, estos impuestos serían, IVA y Renta y de ser necesario otros ya existentes o la creación de nuevos impuestos apegados a las nuevas tecnologías.

Estas son las recomendaciones dadas, apegadas a lo ya establecido en el cuerpo del trabajo, en la búsqueda de la mejora del país, de las normas existentes y las nuevas normativas que se necesiten, con el fin de hacer reflexión en que las leyes deben estarse adecuando a los diversos avances que va sufriendo el país en un mundo cada vez más globalizado.

BIBLIOGRAFÍA

LIBROS:

Basante Andrade, Andrea Verenice, Mónica Cecilia Gallegos Varela, Cathy Pamela Guevara Vega, y otros, *Comercio Electrónico*, Imprenta Universitaria, Universidad Técnica del Norte. Ibarra, Ecuador, 2016.

Cabanellas de Torres, Guillermo, *Diccionario Jurídico Elemental Nueva Edición Actualizada por Guillermo Cabanellas de las Cuevas*, Editorial Heliasta S.R.L. undécima edición, 1993.

Cardona Madariaga, Diego Fernando, *El gobierno electrónico. Una herramienta estratégica de toma de decisiones*, Univ. Empresa. Bogotá. Colombia, 2004.

Corominas, Joan, *Breve Diccionario Etimológico de la Lengua Castellana*. Editorial Gredos, tercera edición muy revisada y mejorada, Madrid, 1987.

Fernández Domingo, Jesús Ignacio, *La firma electrónica: aspectos de la ley 59/2003, de 19 de diciembre*, Editorial Reus, Madrid, 2006

Martínez Nadal, Apollonio, *Comercio Electrónico, firma digital y autoridades de Certificación*, Editorial Civitas, 3era ed. Madrid, España, 2001

Hernández Rivera, Laura Nathalie, *El ABC de la Protección de Datos Personales*, Categoría de los datos personales, 2019.

Real Academia Española, *Diccionario de la Real Academia Española RAE*. Vigésimo tercera edición, 2014.

PUBLICACIONES PERIÓDICAS:

Centro de Trámites de Importaciones y Exportaciones Banco Central de Reservas, “E-Commerce: Herramienta de facilitación del Comercio Internacional”, INFOCIEX, n. 3 año 19, (julio-septiembre 2017).

FUSADES – Análisis legal e institucional, “Observaciones a los proyectos de Ley de Protección de Datos Personales, Parte I: Introducción, antecedentes normativos, principios internacionales y derecho comparado”, n. 199 (2019).

Gayá, Romina, Conexión INTAL, Banco Interamericano de Desarrollo (BID), “El comercio electrónico y la inserción internacional de América Latina y el Caribe”, n. 229, (15 octubre 2015).

Pabón Cadavid, Johnny Antonio, “La Criptografía y la Protección a la Información Digital”, Revista la Propiedad Inmaterial, n. 14 (2010).

Rojas Bejarano, Marcela, NOVUM JUS, Universidad Católica de Colombia, “Evolución del Derecho de Protección de Datos Personales en Colombia respecto a estándares Internacionales”, n. 8, (enero-junio 2014).

PUBLICACIONES PERIÓDICAS DIGITALES:

Biblioteca del Congreso de la Nación, “Dossier Legislativo, Legislación y Doctrina Extranjera, Firma Digital y Gobierno Electrónico”, Dirección Servicios Legislativos, año IV, n. 103, (mayo 2016)
<https://bcn.gob.ar/uploads/Dossier-103---Legislacion-Extranjera---Firma-Digital-y-Gob.-Electronico>

Informática Jurídica, “Análisis comparativo de la legislación y proyectos a nivel mundial sobre firmas y certificados digitales”, (1 de enero de 2015), <http://www.informatica-juridica.com/trabajos/analisis-comparativo-de-la-legislacion-y-proyectos-a-nivel-mundial-sobre-firmas-y-certificados-digitales/>

Ixtlapale Carmona, Carlos Eric, “El reto de la firma electrónica notarial: su posible uso para autorizar todos los instrumentos notariales”, Revista IUS, vol. 9, n. 36, jul/dic (2015) http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472015000200303

TESIS:

Amaya Tario, Tomas Alberto; Andrea Karina Avalos Cisneros, Karen Nathaly, Jule Moreno, “Respeto al Derecho de Intimidad en la Estructura de la Ley de Intervenciones de Telecomunicaciones”, (tesis de grado, optando al título de Licenciatura en Ciencias Jurídicas, Universidad de El Salvador, 2012).

Galán Cortez, Jeannie Elizabeth; Laura Azucena García Mejía, Vilma Verónica Gómez Barahona, “La Firma Digital como medio de seguridad y consentimiento en las transacciones del Comercio Electrónico”, (tesis de grado, optando al título de Licenciatura en Ciencias Jurídicas, Universidad de El Salvador, 2006).

López Flores, Sarbelio Enrique; “La Firma Electrónica, Tecnología del Siglo XXI en la Legislación Salvadoreña”, (tesis de grado, optando al título de Licenciatura en Ciencias Jurídicas, Universidad de El Salvador, 2007).

Rioseco San Martín, Constanza Alejandra; “Introducción a la Criptografía”, (memoria para optar al título de profesor de enseñanza media en educación matemática, Universidad del Bío-Bío, 2016).

Urrego, Elizabeth; Vargas Aguirre, Maribel; Chica Echavarría, Verónica, “Propuesta de Implementación de la Firma Digital para la Cooperativa CCOPSERP”, (tesis de grado, para optar a la licenciatura en Ciencias Económicas y Administrativas, Universidad de Medellín, 2011)

Zarceño García, Javier Armando; Pedro de Jesús Canales Garay, “La Protección de Datos Personales: un Análisis Constitucional de la Ley de Acceso a la Información”, (tesis de grado, optando al título de Licenciatura en Ciencias Jurídicas, Universidad de El Salvador, 2013).

Zuñiga, Víctor Alejandro, “La Actividad Comercial”, (tesis de grado, optando al título de Licenciatura en Administración de Empresas, Universidad de las Américas Puebla, México, 2017).

SITIOS WEB:

Banco Interamericano de Desarrollo, Red GEALC: Cinco años de apoyo al E-Gobierno en América Latina y el Caribe, 2010.
<https://www.oas.org/es/sap/dgpe/pub/GEALC4.pdf>

Certificación Electrónica, Banco Central del Ecuador, Preguntas Frecuentes, acceso el 10 de febrero de 2021,
<https://www.eci.bce.ec/preguntas-frecuentes>

Informática jurídica, La Firma Digital y Entidades de Certificación, acceso el 13 de febrero de 2021,
<http://www.informatica-juridica.com/trabajos/la-firma-digital-y-entidades-de->

[certificacion/#3.1.%20FUNCIONES%20DE%20LAS%20AUTORIDADES%20DE](#)

Ministerio de Economía de El Salvador, Definición de los Proveedores de Servicios de Certificación, acceso el 13 de febrero de 2021, <https://firmaelectronica.minec.gob.sv/portfolio-view/video-format/>

Ministerio de Economía de El Salvador, Definición de los Proveedores de Servicios de Certificación, acceso el 15 de febrero de 2021, <https://firmaelectronica.minec.gob.sv/portfolio-view/proveedor/>

Ministerio de Economía de El Salvador, Preguntas y Respuestas, ¿Qué es la Firma Electrónica?, acceso el 26 de octubre de 2020, <https://firmaelectronica.minec.gob.sv/about/faqs/>

Ministerio de Economía de El Salvador, Unidad de Firma Electrónica, Tasas de los certificados Digitales, acceso el 10 de febrero <https://firmaelectronica.minec.gob.sv/>

Secretaría General de la Comunidad Andina, Comunidad Andina, El comercio electrónico en los países en desarrollo: Oportunidades y retos para las pequeñas y medianas empresas, acceso el 10 de marzo de 2021, <http://www.comunidadandina.org/Prensa.aspx?id=3400&accion=detalle&c at=AP&title=el-comercio-electronico-en-los-paises-en-desarrollo-opportunidades-y-retos-para-las-pequenas-y-medianas-empresas>

BLOG O COMENTARIO:

Ale Ortega, Tipos de Firma Electrónica: Conoce los tipos de firmas y encuentra la mejor opción para tu negocio (Blog) Mifiel, 2019, <https://blog.mifiel.com/comparacion-tipos-de-firmas/>

Leyre Soto, ¿Qué es una firma digital? (Blog) Signaturit, 18 de agosto de 2020, <https://blog.signaturit.com/es/que-es-una-firma-digital>

NORMAS JURÍDICAS:

Concerning Electronic Signatures and Certification Services. Japón: La Cámara de Representantes, 2000

Constitución de la República de El Salvador. El Salvador: Asamblea Legislativa de El Salvador, 1983

Decreto N° 875 de la Ley de Protección de Datos Personales. El Salvador, Asamblea Legislativa de El Salvador, 2021

Decreto 892/2017. Argentina: Congreso de la Nación Argentina, 2017

Electronic Communications Act 2000. Reino Unido: Parlamento de Westminster, 2000

Electronic Communication and Transactions Act. 2002. Sudáfrica: Parlamento de Sudáfrica, 2002

German Signature Law of 2001. Alemania: Bundesrat, 2001

Ley de Comercio Electrónico. El Salvador: Asamblea Legislativa de El Salvador, 2020

Ley E-SIGN. Estados Unidos de América: Congreso de los Estados Unidos, 2000

Ley de Firma Digital 25.506. Argentina: Congreso de la Nación Argentina, 2001

Ley de Firma Electrónica. China: Congreso Nacional del Pueblo, 2004

Ley de Firma Electrónica. El Salvador: Asamblea Legislativa de El Salvador, 2015

Ley de Firma Electrónica Avanzada. México: Congreso General de México, 2011

Ley de Transacciones Electrónicas. Australia: Parlamento de Australia, 1999

Ley N° 51. Panamá: Asamblea Nacional de Panamá, 2008

Ley N° 82. Panamá: Asamblea Nacional de Panamá, 2012

Ley N° 527. Colombia: Congreso de la República de Colombia, 1999

Ley N° 2364. Colombia: Congreso de la República de Colombia, 2012

Ley 59/2003, de 19 de diciembre, de firma electrónica. España: Congreso de los Diputados, 2003

Ley 8454. Ley de Certificados, Firmas Digitales y Documentos Electrónicos.
Costa Rica: Asamblea Legislativa de Costa Rica, 2005

Reglamento de la Ley de Firma Electrónica. El Salvador: Asamblea
Legislativa, 2016

Reglamento de la Ley de Firma Electrónica Avanzada. México: Congreso
General de México, 2014

Uniform Electronic Transaction Act. Estados Unidos de América: Congreso
de los Estados Unidos, 1999

SENTENCIAS:

Sala de lo Constitucional, Sentencia de Amparo, Referencia: 642-99. 2000.
El Salvador, Corte Suprema de Justicia, 2000.

Sala de lo Constitucional, Sentencia de Amparo, Referencias: 934-2007.
2011. El Salvador, Corte Suprema de Justicia, 2011