BANCO DE DESARROLLO DE AMÉRICA LATINA

Sistema Económico Latinoamericano y del Caribe

Latin American and Caribbean Economic System

Sistema Econômico Latino-Americano e do Caribe

Système Economique Latinoaméricain et Caribéen

Fundamentos de la firma digital y su estado del arte en América Latina y el Caribe

Relaciones Intrarregionales

Secretaría Permanente del SELA
Caracas, Venezuela
Mayo de 2012
SP/Di N° 7-12

C O N T E N I D O

P R E S E N T A C I Ó N

La Secretaría Permanente del SELA se complace en presentar el documento de consulta "Fundamentos de la firma digital y su estado del arte en América Latina y el Caribe", preparado como parte integral del Proyecto piloto de interoperabilidad y armonización de las Ventanillas Únicas de Comercio Exterior en el marco del Arco del Pacífico Latinoamericano, objeto del Convenio de Cooperación Técnica suscrito entre CAF – Banco de Desarrollo de América Latina y el SELA.

De esta manera, la Secretaría Permanente da seguimiento a la recomendación de los Estados Miembros expresada en la XXXVII Reunión Ordinaria del Consejo Latinoamericano del SELA, celebrada en Caracas, del 19 al 21 de octubre de 2011, de coadyuvar en el desarrollo de la facilitación del comercio internacional, con particular énfasis en las Ventanillas Únicas de Comercio Exterior (VUCE) en tanto que herramienta de primerísima importancia en el avance del comercio sin papel transfronterizo, con criterios de transparencia, simplificación, seguridad jurídica y técnica y, eficiencia.

Para cumplir con estos propósitos se consideró imprescindible analizar y sistematizar los distintos criterios que fundamentan el uso de la firma digital y/o electrónica avanzada o calificada, la seguridad que le es intrínseca, los mecanismos equivalentes, la capacidad probatoria y, en general, cómo los servicios de certificación digital (Certificate Authorities - CA) posibilitan la instrumentación de esquemas de documentación electrónica con validez jurídica.

El fin de este documento es, por tanto, ofrecer una guía útil de consulta para actores gubernamentales y privados, interesados en la instrumentación de la firma digital y/o electrónica avanzada o calificada - concebida como un nuevo fenómeno de interoperabilidad entre países-, y en conocer los atributos de ésta requeridos en las leyes, para facilitar así, el flujo documental electrónico que tiene lugar al interior de cada VUCE nacional y su posibilidad de incidir en el comercio intrarregional y de la región con el resto del mundo.

A partir de este análisis se pretende obtener algunas conclusiones útiles para pensar y actuar con respecto al desarrollo de las Ventanillas Únicas de Comercio Exterior y en los procesos que, como la firma digital, le

son consustanciales, en los países de America Latina y el Caribe.

Después de la introducción, el trabajo se divide en cinco secciones, a saber: Riesgos técnicos y jurídicos de la información electrónica; Principios asociados a los medios electrónicos, abordándose en este punto la equivalencia funcional, la neutralidad tecnológica, la inalterabilidad del derecho preexistente, la buena fe y la libertad contractual. Seguidamente, en una tercera sección, se analizan las Manifestaciones del principio de la equivalencia funcional, esto es, el equivalente funcional de escrito, de firma, de original, de archivo y conservación y, de fecha y hora, para acometer, en la sección cuarta, un resumen del Estado del Arte de la Firma Digital y/o Electrónica avanzada o calificada en América Latina y el Caribe, en el cual se relaciona, por país, la referencia de ley que contiene temas específicos en la materia.

Finalmente, se extraen algunas conclusiones y se recomiendan acciones concretas a los países de América Latina y el Caribe, entre las cuales destaca la necesidad de que las VUCE de la región cuenten con plenas garantías probatorias para mitigar los riesgos asociados a la comunicación electrónica, y establezcan de forma conjunta y decidida, como estándar de seguridad jurídica y técnica, el mecanismo de la firma digital y/o electrónica avanzada o calificada emitida por un prestador o entidad de certificación, con el propósito de hacer posible la implementación de funcionalidades y trámites totalmente electrónicos, aportando a los objetivos del gobierno electrónico y las directrices de cero papel, así como a preparar su sistema a la interoperabilidad como fase indispensable en la facilitación del comercio, desde una perspectiva que enfatice la importancia de la integración regional.

Este documento de consulta ha sido elaborado por la Dra. Marcela Bello Zuluaga, a quien la Secretaría Permanente expresa su mayor reconocimiento.

I. INTRODUCCIÓN

La Secretaría Permanente del Sistema Económico Latinoamericano y del Caribe (SELA), organismo regional intergubernamental que promueve un sistema de consulta y coordinación para concertar posiciones y estrategias comunes de América Latina y el Caribe, ha venido apoyando los distintos proyectos de Ventanillas Únicas de Comercio Exterior (VUCE) como estrategia de primerísima importancia en el marco de la facilitación del comercio en la región, con el propósito de fomentar el intercambio de experiencias y hacer posible la interoperabilidad y la armonización para materializar el intercambio de información electrónica y hacer posible un comercio sin papel, técnica y jurídicamente seguro.

A tal efecto, el SELA ha instrumentado diferentes mecanismos de apoyo con el objeto de promover la aplicación efectiva de las Tecnologías de Información y Comunicación (TIC) en sus Estados Miembros, con énfasis en aquellos aspectos de especial interés como es la seguridad técnica y jurídica de las comunicaciones, específicamente, en temas relacionados con Firmas Digitales y/o Electrónicas los cuales, de conformidad con los diferentes ordenamientos jurídicos, constituyen una pieza clave para garantizar los atributos requeridos en las Leyes y hacer realidad el flujo documental electrónico de las VUCE en cada país e intrarregionalmente.

En este accionar de la Secretaría Permanente del SELA, se inscribe la elaboración del presente documento de consulta como parte de los avances del "Proyecto piloto de interoperabilidad y armonización de las Ventanillas Únicas de Comercio Exterior (VUCE) en el marco del Arco del Pacífico Latinoamericano", objeto del Convenio de Cooperación Técnica entre CAF - Banco de Desarrollo de América Latina y el SELA.

Por lo anterior, el presente documento, titulado "Fundamentos de la Firma Digital y su Estado del Arte en América Latina y el Caribe", se propone brindar un instrumento de consulta para actores gubernamentales y privados interesados en la materia, dándoles a conocer de forma general los detalles que fundamentan el uso de la firma electrónica, la seguridad que aporta, los mecanismos equivalentes, la capacidad probatoria y, en general, cómo los servicios de certificación digital o las denominados prestadores o entidades de certificación digital (Certificate Authorities - CA) cumplen un ejercicio que posibilita la instrumentación de esquemas de documentación electrónica válidos.

El insumo principal para el temario de este documento de consulta se basó en las principales inquietudes en la materia, recabadas durante los últimos cuatro encuentros de VUCE organizados por el SELA, a saber: "I Encuentro Regional Latinoamericano y del Caribe sobre Ventanillas Únicas de Comercio Exterior" (Bogotá, 5 y 26 de marzo de 2010; "I Taller Ventanillas Únicas de Comercio Exterior: consideraciones y propuestas para la acción regional en el marco del Foro del ARCO del Pacífico Latinoamericano" (Valparaíso, Chile 30 de noviembre y 1° de diciembre de 2010); "II Encuentro Regional Latinoamericano y del Caribe sobre Ventanillas Únicas de Comercio Exterior: avances y retos pendientes" (Valparaíso, Chile, 1 y 2 de diciembre de 2010); y "III Encuentro Regional Latinoamericano y del Caribe sobre Ventanillas Únicas de Comercio Exterior: comercio exterior sin papeles y la gestión de riesgos en las operaciones de comercio" (Cámara de Comercio de Lima, 28 y 29 de noviembre de 2011, Lima, Perú).

II. RIESGOS TÉCNICOS Y JURÍDICOS DE LA INFORMACIÓN ELECTRÓNICA

El primer aspecto que interesa abordar se refiere a los riesgos asociados a la implementación de canales electrónicos destacándose su incidencia probatoria y en la validez jurídica. Así se han identificado seis tipos de riesgos, los cuales se definen a continuación:

1. Suplantación

Se refiere al hecho posible de que al estar en presencia de canales electrónicos de comunicación, por ejemplo la red pública de Internet, exista un alto riesgo de que la persona con la que interactúe el sistema no sea quien dice ser, por lo que se hace imprescindible verificar la autenticidad y la garantía de origen en los entornos electrónicos.

En este sentido, la determinación de la autoría es necesaria para verificar, entre otros aspectos, la capacidad y competencia de las partes involucradas en una comunicación electrónica; por ejemplo la representación legal o poder de representación de la persona jurídica o moral es la única que puede vincular de manera efectiva y legal a dicha persona jurídica o moral con una actuación determinada.

2. Alteración

Los medios electrónicos y, en general, la información electrónica contenida en los distintos tipos de de archivos, como son: Word, Excel, pdf, .ppt, o cualquier tipo de procesador de texto, imágenes y video son susceptibles de ser modificados o alterados, lo que por ende puede comprometer la integridad de la información electrónica. En este sentido, la integridad se refiere al atributo requerido para mitigar el riesgo de alteración, y consiste en la confirmación de que el mensaje de datos o información electrónica recibida corresponda a la enviada, por cuanto en la comunicación electrónica dicha información o mensaje es susceptible de ser modificado o alterado. Por ejemplo, una persona sin ningún conocimiento previo en sistemas, puede alterar un correo electrónico recibido, con sólo escribir sobre el texto y remitiéndolo o guardándolo con un contenido que no es el originalmente enviado por su emisor.

Igualmente, en el proceso de transmisión o envío de información electrónica existen trasiegos susceptibles de toma no autorizada de la información y posible modificación de la misma, así como la posibilidad de manipulación de la información durante el proceso de conservación y archivo a lo largo de su ciclo de vida.

3. Pérdida de confidencialidad

El atributo de confidencialidad implica que la información sólo sea compartida entre las personas u organizaciones autorizadas. En el contexto de la red pública Internet, la seguridad y confidencialidad constituyen un verdadero reto habida cuenta que la información y los sistemas que hacen posible su transmisión y acceso en Internet, son susceptibles de ser interceptados por personas no autorizadas. La no pérdida de la confidencialidad es un atributo imprescindible en las comunicaciones electrónicas con importante implicaciones jurídicas y legales.

4. Rechazo o repudio

Se refiere al riesgo jurídico de rechazo de la autoría o de la integridad de información trasmitida por medios electrónicos.

5. Negación de recepción

En la mayoría de sistemas de información electrónica, especialmente en la mensajería a través de correo electrónico, la recepción del mensaje queda atada al accionar del destinatario o receptor, lo que posibilita su negación.

En el caso de un correo electrónico los acuses de lectura tradicionales dependen de que el receptor autorice dicha respuesta de lectura al emisor. Sin embargo, estos parámetros pueden ser fácilmente alterados, ya que los "acuse de recibo" corresponden a un texto simple sin protección y no contienen ningún tipo de información acerca del contenido del mensaje; esto mismo puede suceder en otros sistemas de transmisión de datos, por lo que su capacidad probatoria, y por ende, su validez jurídica, son muy limitadas.

6. Conflictos en la fecha y hora

La fecha y hora en la generación, envío y recepción de información electrónica juega un papel de alta importancia en materia probatoria.

La fecha y hora de generación de un documento en un procesador de texto vinculará la fecha y hora del computador de su emisor, y esta fecha podría estar errada, desincronizada, o no atender la fecha y hora del país donde se van a producir los efectos jurídicos de la transacción. Es posible redactar y enviar correos electrónicos sin estar conectado a Internet, sin embargo, dicho correo asocia como fecha y hora de envío la del momento en que se activó "enviar" aunque el correo permanezca aún en la bandeja de salida.

En tal sentido, cabe destacar que los proyectos de sistemas de información que buscan automatizar procesos, procedimientos o trámites administrativos, como lo son las Ventanillas Únicas Electrónicas de Comercio, deben tener en cuenta los anteriores riesgos asociados a medios electrónicos, con el propósito de analizar su impacto y establecer los mecanismos que los mitiguen y poder garantizar así su validez jurídica.

Por otra parte, sumados a los riesgos antes expuestos, existen una serie de retos que deben ser abordados en relación a los documentos tradicionales en papel, a saber:

- El contenido de un documento electrónico está consignado sobre un soporte electrónico no apreciable por los sentidos;

- La obsolescencia de las tecnologías que intervienen en la generación y el almacenamiento de estos documentos, equipos y aplicaciones, y la fragilidad de los soportes en los que se conservan, teniendo en cuenta el desarrollo y evolución de la tecnología;

- La virtualidad de la información, como es el caso del correo electrónico, que puede ser eliminado muy fácilmente, dejando sin soporte a las transacciones u operaciones con incidencia jurídica;

- La ubicación de la información utilizada por varios organismos que la comparten, lo que impide, en muchos casos, identificar al creador o generador de la misma;

- Las dificultades para identificar el tipo y la forma documental de estos documentos. El formato documental (original, copia) tiene especial relación con el valor probatorio de estos documentos, o, lo que es lo mismo, con su validez jurídica.

En virtud de lo expuesto, el presente documento de consulta se propone abordar varios de los mecanismos técnicos y jurídicos destinados a evitar los riesgos antes enunciados, y a su vez incentivar el uso de medios electrónicos de manera confiable, los que sin duda ofrecen mayor seguridad técnica y jurídica a la información que la brindada por los soportes físicos, agregando además eficiencia y eficacia a los procesos.

III. PRINCIPIOS ASOCIADOS A LOS MEDIOS ELECTRÓNICOS

La mayoría de los países latinoamericanos y caribeños han hecho esfuerzos importantes en el diseño e instrumentación de políticas públicas de gobierno electrónico sustentadas en el "cero papel", con miras a promover la transparencia, la seguridad, la eficiencia y la eficacia administrativa. En tal sentido, han incentivado la instrumentación de trámites por medios electrónicos como son: i. los servicios que el Estado le presta al ciudadano y a los empresarios a través de las Ventanillas Únicas Electrónicas cuyo objetivo es racionalizar y simplificar los trámites de comercio a lo largo de toda la cadena de suministros, ii. la prestación de servicios de factura electrónica que facilitan el control de la evasión de impuestos e incrementan la eficiencia empresarial y, iii. lo relacionado con los sistemas electrónicos de contratación que propenden a la transparencia y democratización de las compras públicas, entre otras iniciativas de gobierno en línea.

La instrumentación efectiva de las iniciativas "cero papel" de gobierno electrónico dependen y requieren de manera imprescindible de marcos jurídicos de operación, por lo que en los últimos diez años los países de América Latina y el Caribe se han preocupado por contar con leyes y normas que habiliten el uso de las tecnologías y, en consecuencia, regulen los mecanismos de aseguramiento y otorguen garantías a las partes.

Teniendo en cuenta lo antes dicho, los marcos jurídicos regionales existentes y en proceso de emisión, deben involucrar y atender los siguientes principios medulares:

1. Equivalencia Funcional: "Catalogado como el principio vector de los medios electrónicos"

Es el principio que permite que todo aquello que se pueda realizar por un medio físico o tradicional pueda ser realizado por medios electrónicos con el mismo valor jurídico y probatorio.

Es decir, la función jurídica que cumple la instrumentación escrita y autógrafa respecto de todo acto jurídico, o su expresión oral, la cumple de igual forma la instrumentación electrónica a través de un mensaje de datos (información electrónica), con independencia del contenido, extensión, alcance y finalidad del acto.

Desde esta perspectiva, la equivalencia funcional trae consigo la no discriminación de la información electrónica (mensajes de datos) con respecto al medio escrito tradicional, lo que permite darle el mismo tratamiento desde el punto de vista probatorio y jurídico. Con ello aspira, que a través de las Tecnologías de la Información y Comunicación (TIC) se reproduzca enteramente toda garantía que el medio físico o procedimiento tradicional exija o requiera.

2. Neutralidad tecnológica: "Principio que permite dar perdurabilidad a las normas"

Es el principio que establece que la ley y su implementación no debe estar atada a una tecnología en particular, sino que debe considerar las tecnologías que propiciaron su elaboración y reglamentación, así como las tecnologías que se están desarrollando y están por desarrollarse.

3. Inalterabilidad del derecho preexistente: "No se altera, ni modifica el actual régimen sustancial del derecho"

El comercio electrónico no implica una modificación de la sustancialidad del actual derecho de las obligaciones. Ello es así, porque el canal electrónico y su aplicabilidad jurídica sobre todo tipo de transacciones es esencialmente un nuevo soporte y medio de transmisión de las voluntades negóciales o pre-negóciales. De esta manera, si se realiza una maniobra engañosa para obtener un beneficio económico por la vía de una estafa, utilizando un canal electrónico, se aplica el código penal del país respectivo, sin que el canal electrónico tenga relevancia alguna, por la única razón de que sea electrónico. De hecho, el canal electrónico no produce efecto o procedimientos distintos ante una actuación. Si se habla de temas administrativos, aplicará el denominado código contencioso administrativo, si son de tipo procesal se aplicará el código de procedimiento civil, y si son de tipo comercial, se aplicará el código de comercio y así sucesivamente.

Cabe destacar que la práctica de este principio en los ordenamientos jurídicos regionales ha sido el habilitar, a través de instrumentos normativos especiales, el uso de canales electrónicos en cada rama del derecho.

4. Buena fe: "Este principio es simplemente una reafirmación del fundamento que informa a nivel general todo el derecho"

Cuando se hace referencia al intercambio nacional o internacional de bienes y servicios, o cuando hablamos de comercio electrónico, este principio adquiere especial relevancia por las características del intercambio que se realiza mediante el uso de soportes tecnológicos donde la buena fe, como principio esencial de los negocios, representa la base fundamentada en la igualdad, el trato digno y la confianza.

5. La libertad contractual:

La libertad contractual es la manifestación o consecuencia necesaria del principio de la inalterabilidad del derecho preexistente en el contexto del comercio electrónico. La libertad contractual es un derecho que se debe contextualizar en el marco de la libertad de empresa, de la autonomía privada y de la libertad de competencia.

A continuación se hace especial referencia al principio de la equivalencia funcional y sus manifestaciones, por considerarse de la mayor relevancia en el contexto del comercio sin papel y de la información electrónica.

IV. MANIFESTACIONES DEL PRINCIPIO DE LA EQUIVALENCIA FUNCIONAL

En la actualidad puede afirmarse que en la mayoría de los países de América Latina y el Caribe no se le niegan efectos jurídicos, validez o fuerza obligatoria a información alguna por el sólo hecho de estar en forma de mensajes de datos o ser información electrónica.

Las leyes o normas en la región, aunque con diferencias en materia nominativa, han utilizado como marco de referencia la ley de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (en lo sucesivo UNCITRAL por sus siglas en inglés) de 1996, la cual establece como mecanismo de aseguramiento jurídico y técnico de las comunicaciones, la denominada firma digital o electrónica emitida por un prestador o entidad de certificación digital. Posteriormente se abordarán estos conceptos.

A la fecha han sido identificadas cinco (5) manifestaciones del principio de equivalencia funcional antes descrito, todas presentes en el tratamiento del fenómeno por medios informáticos, así se tienen:

1. El equivalente funcional de escrito

Este principio establece que cuando se requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos o información electrónica siempre que la información que éste contenga sea accesible para su posterior consulta.

Por tal razón, en materia de información electrónica se puede abordar, con plena validez, el documento electrónico como noción procesal de documento, entendiendo con ello que su soporte, para cualquier caso de instrumentación de sistemas de información o virtualización, será el denominado mensaje de datos: es decir, información contenida en un medio electrónico que permita la accesibilidad a la misma a través del tiempo.

2. El equivalente funcional de firma

Las leyes o normas en la materia establecen el equivalente funcional de firma cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma en relación con un mensaje de datos o información electrónica. Así se entenderá satisfecho dicho requerimiento al cumplirse las siguientes condiciones:

- Cuando se ha utilizado un método que permita identificar al iniciador de un mensaje de datos o información electrónica y para indicar que el contenido cuenta con su aprobación.

- Cuando el método sea tanto confiable como apropiado para el propósito del mensaje generado o comunicado.

Las firmas manuscritas existen en los ordenamientos jurídicos latinoamericanos y caribeños desde hace aproximadamente 65 años. Generalmente, se encuentran contenidas en el código de comercio y corresponden a la representación gráfica de la voluntad única y exclusiva de cada individuo y sobre la cual en materia probatoria se pueden aplicar conceptos de peritaje grafológico para análisis de su autenticidad. La firma manuscrita ha sido el mecanismo jurídico por excelencia en el medio físico o tradicional, pues garantiza dos atributos inherentes a su aplicación: el de autenticidad que establece que la persona firmante es quien dice ser, y el de no repudio que establece que la persona firmante estuvo de acuerdo con los compromisos adquiridos y suscribió el documento reconociendo su contenido. Por lo tanto, al estar en presencia de un documento físico firmado manuscritamente, se considera que dicho documento goza de autenticidad y no repudio otorgando capacidad probatoria al documento.

Cabe destacar, que en la búsqueda del equivalente electrónico de la firma manuscrita era indispensable que se pensara en un mecanismo que, como mínimo, garantizara los

atributos de la firma manuscrita para ser aplicados a documentos electrónicos. Es así como los ordenamientos jurídicos de América Latina y el Caribe acogieron los estándares de las Naciones Unidas, y confirmaron que dicha equivalencia se daría en presencia de una firma digital o electrónica avanzada, certificada o calificada según la denominen en el respectivo país (las diferencias solamente son de carácter nominal), pues de dicha firma digital o electrónica se derivarían los atributos de la firma manuscrita antes descritos, es decir: la autenticidad y el no repudio, y, adicionalmente, -gracias a los estándares que utiliza la misma cuenta con un atributo que supera la firma manuscrita-, la integridad, pues cuando un documento se firma electrónicamente o digitalmente, es posible evidenciar, en el proceso de verificación, si el documento ha sufrido alteraciones o cambios, garantizándose así que el documento se ha mantenido íntegro en todo momento.

En este sentido, cuando se está en presencia de pruebas documentales, que se encuentren firmadas manuscritamente, presentadas ante una autoridad judicial, la contraparte dentro de un proceso judicial podría cuestionar el contenido y su integridad aludiendo que dicho documento físico sufrió alteraciones, porque siendo esa su firma, el contenido es diferente. Por oposición, si la prueba es electrónica y el documento está firmado digital o electrónicamente, el sistema permite validar la integridad del contenido a través de una operación que funciona básicamente de la siguiente manera:

> i. Al efectuarse un procedimiento de firma digital o electrónica avanzada, certificada o calificada, el usuario procede a firmar dando una clave única que está bajo su control lo que le permite acceder al medio de almacenamiento de su firma (USB criptográfica, una tarjeta inteligente o en un medio lógico en su computador).
> ii. Seguidamente, el sistema realiza un procedimiento de cifrado del contenido generando un resultado matemático único por documento compuesto por todos los caracteres del mismo, independientemente del número de páginas.
> iii. Al intentarse hacer una modificación -por mínima que sea, como por ejemplo, cambiar una minúscula por una mayúscula-, en el proceso de verificación, el sistema revalida el resultado matemático, de detectarse un cambio de carácter, el resultado matemático no será el mismo y advertirá su alteración, por lo que la firma será invalidada.
> iv. Si, por el contrario, el documento electrónico firmado se mantuvo inalterado, el proceso de verificación notificará el éxito y corresponderá a un documento totalmente íntegro que nunca podrá ser cuestionado por la contraparte.

En todo caso, para que la firma digital y/o electrónica goce de los atributos de la firma manuscrita, debe cumplir con unos requisitos que las leyes le han impuesto con el propósito de garantizar su confiabilidad y apropiabilidad. En tal sentido, en cuanto atañe a los atributos jurídicos de esta firma, es útil recordar cuáles son las funciones de mayor relevancia, a saber:

- Autenticidad. La firma garantiza que las personas que intervienen son quiénes dicen ser. Es decir, el contenido del mensaje se encuentra resguardado por medio de algoritmos matemáticos, salvaguardando la autenticidad del mensaje inicial;

- Integridad. Se logra verificar que el mensaje no fue modificado en el proceso de comunicación electrónica, garantizándose que el mensaje transmitido no se ha manipulado. Tratándose de la firma digital y/o electrónica, ésta se halla

directamente relacionada con el documento por lo que cualquier cambio en el texto inhabilita la firma;

- Confidencialidad. El mensaje resulta secreto o confidencial para las partes de la comunicación electrónica, impidiendo que terceros, ajenos al mensaje, puedan conocerlo; y

- No Repudio. La doctrina ha desarrollado la función del no repudio consistente en que el suscriptor no pueda negar que ha firmado digitalmente o electrónicamente el respectivo mensaje.

Ahora bien, de conformidad con las referencias legislativas latinoamericanas y del Caribe, es importante explicar la diferencia entre las denominadas firmas electrónicas (simples) y las firmas digitales y/o electrónicas avanzadas, certificadas o calificadas según corresponda a la denominación del país. De esta manera la firma electrónica (simple) es el género de los mecanismos de autenticación que se pueden definir como cualquier mecanismo que permita identificar a una persona ante un sistema de información. Se trata de un concepto genérico, que puede tener múltiples aplicaciones.

De la definición de firma electrónica (simple) se pueden extraer diferentes elementos: i. Se trata de un mecanismo técnico, ii. que permite identificar a una persona ante un sistema de información y iii. debe ser confiable y apropiable.

Esta última característica -la confiabilidad y la apropiabilidad– es la más controversial en la operación de una firma electrónica, pues se trata de conceptos técnicos subjetivos que no tienen un referente legal claro, y que, normalmente, están enunciados en acuerdos previos entre las partes que utilizan comunicaciones electrónicas. Piénsese en los contratos bancarios, en los que, precisamente, se establece que los sistemas de PIN y claves son mecanismos técnicos que permiten autenticar al consumidor financiero ante su Banco, y en el mismo contrato se señala que ese mecanismo es confiable y apropiable. Así pues la clave de un cajero, la contraseña, y un PIN son firmas electrónicas que utilizamos cotidianamente. La firma electrónica entonces tiene plena vigencia, y lo que será determinante dentro del modelo utilizado, es que las partes de una comunicación electrónica hayan establecido, a través de un acuerdo previo, la confiabilidad y apropiabilidad del mecanismo en cuestión.

Al definirse la firma electrónica en los mecanismos de autenticación reconocidos por los ordenamientos jurídicos de la región, tanto aquellos existentes como los próximos a emitirse, se podrá afirmar que la firma electrónica avanzada (aquella que utiliza de manera prevalente tecnología PK y un tercero de confianza para su emisión), es su más importante especie, pues goza en todos los ordenamientos jurídicos de una presunción de confiabilidad y apropiabilidad. La denominación firma electrónica avanzada, utilizada en México, para distinguirla de la firma electrónica simple, es propia del modelo de la Directiva Europea de Comercio Electrónico, pero en las legislaciones latinoamericanas y caribeñas ha sido denominada de manera distinta. Así, en países como Colombia y Chile, se le denomina firma digital, mientras que otros utilizan el concepto de firma electrónica certificada, tales son los casos de Venezuela y Brasil, y en otros, como Panamá, se denomina firma electrónica calificada. Para agregar mayores elementos a las posibilidades de denominación de este mecanismo en la región existen algunas legislaciones, como la ecuatoriana, donde se define estrictamente como firma electrónica, sin otros adjetivos.

En resumen, una firma electrónica avanzada, digital, certificada o calificada, puede definirse como un procedimiento matemático que permite identificar de manera idónea a una persona en medios electrónicos (autenticidad) y que permite verificar del lado del destinatario de un mensaje de datos, si éste se ha alterado o no (integridad), lográndose de esta manera los atributos de seguridad jurídica que son propios de la firma manuscrita, como son la autenticidad y el no repudio.

En relación con las características de aseguramiento jurídico y técnico de las firmas digitales y/o electrónicas avanzadas, certificadas o calificadas, los legisladores de los países latinoamericanos y caribeños, adoptaran con respecto de éstas una presunción de confiabilidad y apropiabilidad a su favor.

Es decir, la diferencia entre una firma digital y/o electrónica avanzada, certificada o calificada y una firma electrónica simple es que la primera tiene mayor fuerza probatoria, pues no será necesario determinar su confiabilidad y apropiabilidad, gozando de esa presunción, no solo por la tecnología utilizada, sino porque exige la intervención de un prestador de servicios de certificación o entidad de certificación digital, quien compromete su responsabilidad en la identificación inequívoca de una persona en medios electrónicos.

El prestador de servicios de certificación o entidad de certificación digital es precisamente un tercero de confianza que garantiza –incluso a nivel de responsabilidad patrimonial– la identidad de las personas en medios electrónicos. Es decir, es un tercero que a través de distintos procesos auditados verifica la identidad de una persona para que pueda desarrollar trámites y actuaciones a través de medios electrónicos.

En ese contexto, el prestador de servicios de certificación o entidad de certificación son personas autorizadas bajo los requisitos gubernamentales en cada país, para emitir certificados electrónicos en relación con las firmas electrónicas de terceros. Tales entidades ofrecen o facilitan los servicios de registro y estampado cronológico en las transmisiones de mensajes de datos o información electrónica (Sello digital de tiempo o fechado electrónico, dependiendo de la legislación) y realizan otras funciones relativas a las firmas electrónicas.

En virtud de lo expuesto, vale destacar algunas conclusiones del equivalente funcional de firma:

- Las claves y contraseñas utilizadas por las entidades financieras o como medios de acceso a sistemas de información de las empresas, son firmas electrónicas simples que no han sido emitidas o avaladas por un prestador o tercero confiable, por lo que su confiabilidad y apropiabilidad dependerán de la sana crítica del juez en casos probatorios.

- Es decir, cuando se está en presencia de una firma electrónica y/o digital avanzada, certificada o calificada por un tercero de confianza o prestador de servicios de certificación digital, dicha firma se presume confiable y apropiada y la carga de la prueba está en cabeza de la entidad de certificación digital de emisión, en cuyo caso la entidad invirtió la carga probatoria.

- Por oposición, cuando se está en presencia de una firma electrónica simple, no avalada por un tercero de confianza, la carga de la prueba está en cabeza de la entidad emisora y deberá demostrar que el mecanismo aseguró adecuadamente la transacción.

- Una firma electrónica autogenerada (contraseña y clave) no puede tener el mismo valor probatorio que aquel tipo de firma en la que quien comprueba la identidad es un tercero de confianza, que además tiene el deber profesional de hacerlo.

- La intervención del tercero (prestador de servicios de certificación) resulta fundamental, pues permite garantizar la identidad de los firmantes ante cualquier parte, no únicamente entre quienes se establece la comunicación, y por ello teniendo en cuenta el procedimiento de generación de la firma, las leyes han establecido a su favor tres atributos fundamentales en el aseguramiento jurídico de la información electrónica, ya explicados, a saber: i. La autenticidad, en la medida que se puede verificar en un mensaje de datos quien es su autor, quien se compromete jurídicamente; ii. La integridad, pues el destinatario de ese mensaje de datos podrá verificar si la información ha sido o no alterada en el proceso de comunicación electrónica; y iii. El no repudio, pues quien firma se compromete con la suscripción respectiva y posteriormente no le es dado retractarse o refutar dicho acto. Cabe mencionar que los legisladores latinoamericanos y caribeños le han conferido a la firma digital y/o electrónica avanzada, certificada o calificada estas características probatorias, precisamente porque en el proceso de la emisión se encuentra un tercero que avala la identidad del titular de la firma.

- De conformidad con lo anterior, puede concluirse que en los ordenamientos electrónicos en América Latina y el Caribe se encuentran reconocidas tanto la firma electrónica simple como la firma digital y/o electrónica avanzada, certificada o calificada según corresponda su denominación, y que si bien las dos pueden producir los mismos efectos jurídicos como mecanismos de autenticación, también es cierto que existen profundas diferencias en la carga probatoria de los atributos de seguridad jurídica arriba explicados, gracias a la intervención del tercero denominado prestador de servicios de certificación digital o entidad de certificación. La diferencia entonces es fundamentalmente probatoria, pues si bien la firma digital y/o electrónica avanzada, certificada o calificada de manera automática incorpora la autenticidad, la integridad y el no repudio, en la firma electrónica simple es necesario probarla, además de determinar que se trata de un mecanismo confiable y apropiable.

- La firma electrónica o digital avanzada, certificada, o calificada corresponde a un mecanismo de autenticación que puede ser aplicado para mitigar los riesgos propios de las comunicaciones electrónicas, antes explicados, como son: i. Riesgo de suplantación; ii. Riesgo de Alteración; iii. Riesgo de Repudio; y iv. Riesgo de Confidencialidad.

- Finalmente y dado lo expuesto, se puede afirmar que la firma digital y/o electrónica avanzada, certificada o calificada, impuesta a través del uso de un certificado digital previamente emitido por una entidad prestadora de servicios de certificación digital –debidamente autorizada por Ley en cada país– se considera el equivalente idóneo de la firma manuscrita, pues la misma se considera confiable y apropiable.

3. El equivalente funcional de original

El concepto de "original" en materia de medios electrónicos, establece que cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos o información electrónica, al darse las siguientes condiciones:

a) La existencia de alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva como mensaje de datos o en alguna otra forma;

b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar.

Este equivalente supone un cambio de paradigma en lo que corresponde a la originalidad desde el punto de vista de los documentos físicos o tradicionales. Lo que se entiende por un documento original en el mundo físico es el primero elaborado y lo que se derive de él serán las denominadas copias. Sin embargo, sostener el mismo concepto en medios electrónicos es imposible, esto es así dada la asidua reproducción de un documento electrónico, supóngase por ejemplo el envío de un PDF a una persona, quien, a su vez, lo envía a 100 destinatarios y esos cien a otros mil ¿cuál, entonces, es el primero elaborado? Es imposible determinarlo.

En razón de lo expuesto, los legisladores han adoptado el concepto emitido por la UNCITRAL en materia de originalidad en el medio electrónico, considerando que un documento o mensaje de datos es original en el medio electrónico si es íntegro.

La originalidad es igual a la integridad que, básicamente, se refiere a que el documento no haya sufrido ninguna alteración o cambio, se mantenga inalterado desde su creación, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación.

Lo anterior nos lleva a concluir que en el canal electrónico pueden existir varios originales del mismo documento siempre y cuando de cada uno se pueda derivar su integridad.

La utilización de la firma digital y/o electrónica garantiza la integridad de la información como anteriormente se explicó en el equivalente de firma manuscrita. La firma digital y/o electrónica de un documento permite afirmar que la información ha permanecido íntegra desde su suscripción y que permanecerá así, por lo menos, mientras la firma conserve la característica de unicidad.

Todo documento que requiera como deber formal ser aportado en original, si se encuentra firmado digitalmente y/o electrónicamente por quien debe ser su emisor, cumple con las condiciones para ser original.

4. El equivalente funcional de archivo y conservación

Con respecto a la conservación de los mensajes de datos y documentos electrónicos, las leyes claramente establecen que cuando es un requisito legal que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre y cuando se cumplan las siguientes condiciones en su archivo y conservación electrónica:

a) La información debe ser accesible para su posterior consulta.

b) El mensaje de datos o documento conservado, debe estar en el formato en el que se haya generado, enviado o recibido, o en un formato que permita verificar que se reprodujo con exactitud la información conservada.

c) La conservación de la información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o reproducido el documento.

Al existir un documento electrónico como lo ha determinado la Ley, es procedente que exista la posibilidad de archivarlo y conservarlo de manera electrónica.

De conformidad con lo anteriormente expuesto, si los documentos contenidos en dicho expediente se encuentran firmados digitalmente y/o electrónicamente se podrá cumplir con los requisitos de origen, autenticidad, integridad y, en el caso de determinación de fecha, podremos acudir al servicio de estampado cronológico, fechado electrónico o sellado de tiempo (como más adelante detalla el equivalente de fecha y hora) a través del cual se otorga la certeza de la fecha y hora exacta en que se genera, se envía o se recibe un documento electrónico, aportándose de esta manera los extremos temporales de conservación del documento.

5. El equivalente funcional de fecha y hora

La noción de "tiempo", se presume como un hecho irreversible que afecta globalmente a todas las actividades humanas y es un componente clave para todas las relaciones causales entre procesos. Las relaciones de dependencia entre unos hechos y otros son función del orden en el que se realiza cada uno de ellos y suelen ser manifestación de las relaciones causales que los unen.

La precisión en el tiempo y los contenidos de las transacciones resultan de importancia vital en el comercio electrónico. Sin embargo, las transacciones en general se realizan usando fuentes de tiempo de los propios computadores, por tanto el "tiempo" no es confiable y puede ser fácilmente manipulado y repudiado. Tal situación problemática es susceptible de ser corregida aplicando estampas cronológicas, fechados electrónicos o sellos de tiempo en los documentos electrónicos, con lo que se garantiza que las transacciones han ocurrido en un momento específico y particular y que sus contenidos no han sido alterados desde entonces, utilizando para ello el denominado "reloj atómico" o la hora legal provista por la entidad pública encargada de ésta en el país.

El reloj de un computador es fácilmente manipulable, los documentos son fácilmente editables. Pero si se intenta hacer del comercio electrónico una realidad y digitalizar buena parte de la actividad humana, se debe aplicar y socializar el equivalente de aquella seguridad física a la que los ciudadanos se han acostumbrado y en la que se han basado las leyes. Es en este momento cuando aparecen los sistemas de fechado digital que correlacionan la existencia de los bits a los eventos humanos de referencia en general, y, en particular, al convenio de tiempo absoluto avalado a través de un prestador de servicios de certificación que además de certificar firmas digitales y/o electrónicas, ofrece este servicio de sellado de tiempo electrónico conocidos mundialmente como T*ime Stamp Authority* (TSA).

Con las anteriores descripciones de los equivalentes funcionales en materia de uso de medios electrónicos, así como, por el gran numero de países que han acogido leyes, normas y procedimientos o se encuentran promoviendo proyectos legislativos para la implementación de canales electrónicos, es posible concluir que se está muy cerca de contar con implementaciones de firma digital o electrónica avanzada, certificada o

calificada en la mayoría de los países de América Latina y del Caribe con miras a promover un comercio transparente, jurídica y técnicamente seguro, y con ello hacer posible, en gran medida, la necesaria interoperabilidad del comercio intrarregional.

Sin embargo, existen importantes retos que deben ser abordados y superados para materializar realmente el uso y masificación del mecanismo de firma digital o electrónica avanzada, certificada o calificada, que abarcan desde temas como la sensibilización, socialización y capacitación, hasta su uso práctico en proyectos tanto de índole gubernamental como privada.

V. ESTADO DEL ARTE DE LA FIRMA DIGITAL Y/O ELECTRÓNICA EN AMÉRICA LATINA Y EL CARIBE

A continuación se relaciona, por país, la referencia de ley que contiene temas específicos en materia de Firma Electrónica. Muchos de los países de la región han adoptado la ley modelo de la UNCITRAL en su estructura y alcance, pero se asimila en cada país según sus particularidades. Así, existen diferencias nominales en materia de firma electrónica certificada a través de un tercero de confianza. En todo caso, existe homogeneidad en los propósitos generales y equivalencias funcionales ya comentadas a lo largo del presente documento básico de consulta.

Todos los países que cuentan actualmente con una ley en materia de validez jurídica y probatoria de mensajes de datos, o regulan condiciones jurídicas del comercio electrónico, ha optado por reconocer a través de criterios de equivalencia funcional la eficacia jurídica de las firmas electrónicas y/o digitales certificadas como mecanismos para otorgar seguridad jurídica a las transacciones electrónicas, promoviendo el comercio electrónico seguro y la identificación en forma fehaciente de los sujetos que realicen transacciones electrónicas.

El estado del arte de la firma digital y/o electrónica en la región se resume así:

País	Ley o Norma de Firma Electrónica
1. Argentina	Ley 25506 del 2001 – Ley de Firma Digital Reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica.
2. Bahamas	Ley de Comunicaciones y Transacciones Electrónicas, 2003 (Electronic Communications and Transactions Act,2003) Esta ley da reconocimiento legal a los documentos, contratos, firmas e información electrónica.
3. Barbados	Ley de Comunicaciones y Transacciones Electrónicas, 2003 (Electronic Communications and Transactions Act,2003) Esta ley da reconocimiento legal a los documentos, contratos, firmas e información electrónica.
4. Belice	Ley de Comunicaciones y Transacciones Electrónicas, 2003 (Electronic Communications and Transactions Act,2003) Esta ley da reconocimiento legal a los documentos, contratos, firmas e información electrónica.
5. Bolivia	Ley 080 de 2007 – Ley de Documentos, Firmas y Comercio Electrónico de 2007. Esta ley reconoce el valor jurídico y probatorio de: i. Los actos jurídicos

	celebrados mediante medios electrónicos u otros de mayor avance tecnológico realizados por personas naturales, jurídicas, empresas colectivas o unipersonales, comunidades de bienes y otras entidades que constituyan una unidad económica sujeta a derechos y obligaciones, ii. El uso de firmas electrónicas debidamente certificadas por una Entidad de Certificación acreditada bajo lo estipulado en la presente ley, iii. Los actos civiles y comerciales que utilicen directa o indirectamente medios electrónicos u otros de mayor avance tecnológico para realizar actividades del comercio electrónico.
6. Brasil	Decreto Ley 3.996 de 2001 y Decreto Ley 4.414, de 2002. Regula la prestación del servicio de certificación digital de firma electrónica. Se ha intentado promover proyectos en materia de ley de comercio electrónico, pero el país considera suficiente la normativa existente en otras normas que han habilitado el uso de firma electrónica, además de contar ya con decretos en materia específica que regulan dicha prestación de servicio. Brasil es un país de la región que se reconoce por la masificación efectiva del uso de firma electrónica avanzada, exigiendo su uso en materia tributaria.
7. Chile	Ley 19.799 de 2002 - Ley de Documentos Electrónicos La ley adopta las disposiciones relativas a los documentos electrónicos, firmas electrónicas y servicios de certificación de las firmas.
8. Colombia	Ley 527 de 1999. Ley de Validez Jurídica y Probatoria de los mensajes de datos. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones. Colombia ha desarrollado infinidad de habilitantes normativos que han permitido ir abonando un camino hacia la masificación.
9. Costa Rica	Ley 8454 de 2005 - Ley de certificados, firmas digitales y documentos electrónicos Establece el marco jurídico general para la utilización segura de los documentos electrónicos y la firma digital en las entidades públicas y privadas
10. Cuba	En Cuba no existe una legislación especial que regule el comercio electrónico, sin embargo existen normas que habilitan su uso en diferentes disciplinas del derecho.

11. Ecuador	Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos de 2002 Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.
12. El Salvador	En El Salvador no existe una legislación especial que regule el comercio electrónico, sin embargo existen normas que habilitan su uso en diferentes disciplinas del derecho.
13. Grenada	Ley de Transacciones Electrónicas, 2008 (Electronic Transactions Act, 2008) Esta ley da reconocimiento legal a los documentos, contratos, firmas e información electrónica.
14. Guatemala	Ley Decreto 47 de 2008 -Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.
15. Guyana	No se encontró ningún tipo de antecedente legislativo en fuentes públicas de información.
16. Haití	No se encontró ningún tipo de antecedente legislativo en fuentes públicas de información. Al parecer no existe una legislación especial que regule el comercio electrónico, sin embargo existen normas que habilitan su uso en diferentes disciplinas del derecho.
17. Honduras	Dentro del marco jurídico hondureño no existe una ley especial que regule el comercio electrónico ni la contratación electrónica, sin embargo, les resultan aplicables diversas normas generales del ámbito civil y mercantil. La Ley del Sistema Financiero reconoce en su artículo 51 los efectos jurídicos de la firma electrónica, la cual tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita.
18. Jamaica	Ley de Transacciones Electrónicas, 2007 (Electronic Transactions Act, 2007) Esta ley da reconocimiento legal a los documentos, contratos, firmas e información electrónica.
19. México	Ley de Firma Electrónica Avanzada de 2012. Corresponde a una nueva Ley de Comercio Electrónico que incluye modificaciones al Código Civil y otras leyes que le dan marco jurídico a la firma electrónica. Regula el uso de la firma electrónica avanzada en los actos previstos en la Ley y la expedición de certificados digitales, servicios relacionados con la firma electrónica avanzada y su homologación.
20. Nicaragua	Ley 729 de 2010 – Ley de Firma Electrónica Habilita las comunicaciones por medios electrónicos, cuando sea posible establecer con toda precisión, por medio de registros fidedignos, la identificación del emisor y el receptor, la hora, la fecha y el contenido del mensaje.
21. Panamá	Ley No. 51 de 22 de Julio de 2008 la cual define y regula los documentos electrónicos y las firmas electrónicas y la prestación de

	servicios de almacenamiento tecnológico de documentos y de certificación de firmas electrónicas y adopta otras disposiciones para el desarrollo del comercio electrónico. En este momento el país se encuentra tramitando una reforma a dicha ley.
22. Paraguay	La reglamentación de la Ley Nº 4017/10, "De validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico", a través del decreto Nº 7.369. Este decreto especifica aspectos como la reproducción de documentos originales por medios electrónicos, la digitalización de archivos públicos, así como la certificación de los documentos y requisitos para su aplicación. En cuanto al servicio de archivo y conservación de documentos y datos en mensajes de datos, el decreto enuncia que las entidades que realicen la reproducción de documentos originales por medios electrónicos o que presten los servicios de almacenamiento deben incorporar un procedimiento estampado que garantice los efectos del documento electrónico. Esto equivale al documento físico que almacena.
23. Perú	Ley No. 27269 de 2000 – Ley de Firmas y Certificados Digitales Regula la utilización de la Firma Electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve una manifestación de la voluntad.
24. República Dominicana	Ley 126 de 2002 – Ley de Comercio electrónico, Documentos y Firmas Digitales. Esta ley es aplicable a todo tipo de información en forma de documento digital o mensaje de datos.
25. Suriname	No se encontró ningún tipo de antecedente legislativo en fuentes públicas de información. Al parecer no existe una legislación especial que regule el comercio electrónico, más bien, diversas leyes generales le son aplicables. Se han implementado estrategias de gobierno en línea, donde se ha hecho uso de mecanismos de aseguramiento técnico a través de firmas electrónicas simples como claves y contraseñas.
26. Trinidad y Tobago	Ley de Transacciones Electrónicas, 2011 (Electronic Transactions Act 2011) Esta ley da reconocimiento legal a las transacciones electrónicas e introduce temas relativos a la firma digital.
27. Uruguay	Ley 18.600 de 2009 – Ley de Documento electrónico y firma electrónica. Esta Ley reconoce la admisibilidad, validez y eficacia jurídica del documento electrónico y de la firma electrónica.

28. Venezuela	Decreto Ley Nº 1204 de 2001, Ley de Mensajes de Datos y Firmas Electrónicas El Decreto Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regula todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.
29. Antigua y Barbuda	Ley de Transacciones Electrónicas, 2006 (Electronic Transactions Act 2006) Esta ley da reconocimiento legal a los documentos, contratos, firmas e información electrónica.
30. Dominica	No se encontró ningún tipo de antecedente legislativo en fuentes públicas de información.
31. San Cristóbal y Nieves	No se encontró ningún tipo de antecedente legislativo en fuentes públicas de información.
32. San Vicente y las Granadinas	Ley de Transacciones Electrónicas, 2007 (Electronic Transactions Act 2007) Esta ley da reconocimiento legal a los documentos, contratos, firmas e información electrónica.
33. Santa Lucía	Ley de Transacciones Electrónicas, 2007 (Electronic Transactions Act 2007) Esta ley da reconocimiento legal a los documentos, contratos, firmas e información electrónica.

VI. CONCLUSIONES Y RECOMENDACIONES

a) De acuerdo con lo expuesto, es importante evaluar el tema de la firma digital y/o electrónica en América Latina y el Caribe como un nuevo fenómeno de interoperabilidad entre países, que permitirá la transparencia, la simplificación, la racionalización y la eficiencia de los procesos en el comercio intrarregional y de la región con el resto del mundo.

b) Asimismo, será necesario que los países de la región incorporen mecanismos de autenticación dentro de las políticas públicas que cada uno ha diseñado en materia de gobierno electrónico.

c) Los principales multiplicadores de uso de firmas digitales y/o electrónicas o servicios de certificación digital son el gobierno y sus sistemas de información. Por lo tanto, los sistemas de información llamados a multiplicar la firma electrónica y/o digital como mecanismo para asegurar y mitigar los riesgos de la comunicación electrónica y propiciar los trámites y procesos electrónicos son: i. Las entidades de impuestos y tributos del estado; ii. Las entidades de seguridad social y salud, y iii. El sector financiero.

d) La región debería propiciar a través de algún instrumento normativo supranacional el reconocimiento de las firmas electrónicas y/o digitales de cada país bajo las leyes y normas de dicho país de origen de la firma. Un ejemplo de

ello es el proyecto de reconocimiento de la Asociación Latinoamericana de Integración (ALADI) para el sistema de certificación digital de origen, o el Federal Bridge Certification Authority que da validez a las firmas digitales emitidas en los diferentes ordenamientos jurídicos de los Estados Unidos.

e) La integración de firmas digitales y/o electrónicas avanzadas, certificadas o calificadas, según se denominen en cada país, emitidas por una entidad prestadora de servicios de certificación, permitirán garantizar:

- La autenticidad del origen;
- La integridad de la información transaccional a lo largo de su ciclo de vida;
- El no repudio a las transacciones;

En consecuencia, cada país debería evaluar su estado actual de la firma digital y/o electrónica en atención a:

- Si existe una ley especifica y sus reglamentarios, si son del caso;
- Si existe un prestador de servicios de certificación digital ya sea público o privado;
- Si existe ya sea integración y/o normatividad habilitante específica en sistemas multiplicadores como temas de comercio en ventanillas únicas, tributarios, trámites de gobierno, seguridad social, etc.

De conformidad con las respuestas anteriores que tenga cada país, podrá conocer su estado actual y evaluar la adopción de las recomendaciones que a continuación se presentan.

a) Los países que cuentan con una ley en materia de uso de medios electrónicos, con independencia de su denominación y que además han reglamentado dichas normas y cuentan con terceros de confianza o prestadores de servicios de certificación para la emisión de firmas digitales y/o electrónicas certificadas, deberían concentrar sus esfuerzos en la integración de servicios de certificación digital de firma electrónica y/o digital certificada en diferentes sistemas transaccionales públicos, junto con la emisión de los correspondientes instrumentos normativos que habiliten su uso en dichas actuaciones, procesos y procedimientos públicos. De esta manera, se abordaría el camino hacia la masificación de uso y cobertura, ampliando la pluralidad de prestadores y mejorando los precios y la competencia, el número de suscriptores de firma y el número de sistemas que la utilizan. Con ello se apunta a consolidar los aspectos medulares en el contexto del gobierno electrónico sin papel.

b) Es importante destacar la necesidad de que las Ventanillas Únicas Electrónicas de Comercio de la región, que por su naturaleza suelen ser sistemas administrados por entidades públicas y que requieren de conformidad con sus ordenamientos jurídicos, contar con plenas garantías probatorias y mitigar los riesgos asociados a la comunicación electrónica, establezcan de forma conjunta y decidida, como estándar de seguridad jurídica y técnica, el mecanismo de la firma digital y/o electrónica avanzada o calificada emitida por un prestador o entidad de certificación, con el propósito de hacer posible la implementación de funcionalidades y trámites totalmente electrónicos, aportando a los objetivos del gobierno electrónico y las directrices de cero papel, así como a preparar su sistema a la interoperabilidad como fase indispensable en la facilitación del comercio.

c) Se recomienda que en materia de facilitación del comercio, los proyectos en proceso de diseño y de implementación de Ventanillas Únicas Electrónicas de Comercio -consideradas de la más alta relevancia en las estrategias de gobierno electrónico y del comercio sin papel-, incorporen mecanismos de firma electrónica y/o digital certificada, siguiendo el patrón de desarrollo de las Ventanillas Únicas ya consolidadas en la región y en el mundo. De la misma manera, algunos ordenamientos jurídicos que han implementado la factura electrónica han considerado la necesidad de obligar el uso de firma electrónica y/o digital para operar el sistema de manera más efectiva y segura.

d) Los países que cuentan con leyes en materia de medios electrónicos, pero que todavía no han reglamentado temas específicos de firmas digitales y prestadoras de servicios, deberían concentrar sus esfuerzos en emitir dicha reglamentación y construir un ambiente propicio que promueva la constitución de entidades de certificación, ya sean públicas o privadas. Posterior a ese esfuerzo legislativo, tendrían que considerar estrategias de uso y de masificación como se establece en el inciso anterior, a fin también de garantizar la estabilidad y sostenibilidad del prestador y en general del sistema registral de firmas digitales y/o electrónicas certificadas.

e) Para facilitar la constitución de prestadores de servicio de certificación, los países podrán apoyarse en infraestructura de otros prestadores de la región que faciliten la implementación y viabilicen costos de inversión para la entidad pública o privada interesada.

f) Por último, los países de la región que finalmente no cuentan con ninguna ley en materia de uso de medios electrónicos, tienen varios ejemplos normativos interesantes, el más replicado es el de la ley modelo de 1996 de la UNCITRAL o en su defecto la directiva Europea de comercio electrónico de 1993, así como la misma ley modelo de firmas electrónicas de 2005. Adicionalmente, existen normas de nivel regional que se han convertido en paradigmas regulatorios para otros países, como es el caso de las leyes de Colombia y Chile y los estándares y desarrollos técnicos del Brasil, experiencias éstas que han consolidado su liderazgo por cuanto han sido los primeros países en contar con prestadores de servicios de certificación.

Los anteriores retos y recomendaciones se orientan a promover el uso y la masificación de la firma digital y/o electrónica que materializará la interoperabilidad segura y los proyectos de *cero papel* tanto en ambientes de comercio como de gobierno electrónico en América Latina y el Caribe.