La implementación de la Firma Digital en Bolivia

The implementation of the Digital Signature in Bolivia

***PhD. Dra. Karina Ingrid Medinaceli Díaz**
Carrera de Derecho
Facultad de Derecho y Ciencias Políticas
Universidad Mayor de San Andrés
La Paz - Bolivia
Autor de correspondencia: *karina.medinaceli@gmail.com

PhD. Dr. Eugenio Gil López
Escuela Superior de Ingeniería y Arquitectura
Universidad Pontificia de Salamanca
Madrid - España
eugenio.gil@upsam.es

Resumen

El presente artículo realiza una revisión de los principales conceptos relacionados con la firma digital como la criptografía, el sellamiento electrónico (funciones Hash), los problemas relativos a la seguridad (autenticidad, integridad, no repudio y confidencialidad), los prestadores de servicios de certificación, los certificados electrónicos y la utilización de la firma digital por el sector público y privado. Posteriormente, se muestra un panorama acerca de las Entidades Certificadoras de Bolivia, la Agencia para el Desarrollo de la Sociedad de la Información (ADSIB) y la Asociación de Bancos Privados de Bolivia (ASOBAN), finalmente la implementación de la firma digital en el Sistema Único de Modernización Aduanera (SUMA). La firma digital es cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita.

Palabras clave: firma digital; entidad certificadora; certificado digital; clave pública; clave privada.

Abstract

This article reviews the main concepts related to the digital signature as cryptography, electronic seal (Hash functions), security related problems (authenticity, integrity, non-repudiation and confidentiality), certification services providers, electronic certificates and the use of digital signature by the public and private sectors. Subsequently, the article shows an overview about the Certification Authority of Bolivia, the Agency for the Development of the Information Society (ADSIB) and the Association of Private Banks of Bolivia (ASOBAN); and finally it talks about the implementation of the digital signature in the of Customs Modernization Unique System (SUMA). The digital signature is any method or symbol based on electronic means, used or adopted by a party with current intention to join or authenticate a document, fulfilling all or some of the typical functions of a handwritten signature.

***Keywords**: digital signature; certification authority; digital certificate; public key; private key.*

Introducción

La presente investigación tiene como objetivo conocer la implementación de la firma digital en Bolivia desde la aprobación de la Ley Nº 164 General de Telecomunicaciones, Tecnologías de Información y Comunicación de fecha 8 de agosto de 2011 y el Decreto Supremo Nº 1793 Reglamento a la Ley Nº 164 para el desarrollo de tecnologías de información de fecha 13 de noviembre de 2013.

Pasaron casi 5 años desde la promulgación de la Ley Nº 164 para que la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) pueda prestar el servicio de certificación para el sector público y la población en general a nivel nacional.

El uso de la firma digital es impulsado por el actual Gobierno a través de la ADSIB, Autoridad de Regulación y Fiscalización de las Telecomunicaciones y Transportes (ATT) y la Agencia de Gobierno Electrónico y Tecnologías de las Información y Comunicación (AGETIC).

La firma digital provee un nivel de seguridad máximo para proteger la identidad del signatario y la integridad a los documentos firmados (contrato, factura, notificación, expediente, historia clínica). Un documento firmado digitalmente tiene la misma validez jurídica que otro firmado con firma manuscrita[2].

Para firmar un documento electrónico o digital el usuario dispondrá de un dispositivo hardware (*token* USB, tarjeta inteligente o computadora) que contiene su clave pública y Certificado Digital (equivalente a la cédula de identidad o pasaporte en el ámbito electrónico).

La Aduana Nacional es una de las instituciones pioneras en implementar el uso de la firma digital a través del Sistema Único de Modernización Aduanera (SUMA).

Métodos

La presente investigación aplica el método descriptivo, partiendo del análisis de la bibliografía existente sobre Firma Digital, Entidades de Certificación y Certificado electrónico y la legislación vigente en Bolivia Ley Nº 164 General de Telecomunicaciones, Tecnologías de Información y Comunicación, el Decreto Supremo Nº 1793 Reglamento a la Ley Nº 164 para el desarrollo de tecnologías de información y comunicación y las Resoluciones Administrativas Regulatorias emitidas por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.

Resultados

En cuanto a los resultados, se deber indicar que la finalidad de la investigación es mostrar el panorama actual en Bolivia en relación a la firma digital y la normativa vigente.

Tal y como se comprobará del análisis del trabajo, la implementación de la firma digital se ha realizado de forma tardía en relación a otros países de Latinoamérica.

Por otra parte, la implementación de la firma digital en Bolivia se encuentra en una fase inicial, todavía no es generalizada, el costo del certificado digital es elevado para la economía boliviana, lo que puede llevar a una implementación ralentizada.

[2] El parágrafo I. del artículo 87 (Valoración) de la Ley Nº 164 establece: *"Los documentos digitales carentes de firma digital, serán admisibles como principio de prueba o indicios".*

Finalmente, las autoridades competentes deben socializar a nivel nacional a través de seminarios, talleres y cursos los beneficios que ofrece el uso de la firma digital en diferentes trámites con la administración pública, el desarrollo del comercio electrónico a través de sitios web seguros, y otros servicios.

Discusión

- La firma electrónica. Si la firma autógrafa es el nombre, apellido o título que una persona escribe de su propia mano en un documento para darle autenticidad o para expresar que aprueba su contenido, la firma electrónica será de igual forma una identificación electrónica que se pondrá en forma electrónica por una persona, sobre un documento electrónico para darle autenticidad o para expresar que aprueba su contenido.

No es necesario acudir a definiciones complejas pues se debe buscar, en un principio, asociar los conceptos en los que solamente cambiará el elemento, bien del soporte –papel o electrónico–, o bien de la representación gráfica de la identificación del firmante, en un escrito sobre un papel o en un escrito sobre soporte electrónico (Davara Rodríguez, 2005).

La Cámara de Comercio Internacional señala que debe entenderse por firma electrónica: "Toda transformación de un mensaje mediante la utilización de un criptosistema asimétrico de modo que una persona en posesión del mensaje firmado y de la clave pública del firmante puedan determinar con exactitud: a) si la transformación fue producida mediante la utilización de la clave privada que se corresponde con la clave pública del firmante y b) si el mensaje firmado ha sido alterado desde que se produjo la transformación".

La Directiva 1999/93/CE la define como: "los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación".

La Ley UNCITRAL indica que firma electrónica consiste en: "los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos".

La Ley Nº 164 General de Telecomunicaciones, Tecnologías de Información y Comunicación de fecha 8 de agosto de 2011 en el numeral 5 del parágrafo IV del artículo 6 define así a la firma digital: "es la firma electrónica que identifica únicamente a su titular creada por métodos que se encuentran bajo el absoluto y exclusivo control de su titular, susceptible de verificación y está vinculada a los datos del documento digital de modo tal que cualquier modificación de los mismos ponga en evidencia su alteración".

El artículo 78 de la misma Ley otorga la validez jurídica y probatoria a la firma digital.

El Decreto Supremo Nº 1793 Reglamento a la Ley Nº 164 para el desarrollo de Tecnologías de Información y Comunicación de fecha 13 de noviembre de 2013 define, en el inciso d) de parágrafo III del Artículo 3, que la firma electrónica: "es el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carece de alguno de los requisitos legales para ser considerada firma digital".

De estas definiciones prácticamente solo se encuentra una total igualdad en el reconocimiento de la firma electrónica como datos en forma electrónica, consignados o asociados a otros datos electrónicos y que sirven para identificar al que firma. Se trata, al igual que la firma manuscrita, de un instrumento cierto de atribución de paternidad a una declaración de voluntad. Por medio del mismo se conoce la persona que emite la declaración y se establece con positiva certeza que la declaración emitida corresponde a la voluntad o conocimiento declarado del remitente (García Más, 2004).

- La criptografía. Comprende la transformación, ocultación de la información, convirtiendo el mensaje en ininteligible (cifrado) aparentemente y el procedimiento a la inversa transformando el mensaje en inteligible (descifrado) para aquellos destinatarios deseados. Dicho de otra manera, "es un conjunto de técnicas que permiten cifrar y descifrar información".

La criptografía en el presente estudia los principios, métodos y medios de transformar los datos para ocultar información contenida en ellos, garantizar su identidad, autenticidad y prevenir su repudio (Roselló Moreno, 2001).

Básicamente, se utilizan dos técnicas para encriptar y desencriptar. De modo que se distingue básicamente entre la denominada técnica de cifrado simétrico, también conocida como cifrado en clave convencional, secreta, privada, criptografía de clave simétrica, y por otro lado la técnica de cifrado asimétrico, identificada también como de clave pública, criptografía de clave asimétrica.

La primera de ellas es una técnica sencilla donde tanto emisor como receptor del mensaje del mensaje comparten una única clave que permitirá cifrar y descifrar la información. La técnica de cifrado asimétrico es más complicada que la anterior, consiste en la utilización de una par de claves (clave privada y clave pública) para cada uno de los interlocutores (emisor y receptor), asociadas matemáticamente de forma que lo que se cifra con una, solo puede ser descifrado con su pareja y viceversa. El cifrado asimétrico, se utiliza para conseguir una comunicación cifrada como para el proceso de firma electrónica.

Por lo tanto intervienen dos claves, por un lado la clave privada que tiene finalidad doble, en función de si es utilizada en el ámbito del cifrado, o en el de la firma electrónica. En el primero, en el cifrado, es usada para descifrar la información recibida y en el segundo, firma electrónica, es indispensable para su creación. En todo caso, es fundamental que la clave privada se mantenga en secreto por lo que es aconsejable que esté bien guardada, ya sea en la computadora, ya sea en una tarjeta inteligente de uso personal, *token* USB y si se desea todavía mayor seguridad, accediendo a ella mediante un número de identificación personal, o incluso utilizando sistemas de identificación biométricos como pueden ser el reconocimiento de la voz, la huella digital (De Quinto Zumárraga, 2004).

Por otro lado, la clave privada sirve para poder cifrar la información en el ámbito del cifrado y para verificar la firma en el campo de la firma electrónica. A diferencia de lo que ocurre con la clave privada, la pública ha de ser ampliamente conocida por todos y fácilmente accesible.

Ambas claves se encuentran relacionadas entre sí por operaciones matemáticas. Al inicio se trata de simples operaciones

aritméticas (generalmente operando con números primos), más tarde se recurrió a operaciones algebraicas más complicadas y en la actualidad se emplean técnicas de encriptación o cifrado que utilizan un sistema de curvas elípticas. El algoritmo de clave asimétrico más conocido es RSA (Rivest, Shamir y Adleman).

Con el conocimiento de una de las claves es imposible deducir la otra clave asociada como tampoco es posible que exista un par de claves iguales, debido a que el par de claves ha de ser único de cada persona o entidad. En caso contrario, se crearía confusión sobre la autoría de los mensajes, comprendiendo la confidencialidad. Por último, es necesario que el proceso de generación de claves sea fiable y seguro.

- Sellamiento electrónico, funciones *Hash*.

Para la prueba de integridad e individualización del documento, para evitar la duplicación o su confusión con otro de la misma fecha y contenido, se emplean los "sellos o sellamiento electrónico" o funciones *Hash* conjuntamente con la firma electrónica.

El sellamiento introduce la fecha y la hora de la transacción que queda integrada en el documento que será firmado junto con su contenido con la clave privada del remitente. Se trata de una condensación algorítmica del mensaje o contrato completo, que se incluye en el mismo mensaje y que se procesa éste cada vez que se transmite el documento, así se puede comparar si coincide con el sello original.

Las funciones de *hash* consisten en sistemas que, partiendo de todos los datos del documento, calculan un compendio codificado (*digest*) que se firmaría electrónicamente con la operativa antes indicada, formando así la firma electrónica. Posteriormente el destinatario recuperará, con la clave pública del remitente, el resumen *hash* recibido de la firma del documento y lo comprobará con el *hash* que le resulte del documento recibido y si ha variado es que ha perdido la integridad, y/o la autoría del documento recibido, en cambio si coincide, no cabría duda de la integridad del documento (Vázquez Iruzubieta, 2002).

Las características fundamentales de la función *hash* estriban en su carácter único, dado que no pueden existir dos mensajes diferentes con el mismo resumen, siendo detectable por tanto cualquier alteración, es irreversible, ya que no se puede obtener el texto completo a partir del resumen.

En conjunto, las funciones *Hash*, Sellamientos Electrónicos, Firma Electrónica, Centros de Compensación, Acuerdos de Intercambio forman la base de la firma y contratación electrónica.

- Problemas relativos a la seguridad. La actual deficiente seguridad en la transmisión de información a través de Internet hace necesario el establecimiento y cumplimiento de unos objetivos concretos que permitan paliar este problema, a los que se les identifica como autenticación, integridad, no repudio y confidencialidad.

- *La autenticación:* permite asegurar que quién envía la información es realmente quien dice ser y no un tercero. Por ejemplo, A recibe un mensaje de **B** y quiere estar seguro que es ***B*** quién lo envía y no otra persona. Los problemas se pueden plantear cuando alguien suple la identidad de una persona o empresa.

- *La integridad:* supone tener la certeza de que el mensaje no ha sido manipulado ilícitamente durante la transmisión, o como

mínimo si se ha manipulado tener conocimiento de ello. Es importante conocer si un mensaje ha sido alterado ya que, en caso contrario, pueden cambiar, suprimir las manifestaciones realizadas e incluso atribuir unas nuevas. Para evitar la manipulación de los mensajes, se acudirá de nuevo a una solución técnica como es la firma electrónica, que mediante la aplicación de una determinada función con unos caracteres específicos, permite averiguar cualquier cambio que se haya producido en la información transmitida.

- *El no repudio:* se vincula con la obtención de seguridad, en el sentido de que no se pueda negar la participación de los intervinientes en una comunicación electrónica. Bajo este concepto, se puede diferenciar dos acepciones: no repudio de origen, que implica que el emisor del mensaje no niegue a posteriori haberlo enviado y no repudio de destino, que conlleva que el receptor no niegue más tarde la recepción del mensaje. En definitiva se protege a las partes de la comunicación frente a la negación de que dicha comunicación haya tenido lugar. Para tener prueba de la transmisión se recurrirá a la firma electrónica avanzada, que permite la vinculación de una persona concreta a un texto determinado mediante un sistema de claves. Como se puede observar el no repudio se encuentra íntimamente ligado a la autenticación.

- *La confidencialidad:* se asocia a la seguridad de que la información enviada a través de la red sólo puede ser conocida por su destinatario, de forma que resulte infructuoso para terceros el conocimiento de aquélla en caso de interceptación ya sea accidental o voluntariamente. Para conseguirla en las comunicaciones electrónicas se acudirá por lo general a soluciones técnicas basada en la criptografía (Martínez Nadal, 2004).

- Los prestadores de servicios de certificación. Los prestadores de servicios de certificación, Autoridad de Certificación, Entidades Certificadoras o Entidades de Certificación han de ser terceras partes de confianza *(Trusted Third Party)* y su misión primaria es la de certificar que determinada clave pública pertenece a una persona y que se encuentra vigente y podrán para ello generar, distribuir y controlar las parejas de claves, sin almacenar ni copiar la privada que es secreta, así como garantizar facultades de representación y cualquier otro atributo o circunstancia del expedidor del mensaje que se considere de relevancia jurídica para la validez del contrato informático a realizar.

Una entidad certificadora puede ser cualquier persona física[3] o jurídica, no tiene por qué ser un organismo público ni es necesario que tenga relación alguna con una entidad pública. Cualquier empresa o entidad que cumpla con los requisitos que establece la normativa, puede ser una entidad certificadora.

Los servicios relacionados con la firma electrónica más comunes, son los servicios de consignación de fecha y hora (*time stamping*), los de directorio o los de archivo de documentos electrónicos, pero no se agotan aquí. Los servicios enunciados no constituyen una lista cerrada, sino abierta a cualquier otro servicio que pueda aparecer y éste vinculado a la firma electrónica. (Martínez Nadal, 2004).

Ni la técnica más sofisticada de firma electrónica ha conseguido el objetivo

[3] El numeral 2.2 del artículo 2 de la Ley 53/2003 Firma Electrónica de España señala: *"Se denomina prestador de servicios de certificación la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica".*

anhelado de asegurar la identificación del autor del mensaje, pues aunque el certificado reconocido integre en la firma electrónica como uno de sus elementos, lo cierto es que la técnica no ha podido funcionar por sí misma, que la máquina ha llamado en su auxilio al hombre, a fin de cuentas, quien garantiza que la clave pública pertenece a una persona determinada no es la firma electrónica en sí, sino la entidad certificadora por medio de un certificado digital incorporado a la firma (Rodríguez Adrados, 2004).

La Ley Nº 164 General de Telecomunicaciones, Tecnologías de Información y Comunicación de fecha 8 de agosto de 2011 de Bolivia establece en el artículo 82 a la Entidad Certificadora: "Pueden constituirse y operar como entidades certificadoras, las personas jurídicas de derecho público o privado en la prestación de servicios de certificación digital, las que deben cumplir con los requisitos técnicos, económicos y legales establecidos en la presente Ley y su reglamento".

- Certificados electrónicos. Las entidades certificadoras tienen como principal misión la expedición de certificados electrónicos o certificados digitales.

El numeral 1 del parágrafo IV del artículo 6 de la Ley Nº 164 define al Certificado Digital como "un documento digital firmado digitalmente por una entidad certificadora autorizada que vincula unos datos de verificación de firma a un signatario y confirma su identidad. El certificado digital es válido únicamente dentro del período de vigencia, indicado en el certificado digital".

El inciso g) del artículo 6 del Decreto Supremo Nº 1793 Reglamento de la Ley Nº 164 formula el concepto de signatario "es el titular de una firma digital que utiliza la misma bajo su exclusivo control y el respaldo de un certificado digital proporcionado por entidades certificadoras autorizadas".

La categoría más elevada de estos certificados electrónicos son los certificados reconocidos, aquellos otros certificados que no reúnan todos sus requisitos pueden llamarse certificados simples. El certificado se habrá de solicitar a la entidad certificadora de su elección. Aunque existen certificados para una operación concreta, en la práctica suelen expedirse para todas las operaciones de determinada especie que el solicitante pueda realizar durante un período de tiempo determinado (Martínez Nadal, 2004).

- Utilización de la firma electrónica. El uso de la firma electrónica no se encuentra limitado a sectores concretos ni a personas o entidades determinadas, pudiendo utilizarse tanto en el sector público como en el sector privado, bien por particulares, bien por empresas.

En el sector privado, su utilización puede estar vinculada a cuestiones relacionadas con la contratación privada por vía electrónica, entre empresa y consumidor (por ejemplo compraventa de bienes de consumo), entre empresa y empresa (por ejemplo pedido a un suministrador) o incluso entre consumidores particulares (por ejemplo compraventa de una colección de sellos).

Por otra parte, la utilización de la firma electrónica en el sector público (incluye las relaciones entre administración y los entes públicos y entre aquella y los ciudadanos, respectivamente) puede estar relacionada con actuaciones tan habituales como la

renovación de documentos oficiales (por ejemplo el Documento Nacional de Identidad - DNI); la solicitud de prestaciones sociales a los organismos competentes por medios electrónicos (por ejemplo prestación por incapacidad permanente); la remisión electrónica de documentos de la Seguridad Social; la presentación de documentos para adjuntar a un expediente administrativo abierto; las declaraciones de impuestos, etc.

La diferencia de uso en uno u otro sector radica en que en el sector público su utilización puede quedar supeditada al cumplimiento de unas condiciones adicionales establecidas por norma que en todo deberán ser objetivas, razonables y no discriminatorias y en ningún caso obstaculizarán la prestación de servicios al ciudadano cuando intervengan diferentes administraciones públicas nacionales o extranjeras (Rodríguez Adrados, 2004).

- La Entidad Certificadora Autorizada: Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB). Se crea la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia - ADSIB mediante el Decreto Supremo Nº 26553 de fecha 19 de marzo de 2002, es una entidad descentralizada bajo tuición de la Vicepresidencia de la República de Bolivia. La ADSIB es la encargada de proponer políticas, implementar estrategias y coordinar acciones orientadas a reducir la brecha digital en el país, a través del impulso de las Tecnologías de la Información y Comunicación (TIC) en todos sus ámbitos, teniendo como principal misión favorecer relaciones del Gobierno con la Sociedad, mediante el uso de tecnologías adecuadas (ADSIB, 2016).

La Ley Nº 164 establece que la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB), prestará el servicio de certificación para el sector público y la población en general a nivel nacional. La ADSIB cuenta con la Infraestructura de Clave Pública (PKI) para funcionar como una Entidad Certificadora.

En una primera etapa la ADSIB ha suscrito convenios interinstitucionales con entidades del sector público como la Aduana Nacional, la Autoridad de Supervisión del Sistema Financiero (ASFI), Vicepresidencia del Estado Plurinacional y Empresa Azucarera San Buena Aventura (EASBA) para iniciar, como piloto, el servicio de certificación y firma digital.

En la gestión 2015 ha sido auditada por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), quién verifico que cumplía con los requisitos técnicos, económicos y legales establecidos en la Ley, sus reglamentos y resoluciones administrativas, posteriormente ha procedido a autorizarla para que preste servicios de certificación y firma digital (ADSIB, 2015).

La ADSIB emite tres (3) tipos de certificados digitales con diferentes costos para 1) Personas naturales 195 Bs., 2) Personas jurídicas 370 Bs. y 3) Cargo público 450 Bs., estos precios son oficiales y han sido aprobados mediante Resolución Administrativa Regulatoria de la ATT.

La validez del contrato con la ADSIB es de un (1) año prorrogable a dos (2) años para certificados digitales de personas naturales y jurídicas. Asimismo, el artículo 29 del Decreto Reglamentario de la Ley Nº 164 establece la vigencia de dos (2) años para los certificados de cargos públicos[4].

[4] En el evento, el director de ADSIB, Sylvain Lesage, precisó que hasta la fecha se han emitido *"450 certificados, con puntos de registro en La Paz,*

El costo del *token* USB o la tarjeta inteligente es aproximadamente de 313 Bs. (45 USD); el *token* no es provisto por la ADSIB, el interesado en contratar el servicio debe llevar a la ADSIB el dispositivo de su elección (*token* USB o tarjeta inteligente). El costo aproximado de un certificado digital para persona natural que incluye el *token* o tarjeta inteligente es aproximadamente de 508 Bs. (73 USD).

La ADSIB se constituye en Agencia de Registro[5] y Entidad de Certificación, como objetivo inicial quiere alcanzar un numero de 5000 (cinco mil) usuarios.

- La Entidad Certificadora Asociación de Bancos Privados de Bolivia (ASOBAN). Tiene como misión ser una organización representativa del sistema bancario reconocida por su confiabilidad y liderazgo, que contribuye a la integración entre asociados, mercados, comunidad y región latinoamericana (ASOBAN, 2016).

La Entidad Certificadora ASOBAN presta servicios de certificación y firma digital desde el año 2002, tiene dos (2) tipos de certificados: 1) Certificado Digital Clase 2 para correo electrónico seguro que tiene un costo de 1.265 Bs. (182 USD), si se adquiere más de 20 certificados el costo baja a 860 Bs. (123 USD) y 2) Certificado Digital Clase 3 para personas jurídicas, servicio adquirido por ejemplo por las entidades financieras para garantizar que el portal del banco es un sitio web seguro (ASOBAN, 2015).

ASOBAN no cuenta con *token* USB o tarjeta inteligente, el software debe bajarlo directamente al dispositivo donde se vaya a firmar digitalmente. El contrato tiene una vigencia de un (1) año.

ASOBAN, pese a estar funcionando desde el año 2002 como Entidad Certificadora, no cuenta con la autorización de funcionamiento de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT) conforme establece el artículo 81 (Autoridad y atribuciones)[6] de la Ley Nº 164. ASOBAN se ampara en el artículo 80 (Certificados emitidos por entidades

Santa Cruz y Cochabamba", en trabajo coordinado con la Aduana Nacional, institución que hace uso de este recurso para facilitar los trámites de exportaciones. Asimismo, las universidades privadas Los Andes y San Francisco de Asís han recibido la certificación para simplificar el trámite de titulación para sus estudiantes…No obstante, la cobertura aún es escasa y no se cuenta con alcance nacional, además que en el público existe un desconocimiento del concepto de firma digital. Entre las perspectivas está trabajar para hacer seguro y confiable el uso de la firma digital desde celulares, y lograr la "sensibilización y capacitación a través de talleres con entidades públicas, para ver cómo pueden incorporar la firma digital en sus procedimientos internos". Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (2016). *Ayudar al ciudadano a realizar sus trámites más rápido y de forma segura por la red: experiencia boliviana a un año de la firma digital* [en línea]: https://adsib.gob.bo/Ayudar-al-ciudadano-a-realizar-sus [Consulta: 20/09/2016]

[5] Agencia de Registro: *"Es la agencia dependiente de una entidad certificadora, encargada de realizar el registro y la identificación de la persona natural o jurídica en forma fehaciente y completa, debe efectuar los trámites con fidelidad a la realidad. Además es quién se encarga de solicitar la aprobación o revocación de un certificado digital. Su objetivo primario es asegurarse de la veracidad de los datos que fueron utilizados para solicitar el certificado digital"* (numeral 3 del Artículo 37 (Estructura jerárquica) del D.S. Nº 1793 Reglamento a la Ley Nº 164 para el Desarrollo de Tecnologías de Información y Comunicación).

[6] Artículo 81 (Autoridad y atribuciones).- *"La Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes es la encargada de autorizar, regular, fiscalizar, supervisar y controlar a las entidades certificadoras de acuerdo a lo establecido en la presente Ley y su reglamentación".*

extranjeras)[7] de la misma Ley, pero para que sus certificados tengan la misma validez y eficacia jurídica deberán ser reconocidos por una entidad certificadora autorizada nacional como lo es hoy la ADSIB.

La Entidad Certificadora ASOBAN actúa en el marco contractual que establece CertiSur y VeriSign, ésta última entidad conocida a nivel mundial como Entidad Certificadora Raíz de Firma Digital.

Cabe aclarar que ASOBAN se configura para CertiSur y VeriSign más como un Agente de Registro que como una Entidad Certificadora propiamente dicha, su principal función es mediar entre la Entidad Certificadora internacional y la institución privada o pública que quiere adquirir un certificado y firma digital en Bolivia (ASOBAN, 2015).

- El Sistema Único de Modernización Aduanera (SUMA) y la firma digital. La Aduana Nacional es una entidad pionera en el uso de la Firma digital como una herramienta para modernizar los trámites aduaneros a partir del Sistema Único de Modernización Aduanera (SUMA). Su uso está amparado en la Ley Nº 164 General de Telecomunicaciones, Tecnologías de Información y Comunicación, en su Reglamento aprobado mediante Decreto Supremo Nº 1793 y en el Reglamento para uso de la Firma Digital aprobado mediante Resolución de Directorio Nº RD 01-003-16 de fecha 15 de febrero de 2016 emitida por la Aduana Nacional (Circular N° 032/2016).

A través de sus representantes o titulares, los Operadores de Comercio Exterior deberán utilizar la Firma Digital para la suscripción y presentación de Declaraciones de mercancías, manifiestos de carga y otros documentos aduaneros que así lo requieran. Para firmar digitalmente, las personas interesadas deberán solicitar la emisión de sus Certificados Digitales y descargar los mismos en un dispositivo Token[8] que será provisto por la Aduana Nacional (Aduana Nacional, 2016).

Inicialmente la Firma Digital se aplicará en los despachos de exportación de acuerdo a lo establecido en el Procedimiento para el Despacho Aduanero de Exportación de Mercancías UEP-X01 Versión 02 aprobado mediante Resolución de Directorio N° RD-01-002-16 de fecha 15 de febrero de 2016. Su aplicación se extenderá de forma gradual a otros regímenes aduaneros y trámites, una vez que se emitan procedimientos o reglamentos que incorporen su utilización (Aduana Nacional, 2016).

Podrán solicitar Certificados Digitales para Firma Digital las personas que se encuentren registradas en el Padrón de Comercio Exterior de la Aduana Nacional: 1) El Representante Legal Principal o Titular de empresa unipersonal y 2) El o

[7] Artículo 80 (Certificados emitidos por entidades extranjeras).- *"Los certificados digitales emitidos por entidades certificadoras extranjeras tienen la misma validez y eficacia jurídica reconocida en la presente Ley, siempre y cuando tales certificados sean reconocidos por una entidad certificadora autorizada nacional que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, el procedimiento, así como la validez y vigencia del certificado".*

[88] Token: *"Dispositivo criptográfico donde se almacena el Certificado Digital para proceder con la Firma Digital en declaraciones de mercancías, manifiestos de carga y otros documentos digitales habilitados por la Aduana Nacional"* (inciso g) del Artículo 5 (Definiciones) del RD 01-003-16 de fecha 15 de febrero de 2016).

los Representantes Legales para Firma que sean habilitados[9].

Conclusiones

Cabe mencionar que en Bolivia la Firma Digital cuenta con el marco legal correspondiente con la aprobación de la Ley Nº 164 General de Telecomunicaciones, Tecnologías de Información, Decreto Reglamentario y Resoluciones Administrativas Regulatorias (RAR) emitidas por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT). A nivel latinoamericano ha sido uno de los últimos países en regular la Firma Digital.

La Aduana Nacional es una entidad pionera en el uso de la Firma digital como una herramienta para modernizar los trámites aduaneros a partir del Sistema Único de Modernización Aduanera (SUMA).

El costo del Certificado Digital y el *Token USB* o Tarjeta Inteligente, que se constituye en el soporte del certificado y la firma digital, pueden ser una barrera para la implementación de la Firma Digital en Bolivia, el precio es bastante alto para la economía de boliviano, más aún cuando el salario mínimo nacional es de 1.805 Bs (260 USD), lo cual puede generar una brecha en el acceso al servicio.

La implementación de la firma digital es todavía escasa en Bolivia por falta de conocimiento de sus beneficios, por otra parte, no tiene alcance nacional, porque no cuenta con un Agente de Registro oficial en cada departamento.

La Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB), la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT) y Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación (AGETIC) deben trabajar en la capacitación sobre la firma digital a través de seminarios, talleres y cursos en el ámbito público y privado.

[9] Para presentarse en el Punto de Registro seleccionado se debe portar la siguiente documentación: 1) Formulario de Solicitud impreso y suscrito; 2) Fotocopia simple del carnet de identidad; 3) Original y copia del Testimonio de Poder o en caso de personas jurídicas de derecho público el documento de designación vigente; 4) Fotocopia simple del NIT; 5) Copia del Recibo de Pago por Adquisición del Token; 6) Copia del comprobante de pago por el Servicio de Certificación Digital; 7) Adicionalmente se deberá presentar una Autorización Expresa firmada por el Representante Legal de acuerdo a formato establecido por la ADSIB. Una vez que se presente en el Punto de Registro, el Agente de Registro evaluará la documentación presentada, de no encontrar observaciones imprimirá el Contrato de Adhesión, registrará el número de serie del Token y emitirá el Acta de Entrega y aprobará la solicitud.

Referencias

Aduana Nacional (2016). *La Firma Digital en la Aduana* [en línea]: http://www.aduana.gob.bo/firmadigital/ [Consulta: 19/09/2016]

Aduana Nacional (2016). *Recursos: Preguntas Frecuentes* [en línea]: http://www.aduana.gob.bo/infosuma/preguntas.php?filtro=5-Firma%20digital [Consulta: 19/09/2016]

Aduana Nacional (2016). *Reglamento para uso de la Firma Digital.* Resolución de Directorio Nº RD 01-003-16 de fecha 12 de febrero de 2016.

Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (2015). *Firma Digital* entrevista a la Encargada de Planificación y Proyectos, Lic. Kantuta Muruchi en fecha 14 de agosto de 2015.

Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (2016). *Misión y Visión de la Institución* [en línea]: https://adsib.gob.bo/Mision-y-Vision-de-la-Institucion-107 [Consulta: 19/09/2016]

Asociación de Bancos Privados de Bolivia (2015). *Entidad Certificadora ASOBAN* entrevista con Ing. Ricardo Primintela, Administrador de Sistemas de la Administradora de Cámaras de Compensación y Liquidación – ACCL S.A. en fecha 21 de septiembre de 2015.

Asociación de Bancos Privados de Bolivia (2016), *Misión* [en línea]: http://www.asoban.bo/nosotros/nuestra-filosofia [Consulta: 18/09/2016]

Boletín Oficial del Estado (2003). *Ley 59/2003 de 19 de diciembre de Firma Electrónica.*

Davara R., M. (2005). *La seguridad en las transacciones electrónicas: La Firma Electrónica.* Editorial Vodafone Fundación España. Madrid

De Quinto Z., F. (2004). *La firma electrónica. Marco legal y aplicaciones prácticas.* Editor Difusión Jurídica y Temas de Actualidad S.A., Barcelona.

Gaceta Oficial del Estado Plurinacional de Bolivia (2011). *Ley Nº 164 General de Telecomunicaciones, Tecnología de Información y Comunicación* de fecha 8 de agosto de 2011.

Gaceta Oficial del Estado Plurinacional de Bolivia (2013). *Decreto Supremo Nº 1793 Reglamento a la Ley Nº 164 para el desarrollo de Tecnologías de Información y Comunicación* de fecha 13 de noviembre de 2013.

García M., F. J. (2004). *Comercio y firma electrónicos (análisis jurídico de los servicios de la sociedad de la información).* Editorial Lex Nova, Segunda Edición, Valladolid.

Martínez N., A. (2004). *Comentarios a la Ley 59/2003 de Firma Electrónica.* Civitas Ediciones S.L. Madrid.

Rodríguez A., A. (2004). *Firma Electrónica y Documento Electrónico*. Edita Consejo General del Notariado. Madrid.

Roselló M., R. (2001). *El Comercio Electrónico y la protección al consumidor*. Cedecs Editorial S.L. Barcelona.

Vázquez I., C. (2002). *Comercio electrónico, firma electrónica y servidores.* DIJUSA Editorial S.L., Madrid.

Presentado: La Paz, 22 de septiembre de 2016.

Aceptado: La Paz, 10 de octubre de 2016.