



Recepción: 17 / 02 / 2017

Aceptación: 30 / 05 / 2017

Publicación: 15 / 07 / 2017



Ciencias de la computación

Artículo de investigación

## Algo sobre la firma electrónica en el contexto actual

*Something about electronic signature in the current context*

*Alguma coisa sobre assinatura eletrônica no contexto atual*

Luís D. Muñoz- Mendoza <sup>I</sup>

[ldmunoz@sangregorio.edu.ec](mailto:ldmunoz@sangregorio.edu.ec)

Jodamia U. Murillo-Rosado <sup>II</sup>

[jumurillo@sangregorio.edu.ec](mailto:jumurillo@sangregorio.edu.ec)

Cristian R. Amen-Chinga <sup>III</sup>

[cramen@sangregorio.edu.ec](mailto:cramen@sangregorio.edu.ec)

Correspondencia: [ldmunoz@sangregorio.edu.ec](mailto:ldmunoz@sangregorio.edu.ec)

<sup>I</sup> Magister en Telecomunicaciones, Ingeniero en Sistemas Informáticos, Docente de la Universidad San Gregorio de Portoviejo, Portoviejo, Ecuador.

<sup>II</sup> Magister en Informática Empresarial, Ingeniero en Sistemas Informáticos, Docente de la Universidad San Gregorio de Portoviejo, Portoviejo, Ecuador.

<sup>III</sup> Ingeniero Comercial, Docente de la Universidad San Gregorio de Portoviejo, Portoviejo, Ecuador.

## Resumen

Hoy, en diferentes lugares del mundo se emplea la firma electrónica, sin embargo aún existen divergencias conceptuales, temores y analfabetismo para su utilización. En este trabajo se explica qué se entiende por firma electrónica, los tipos de firma existentes y los diferentes países que la utilizan. Para ello se hace una búsqueda bibliográfica por diferentes recursos de información de Internet y se hace un análisis documental.

**Palabras clave:** Firma electrónica; tecnologías de información y comunicación; firma digital.

## Abstract

Today, electronic signatures are used in different parts of the world, but conceptual differences, fears and illiteracy still exist. This paper explains what is meant by electronic signature, the types of existing firm and the different countries that use it. For this, a bibliographic search is made for different information resources of the Internet and a documentary analysis is done.

**Keywords:** Electronic signature; information and communication technologies; digital signature.

## Resumo

Hoje, as assinaturas eletrônicas são usadas em diferentes partes do mundo, no entanto, diferenças conceituais, medos e analfabecias ainda existem para seu uso. Este artigo explica o que se entende por assinatura eletrônica, os tipos de empresas existentes e os diferentes países que a utilizam. Para isso, uma pesquisa bibliográfica é feita para recursos de informação diferentes da Internet e uma análise documental é feita.

**Palavras chave:** Assinatura eletrônica; tecnologias de informação e comunicação; assinatura digital.

## Introducción

La Firma Electrónica, es una de las herramientas que permite que se haga efectivo el comercio electrónico, que en un sentido amplio es toda transacción realizada a través de redes electrónicas de información conocidas en la actualidad como el Internet.

La firma electrónica, es muy utilizada hoy en varios países del mundo para asegurar las comunicaciones electrónicas.

El sistema comercial sustentado en papel se encuentra viviendo la transición a un comercio electrónico de documentos y Firmas Electrónicas, que deben ofrecer a sus usuarios la misma seguridad jurídica del sistema comercial respaldado en papel. (Tobar Estrella, 2006).

En este sentido, los términos "firma electrónica" y "firma digital" se utilizan indistintamente y en ocasiones se consideran como sinónimos.

En este trabajo se explica qué se entiende por firma electrónica, los tipos de firma existentes y los diferentes países que la utilizan.

Para ello se hace una búsqueda bibliográfica por diferentes recursos de información de Internet y se hace un análisis documental.

## **Desarrollo**

La firma es un conjunto de letras o signos que identifican a la persona que la estampa. En el concepto tradicional la firma de un documento, ya sea este privado o público, debe efectuarse de manera manuscrita u hológrafa. (Fernández del Pech, s/f).

La firma es el lazo o nexo que une a la persona con el documento, para ello no necesariamente tiene que ser nominal ni legible, pero sí ponerse por el firmante en persona. Por lo tanto, la función primordial de la firma, más allá de la identificación del firmante, es la de ser una prueba de declaración de voluntad.

La firma electrónica es una firma que se inserta digitalmente en la factura o documento digital y que permite al receptor de un mensaje verificar la autenticidad del emisor de la información así como verificar que dicha información no ha sido modificada desde su generación. Se necesita el consentimiento de ambas partes (emisor y receptor) y se tienen que dar tres condicionantes para que la firma electrónica sea reconocida:

- Que sea una firma electrónica avanzada, es la que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere.
- Que esté basada en un certificado reconocido.

- Que sea generada mediante un dispositivo seguro de creación de firma. (Practical Team, s/f).

Para tener una firma electrónica es preciso poseer un certificado electrónico reconocido, una certificación de que la persona receptora es la que realmente firma. Dicho certificado puede ser en formato software (un archivo en el ordenador) o en formato tarjeta, en este caso se necesita un lector de tarjetas (como el del DNI Electrónico). (Practical Team, s/f).

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

Es aquel conjunto de datos, como códigos o claves criptográficas privadas, en forma electrónica, que se asocian inequívocamente a un documento electrónico (es decir, contenido en un soporte magnético ya sea en un disquete, algún dispositivo externo o disco duro de una computadora y no de papel), que permite identificar a su autor, es decir que es el conjunto de datos, en forma electrónica, anexos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge. (Reyes Krafft, s/f).

Técnicamente se podría definir a la Firma Electrónica como "un conjunto de datos digitales que se añaden a un archivo digital, que identifica al firmante, quien aprueba y reconoce la información ahí contenida" (González, s/f).

La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante. Permite autenticando las comunicaciones generadas por el firmante. Los datos de creación de firma son los datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica. El firmante es la persona que está en posesión de un dispositivo de creación de firma y que actúa en su propio nombre o en el de la entidad o persona física o jurídica a la que representa. (Merchan Arribas, 2013).

La firma electrónica hace referencia, a la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, a un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje. (Fundación Wikimedia, 2017).

La firma electrónica es una herramienta tecnológica que sirve para asegurar las comunicaciones electrónicas (...) Datos en forma electrónica consignados en una comunicación electrónica, o adjuntado o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante con relación a la comunicación electrónica e indicar que el firmante aprueba la información recogida en la comunicación electrónica (...) La firma electrónica es el análogo en el mundo digital para la firma manuscrita y sirve para asegurar la identidad del firmante, que la información no ha sido modificada después de ser firmada, y que el firmante no puede negar que firmó. (Santizo Ochoa, 2010).

La firma electrónica de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido y, seguidamente, aplicar el algoritmo de firma (en el que se emplea una clave privada) al resultado de la operación anterior, generando la firma electrónica. (Fundación Wikimedia, 2017).

Se puede decir entonces que la firma electrónica es el conjunto de datos, en forma electrónica, utilizados como medio para identificar formalmente al autor del documento que la recoge. Sirve para asegurar la identidad del firmante, que la información no ha sido modificada después de ser firmada, y que el firmante no puede negar que firmó.

Hay autores que hablan indistintamente de firma digital y firma electrónica:

- Una firma digital es una firma electrónica que se puede usar para autenticar la identidad de quien envía un mensaje o quien firma un documento electrónico, así como asegurar que el contenido original del mensaje o del documento electrónico que ha sido enviado no ha sido modificado. Las firmas digitales son fácilmente transportables y no pueden imitarse. La firma digital puede aplicarse a cualquier tipo de información electrónica, ya sea que se encuentre cifrada o en texto claro. (Morales Sandoval, Díaz Pérez, & Domínguez Pérez, 2013).

- La Firma Electrónica como se encuentra definida en la mayor parte de las normativas del mundo es un término genérico, por lo cual también se contempla dentro de éstas a la firma digital, así cuando se define la Firma Electrónica se hace en un sentido de neutralidad tecnológica, que permite anticiparse al avance de la tecnología donde podrían presentarse otro tipo de firmas que no sean la firma digital o de clave pública (...) la firma digital es aquella que se basa en el uso de la criptografía asimétrica que es una especie de Firma Electrónica caracterizada por agregar elementos de seguridad que la Firma Electrónica no posee (Tobar Estrella, 2006)

Las principales funciones de la firma electrónica son (Merchan Arribas, 2013):

- **Identificación del firmante:** la firma identifica al firmante de forma única igual que su firma manuscrita.
- **Integridad del contenido firmado:** es posible verificar que los documentos firmados no hayan sido alterados por terceras partes.
- **No repudio del firmante:** un documento firmado electrónicamente no puede repudiarse por parte de su firmante.

En la literatura se distingue entre firma simple y firma electrónica avanzada:

La firma simple es el conjunto de datos, en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante. (Merchan Arribas, 2013).

La firma simple se define como 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 (partiendo de la presunción, en materia mercantil, de que el mensaje ha sido enviado usando medios de identificación como claves o contraseñas por ambas partes conocidas, para lo cual se requerirá de un acuerdo previo y firmado en forma autógrafa por las partes. (Reyes Krafft, s/f).

El término firma electrónica simple implica el uso de cualquier medio electrónico para firmar un documento. Es este sentido, el simple escaneo de una firma autógrafa y su inserción como

imagen en un documento digital puede considerarse como firma electrónica. Sin embargo, este tipo de firma electrónica no garantiza los servicios de no repudio, por ejemplo. Otro ejemplo es el uso de un lápiz electrónico para recabar la firma autógrafa (común para expedir credenciales) o mediante la selección de algo en una pantalla táctil por parte del firmante. De igual forma, este tipo de firma no provee los servicios de integridad y no-repudio. (Morales Sandoval et al., 2013).

La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control. (Merchán Arribas, 2013).

La firma digital o firma electrónica avanzada establece que se entiende como tal, aquella firma, que a través de un certificado digital emitido por una entidad de certificación acreditada, incorpore una serie de datos electrónicos que identifican y autentifican al firmante a través de la asignación de una llave pública y otra privada en base a los parámetros de la criptografía asimétrica (o también conocida como de llave pública). Mediante este proceso, se garantiza que en el caso de sufrir variaciones en la firma y/o gestión de documentación electrónica, la responsabilidad es del usuario, ya que al tener esta firma bajo su control exclusivo, el usuario es por tanto el responsable último de todos los procesos asociados a la misma. (Morales Sandoval et al., 2013).

La firma electrónica avanzada la podemos conceptualizar como la firma electrónica que permite la identificación del firmante y ha sido generada bajo su exclusivo control que vincula exclusivamente al mismo con el mensaje de datos al que se adjunta o se asocia, lo que permite que sea detectable cualquier modificación ulterior de éste, entendida como proceso electrónico que permite al receptor de un mensaje de datos identificar formalmente a su autor, mismo autor que mantiene bajo su exclusivo control los medios para crear dicha firma, de manera que esté vinculada únicamente a él y a los datos a que se refiere el mensaje, permitiendo detectar cualquier modificación ulterior al contenido del mismo, garantizando así la identidad del titular y que éste no pueda desconocer la autoría del documento. (Reyes Krafft, s/f).

"(...) El tener al descubierto la clave privada es un riesgo muy grave, ya que la custodia exclusiva de la misma es la garantía de no repudio de nuestras futuras firmas electrónicas, por lo que

cualquier persona que disponga de la misma podrá realizar firmas fraudulentas con el mismo valor legal que si firmara a mano alzada. Por ello, es un riesgo muy grave ya que el conocimiento de una tercera persona de la clave puede traer consigo la suplantación de identidad, se podrá hacer pasar por nosotros y firmar en cualquier sitio" (Echevarría del Blanco, 2016).

Por la revisión de la literatura realizada parece ser que la firma electrónica avanzada es la que tiene presente a la criptografía, especialmente la asimétrica, que utiliza las claves públicas y las claves privadas para la firma digital, pero para que esto funcione es necesario la utilización de los denominados certificados de Firma Electrónica, que asocian la clave pública a una persona determinada, y que deben ser emitidos por las entidades de certificación de información.

Según Echevarría del Blanco (2016), lo que ocurre muchas veces entre las empresas y los usuarios es que presuponen que únicamente ya el uso de una firma electrónica avanzada es una garantía de seguridad, pero esto es un error muy grave si no se tienen en cuenta dos reglas que son claves en este tema:

- La primera de las reglas es tener la certeza de que nuestros certificados han sido generados por un prestador de servicios de certificación confiable y que para la creación de los mismos han hecho uso de un hardware criptográfico, el cual debería estar reconocido internacionalmente y aprobado por un laboratorio especializado en el tema. Esto es importante porque como hemos dicho antes la fuerza de estos certificados o su clave en cuanto a la seguridad reside en sus claves, clave privada, por tanto, la forma en la que ha sido generada la misma también es importante para mantener la seguridad de las mismas.
- La segunda de las reglas es la forma en que se custodian las claves de los certificados de los que hacemos uso. Una de las formas en las que los usuarios guardan estas claves es haciendo uso de una Smart Card que es seguro, pero ¿qué ocurre? Para las empresas hacer uso de este tipo de tarjetas puede hacer que se ralentice el proceso, y por tanto lo que hacen muchas es guardarla directamente en el ordenador para acceder directamente a ella, en cualquier carpeta, vamos como si nosotros dejáramos en nuestro ordenador en un documento de texto accesibles todas nuestras contraseñas de nuestras cuentas. Si a esto le añadimos la ausencia de control y gestión de los usuarios que tienen acceso a las claves dentro de la empresa, estamos corriendo

el riesgo de la suplantación de identidad y de no saber al final quien es la persona que firma realmente. (Echevarría del Blanco, 2016).

Cuando se revisa en la literatura el tema de la firma electrónica aparecen los términos autenticación, integridad, irrenunciabilidad, confidencialidad:

La autenticación se refiere a la seguridad de que el remitente del mensaje es realmente quien dice ser. Una firma electrónica asegura la autenticación porque existe una autoridad certificadora que se encarga de asegurar que la pareja de claves, pública y privada pertenecen exclusivamente a una persona y dicha autoridad ha verificado su identidad. La firma electrónica garantiza la identidad digital del remitente de una comunicación. La autenticidad se refiere cuando el autor del acto expresa su consentimiento y hace propio el mensaje. Es una operación pasiva que no requiere del consentimiento, ni del conocimiento siquiera del sujeto identificado. Proceso activo por el cual alguien se identifica conscientemente en cuanto al contenido suscrito y se adhiere al mismo. (Reyes Krafft, s/f).

La integridad es la propiedad de la información que garantiza que no ha sido modificada intencionalmente, ni debido a errores, de transmisión o de almacenamiento en un período de tiempo determinado.

El no repudio es también conocido como irrenunciabilidad. Hace referencia a la incapacidad de rechazar algo o no aceptarlo, en este caso se refiere a negar que fuera firmada electrónicamente la información que contiene firma. La firma electrónica garantiza que el emisor de un mensaje no podrá negar que firmó el mensaje, debido que, para firmar algo electrónicamente se necesita tanto de la clave privada como su certificado de identidad. El propietario de un certificado digital está obligado por la ley, a custodiar su certificado de identidad y su clave privada.

La confidencialidad de la información es la propiedad que garantiza que únicamente el o los destinatarios podrán tener acceso a ella. La firma electrónica en sí no garantiza la confidencialidad; la confidencialidad es asegurada únicamente si tanto el remitente como el destinatario poseen un certificado digital, porque entonces el emisor puede cifrar el mensaje con la clave pública del destinatario de manera que pueda ser descifrado únicamente con la clave privada del destinatario (que solo él conoce) debido a se trata de un sistema criptográfico

asimétrico. Entonces si un tercero interceptara el mensaje, no sería capaz de leerlo dado que no posee la clave privada del destinatario.

Actualmente entre los países que cuentan con una legislación en materia de firma electrónica podemos enumerar, según (Reyes Krafft, s/f) a los siguientes:

- En Guatemala en septiembre de 2008 se publicó el decreto 47-2008, el cual contiene la "Ley para el reconocimiento de las comunicaciones y firmas electrónicas"; ley que otorga validez legal a la información firmada electrónicamente.
- En México, el diario oficial de la federación, el 11 de enero del año 2012 publicó el decreto por el que se expide la Ley de Firma Electrónica Avanzada. En dicho decreto se menciona (indirectamente) que la firma electrónica estará basada en el uso de certificados digitales por lo que la criptografía de llave pública y el uso de PKIs es requerida. También indica los campos que debe contener el certificado digital y las entidades certificadoras recomendadas para emitir los certificados digitales. A partir de este decreto, varios estados de la república mexicana han emitido leyes para el uso de la firma electrónica, principalmente en trámites y servicios gubernamentales.
- Alemania (El 13 de junio de 1997 fue promulgada la Ley sobre Firmas Digitales y el 7 de junio del mismo año, fue publicado su Reglamento.
- Argentina (El 17 de marzo de 1997, el Sub-Comité de Criptografía y Firma Digital, dependiente de la Secretaría de la Función Pública, emitió la Resolución 45/97 -firma digital en la Administración Pública- el 14/12/2001 Ley de Firma Digital para la República Argentina 25/506.
- C.E.E. (Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre, por la que se establece un marco comunitario para la firma electrónica.- Decisión de la Comisión, de 6 de noviembre de 2000, relativa a los criterios mínimos que deben tener en cuenta los Estados miembros para designar organismos de conformidad con el apartado 4 del artículo 3 de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo por la que se establece un marco comunitario para la firma electrónica (2000/709/CE).
- Canadá (British Columbia Bill 13-2001, The Electronic Transactions Act).

- Colombia (Ley 527 de 1999. 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, y se establecen las entidades de certificación)
- Chile (2002 Ley sobre documentos electrónicos, firma electrónica y servicios de certificación).
- Dinamarca: Act 417 of 31 May 2000 on Electronic Signatures.
- Francia: Décret n° 2001-272 du 30 mars 2001
- Irlanda: Electronic Commerce Act, 2000 (Number 27 of 2000)
- Italia (El 15 de marzo de 1997, fue publicado el "Reglamento sobre: Acto, Documento y Contrato en Forma Electrónica" aplicable a las diversas entidades de la Administración Pública, el 15 de abril de 1999 las reglas técnicas sobre firmas digitales y el 23 de enero del 2002 la ley sobre firma electrónica).
- Japón (1/04/2001 Ley sobre firma electrónica y Servicios de Certificación).
- Luxemburgo: Règlement grand-ducal du 1er juin 2001
- Panamá (3/08/2001 Ley 43 de Comercio Electrónico).
- Portugal: Decree-Law 290-D/99.
- Reino Unido: Electronic Communications Act, 2000.
- Suecia: Qualified Electronic Signatures Act (FSF 2000:832)
- Ecuador cuenta con la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, que regula principalmente la Firma Electrónica y los servicios de certificación, normativa que se la ha emitido siguiendo los principios y procedimientos básicos establecidos en la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional -CENUDMI-, conocida por sus siglas en inglés como -UNCITRAL-. Al igual que la normativa internacional, la Ley de Comercio Electrónico ecuatoriana contiene a la Firma Electrónica, es así como en relación con los documentos electrónicos cumple con las

principales funciones atribuidas a la firma manuscrita, identifica al autor (autenticación) y verifica que el mensaje no haya sido alterado después de firmado (integridad); en complemento a lo expresado, el Reglamento a la Ley contiene la teoría de la neutralidad tecnológica respaldada por la UNCITRAL, que no restringe el uso de otras Firmas Electrónicas concebidas fuera de la infraestructura de clave pública, situación última para que la Ley tenga vigencia en el tiempo ante el cambio de la tecnología. (Tobar Estrella, 2006).

- En España, la Ley de la Firma Electrónica (España, 2003), y la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (España, 2007), dieron la cobertura legal necesaria para permitir que los documentos nacidos electrónicamente se pudieran considerar auténticos. (Giménez Chornet, 2014).

A nivel de organizaciones Reyes Krafft (s/f), habla de que la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI-UNCITRAL) desde su 24º periodo de sesiones celebrado en el año 1991 trabaja el tema mediante el Grupo de Trabajo denominado sobre Pagos internacionales el estudio de los problemas jurídicos del intercambio electrónico de datos (EDI: Electronic Data Interchange).

También la Organización para la Cooperación y Desarrollo Económico desde 1997 trata la utilización de criptografía (Guidelines for Cryptography Policy).

Y la Organización Internacional de Normas ISO, específicamente la norma ISO/IEC 7498-2 (Arquitectura de Seguridad de OSI) regula los servicios de seguridad sobre confidencialidad, integridad, autenticidad, control de accesos y no repudio. A través de su subcomité 27, SC 27, trabaja en una norma de firma digital.

## Conclusiones

Al conocer qué se entiende por firma electrónica y sus tipos, se hace evidente que la firma electrónica presenta beneficios que fortalecen su uso como son una mayor integridad de los documentos; el mismo no puede ser alterado, por lo que se garantiza la autenticidad del mismo; y el contenido del mensaje solo será conocido por quienes estén autorizados a ello (confidencialidad). Además, se elimina el papel y hay una disminución en el tiempo.

Sin embargo, aun cuando se han desarrollado guías de uso, el hecho de tener que aprender a utilizar una nueva tecnología provoca cierta resistencia de aceptación.

## Referencias bibliográficas

Echevarría del Blanco, U. (2016). Los riesgos de la firma electrónica. from <https://blogs.deusto.es/master-informatica/los-riesgos-de-la-firma-electronica/>

Fernández del Pech, H. (s/f). Firma digital. from <http://www.hfernandezdelpech.com.ar/FIRMA%20DIGITAL.pdf>

Fundación Wikimedia, I. (2017). Firma digital. 2017

Giménez Chornet, V. (2014). Criterios ISO para la preservación digital de los documentos de archivo. *Códices*, 10(2), 135-150.

González. (s/f). Firma Electrónica from <http://archivo.larevista.ec/me-sirve/dr-tecno/firma-electronica>.

Merchan Arribas, M. (2013). Identidad digital y firma electrónica.

Morales Sandoval, M., Díaz Pérez, A., & Domínguez Pérez, L. J. (2013). Firma electrónica: concepto y requerimientos para su puesta en práctica México.

Practical Team. (s/f). Todo lo que necesitas saber sobre la firma electrónica. from <http://www.practicalteam.com/blog/todo-lo-que-necesitas-saber-sobre-la-firma-electronica/>

Reyes Krafft, A. A. (s/f). La firma electrónica.

Santizo Ochoa, J. R. (2010). Implementación y Adopción de la Firma Electrónica en Guatemala. Universidad de San Carlos de Guatemala, Guatemala.

Tobar Estrella, M. (2006). Firmas Electrónicas y su Régimen de Aplicación, Análisis de la Normativa en el Ecuador. Universidad Andina Simón Bolívar, Ecuador.