# Propuesta de Implementación de Firma Electrónica en El Salvador para Bancos Cooperativos y Sociedades de Ahorro y Crédito, Basado en la Situación Actual de COMÉDICA DE R.L.

Evelyn Alvarenga
Facultad de Ingeniería
Universidad Don Bosco
La Libertad, El Salvador
eve.carmencita32@gmail.com

Telma Pineda
Facultad de Ingeniería
Universidad Don Bosco
La Libertad, El Salvador
tmpineda9@gmail.com

***Abstract*— Este artículo es un análisis sobre la implementación y funcionamiento de la firma electrónica, de lo cual se deriva una propuesta para su implementación en los bancos cooperativos y sociedades de ahorro y crédito de El Salvador para la cual se tomó como base la situación actual de COMEDICA de R.L.**

***Keywords—firma electrónica; ley; cooperativa; departamento TI; departamento jurídico; marco legal; asociado.***

## I. INTRODUCCIÓN

Es innegable el hecho que a medida transcurren los años cada vez hay más avances tecnológicos, usos de tecnologías, protección de datos etc., de tal manera que procesos que hace algunos años se hacían de forma presencial hoy en día se llevan a cabo de forma virtual desde casa a través de una computadora, un teléfono, Tablet o cualquier otro dispositivo electrónico que cuente con acceso a Internet.

Es así como a través de estos avances tecnológicos, donde principalmente se busca evitar hacer trámites de forma presencial, que surge la firma electrónica misma, la cual pretende tener la misma validez que la firma autógrafa, es por ello que el presente trabajo sugiere una guía de implementación de la misma dirigida al sector de bancos cooperativos.

En América latina países como Argentina, Belice, Bolivia, Brasil, Colombia, Costa Rica, México, Uruguay, entre otros ya cuentan con la implementación de la firma electrónica, sin embargo, en la actualidad El Salvador cuenta con la aprobación de una Ley de Firma Electrónica, la cual fue publicada en el diario oficial en el año 2015, indicando así su vigencia en el país, sin embargo, si bien es cierto que la ley ya se encuentra vigente todavía no se cuenta con su implementación y uso, es decir la ley aún no ha sido aplicada a ningún proceso, lo cual indica que solo se tiene el marco legal y regulatorio para la misma.

## II. FIRMA ELECTRÓNICA

Para poder comprender qué es la firma electrónica y como funciona se deben contemplar dos elementos, las bases legales que describen el marco legal y regulatorio definido y vigente en el país, y las bases teóricas en las que se determina como funciona la firma y que se necesita para hacer uso de la misma.

### *A. Bases Legales*

Desde la publicación de la Ley de Firma Electrónica se ha comenzado a paso lento la puesta en marcha o practica de esta, en ella se encuentran una lista de conceptos que son fundamentales para su cumplimiento.

- **Acreditación:** Es la autorización que otorga la autoridad competente establecida en la presente Ley, a los proveedores de servicios de certificación, para operar y proporcionar certificados electrónicos, y a los proveedores de servicios de almacenamiento de documentos electrónicos, una vez cumplidos los requisitos y condiciones establecidos en la presente Ley.[1]
- **Certificado Electrónico:** Documento proporcionado por un proveedor de servicios de certificación que otorga certeza a la firma electrónica certificada, garantizando la asociación de la persona con dicha firma.[1]
- **Firma Autógrafa:** Marca o signo, que una persona escribe de su propia mano en un instrumento o documento para asegurar o autenticar la identidad de una persona como prueba del consentimiento y verificación de la información contenida en dicho instrumento.[1]
- **Firma Electrónica Simple:** Son los datos en forma electrónica, consignados en un mensaje de datos 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.[1]
- **Firma Electrónica Certificada:** Son los datos en forma electrónica, consignados en un mensaje de datos o lógicamente asociados al mismo, que permiten la identificación del signatario, y que los datos de creación de la firma se encuentran en exclusivo control del signatario, lo que permite que sea detectable cualquier modificación ulterior al contenido del mensaje de datos. [1]

- **Firmante:** La persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona que representa. [1]
- **Proveedor de Servicios de Certificación:** Persona jurídica autorizada por la autoridad competente, dedicada a emitir certificados electrónicos y demás actividades previstas en esta Ley. [1]
- **Proveedor de Servicios de Almacenamiento de** Documentos Electrónicos: Persona jurídica autorizada por la autoridad competente que, por la naturaleza de su negocio, brinda servicios de almacenamiento de documentos electrónicos**.** [1]
- **Signatario:** Persona que posee un dispositivo de creación de firma electrónica certificada y que actúa en nombre propio o a nombre de una persona natural o jurídica que representa. [1]

En la Ley [1] también se define quienes serán las partes involucradas y sus responsabilidades y/o roles en el proceso, entre las que se mencionan:

- Autoridad de Control y Vigilancia.
- Unidad de Firma Electrónica.
- Comité Técnico Consultivo.

De igual forma en la Ley [1] contempla los lineamientos y/o normativas que se deben cumplir para el proceso de firma electrónica dentro de los cuales están:

- Garantías Mínimas que debe Cumplir el Sistema de Almacenamiento de Documentos Electrónicos.
- Requisitos y Efectos de la Firma Electrónica Certificada.
- Presunciones del Empleo de la Firma Electrónica Certificada.
- Inhabilitación en el Uso de Firma Electrónica Certificada.
- Solicitud para el Uso de la Firma Electrónica Certificada por Representantes de Personas Jurídicas.
- Uso de Firma Electrónica Simple.
- Uso de Firma Electrónica Certificada.
- Contenido del Certificado Electrónico.
- Formas de Conservación de Documentos.
- Requisitos para la Conservación de Documentos.
- Garantías Mínimas que debe Cumplir el Sistema de Almacenamiento de Documentos Electrónicos.

### *B. Bases Teóricas*

Para el proceso de firma electrónica es importante tener claro no sólo el marco legal de cada país en la que se implementa, sino también bases teóricas las cuales definen procesos, conceptos, procedimientos incluso requerimientos para poder primero comprender el proceso global y luego proceder a una implementación.

La implementación de la firma electrónica requiere de la utilización de la infraestructura de llave pública conocida como PKI por sus siglas en inglés, la cual se utiliza para autenticar a los usuarios de una transacción por medio de cifrados y elementos criptográficos para cifrar, descifrar, entre otros, para poder mantener la privacidad de la transacción. [2]

Dentro de la criptografía de llave publica hay dos conceptos importantes que conocer que son la llave pública y llave privada, una llave privada es utilizada para firmar documentos y ésta solo es del conocimiento de la persona a la que pertenece mientras que la llave pública es compartida por el dueño a los demás ya que se utiliza para verificar las firmas que se han generado utilizando la llave privada.

Un certificado digital es un medio que permite garantizar la identidad de una persona, para ello se utiliza la clave pública, los certificados digitales permiten que se dé el proceso de firma electrónica de tal forma que el receptor pueda verificar que el mensaje lo envió quien dice enviarlo y que el contenido no ha sido alterado. El certificado es emitido por una entidad certificadora, la cual ha sido autorizada para ello por la autoridad certificadora raíz, que es la mayor de las autoridades certificadoras, sobre ella no hay nadie más. La principal función de la autoridad certificadora es verificar y garantizar la asociación que se ha hecho de una persona natural o jurídica con el certificado digital. [3]

El concepto técnico de firma electrónica según [4] indica que "una firma electrónica es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje. La firma electrónica no implica asegurar la confidencialidad del mensaje; un documento firmado electrónicamente puede ser visualizado por otras personas, al igual que cuando se firma holográficamente. La firma electrónica es un instrumento con características técnicas y normativas. Esto significa que existen procedimientos técnicos que permiten la creación y verificación de firmas electrónicas, y existen documentos normativos que respaldan el valor legal que dichas firmas poseen"

Según [4] el proceso de firma electrónica consta de dos etapas, la primera de ellas es el proceso para generar la firma electrónica, ya se sabe que una persona tiene un par de llaves, una pública y una privada. El emisor genera un documento, el que desea enviar firmado, dicho documento es procesado por una función hash para posteriormente ser cifrado utilizando la llave privada del emisor, obteniendo así la firma electrónica misma que debe ser agregada al documento y enviarlo al receptor.

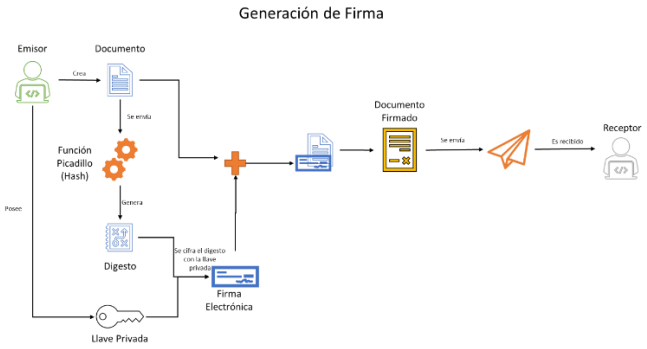


Fig. 1. Diagrama para la generación de firma Electrónica

La segunda etapa del proceso consiste en la verificación de la firma por parte del receptor, para necesita tener el certificado digital válido del emisor ya que en él se encuentra la llave pública del mismo. Una vez el receptor tiene el documento firmado debe separarlo, es decir obtener el documento original de la firma, con el documento original lo que debe hacer procesarlo a través de una función hash para obtener su digesto y la firma descifrarla utilizando la llave pública de emisor, misma que se encuentra en el certificado. Al descifrar la firma lo que se obtiene es el digesto generado por el emisor del documento original que él envió, ahora deben compararse ambos digestos, el que venía con la firma del emisor y el que obtuvo el receptor del documento, si ambos son iguales entonces la firma es válida y quiere decir que el documento no fue alterado, que el mismo que fue enviado.

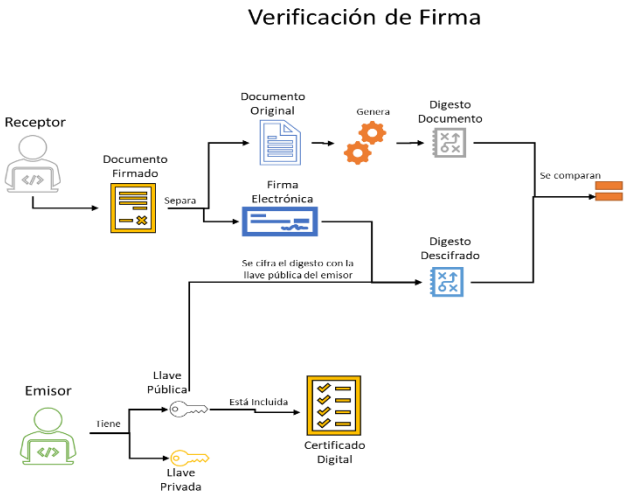


Fig. 2. Diagrama para la verificación de la firma electrónica

## III. Metodología

La recopilación de información para esta investigación está determinada primero por el análisis de contenido tanto de la Ley de Firma Electrónica, el Reglamento de la misma, así como también el proceso de firma electrónica generalizado y como éste debe ser ajustado según lo que se menciona en la Ley. Una vez realizado el análisis de contenido se identificaron las áreas que se van a ver mayormente impactadas cuando entre en funcionamiento la Ley de Firma Electrónica para el caso particular de COMÉDICA de tal forma que fuese posible entrevistar a uno o dos representantes de cada una de ellas.

Dentro de lo que constituye el marco legal y regulatorio se debe analizar

- Ley de Firma Electrónica.
- Reglamento de Ley de Firma Electrónica.
- Normativa de bancos cooperativos y sociedades de ahorro y crédito.
- Superintendencia del Sistema Financiero (como regidor de varios de los procesos de bancos cooperativos).

Adicionalmente es importante que dentro de una cooperativa se analice internamente la situación y/o procesos actuales, por lo cual dentro de la misma se determinaron los siguientes departamentos como los principales involucrados en el proceso:

- Gerencia y Departamento de TI.
- Gerencia y Departamento de Operaciones y Agencias.
- Departamento Jurídico.

## IV. Guia de Implementación

La implementación de la firma electrónica para bancos cooperativos y sociedades de ahorro y crédito basados en la situación de COMÉDICA, debe ser tratado como un proyecto institucional y por lo tanto, tomarse el tiempo necesario para llevarlo a cabo, no puede ser incorporado radicalmente de un día a otro pues se requiere que los departamentos involucrados (ya sea operativos o de apoyo) identifiquen el grado de impacto que esto conlleva.

Lo anterior tiene como objetivo generar los insumos necesarios para que la junta directiva tome las decisiones correctas y basados en la realidad de la cooperativa, así como también tomar en cuenta que todo cambio en el sistema y en los procesos requiere de capacitaciones, tanto para los empleados como para los clientes y/o partes interesadas de la entidad.

En la siguiente figura se pueden observar a gran escala los procesos que deben llevarse a cabo para la implementación de la firma electrónica por cada uno de los departamentos de interes.

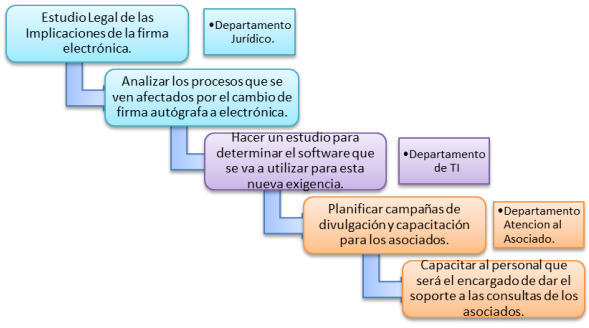


Fig. 3. Procesos a realizar para la implementación de la firma electrónica

*A. Departamento Jurídico*

Como primer paso para la implementación de la firma electrónica, el departamento jurídico debe comenzar por analizar a profundidad el contenido de la Ley de Firma Electrónica, así como su reglamento, de tal manera que se pueda determinar el actuar jurídico correcto por el cual debe optar la entidad, y ver como se ve involucrada la firma electrónica con otras leyes o bien cómo afectan los procesos legales que son llevados a cabo actualmente.

Posterior a la revisión exhaustiva de la ley, se deben de analizar uno a uno los principales procesos de la entidad desde el enfoque de su marco de acción jurídico, para poder determinar en cuáles de ellos se sustituirá la firma autógrafa por la electrónica, y en cuál de ellos puede ser necesario que los asociados/clientes sigan utilizando su firma autógrafa. Esta actividad de preferencia debe ser realizada en conjunto con el departamento de atención al asociado, ya que son ellos los que mejor conocen toda la operatividad actual que se realiza con los asociados.

*B. Departamento de TI*

Una vez que el departamento jurídico y de atención al asociado, determinen las modificaciones a los procesos y estos sean avalados por la junta directiva de la cooperativa, se deben presentar los requerimientos del software y hardware necesarios para la correcta implementación y uso de esta nueva tecnología. El departamento de TI debe ser el encargado de recopilar y registrar dichos requerimientos para poder solventarlos a la brevedad posible.

Primero que nada, debe comenzar por analizar el nivel de impacto que estos implican, de tal forma que puedan determinar por cuál de las opciones se van a inclinar, lo cual debe ser debidamente avalado por la junta directiva. Las opciones que el departamento de TI debe considerar son: desarrollar el software, es decir utilizar su propio software hecho a la medida de las necesidades y en casa, o bien, comprar un software de terceros a alguna empresa que ya tenga experiencia con este tema.

Si el software va a ser desarrollado por la cooperativa, el primer paso debe ser definir (si es que no lo está) con los departamentos a cargo de cada proceso clave de la cooperativa, cuál es la información más importante almacenada (la más sensible), es decir la que se debe y desea proteger prioritariamente, la cual debería ser parte del certificado del asociado, permitiendo realizar de forma adecuada y exitosa el procedimiento de verificación de firma.

De igual forma debe evaluarse la forma de almacenamiento del certificado digital de cada uno de los asociados, de manera que se determine si se tendrá un servidor dedicado para esto utilizando algún tipo de mecanismo de cifrado para su protección, o bien almacenado como un atributo más a una tabla siempre con un mecanismo para su correcto y seguro resguardo.

El Project Manager o el Gerente del Departamento de TI debe realizar la estimación de tiempo para el desarrollo de esta nueva necesidad, contemplando tanto los recursos materiales como humanos de los que dispone y los requeridos para llevar a cabo el proyecto, contemplando también que es necesario impartir capacitaciones al personal de las distintas áreas de la entidad, las cuales deberán abarcar tanto el marco legal que ampara la firma electrónica como las nuevas tecnologías que permitirán su correcta utilización dentro de la operatividad normal.

Es importante mencionar que dichas capacitaciones no son solo para las áreas operativas y administrativas, sino también para el departamento de TI, pues como desarrolladores de software deben ser conscientes que algún tipo de error de desarrollo puede involucrar procesos legales costosos para la entidad.

Para la estimación de tiempo se deben tener en cuenta que el software debe permitir la incorporación del uso de funciones picadillo (hash y métodos criptográficos que utilicen llaves públicas y privadas.

En conjunto con esto, es importante que se analice la compatibilidad de los sistemas actuales utilizados dentro de la entidad en cuanto a la incorporación de estas nuevas herramientas para firma electrónica, verificando el grado de dificultad que se presentaría a la hora de implementarlas.

Si se llega a dar el caso en que desarrollar el software sea algo demasiado complejo para la cooperativa y/o requiera mucho esfuerzo, tiempos y/o recursos; debe evaluarse la opción de comprar el software a un tercero, para ello debería buscarse de preferencia en países que ya cuenten con la implementación de firma electrónica.

Para esta opción es de alta importancia establecer comparativas entre el marco legal vigente del país en cuestión con el de El Salvador, de tal forma que debe buscarse una opción de software con países en los que el marco legal sea parecido al de El Salvador, así los ajustes que se necesitarían para su adaptación a la entidad serian mínimos o por lo menos no requerirían tanta dedicación.

De igual forma el departamento de TI debe recibir capacitación de la empresa a la que se le compre el software, de preferencia también el código fuente o negociar un contrato de soporte en el caso que este no esté incluido en la compra del software, de tal forma que el departamento de TI esté preparado ante cualquier emergencia o incidente para poder capacitar y dar soporte a los otros departamentos que lo requieran.

*C. Departamento de Atención al Asociado.*

El personal del departamento de TI capacitará a una parte del equipo del departamento de atención al asociado para que los capacitados sean los encargados de retransmitir el conocimiento a todos los que se verán involucrados en la utilización del nuevo software.

De igual manera se debe de crear junto con el departamento correspondiente una campaña de difusión masiva para los asociados de tal manera que sean informados de los pasos que deben seguir para hacer el cambio de firma autógrafa a firma electrónica, anunciar que las plataformas y procesos van a cambiar y cuáles son los cambios que estas sufrirán.

Adicionalmente se debe de hacer énfasis las ventajas de seguridad que brinda la utilización de firma electrónica, ya que

suele darse la desconfianza o escepticismo principalmente por los usuarios de mayor edad, en cuanto al uso de tecnología, más para este caso tan delicado como lo es la firma autógrafa, que es un mecanismo de aceptación de acuerdo legales entre otros ámbitos.

## V. Conclusiones.

Al analizar detenidamente todo lo relacionado con firma electrónica, podemos destacar los siguientes puntos:

- El país necesita determinar las entidades responsables de velar por que se cumplan las regulaciones dictadas en la Ley de Firma Electrónica y los recursos necesarios para su correcto resguardo, generación, verificación y utilización.
- Se necesita revisar el marco legal en torno a la firma electrónica, es decir, verificar si dicha ley no choca con otras dictadas anteriormente, como por ejemplo aquellas que tiene que ver con el ejercicio notarial.
- Se necesita, como es de esperar al inculcar una nueva tecnología, de capacitaciones que vayan dirigidas a todas las partes involucradas en este proyecto, tanto a nivel país como a nivel institución.
- Las instituciones que opten por hacer uso de esta tecnología, deben realizar un estudio a sus sistemas y procesos operativos internos, con el fin de determinar si esta proporcionara beneficios suficientes hacia sus partes interesadas.

## Referencias.


[1] Ley de Firma Electrónica [en línea]. Diario Oficial, San Salvador, El Salvador, 2015. Disponible en: https://www.transparencia.gob.sv/institutions/dc/documents/255011/download David Salomon, Giovanni Motta, David Bryant (2007), “Data Compression. The Complete Reference”

[2] IBM Knowledge Center. Infraestructura de claves públicas (PKI) [en línea] [fecha consulta: 3 de septiembre 2019]. Disponible en: https://www.ibm.com/support/knowledgecenter/es/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009900_.htm.

[3] Certificados digitales. Center [en línea] [fecha consulta: 4 de septiembre 2019]. Disponible en: https://publib.boulder.ibm.com/tividd/td/TRM/SC23-4822-00/es_ES/HTML/user276.htmG. Caso, Natalia, “SCRUM development process”, Universidad Tecnológica Nacional de Buenos Aires. Septiembre 2004.

[4] Portal Electrónico de la Unidad de Firma Electrónica: Preguntas [en línea] [fecha consulta: 7 de septiembre 2019]. disponible en: http://firmaelectronica.minec.gob.sv/about/faqs/