UNIVERSIDAD DON BOSCO

VICERRECTORÍA DE ESTUDIOS DE POSTGRADO

TRABAJO DE GRADUACIÓN

PROPUESTA DE CREACIÓN DE UNA AUTORIDAD CERTIFICADORA PARA LA EMISIÓN DE FIRMAS ELECTRÓNICAS CERTIFICADAS EN EL SALVADOR

PARA OPTAR AL GRADO DE

MAESTRO EN SEGURIDAD Y GESTIÓN DE RIESGOS INFORMÁTICOS

ASESORA:

DOCTORA MARÍA DE LOURDES LÓPEZ GARCÍA

PRESENTADO POR:

ALDO JOSÉ GUILLERMO QUIJANO

JAIME ERNESTO ERAZO BELTRÁN

Antiguo Cuscatlán, La Libertad, El Salvador, Centroamérica

Agosto de 2016

Propuesta de creación de una Autoridad Certificadora para la emisión de firmas electrónicas certificadas en El Salvador

Quijano Aldo José Guillermo, Erazo Beltrán Jaime Ernesto
UNIVERSIDAD DON BOSCO
ANTIGUO CUSCATLAN, EL SALVADOR
aldojq@gmail.com
jaimin84@gmail.com

Resumen— En la actualidad una de las medidas importantes en temas de la seguridad informática son las Firmas Digitales. A nivel internacional, dichas firmas están tomando un papel fundamental en los accesos a la información, debido a la vulnerabilidad que pueda existir en el entorno informático.

En El Salvador existe la Ley de Firma Electrónica, la cual comprende la necesidad de creación de una Autoridad Certificadora que bajo norma pueda cumplir con los requisitos adecuados para darle la seguridad que ameritan las Firmas Digitales. En la búsqueda de la formación de dicha entidad, se plantea la siguiente investigación para facilitar la información necesaria en la creación y ejecución de las operaciones de una Autoridad Certificadora y cómo ésta debe llevarse a cabo.

La presente investigación se basa en el marco legal que plantea la Ley de Firma Electrónica en El Salvador, por lo que, en este documento se hace mención a todos los puntos relevantes e importantes de esta ley.

Índice de Términos—Firma Digital, Confidencialidad, Disponibilidad, Integridad, Autoridad Certificadora, llaves públicas, llaves privadas, CRL, SSL.

I. INTRODUCCIÓN

Hoy en día, se busca manejar la información de la manera más eficiente posible, disminuyendo los tiempos de respuesta de los procesos en las empresas, es por esto que, los cambios tecnológicos conllevan a que la información que se maneja de forma digital, garantice los principios de autenticidad, integridad, confidencialidad y no repudio de los datos.

Un ejemplo de ello es la firma electrónica o digital, la cual, es una herramienta criptográfica que acopla una entidad con un mensaje a través de funciones matemáticas que garantizan esa unión.

Es importante mencionar, que la firma digital usa un par de llaves: una privada y una pública. La primera, la conoce sólo el dueño de la misma y es fundamental para la generación de la firma; la segunda, es conocida por todos y su participación es en la verificación de la firma. Ambas llaves están asociadas, es por ello que la generación y la verificación son procedimientos funcionales. Sin embargo, es muy sencillo usurpar la llave pública y como consecuencia validar exitosamente una firma falsa. Afortunadamente, los certificados digitales son herramientas que vinculan una persona o entidad con una llave pública, evitando así el ataque de usurpación.

En la actualidad, en El Salvador se cuenta con una Ley de Firma Electrónica, donde el objetivo es acompañar los esfuerzos de modernización e innovación que encaminan a la sociedad en general hacia una transición sana e inclusiva a la sociedad del conocimiento. La aprobación de la ley en mención, otorga el valor a la firma electrónica certificada a toda información en formato electrónico que se encuentre suscrita con ésta.

Por lo antes expuesto, el propósito de esta investigación es elaborar una propuesta de diseño para la creación de una autoridad certificadora que emita certificados digitales, y que garantice la validez legal y fiscal de la firma electrónica en El Salvador.

De tal manera que la Autoridad Certificadora pueda realizar funciones de renovación, publicación, almacenamiento y registro de certificados, así como la seguridad de los canales de

comunicación de los certificados digitales, la investigación sobre fraudes, la falsificación de identidades o errores por falta de controles en la ley estipulada e investigación sobre la existencia de sistemas de revocación que permitan verificar la vinculación de llaves, entre otros.

Cabe aclarar que dentro de la Ley se encuentra considerado todo lo relativo a los proveedores de servicios de certificación, por lo que en esta investigación se propone un diseño para la creación de una autoridad certificadora que emita certificados digitales, y que se encuentren dentro del marco legal del país.

El resto del documento está organizado de la siguiente manera: En la sección 2, se presenta el marco legal de la firma electrónica en El Salvador, donde se describen los artículos principales de la Ley y la institucionalidad de la Firma Electrónica. En la sección 3, se describe a detalle sobre Las Firmas Digitales, el uso de la firma electrónica, teoría sobre el algoritmo Hash y el significado de un certificado digital. Se menciona, en la sección 4, información relacionada con la Infraestructura PKI, funcionamiento, componentes de la llave pública, contenido y creación de un certificado digital. En la sección 5 se presenta la propuesta de la Autoridad Certificadora, según la Ley de Firma Electrónica de El Salvador, considerando: la acreditación de una Autoridad Certificadora, obligaciones de los proveedores y un esquema del proceso propuesto para la Autoridad Certificadora. Por último, se presentan las conclusiones en la sección VI.

II. FUNDAMENTACIÓN LEGAL

La normativa en la que se basa esta investigación, es en la Ley de Firma Electrónica, aprobada en El Salvador en el año 2015, la cual establece la vinculación de un mensaje de datos con su titular de manera exclusiva, permite la verificación inequívoca de la autoría e identidad, y asegura que los datos estén bajo control exclusivo del dueño.

La Firma Electrónica es un método que asocia la identidad de una persona, con un mensaje o documento electrónico, para asegurar la autoría y la integridad del mismo.

La importancia de fomentar la Ley de Firma Electrónica radica en la rápida, creciente y efectiva utilización de la tecnología para las relaciones entre los diversos actores de la sociedad, para fomentar un clima de negocios ágil y seguro para las inversiones tanto locales como internacionales.

El objetivo de esta Ley es el de verificar la firma electrónica simple y firma electrónica certificada con la firma autógrafa, además, otorgar y reconocer el valor jurídico a la firma electrónica certificada, a toda información en formato electrónico que se encuentren suscritos con una firma electrónica certificada, independientemente de su soporte material; así como también, regular lo relativo a los proveedores de servicios de certificación y a los proveedores de servicios de almacenamiento de documentos electrónicos.

A. Principales artículos de la Ley de Firma Electrónica.

Los artículos de mayor interés, se mencionan a continuación [1]:

Art. 8.

- Los documentos en soporte electrónico utilizando firma electrónica tendrán el mismo valor que los consignados de manera tradicional. Quedan exentos aquellos documentos o actos jurídicos que para su perfeccionamiento requieren formalidades y solemnidades especiales.

Art. 35.

- Créase la Unidad de Firma Electrónica, como parte del Ministerio de Economía. El Ministro nombrará al funcionario que estará a cargo de esta Unidad.

Art. 44.

- El servicio de certificación sólo podrá ser prestado por aquellas personas jurídicas, públicas o privadas, nacionales o extranjeras, que cumplan con los requisitos establecidos en las leyes competentes para operar en el país.

Las instituciones oficiales autónomas y demás instituciones públicas con personalidad jurídica propia, establecidas conforme a las leyes de la República de El Salvador, quedan facultadas para prestar los servicios regulados por esta Ley. Dichas instituciones deberán cumplir los requisitos establecidos en el presente artículo para ser acreditadas.

B. Institucionalidad de la firma electrónica.

En la figura 1 se muestra la institucionalidad de la firma electrónica, la cual se compone de tres grandes grupos:

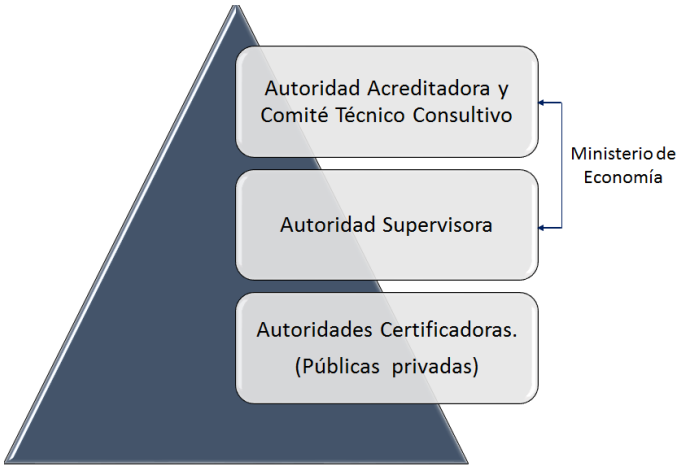

Fig. 1. Institucionalidad de la Firma Electrónica [1].

Según [1], los principales roles que pueden tomar las autoridades son:

- Acreditadora:

Otorgar, registrar o revocar la acreditación otorgada a prestadores de servicios de firma electrónica o de almacenamiento de documentos electrónicos; validar los certificados electrónicos emitidos a favor de los proveedores de servicios de certificación y de almacenamiento de documentos electrónicos; elaborar las normas, los reglamentos técnicos que sean necesarios para la implementación de la ley.

- Supervisora:

Supervisar, verificar e inspeccionar a certificadores y prestadores de servicios de almacenamiento de documentos electrónicos, a fin de que éstos cumplan con los requisitos contenidos en la presente ley, su reglamento, así como las normas y reglamentos técnicos aplicables; instruir de oficio o a instancia de parte, sustanciar y decidir los procedimientos administrativos relativos a presuntas infracciones a esta Ley; realizar, directamente o por contratación, auditorías de los proveedores de servicios de certificación y a los prestadores de servicios de almacenamiento.

- Certificadora:

Contar con suficiente capacidad técnica para garantizar la seguridad, la calidad y la fiabilidad de los certificados emitidos, de conformidad a los requerimientos contenidos en las normas técnicas; contar con el personal técnico adecuado, con conocimiento especializado y experiencia en el servicio; poseer la capacidad económica y financiera suficiente para prestar los servicios autorizados; rendir fianza por un monto adecuado al riesgo asumido para prestar los servicios de certificación.

Cabe mencionar que esta Ley, toma como modelo la normativa internacional, y la clasifica en dos partes: la firma simple y la certificada. Esta última tendrá valor probatorio y designa una entidad competente como el Ministerio de Economía que garantice la seguridad requerida y que no sea falsificada por nadie, como lo menciona el artículo 3 sobre los proveedores de servicios de almacenamiento de documentos electrónicos.

Además, para validar la firma electrónica el artículo 6 establece que la firma electrónica simple tendrá la misma validez jurídica que la autógrafa, mas no validez probatoria: "La firma electrónica simple no tendrá validez probatoria en los mismos términos a los concedidos por esta ley a la firma electrónica certificada".

La Legislación en Firma Electrónica es un reconocimiento al Artículo 2 de la Constitución de la República, el cual establece “el derecho a la seguridad jurídica de toda persona, por lo que el Estado debe crear un marco legal que brinde seguridad a los usuarios de las comunicaciones electrónicas, y a las transacciones autorizadas mediante las aplicaciones de la tecnología o la suscripción electrónica de las mismas, brindándole validez jurídica”.

En resumen, la aprobación de esta ley, ayudará a facilitar las transacciones internacionales de importación y exportación, además facilitará la movilidad, puesto que los usuarios podrán realizar sus trámites desde cualquier lugar al tener registrada la firma electrónica.

III. FIRMAS DIGITALES

Una firma digital se usa para autenticar información digital utilizando un cifrado computacional [8].

Las firmas digitales ayudan a garantizar lo siguiente:

- Autenticidad: La firma digital ayuda a asegurar que el firmante es quién dice ser.
- Integridad: La firma digital ayuda a asegurar que el contenido no se ha cambiado ni manipulado desde que fue firmado digitalmente.
- Sin rechazo: La firma digital ayuda a demostrar el origen del contenido firmado a todas las partes. "Rechazo" se refiere al acto de denegar un firmante cualquier asociación con el contenido firmado.

A. Firma Electrónica

La Firma Electrónica es un método que asocia la identidad de una persona, con un mensaje o documento electrónico, para asegurar la autoría y la integridad del mismo. La firma electrónica se divide en dos:

- **Firma electrónica Simple**

Son mensajes de datos que pueden ser utilizados para identificar a la persona que firma en relación con el mensaje de datos, e indicar que el firmante ha aprobado la información que se encuentra recogida en dicho mensaje de datos.

- **Firma electrónica Certificada**

Son mensajes de datos que permiten la identificación de la persona que firma y que los datos de creación de la firma se encuentran en exclusivo control del signatario, lo que permite garantizar que cualquier modificación al contenido del mensaje de datos sea detectable.

Es decir, que un documento redactado en un procesador de textos u otros documentos electrónicos, firmado con “Firma Electrónica Certificada”, es equivalente a un documento impreso con firma manuscrita.

La firma electrónica no puede ser generada más que por el emisor del documento, a excepción de aquellos casos donde la ley permite que la firma electrónica de una persona jurídica o natural esté a la custodia de otra persona, y así sea expresado en el certificado digital. Además, el beneficio de utilizar la firma digital es que permite transacciones en tiempo real sin necesidad de la presencia de las partes involucradas y facilita la eficiencia, automatización de los procesos y la reducción de costos para las empresas.

B. Uso de la firma electrónica

En la figura 2, se observa el proceso que se utiliza para la implementación de la firma electrónica, en donde se deben tener en cuenta los siguientes puntos:

1. El contenido del documento electrónico puede ser correo electrónico, transacción bancaria, imagen, audio, video, entre otros; los que son codificados de forma digital.

2. Garantizar la integridad y la inalterabilidad de los documentos ya firmados con la firma electrónica certificada. Lo anterior se realiza con la función hash que selecciona los datos de un mensaje digital por medio de un conjunto de códigos de la siguiente forma: el emisor del documento aplica una función

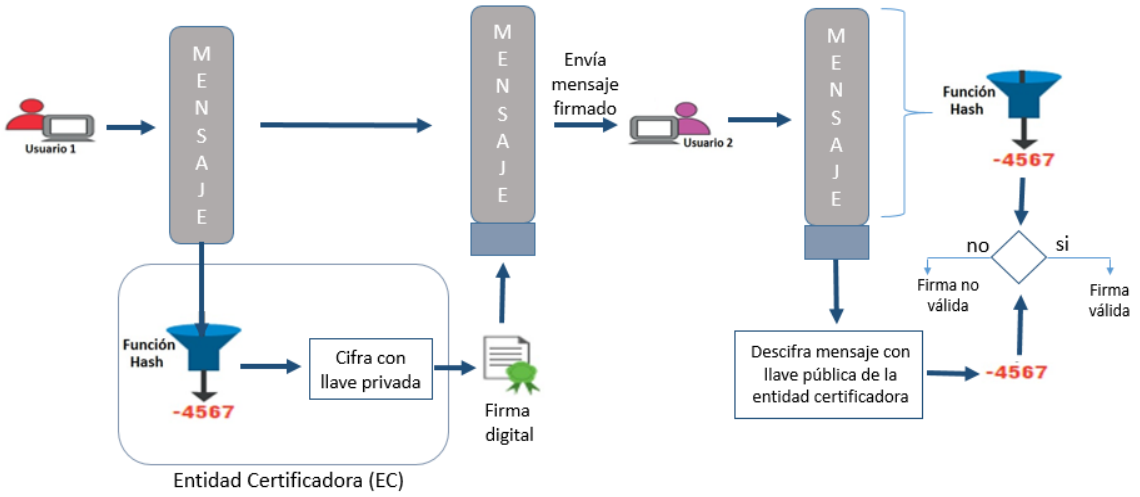

Fig. 2. Uso de la firma electrónica [9].

hash obteniendo un número finito, que es el resumen del documento, el cual se cifra en una llave privada de la firma electrónica certificada, luego el emisor envía al receptor el documento electrónico cifrado y el receptor aplica la función hash al resumen sin cifrar y descifrar.

3. El documento electrónico es cifrado por medio de la llave privada, con lo que no existe posibilidad de obtener dos llaves privadas iguales, y el resultado del proceso de cifrar el documento electrónico es la firma digital, que es enviada junto al mensaje original. La llave privada es de uso exclusivo del firmante, y puede ser guardada en dispositivos electrónicos (Memorias USB, archivos electrónicos, etc.).

4. La llave pública se utiliza para verificar la identidad de quien posea un certificado digital o para verificar la integridad de un documento firmado digitalmente. La llave pública es de uso general, y son publicadas en la web por los proveedores de certificados.

5. Los certificados digitales son documentos digitales donde el proveedor de servicios de certificación garantiza la vinculación entre la identidad de un individuo o entidad, y una llave pública; como se muestra en la figura 3. La existencia de firmas en los certificados asegura por parte del proveedor de servicios de certificación, quien es el firmante del certificado, que la información de identidad y la llave pública perteneciente al usuario o entidad referida en el certificado digital están vinculadas. Para cumplir la función de identificación y autenticación, el certificado necesita del uso de la llave privada (que sólo el titular conoce).

Los componentes principales de un certificado digital son: titular, una llave pública, emisor, y período de validez.

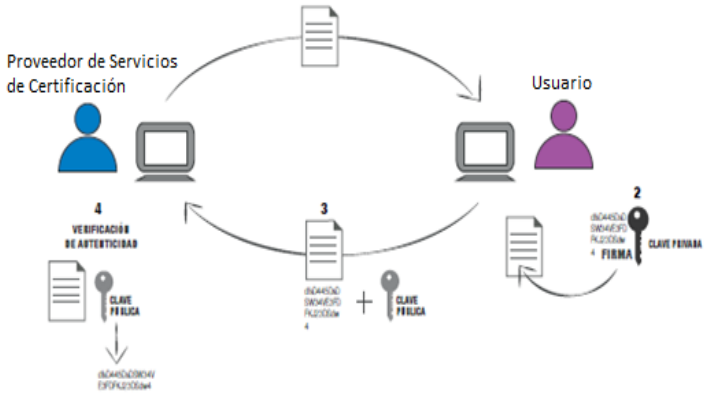

Fig. 3. Certificación de firma digital [9].

Al estudiar sobre la firma electrónica, es importante conocer la función de la infraestructura de llave pública, ya que es la plataforma de gestión de los certificados digitales y que ayudan al mecanismo tanto de la autenticación, como de la firma electrónica como tal. Esta infraestructura utiliza algoritmos criptográficos para que los certificados digitales sean seguros en el mecanismo de autenticación y de esta forma logren garantizar el control de accesos seguros por los medios electrónicos y el no repudio de las transacciones.

C. Función Hash

La función hash $H:\{0,1\}^* \rightarrow \{0,1\}^n$ es una función que tiene como parámetro de entrada una cadena de longitud arbitraria y arroja como resultado una cadena de longitud fija *n*, el resultado de la aplicación de H sobre *x* es conocido como digesto o picadillo [2].

Es decir, que las funciones hash o picadillo son algoritmos que, teniendo una entrada ya sea texto, contraseña o archivo, consiguen crear una salida alfanumérica de longitud fija que representa un resumen de esa información, la cual solamente puede volverse a crear con esos mismos datos.

Cabe mencionar que los sistemas de llave pública son muy lentos [3]; es por eso que, en lugar de firmar digitalmente el mensaje completo, en un sistema criptográfico se incluirá como firma digital una operación con la llave privada sobre un resumen o hash de dicho mensaje representado por una centena de bits.

Además, algunos de los propósitos de las funciones hash son:

- Asegurar que no se ha modificado ningún archivo en una transmisión.
- Hacer ilegible una contraseña.
- Firmar digitalmente un documento.

En la figura 4 se puede observar un ejemplo detallado de la función hash:

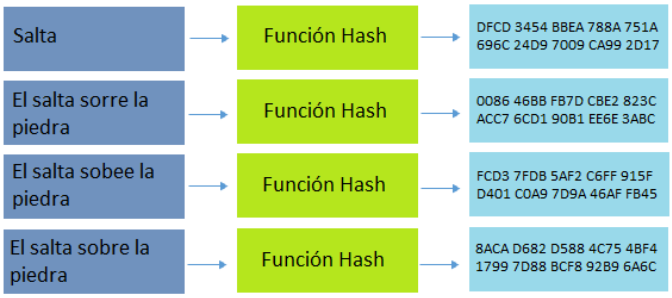

Fig. 4. Funcionamiento de la función hash.
Fuente: Elaboración Propia

- Propiedades de la *Función Hash* [3].

- Unidireccionalidad: conocido un resumen *h(M)*, debe ser computacionalmente imposible encontrar M a partir de dicho resumen.
- Compresión. A partir de un mensaje de cualquier longitud, el resumen *h(M)* debe tener una longitud fija. Lo normal es que la longitud de *h(M)* sea menor.
- Facilidad de cálculo. Debe ser fácil calcular h(M) a partir de un mensaje M.
- Difusión. El resumen h(M) debe ser una función compleja de todos los bits del mensaje M. Si se modifica un bit del mensaje M, el hash h(M) debería cambiar aproximadamente en la mitad de sus bits.
- Colusión simple. Conocido M, será computacionalmente imposible encontrar otro M' tal que h(M) = h(M'). Se conoce como resistencia débil a las colisiones.
- Colisión fuerte. Será computacionalmente difícil encontrar un par (M, M') de forma que h(M) = h(M'). Se conoce como resistencia fuerte a las colisiones.

D. Certificado Digital

Según [4], un certificado digital es un documento firmado digitalmente por una persona o entidad denominada autoridad certificadora. Dicho documento establece un vínculo entre un sujeto y su llave pública, es decir, el certificado digital es un documento firmado por una autoridad certificadora, que contiene el nombre del sujeto y su llave pública. La idea es que quienquiera que conozca la llave pública de la Autoridad Certificadora, puede autentificar un certificado digital de la misma forma que se autentifica cualquier otro documento firmado.

Si el certificado es auténtico y la Autoridad Certificadora es confiable, entonces, se determina que el sujeto identificado en el certificado digital posee la llave pública que se señala en dicho certificado. Es decir que, si un sujeto firma un documento y anexa su certificado digital, cualquiera que conozca la llave pública de la Autoridad

Certificadora podrá autentificar el documento.

Los certificados digitales pueden estar en un soporte físico y electrónico, o ser un archivo contenido en una computadora. Posee dos partes, una privada y una pública.

IV. INFRAESTRUCTURA PKI

Una infraestructura de llave pública (PKI) es un sistema de certificados digitales, entidades de certificación y autoridades de registro que comprueban y autentican la validez de cada entidad implicada en una transacción electrónica mediante el uso de la criptografía de llave pública.

A. Componentes de la PKI

Los principales componentes de la infraestructura de llave pública son:

- La autoridad certificadora, que se encarga de crear el certificado solicitado después de verificar la identidad del usuario.
- Certificado digital, es una prueba de que existe vinculación entre el usuario y su llave pública.
- Punto de publicación de certificados (*CPP – Certificate Publication Point*), que es el lugar donde la autoridad certificadora deposita los certificados que fueron solicitados y otorgados.
- Lista de certificados revocados (*CRL – Certificate Revocation List*). Los certificados pueden ser revocados antes de su vencimiento, por varias razones: que se haya comprometido la llave privada, lo que implica generar un nuevo par de llaves e invalidaría la llave pública contenida en el certificado digital; que el usuario olvide la frase que le permite obtener la llave privada, acción que requiere la renovación del par de llaves, etc.
- Aplicaciones para manejo de certificados, son necesarios para poder solicitar, otorgar o instalar los certificados. La petición puede hacerse en línea o fuera de línea. En el primer caso, la comunicación con la Autoridad Certificadora es constante ya que cada vez que se requiera el certificado de una entidad, se hace una comunicación inmediata con la misma. En el segundo caso, la Autoridad Certificadora entrega el certificado al usuario, y éste a su vez, entrega el certificado a toda entidad que desee verificar su firma, de tal manera que no es necesario la comunicación en tiempo real con la autoridad certificadora.

B. Funcionamiento de PKI

El componente principal de la infraestructura de llave pública es el certificado, ya que verifica la correspondencia entre una entidad y su respectiva llave pública.

Para que el certificado sea válido, debe estar firmado digitalmente por la autoridad certificadora emisora; además, conociendo la llave pública de la autoridad certificadora se verifica que la firma digital es legítima, la cual debe estar certificada por otra autoridad certificadora que, a su vez, esté certificada (tipo raíz) y que valida que la firma es legal; así como se muestra en la figura 5.

Para una mejor comprensión, se ilustra el procedimiento con el siguiente ejemplo:

- Existen dos usuarios: A y B; y una autoridad Certificadora. que es de tipo raíz y por lo tanto se otorga un certificado a sí misma.
- El usuario A debe primero instalar el certificado de la Autoridad Certificadora. Esto es, que va a confiar en todos los certificados otorgados por esta Autoridad Certificadora.
- Luego A solicita un certificado para sí mismo, cumpliendo con las condiciones que exige la Autoridad Certificadora para otorgar los certificados.
- Suponiendo que la Autoridad Certificadora otorga su certificado procede a instalarlo.

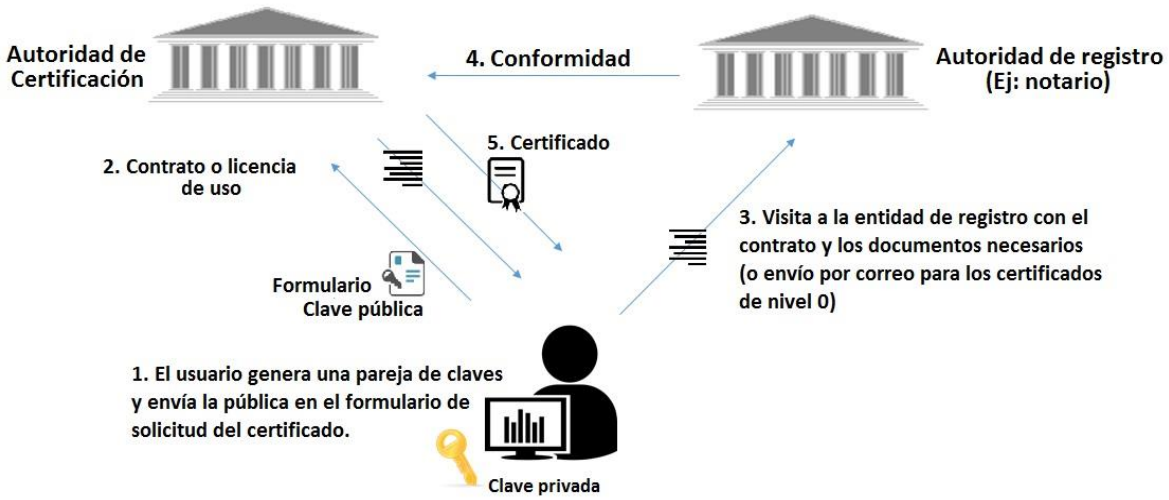

Fig. 5. Funcionamiento de la estructura de llave pública [12].

- El usuario B procede de la misma forma: instala el certificado de la Autoridad Certificadora, solicita un certificado para sí mismo, que es otorgado e instalado. Hasta este momento tenemos tres certificados: el de la Autoridad Certificadora, el de A y el de B. Cada usuario tiene instalado el de la Autoridad Certificadora y el propio.
- Si A envía un mensaje a B, firmado digitalmente, esto es, cifrando el hash con su llave privada, debe enviarle también su llave pública. Y esto lo hace adjuntando su propio certificado, que contiene la llave pública.
- Cuando B recibe el mensaje, obtiene del certificado la llave pública que le permite verificar la firma digital. Si B agrega a A, a su lista de contactos, además está instalando el certificado de A.
- Luego B debe proceder igual que A, enviando un mensaje firmado digitalmente, con lo cual A, procediendo en forma análoga, instala el certificado de B
- Partiendo de que A y B poseen tanto su propio par de llaves, como la pública del otro, pueden intercambiar mensajes cifrados y firmados entre ellos.

C. Contenido del Certificado

El certificado digital posee formatos estándares reconocidos internacionalmente. El contenido de un certificado incluye los siguientes campos:

- Nombre del titular
- Identificación del titular del certificado electrónico, indicando su domicilio y dirección electrónica.
- Identificación del proveedor de servicios de certificación que proporciona el certificado electrónico, indicando su domicilio y dirección electrónica.
- Fecha de la acreditación y caducidad asignada al proveedor de servicios de certificación por la Unidad de Firma Electrónica.
- Fecha de emisión y expiración del certificado.
- Número de serie o de identificación del certificado.
- La firma electrónica certificada del prestador de servicios de certificación que emitió el certificado.
- Datos de verificación de la firma, los cuales deben corresponder a la información de su creación y que están bajo el control del

firmante.

- Cualquier información relativa a las limitaciones de uso, vigencia y responsabilidad a las que esté sometido el certificado electrónico.
- Indicación de la ruta de certificación.
- Si el certificado ha sido emitido por una persona que ha actuado en representación de una persona natural o jurídica; en tal caso, el certificado deberá incluir una indicación del documento legal, público, o privado autenticado, que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona física o jurídica a la que representa.

D. Autoridades certificadoras

Las Autoridades certificadoras, son entidades que garantizan la autenticidad y veracidad de los datos recogidos en el certificado digital expedido.

El procedimiento de la Autoridad de Certificación se realiza haciendo uso de una llave privada que garantiza la identidad del propietario del certificado digital. Esto provoca la posibilidad de firmar electrónicamente los certificados emitidos.

Además, la Autoridad de Certificación ofrece el servicio de verificación de validez de los certificados, ya que éstos pueden ser revocados, ya sea porque se vulneró la llave privada por parte del usuario o por que la llave privada expiró.

El certificado de la última Autoridad de Certificación es avalado, para asegurar su autenticidad, mediante su instalación en un almacén de certificados del propio servidor, que luego usarán los navegadores. Así, se descarga el certificado raíz de la Autoridad de Certificación desde su sitio Web, ofreciendo confianza en la seguridad que ofrece su propia página.

- *Servicios de una Autoridad Certificadora*

Según la Ley de Firma Electrónica de El Salvador [1], los servicios que debe de tener una Autoridad Certificadora son:

- Contar con suficiente capacidad técnica para garantizar la seguridad, la calidad y la fiabilidad de los certificados emitidos, de conformidad a los requerimientos contenidos en las normas técnicas;
- Contar con el personal técnico adecuado con conocimiento especializado comprobable en la materia y experiencia en el servicio a prestar.
- Poseer la capacidad económica y financiera suficiente para prestar los servicios autorizados como proveedor de servicios de certificación. La capacidad antes mencionada es medida, no sólo por los equipos, insumos, licencias y otros bienes con los que cuente el proveedor de servicios de certificación para prestar sus servicios, sino también por el capital de trabajo con el que funcionará. Esta constatación la realizará la Unidad de Firma Electrónica, mediante las auditorías y estudios que considere conveniente, y se revisará durante el tiempo de funcionamiento del proveedor.
- Rendir fianza por un monto adecuado al riesgo asumido por la prestación de los servicios de certificación, el que se calculará conforme a los requerimientos definidos en el reglamento de la Ley de Firma Electrónica. Esta fianza será utilizada para indemnizar los daños y perjuicios que se ocasionasen a los usuarios de los servicios de certificación. La fianza será revisada anualmente tomando en cuenta los cambios en el nivel de riesgo asumido por el proveedor de servicios de certificación.
- Contar con un sistema de información de alta disponibilidad, actualizado y eficiente, en el cual se publiquen las políticas y procedimientos aplicados para la prestación de sus servicios, así como de los certificados electrónicos que hubiere proporcionado, revocado, suspendido o cancelado y las restricciones o limitaciones aplicables a éstos.

- *Revocación de certificados*

Revocar un certificado es anular su validez antes

de la fecha de caducidad que consta en el mismo. La revocación puede ser solicitada en cualquier momento, y en especial, cuando el titular crea que sus llaves privadas han sido vulneradas, extraviadas u olvidadas.

Cuando una Autoridad Certificadora emite un certificado digital, lo hace con un periodo máximo de validez que oscila entre tres y cinco años. El objetivo de este periodo de caducidad es obligar a la renovación del certificado para adaptarlo a los cambios tecnológicos. Así se disminuye el riesgo de que el certificado quede comprometido por un avance tecnológico. La fecha de caducidad viene indicada en el propio certificado digital.

Sin embargo, existen otras situaciones que pueden invalidar el certificado digital aun cuando no ha caducado, de manera inesperada:

- El usuario del certificado cree que su llave privada ha sido robada.
- Desaparece la condición por la que el certificado fue expedido. Por ejemplo, el cambio de apoderado de una entidad jurídica.
- El certificado contiene información errónea o información que ha cambiado. Por ejemplo, una errata en los apellidos.
- Una orden judicial.

Por tanto, debe existir algún mecanismo para comprobar la validez de un certificado antes de su caducidad, para ello, las listas de Revocación de Certificados (CRL – Certificate Revocation List) son uno de estos mecanismos.

Las listas de revocación son archivos que contienen la lista con los números de serie de los certificados que han sido revocados, para efectos de la validación del estado del certificado.

- *Propiedades y obligaciones de una autoridad certificadora.*

En la actualidad, las Autoridades de Certificación se someten a leyes y reglamentos que plantean serios retos operativos, además de normas y estándares que les hacen asumir importantes responsabilidades.

Según la Ley de Firma Electrónica en El Salvador [1], las propiedades y obligaciones que debe de tener una autoridad certificadora se detallan a continuación:

Propiedades:

- Contar con suficiente capacidad técnica para garantizar la seguridad, la calidad y la fiabilidad de los certificados emitidos, de conformidad a los requerimientos contenidos en las normas técnicas.
- Contar con el personal técnico adecuado, con conocimiento especializado y experiencia en el servicio.
- Poseer la capacidad económica y financiera suficiente para prestar los servicios autorizados; rendir fianza por un monto adecuado al riesgo asumido para prestar los servicios de certificación.

Obligaciones:

- Adoptar las medidas necesarias para determinar la exactitud de los certificados electrónicos que proporcionen, la identidad y la calidad del signatario.
- Garantizar la validez, vigencia, legalidad y seguridad del certificado electrónico que proporcione.
- Garantizar la adopción de las medidas necesarias para evitar la falsificación de certificados electrónicos y de las firmas electrónicas certificadas que proporcionen.
- Verificar la información suministrada por el signatario.
- Crear y mantener un archivo actualizado de los certificados emitidos en medios electrónicos, para su consulta por plazo indefinido.
- Garantizar a los usuarios los mecanismos necesarios para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

- Sin perjuicio de otras obligaciones establecidas en la Ley de Protección al Consumidor, deberá informar a los interesados de sus servicios de certificación, utilizando un lenguaje comprensible, a través de su sitio de internet y a través de cualquier otra forma de acceso público, los términos precisos y condiciones para el uso del certificado electrónico y, en particular, de cualquier limitación sobre su responsabilidad, así como de los procedimientos especiales existentes para resolver cualquier controversia.
- Garantizar la autenticidad, integridad y confidencialidad de la información, y documentos relacionados con los servicios que proporcione. A tales efectos, deberán mantener un sistema de seguridad informática y respaldos confiables y seguros de dicha información, de conformidad a lo establecido en la Ley de Firma Electrónica, su reglamento, y normas y reglamentos técnicos.
- Efectuar las notificaciones para informar a los signatarios y personas interesadas y las publicaciones necesarias, acerca del vencimiento, revocación, suspensión o cancelación de los certificados electrónicos que proporcione, así como de cualquier otro aspecto de relevancia para el público en general, en relación con los mismos.
- Dar aviso a la Fiscalía General de la República, cuando en el desarrollo de sus actividades tenga indicios de la comisión de un delito.
- Renovar anualmente la fianza establecida en el Art 43, literal d) de la Ley de Firma Digital, previa a su vencimiento.
- Cumplir con las demás obligaciones.

- Ejemplos de Autoridades Certificadoras

Las empresas pueden gestionar trámites con las administraciones públicas y cámaras de comercio de forma on-line, por ejemplo, la solicitud de documentos para la exportación, certificado para la facturación electrónica, certificado de servidor seguro.

Se pueden solicitar diferentes tipos de certificados profesionales. A continuación, se detallan algunos ejemplos de Autoridades Certificadoras por país:

- España

- Camerfirma: es la autoridad de certificación de las Cámaras de Comercio españolas que, además, permite actuar bajo una marca cameral común, ampliando su ámbito de validez.
- ANCERT (Agencia Notarial de Certificación): Entidad constituida por el Consejo General de Notariado de España dedicada a la prestación de servicios de certificación necesarios para garantizar la seguridad, validez y eficacia de la emisión y recepción de comunicaciones y documentos.
- CatCert (Agencia catalana de certificación): Tiene como objetivo proporcionar las herramientas e instrumentos necesarios para que las transacciones electrónicas tengan todas las garantías jurídicas, y vigilando que todo el proceso de despliegue de la firma electrónica en la administración sea lo más fácil posible.

- Chile

- e-certchile [5]: Creada en 2002 por la Cámara de Comercio de Santiago (CCS). Actualmente es la principal proveedora del sector público y las instituciones privadas en el ámbito de la Certificación Electrónica, contando también con aplicaciones de facturación electrónica.
- Certinet Identidad Digital [6]: Ha establecido alianzas con VeriSign ahora Symantec, para provisionar el hardware de firma y con Certisur para proveer los servicios de administración de certificados según lo exigido por el Ministerio de Economía.

- Ecuador:

- ANF (Authority of Certification Ecuador S.A.) [7]: fue la primera Autoridad Certificadora de España en quedar oficialmente acreditada en el

año 2000, al estar en posesión de la tecnología necesaria para emitir certificados electrónicos reconocidos, firma electrónica avanzada, sellos digitales de tiempo y verificación en línea del estado de los certificados.

E. Creación de un certificado digital

En este apartado se describe el proceso para la creación de un certificado digital, tanto para ser una Autoridad Certificadora, como para un servidor web.

Inicialmente, se debe tener en cuenta que para obtener seguridad en las comunicaciones de un servidor se debe cifrar la información, esto se realiza haciendo uso de protocolos como HTTPS, el cual funciona con certificados.

El protocolo HTTPS (transferencia de Hipertexto por sus siglas en español), crea dos certificados que corresponden con cualquier dominio, una llave primaria y otra llave pública. Como se mencionó anteriormente, con la llave privada un servidor cifra un paquete de datos y con la llave pública, el cliente puede descifrar esos datos. Para asegurar que los certificados sean los correctos, se crea un tercer certificado, es decir las Autoridades Certificadoras, que se encargan de asegurar y autenticar que los certificados sean los correctos. Un ejemplo de Autoridad Certificadora es Verisign, quien al verificar que la información obtenida es verdadera, firma con su llave, autorizando el certificado.

A continuación, se describe el proceso para la creación de un certificado digital autofirmado, utilizando openssl y se muestra el código de openssl en las figuras 6-8.

1. Instalar openssl

#sudo apt-get install openssl

2. Generar llave privada

#openssl genrsa -out private.key 1024

```
[root@potalaX pruebas]# openssl genrsa -out private.key 1024
Generating RSA private key, 1024 bit long modulus
.............................++++++
.....................++++++
e is 65537 (0x10001)
```

Figura 6. Certificado digital
Fuente: Elaboración Propia

3. Crear un CSR (Certificate Signing Request)

#openssl req -new -key private.key -out request.csr

```
[root@potalaX pruebas]# openssl req -new -key private.key
-out request.csr
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished
Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
Ir you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:ES
State or Province Name (full name) [Berkshire]: San Salvador
Locality Name (eg, city) [Newbury]: San Salvador
Organization Name (eg, company) [My Company Ltd]:Universidad
Don Bosco
Organizational Unit Name (eg, section) []: UDB
Common Name (eg, your name or your server's hostname)
[]:www.udb.edu.sv
Email Address []: aldojq@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:aldito
An optional company name []:udb
[root@potalaX pruebas]#
```

Figura 7. Certificado digital
Fuente: Elaboración Propia

4. Generar el certificado SSL

#openssl x509 -req -days 365 -in request.csr -signkey private.key -out certificado.crt

```
[root@potalaX pruebas]# openssl x509 -req -days 365 -in request.csr
- signkey private.key -out certificado.crt
Signature ok
subject=/C=ES/ST=\x09San Salvador/L=San Salvador/O=Universidad Don
Bosco/OU=UDB/CN=www.udb.edu.sv/emailAddress=aldojq@gmail.com
Getting Private key
[root@potalaX pruebas]#
```

Figura 8. Certificado digital
Fuente: Elaboración Propia

En la figura 9 se muestra el certificado digital generado, según los pasos mencionados. En la figura 10, se observa la estructura del certificado digital y, por último, en la figura 11, se muestra la

verificación que se realiza a un certificado digital.

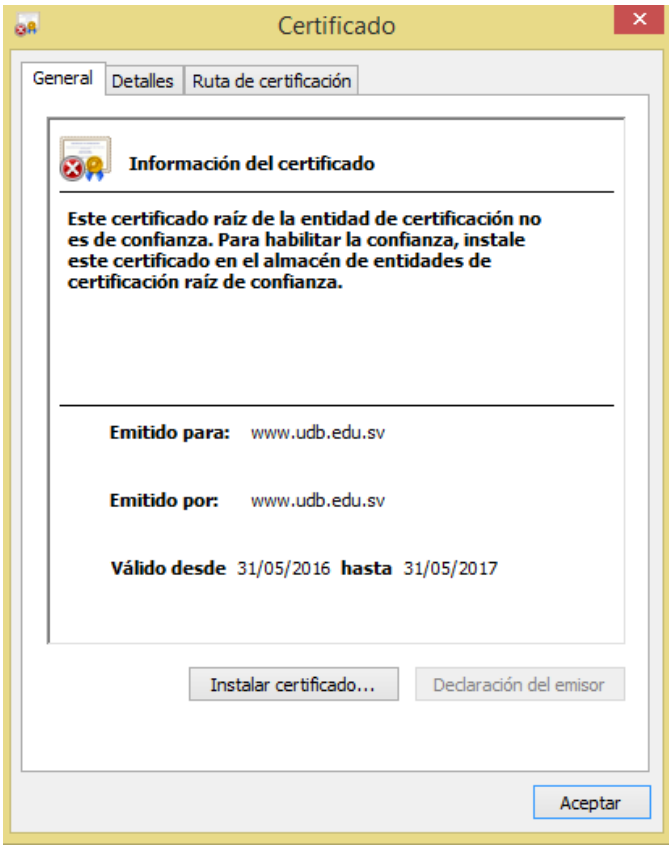

Figura 9. Certificado digital
Fuente: Elaboración Propia

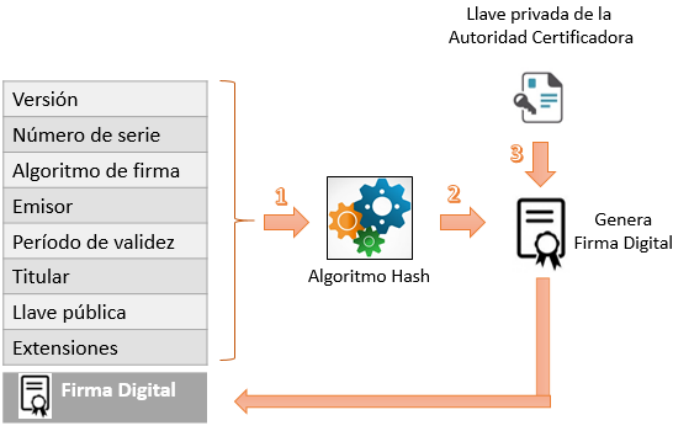

Figura 10. Estructura del Certificado Digital [11].

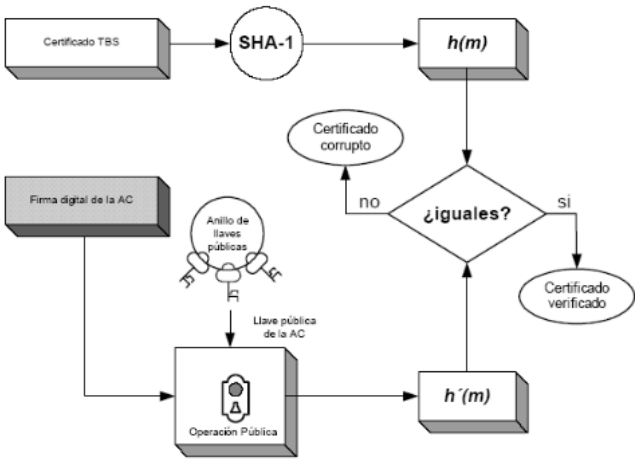

Figura 11. Verificación del Certificado Digital [10].

V. PROPUESTA DEL FUNCIONAMIENTO DE LA AUTORIDAD CERTIFICADORA

Esta propuesta, inicialmente contempla el procedimiento de acreditación de una Autoridad Certificadora, debido a que el servicio de certificación de firmas electrónicas en el país, solo podrá ser prestado por quienes cumplan con los requisitos establecidos en [1]. Adicionalmente se establecen las obligaciones que los proveedores del servicio en mención deberán cumplir. Luego, se determina el contenido del certificado digital emitido por los proveedores del servicio de certificación. A continuación, se describe el esquema propuesto para el funcionamiento de una Autoridad Certificadora. Finalmente, se realiza un análisis que verifique los servicios de seguridad de esta propuesta, mediante la política respectiva.

Según la Ley de Firma Electrónica de El Salvador, el proveedor de servicios de certificación otorga certeza a la firma electrónica certificada, garantizando la asociación de la persona con su llave pública, siendo una persona jurídica autorizada por la autoridad competente, dedicada a emitir certificados electrónicos y demás actividades previstas en la Ley mencionada.

En el Artículo IV, de la Ley de Firma Electrónica en El Salvador sobre Acreditación y prestación de los servicios de certificación [1], se menciona que el servicio de certificación sólo podrá ser prestado por aquellas personas jurídicas, públicas o privadas, nacionales o extranjeras, que cumplan con los requisitos establecidos en las Leyes competentes

para operar en El Salvador, y que demuestren para su autorización y durante todo el período en que se presten los servicios de certificación, cumplir con los siguientes requisitos:

- Contar con suficiente capacidad técnica para garantizar la seguridad, la calidad y la fiabilidad de los certificados emitidos, de conformidad a los requerimientos contenidos en las normas técnicas.

- Contar con el personal técnico adecuado con conocimiento especializado comprobable en la materia y experiencia en el servicio a prestar.

- Poseer la capacidad económica y financiera suficiente para prestar los servicios autorizados como proveedor de servicios de certificación.

- Rendir fianza por un monto adecuado al riesgo asumido por la prestación de los servicios de certificación.

- Contar con un sistema de información de alta disponibilidad, actualizado y eficiente, en el cual se publiquen las políticas y procedimientos aplicados para la prestación de sus servicios, así como de los certificados electrónicos que hubiere proporcionado, revocado, suspendido o cancelado y las restricciones o limitaciones aplicables a éstos.

Las instituciones oficiales autónomas y demás instituciones públicas con personería jurídica propia establecidas conforme a las Leyes de El Salvador, quedan facultadas para prestar los servicios regulados en esta Ley. Dichas instituciones deberán cumplir los requisitos establecidos en el presente artículo para ser acreditadas.

Estas disposiciones serán de obligatorio cumplimiento por las instituciones adscritas al Ministerio de Economía.

- *Acreditación de los Proveedores de Servicios de Certificación.*

En el artículo 44 de la Ley de Firma Electrónica de El Salvador [1], se menciona que los proveedores de servicios de certificación presentarán ante la Unidad de Firma Electrónica, junto con la correspondiente solicitud, los documentos que acrediten el cumplimiento de los requisitos señalados en el Art. 43. El cumplimiento de los requisitos será verificado por la Unidad de Firma Electrónica, a través de una auditoria inicial.

El solicitante acreditará por escrito, el compromiso de adquirir los equipos especializados necesarios y los servicios de personal técnico adecuado en el plazo máximo de 90 días hábiles, prorrogable por una sola vez por un período igual, por la Unidad de Firma Electrónica, siempre que el solicitante demuestre que el incumplimiento no es imputable a él. Si transcurrido el plazo indicado, el solicitante no hubiere cumplido el citado compromiso, se procederá inmediatamente a dejar sin efecto la acreditación otorgada.

El plazo de duración de la acreditación será por tiempo indefinido, siempre que se demuestre el cumplimiento de los requisitos establecidos en el Art. 43 de la Ley en mención [1], los cuales serán revisados anualmente al momento de ser solicitada la renovación anual.

- *Obligaciones de los Proveedores*

En el artículo 48 de La Ley de Firma Electrónica en El Salvador, se menciona que los proveedores de servicios de certificación tendrán las siguientes obligaciones:

- Adoptar las medidas necesarias para determinar la exactitud de los certificados electrónicos que proporcionen, la identidad y la calidad del signatario.

- Garantizar la validez, vigencia, legalidad y seguridad del certificado electrónico que proporcione.

- Garantizar la adopción de las medidas necesarias para evitar la falsificación de certificados electrónicos y de las firmas electrónicas certificadas que proporcionen.

- Verificar la información suministrada por el signatario.

- Crear y mantener un archivo actualizado de los certificados emitidos en medios electrónicos, para su consulta por plazo indefinido.

- Garantizar a los usuarios los mecanismos necesarios para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

- Sin perjuicio de otras obligaciones establecidas en la Ley de Protección al Consumidor, deberá informar a los interesados de sus servicios de certificación, utilizando un lenguaje comprensible, a través de su sitio de internet y a través de cualquier otra forma de acceso público, los términos precisos y condiciones para el uso del certificado electrónico y, en particular, de cualquier limitación sobre su responsabilidad, así como de los procedimientos especiales existentes para resolver cualquier controversia.

- Garantizar la autenticidad, integridad y confidencialidad de la información, y documentos relacionados con los servicios que proporcione. A tales efectos, deberán mantener un sistema de seguridad informática y respaldos confiables y seguros de dicha información, de conformidad a lo establecido en la presente Ley, su reglamento, y normas y reglamentos técnicos.

- Efectuar las notificaciones para informar a los signatarios y personas interesadas y las publicaciones necesarias, acerca del vencimiento, revocación, suspensión o cancelación de los certificados electrónicos que proporcione, así como de cualquier otro aspecto de relevancia para el público en general, en relación con los mismos.

- Dar aviso a la Fiscalía General de la República, cuando en el desarrollo de sus actividades tenga indicios de la comisión de un delito.

- Renovar anualmente la fianza establecida en el Art 43, literal d) de la Ley en mención, previo a su vencimiento.

- *Contenido del Certificado Electrónico*

En el artículo 58 de la Ley de Firma Electrónica de El Salvador [1], menciona que el certificado electrónico deberá contener al menos, la siguiente información:

- Identificación del titular del certificado electrónico, indicando su domicilio y dirección electrónica.

- Identificación del proveedor de servicios de certificación que proporciona el certificado electrónico, indicando su domicilio y dirección electrónica.

- Fecha de la acreditación y caducidad asignada al proveedor de servicios de certificación por la Unidad de Firma Electrónica.

- Fecha de emisión y expiración del certificado.

-Número de serie o de identificación del certificado.

- La firma electrónica certificada del prestador de servicios de certificación que emitió el certificado.

- Datos de verificación de la firma, los cuales deben corresponder a la información de su creación y que están bajo el control del firmante.

- Cualquier información relativa a las limitaciones de uso, vigencia y responsabilidad a las que esté sometido el certificado electrónico.

- Indicación de la ruta de certificación.

- Si el certificado ha sido emitido por una persona que ha actuado en representación de una persona natural o jurídica; en tal caso, el certificado deberá incluir una indicación del documento legal, público, o privado autenticado, que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona física o jurídica a la que representa.

Como puede observarse, los artículos establecidos en la ley de Firma Electrónica de El Salvador, cumplen con los mismos criterios establecidos en los estándares, lo que garantiza que la Firma Electrónica cumpla con la garantía de seguridad de los estándares.

En la figura 12 se describe el esquema del proceso de una Autoridad Certificadora, para la obtención de un certificado digital.

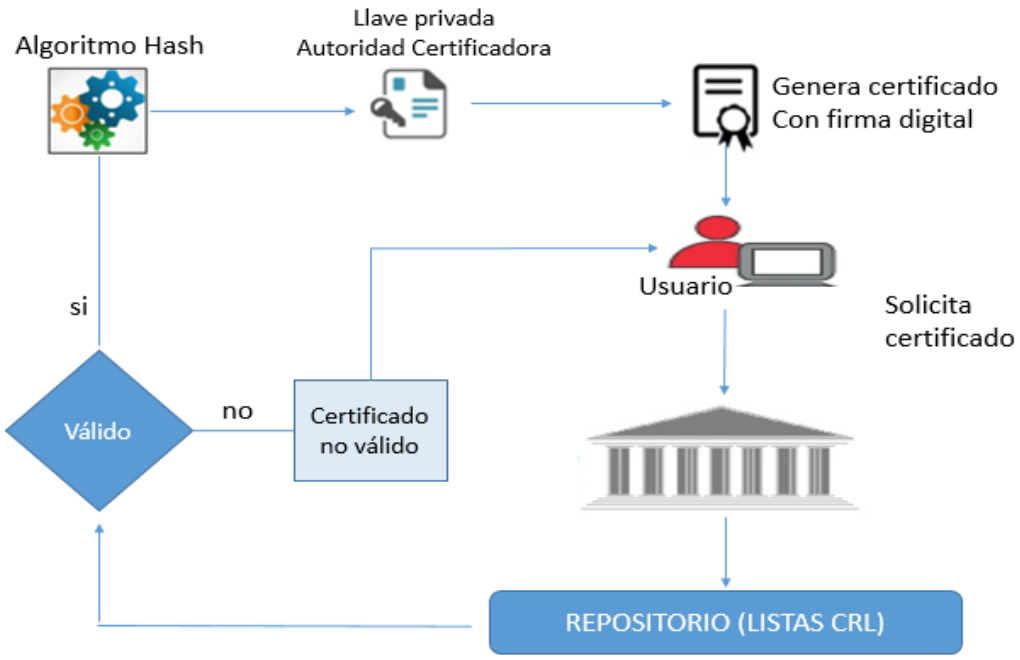

Figura 12. Esquema de proceso de Autoridad Certificadora.
Fuente: Elaboración Propia

- *Análisis de seguridad de una Autoridad Certificadora.*

Para garantizar la seguridad de una Autoridad Certificadora, es necesario definir reglas y formas de manejo y aplicación de los Certificados Digitales por medio de Políticas de la Autoridad Certificadora (PCA).

Una política de seguridad establece la dirección de máximo nivel de una organización sobre seguridad de información, así como los procesos y principios para el uso de la criptografía. Además, incluye declaraciones sobre cómo la empresa debe establecer el nivel de control requerido para afrontar los niveles de riesgo.

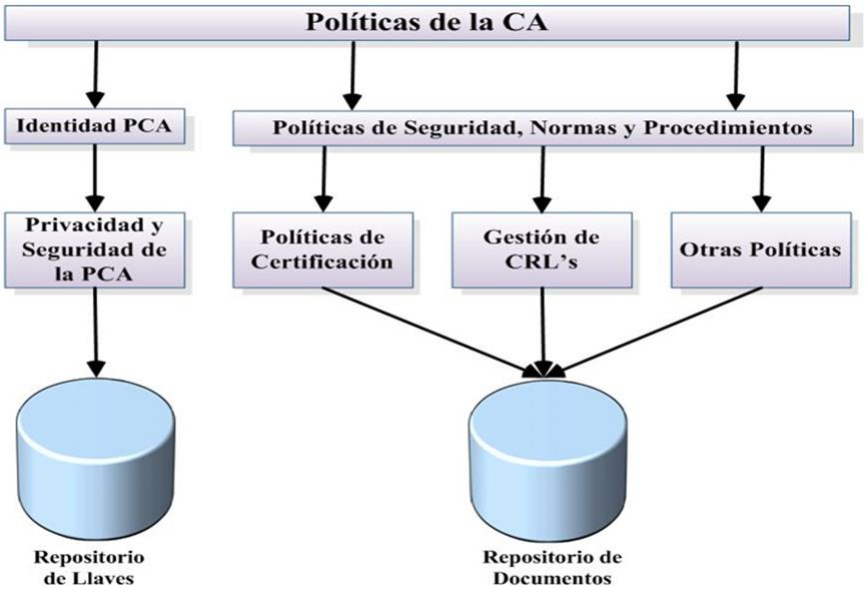

Figura 13. Políticas de una Autoridad Certificadora.
Extraída de: http://www.karapanza.net/politicas-de-la-autoridad-certificadora-pca/

En la figura 13, se describen las variables que debe poseer una política de Autoridad Certificadora. Como se puede observar, dentro de la política de una Autoridad Certificadora existe un módulo que se encuentra relacionado con la seguridad, es decir que la política deberá especificar los siguientes puntos:

- Definir las medidas técnicas y los procedimientos de seguridad que seguirá en la generación y protección de sus llaves.

- Detallar medidas de seguridad para proteger la información recogida en los procesos de certificación.

- Elaborar los documentos sobre normas, procedimientos, deciciones, operaciones, entre otras variables, que se encuentren relacionados a la seguridad de la información para considerarlas dentro de la política.

Se debe tener en cuenta que un documento de política de seguridad en el ambito de la criptografía de llave pública es un plan de acción para afrontar riesgos de seguridad, además, es un documento de alto nivel que describe que tipo de seguridad se pretende lograr y cuales son los objetivos perseguidos.

Con la realización de la política, se logrará obtener la seguridad deseada.

A continuación se describen los servicios de seguridad que se intenta garantizar con la propuesta de diseño de Autoridad Certificadora planteada:

- Integridad: A través de la firma digital, se asegura que la información contenida en ellos no sea modificada por un tercero.

- Confidencialidad: Por la política de la Autoridad Certificadora sobre las medidas de seguridad para proteger la información recogida en los procesos de certificación, se asegura la confiabilidad de la información.

- Autenticación: Se obtiene cuando la Autoridad Certificadora firma el digesto obtenido de los datos del certificado al verificar la información del usuario y consecuentemente anexa al digesto del certificado su firma digital.

- No repudio: A través de la firma digital se garantiza que el usuario no pueda negar quien dice ser.

-Características fundamentales de una Autoridad Certificadora

- Se obtiene Independencia y que posee una usencia de interés financiero en las transacciones realizadas.

- Recursos y capacidad financiera de parte de la Autoridad Certificadora para asumir la responsabilidad por el riesgo de pérdida.

- Experiencia obtenida en tecnologías de llave pública y la utilización de los procedimientos de seguridad que sean adecuados.

- La duración de los certificados la define la Autoridad Certificadora.

- Realización de auditorías por una entidad independiente.

- Existencia de un Plan de Contingencia para casos de emergencia.

- Seguridad interna.

- Capacidad para intercambiar datos con otras autoridades certificadoras.

VI. CONCLUSIONES

La Autoridad Certificadora deberá velar por que se cumplan todos y cada uno de los aspectos mencionados en la Ley de Firma Digital de El Salvador, para otorgar de esta forma el visto bueno de los usuarios que quiera certificar su Firma digital, tomando en cuenta actualizaciones y cambios que la Ley posea a lo largo del tiempo.

La Certificación de la Firma Digital deberán emitirse y tener un registro que permita la trazabilidad de todas y cada una de las certificaciones que hayan sido emitidas para que todo ente Auditor externo o Autoridad Supervisora pueda validad y garantizar que la Autoridad Certificadora cumpla con todos los

requerimientos establecidos en la Ley de Firma Digital.

La Autoridad Certificadora deberá manejar procedimientos eficientes para el otorgamiento de certificaciones, así mismo, deberá velar por cumplir con todos los requerimientos que la Autoridad Acreditadora le solicita a través de la ley.

Es importante concluir que la factibilidad de tener una Autoridad Certificadora en el país, propiciará el mayor uso de la Firma Digital; de esta manera, permitirá el ahorro de recursos y volviendo procesos más eficientes que requieran la autenticación por medio de la Firma. Por lo tanto, es importante que se apoye en la mayor medida la creación de este ente certificador.

Con la utilización de la Firma Digital y la Autoridad Certificadora se obtendrá mayor ahorro de costos ya que se reducirán gastos en manejo de papelería; ahorro de tiempo, al distribuir, visualizar y firmar cualquier documento de forma electrónica y se hará en tiempos menores a los utilizados actualmente; y también ahorro de espacio ya que no se tendrán que imprimir documentos para que sean legales; lo que ayudará mucho en la eficiencia y eficacia de los procesos actuales.

VII. Referencias

[1] Asamblea Legislativa de El Salvador; Ley de Firma Electrónica.

[2] Ochoa Jiménez, J. E. (2013). Función Picadillo Determinista al Grupo G2 y su Aplicación en Autenticación para Dispositivos Móviles (Tesis de maestría). Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional, Distrito Federal, México, 27.

[3] Aguirre, Jorge Ramió. Madrid España (2006). Funciones Hash en Criptografía.

[4] Marrero Yran, ACIMED v.11 n.6 (2003). La Criptografía como elemento de la seguridad informática.

[5] Cámara de Comercio de Santiago E-Certchile, http://www.e-certchile.cl/

[6] Identidad Digital, Certinet, https://www.certinet.cl/

[7] Autoridad de Certificación ANF, http://www.anf.es/

[8] Devoto Mauricio, Comercio Electrónico y Firma Digital.

[9] Área de Sistemas de información y Comunicaciones: Certificados digitales. Universidad Politécnica de Valencia. (2016). Recuperado de: http://www.upv.es/contenidos/CD/info/711250normalc.html

[10] Sistema Nacional de Certificación Digital, Modelo y Estrategia (2016), Recuperado de: http://slideplayer.es/slide/1028515/

[11] Rivas Guillén, Conceptos sobre firma y certificados digitales, XI Reunión de Responsables de Sistemas de Información, Costa Rica, 2009.

[12] Fernando Ramos, Autoridades de Certificación, Anguiano y Asociados, 2016. Extraído de: http://www.arrakis.es/~anguiano/artautcert.html