

# **CAPÍTULO III**

## **CERTIFICADOS ELECTRÓNICOS Y ENTIDADES**

### **HABILITADAS**

Hasta este punto ya contamos con todos los medios para determinar la identidad de los sujetos involucrados en el envío de un mensaje de datos, tenemos vía segura de transmisión y gozamos además de la confidencialidad y seguridad de la inalterabilidad de nuestros documentos, pero falta un elemento de suma importancia en la relación: la confianza y certeza de que el sujeto con quien estamos tratando es en verdad quien dice ser.

Dentro de un grupo cerrado, reducido o en una misma empresa, donde nuestros actos se efectúan con personas conocidas y de confianza, por cuanto utilizamos sistemas criptográficos simétricos o asimétricos sin valor monetario alguno, como el PGP<sup>2425</sup> (*Pretty Good Privacy*), cuyo grado de seguridad es alto, el sistema de transmisión funcionaría sin complicaciones mayores. El problema radica en los negocios de relevancia jurídica entre dos personas que no se conocen.

¿Como garantizamos el vínculo entre una firma electrónica y una persona? ¿De qué nos valemos para determinar el valor legal de la obligación contraída? ¿Qué tercero de confianza avala nuestros actos jurídicos con individuos desconocidos? Todas estas interrogantes se resuelven con la existencia de un tercero fiscalizador, un tercero jurídicamente constituido y controlado generalmente por el Gobierno Central del Estado, un tercero que nos brinda confianza frente a una relación jurídica constituida con un usuario ignoto.

Es por estas razones que para realizar el envío-recepción de mensajes de datos mediante sistemas de autenticación de autoría con reconocimiento legal a través de redes abiertas, es ineludible la existencia de una esfera procesal la cual enmarque todo aquello vinculante

---

<sup>24</sup> Programa desarrollado por Phil Zimmermann (1991) cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

al funcionamiento, esto se lo conoce como infraestructura de clave pública (*Infraestructura PKI*), donde se engloba a los usuarios del cosmos transaccional informático, a las *Entidades de Certificación de Información y Servicios Relacionados* y a las políticas de operación.

Se puede entender como Infraestructura de Clave Pública al conjunto de software, hardware, procedimientos y políticas generales de Firma Electrónica, cuyo objetivo es gestionar la certificación electrónica y servicios relacionados.

Actualmente dicha estructura se constituye como la más completa y funcional; tanto es así, que es considerada la de mayor uso y difusión mundial para la ejecución del comercio electrónico seguro.

Respecto a este tema, en el año 2003, dentro de la legislación ecuatoriana mediante Resolución del CONATEL (584-23-CONATEL-2003), se determinaba a la Infraestructura PKI como elemento gestor para el proceso de firma electrónica. Como es lógico, la normativa legal dentro del ámbito informático no puede estar supedita de manera excluyente a un único proceso de transmisión de datos, por cuanto el avance tecnológico es extremadamente acelerado. Por esta razón, cinco años después nuestros representantes han declarado la improcedencia de dicha norma, dando como resultado su derogación, a fin de dejar abierta la posibilidad de implementar nuevos métodos técnicos que puedan surgir en el futuro, evitando el desuso de la ley.

La derogación que se acaba de mencionar (*Res. 478-20-CONATEL-2008*) instituye un hecho digno de razonamiento y consideración por parte de nosotros como gobernados, ya que no supone la acertada ampliación legislativa, por el contrario, es el resultado de un error por parte de la Administración Pública, la cual ocasionó un retraso considerable en el funcionamiento de tres compañías privadas como Entidades de Certificación (*SISTECION S.A., ESDINAMICO CIA. LTDA. y ECUACERT S.A.*) y por consiguiente la dilación comunitaria en el aprovechamiento de los beneficios que nos brinda esta tecnología, dejando además la calidad de primitiva e inaplicable a cualquier doctrina ecuatoriana que haya versado sobre el tema.

Como ya sabemos, nuestra normativa en comercio electrónico se encuentra vigente desde el 2002, pero desde entonces sus vacíos y falencias no fueron considerados por los legisladores, es por esto que el CONATEL como entidad de regulación, por ingenuidad, buena fe o descuido, decidió emitir resoluciones en las cuales constaban disposiciones necesarias para el funcionamiento de la firma electrónica. Dentro de éstas resoluciones se

incluían figuras como *Título Habilitante, modelos, permisos de funcionamiento...*, que eran nuevas y distintas a las ya constantes en la Ley 67.

Lamentablemente esto se hizo sin considerar el *principio de restricción de contenido* normado en el artículo 67 del Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva (ERJAFE), el cual dice que “Las resoluciones administrativas de carácter particular (*resoluciones del CONATEL*) no podrán vulnerar lo establecido en una disposición de carácter general (*Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos*), aún cuando aquellas tengan grado igual o superior a éstas”, lo cual sumado al artículo 93 del mismo cuerpo legal que dispone que “Cualquier acto administrativo expedido por los órganos y entidades sujetas a este estatuto (*CONATEL forma parte de él*) deberá ser extinguido cuando se encuentre que dicho acto contiene vicios que no pueden ser convalidados o subsanados.” Esto derivó en la necesidad de derogar las dos resoluciones del CONATEL (324-17-2006 y 454-19-2006) en las cuales constaban definiciones y procedimientos para la creación de Entidades de Certificación; disposiciones que fueron aplicadas y cumplidas a cabalidad por las precitadas compañías, a tal punto que ya existieron resoluciones aprobatorias por parte del CONATEL para su permiso y registro (456-19-06, 457-19-06 y 458-19-06), pero en razón de que la normativa a la que ellas se rigieron era improcedente e ineficaz, también se debió derogar sus permisos.

Analizando este suceso, se ratifica la importancia de dos aspectos básicos; por una parte la capacitación y sapiencia jurídica que requieren nuestros funcionarios públicos para la correcta ejecución de sus funciones, y por otra, la preocupación y seguimiento que se debe dar a la normativa naciente por parte del Legislativo, a fin de que se pueda cubrir y subsanar el surgimiento de posibles lagunas legales que afecten su validez y aplicabilidad. Si no enmendamos estos factores, penosamente este hecho pasará de ser aislado a cotidiano, donde el único perjudicado será el Pueblo, el cual vivirá en la incertidumbre constante del posible daño que le causará cualquier desatino administrativo público.

## 1. CERTIFICADOS DE FIRMA ELECTRÓNICA

“Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad.”<sup>25</sup>

Así mismo, la Directiva 1999/93 del Parlamento Europeo y su Consejo define estos certificados como “la certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de esta.”<sup>26</sup>

Como ya se mencionó anteriormente, nuestro principal problema en las actividades comerciales con otros internautas radica en la vinculación del par de claves con la persona física, necesitando un resguardo respecto al nexo sujeto-firma. Es por esto la existencia de Certificados de Firma Electrónica, estos documentos (igualmente digitales) ratifican fehacientemente la pertenencia de la firma electrónica al individuo en cuestión, dejando de lado cualquier posible falsificación o suplantación de identidad que podría existir en el acto o contrato.

A estos certificados se los puede establecer como testimonios intachables que validan la pertenencia e identidad de una persona natural o jurídica respecto a determinada firma electrónica.

### 1.1 Contenido del Certificado

La importancia de estos certificados es tan alta que fácilmente los podríamos comparar con nuestros documentos de identificación personal, los cuales nos validan en relaciones interpersonales como la celebración de contratos, permitiendo la adquisición de derechos y obligaciones, constituyendo garantía suficiente de probidad jurídica como sujetos de derecho.

Considerando el reconocimiento y valor legal que poseen los certificados electrónicos, es necesario determinar cuales son los requisitos mínimos que deben contener estos documentos:

- *Identificación de la entidad de certificación de información*; mediante este dato, además de determinar la institución que controla la actividad jurídica del otro usuario,

---

<sup>25</sup> Art. 20; *Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos* (Ley 67)

<sup>26</sup> HERRMANN FERNÁNDEZ Patricia; *Comercio Electrónico*; Ed. Universidad Técnica Particular de Loja; 2007; p. 124

contamos con el nombre del garante que da fe de la veracidad del sujeto y de su firma, quien además será legalmente responsable en caso de que los datos expedidos en el certificado hayan sido falsos y por esto se nos haya ocasionado algún perjuicio.

- *Domicilio legal de la entidad*; de tal manera se establece el domicilio jurídico de la entidad de certificación, validando su constitución legal.
- *Datos generales del titular*; titular es aquel sujeto con el cual se ha entablado la relación. Estos datos nos ratificarán la identidad del usuario permitiendo conjuntamente su ubicación física en caso de ser requerida.
- *Fecha de emisión y expiración*; Por medio de estas fechas se establece el periodo durante el cual el suscriptor puede firmar documentos digitales utilizando su par de claves. La duración del certificado será establecido dentro del contrato del titular con la entidad de certificación, en caso de no haberse estipulado, el plazo de validez será de dos años contados a partir de que fueron expedidos. Cabe mencionar que dentro de este periodo puede existir la revocación o suspensión del certificado<sup>27</sup>.

La suspensión principalmente podrá darse por disposición expresa y motivada de la Autoridad Reguladora (CONATEL); por falsedad en los datos del suscriptor o por incumplimiento contractual por parte del titular de la firma; esta suspensión será de carácter temporal y deberá ser levantada una vez superadas las causales o a través de una resolución del CONATEL.

En el segundo caso, la motivación para revocar un certificado de firma electrónica radica en los supuestos de que la entidad de certificación haya cesado sus funciones y los certificados vigentes no hayan sido asumidos por otra entidad, o en el caso de existir la quiebra técnica de la entidad de certificación, habiendo sido declarada judicialmente.

Ahora bien, en el caso de que se produzca cualquiera de las limitaciones antes citadas, será obligación de la Entidad de Certificación de Información y Servicios Relacionados contar con mecanismos de ejecución inmediata para la cancelación de certificados, permitir el acceso público, dentro de su página Web, a listados de actualización permanente, en los cuales consten los certificados extintos, suspendidos y revocados, los cuales serán proporcionados por mecanismos automáticos cuya verificación deberá ser en tiempo real y notificar inmediatamente de la revocación a sus usuarios, dentro de las 24 horas posteriores<sup>28</sup>.

---

<sup>27</sup> Art. 25 y 26; *Ley* 67

<sup>28</sup> Anexo de la Resolución 477-20-CONATEL-2008; *Art.3* # 5, *Art.4* #8, 14 y 16.

Queda así demostrado, la seguridad que los legisladores han decidido brindar a los usuarios, otorgando los medios necesarios para que los sujetos que intervienen en el acto puedan verificar la legalidad y vigencia de la firma electrónica de cada uno de ellos; hecho que se basa en lo dispuesto en el artículo 55 de la Ley Modelo de la CNUDMI referente a Firmas Electrónicas, el cual versa “La firma numérica correspondiente a un mensaje, ya sea creada por el tenedor de un par de claves para autenticar un mensaje o por una entidad certificadora para autenticar su certificado, deberá contener por lo general un sello cronológico fiable para que el verificador pueda determinar con certeza si la firma numérica fue creada durante el “período de validez” indicado en el certificado, que es una condición para poder verificar una firma numérica.”

- *Número único de serie del certificado*; a través de esto se crea la individualidad de cada certificado, volviéndose heterogéneo respecto de los demás, facilitando así su búsqueda. A este número se lo conoce como “identificador exclusivo” y constituye obligación de la Entidad de Certificación, emitirlos con esta distinción. De igual forma, este requisito se encuentra reglado dentro de las Políticas de Seguridad que debe contar la Entidad de Certificación (*Art. 3 # 8 Res. 477-20-CONATEL-2008*).
- *Firma electrónica de la entidad*; por medio de esta se garantizará los principios de confidencialidad, integridad, autenticidad y no repudio de la información recibida por parte de la entidad de certificación, donde además quedará constancia de la veracidad del certificado recibido dejando como responsable a la propia entidad en caso de cualquier alteración o falsedad.
- *Limitaciones del certificado*; dentro de este último campo, la entidad dejará constancia expresa de que la información inmersa dentro del certificado podrá ser utilizada como medio ratificadorio de autoría y que el texto que envuelve al mensaje de datos será responsabilidad exclusiva del emisor; pudiendo además incluir otras limitaciones dependiendo de cada legislación.

Finalmente podríamos definir tres funciones fundamentales que cumple un certificado de firma electrónica:

1. Identificar a una persona natural o jurídica y vincularla con su firma digital.
2. Identificar las responsabilidades asociadas tanto de la Entidad de Certificación como del usuario.

3. Garantizar por parte de un tercero de confianza la pertenencia de un sujeto respecto a una firma electrónica y su vigencia de uso.

### **1.2 Certificados Emitidos en el Extranjero**

Con la aplicación de los elementos anteriores, nace una negociación informática legalmente estable y reconocida dentro de un mismo territorio, pero la tendencia del comercio viene a ser internacional, en donde se derriban fronteras y los lazos productivos se dan entre sujetos de nacionalidad dispar.

Es cierto, como lo hemos estado analizando, que la tipificación del tema tiene carácter mundial donde la batuta la llevan las organizaciones internacionales como la ONU, CAN, Unión Europea entre las mas destacadas, las cuales envuelven congregaciones de estados; es por esto que acertadamente se ha incluido el reconocimiento de certificados de firma electrónica emitidos en el extranjero, tal es el caso de la UNCITRAL (CNUDMI), la cual menciona en su artículo 58 que

“... El reconocimiento de certificados extranjeros se realiza generalmente mediante un método denominado “certificación cruzada”. En tales casos es necesario que entidades certificadoras sustancialmente equivalentes (o entidades certificadoras dispuestas a asumir ciertos riesgos con respecto a los certificados emitidos por otras entidades certificadoras) reconozcan mutuamente los servicios prestados, de forma que los respectivos usuarios puedan comunicarse entre ellos de manera más eficaz y con mayor confianza en la fiabilidad de los certificados que se emitan.”

de igual manera lo realiza la Comunidad Europea determinando en su séptimo artículo dictado por la Directiva 1999/93/CE, que “los Estados miembros velarán por que los certificados expedidos al público como certificados reconocidos por un proveedor de servicios de certificación establecido en un tercer país, sean reconocidos como jurídicamente equivalentes a los expedidos por un proveedor de servicios de certificación establecido en la Comunidad...”<sup>29</sup> además de esto, la UE establece ciertos requisitos que el tercer país deberá cumplir:

---

<sup>29</sup> Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica; <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:ES:HTML>

- que el proveedor de servicios de certificación cumpla los requisitos establecidos en la presente Directiva y haya sido acreditado en el marco de un sistema voluntario de acreditación establecido en un Estado miembro;
- que un proveedor de servicios de certificación establecido en la Comunidad, que cumpla las prescripciones de la presente Directiva, avale el certificado;
- que el certificado o el proveedor de servicios de certificación estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad y terceros países u organizaciones internacionales.

Con estos antecedentes, nuestra legislación ha procurado respetar estas disposiciones, declarando que los certificados emitidos en el extranjero tendrán el mismo valor legal que aquellos expedidos en el Ecuador. Este reconocimiento se puede dar por dos vías:

Primero, mediante solicitud de la entidad extranjera para su Acreditación en el país, previo a demostrar su reconocimiento legal de los servicios prestados en el extranjero. Es necesario mencionar que una vez adquirida la Acreditación legal por parte de la Entidad de Certificación Extranjera, ésta gozará de la calidad de entidad de certificación acreditada en el país, teniendo los mismos derechos y obligaciones que cualquier certificadora nacional.

Por otra parte, los certificados extranjeros también adquirirán validez jurídica en el país a través de una revalidación por parte de una Entidad de Certificación acreditada ante el CONATEL, la cual deberá comprobar la fiabilidad, tanto del certificado como de la entidad emisora. Estos hechos se encuentran debidamente tipificados en la Ley de Comercio Electrónico y Reforma al Reglamento General, en los artículos 28 y 2 respectivamente.

Es necesario destacar, que igualmente estos certificados tendrán carácter probatorio una vez validados.

## **2. ENTIDADES DE CERTIFICACIÓN**

Ahora bien, ya demostrada la necesidad de los certificados de firma electrónica como medio para brindar seguridad y confianza a los usuarios en razón del auge del comercio electrónico, nacen las Entidades de Certificación, las cuales son sujetos, públicos o privados, encargadas de generar confianza en las transacciones comerciales por medios electrónicos y que se encuentran bajo el control de un ente público.



La Ley de Comercio Electrónico (Art. 28) las define como “empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y el reglamento que deberá expedir el Presidente de la República.”

Como se desprende de lo citado, la función básica de las Entidades de Certificación radica en la emisión de certificados, pero a más de esto, se encuentran facultados de prestar servicios relacionados, dentro de los principales se encuentran:

- receptor la solicitud de emisión de un certificado electrónico;
- verificar y autenticar los datos que le entrega quien realiza la solicitud;
- generar las claves correspondientes para el certificado;
- grabar estas claves en un dispositivo físico, (token o tarjeta inteligente);
- administrar y mantener el sistema de claves, su estado, validez, y referencias; y
- realizar auditorias periódicas.

Es decir, estas entidades se encargan del funcionamiento y control global de las negociaciones telemáticas, otorgando la seguridad entre sus usuarios, haciendo posible el valor jurídico que éstas merecen.

Reyes Krafft acertadamente puntualiza sus actividades como “la generación, producción, distribución, control, seguimiento y destrucción de las llaves públicas o privadas asociadas con los certificados de llave pública.”<sup>30</sup>

Si bien es cierto, las Entidades de Certificación nacen con la aparición de las nuevas tecnologías y el establecimiento de actos jurídicos y de comercio que se dan a través de ellas, pero sus raíces vienen de una figura preexistente. A pesar de no existir exactitud de funciones, su similitud es evidente con los Notarios Públicos, ya que ambos dan fe, legalmente reconocida, respecto a determinados hechos y su relevancia es pareja en razón de que los dos son importantes en sectores productivos porque brindan certeza sobre el autor y contenido de documentos; brindan seguridad jurídica y además se constituyen en fedatarios, donde la entidad de certificación específicamente es un tercero disipador de conflictos porque conoce la autoría de los mensajes de datos. “La función primordial de esta figura es dar fe que las transacciones electrónicas de datos se han producido, y constituirse como una tercera parte confiable que acredita un vínculo entre una persona y

---

<sup>30</sup> REYES KRAFFT Alfredo; *La Firma Electrónica y las Entidades...*; p. 192

una clave pública, pudiendo considerarse que actúa como una especie de ‘notario electrónico’.”<sup>31</sup>

Ahora bien, habiendo puntualizado la facultad que tienen los sujetos públicos y privados para constituirse en Entidades de Certificación, dentro del campo estatal, el CONATEL mediante Resolución 481-20-CONATEL-2008, con fecha 8 de octubre de 2008, otorgó al Banco Central del Ecuador la acreditación como Entidad de Certificación de Información y Servicios Relacionados, constituyéndose en el primer ente público que recibe esta facultad por parte del Estado ecuatoriano.<sup>32</sup>

## 2.1 Terceros Vinculados

En razón de las diversas obligaciones que posee una Entidad de Certificación, la legislación ha prevenido la facultad para delegar a una segunda entidad, de menor rango, a fin de que cumpla con funciones específicas y aliviane su carga de trabajo. A estas entidades subsidiarias se las conoce como *Terceros Vinculados*, cuyas características son:

- Tienen jerarquía menor a las Entidades de Certificación (EC);
- Es una intermediadora entre el usuario y la EC;
- Sólo se encargan de la fase de recepción de datos, verificación y entrega de los certificados emitidos por la EC al cliente;
- No tienen control sobre los algoritmos de generación, su seguridad ni sobre la administración de los certificados.

La figura de Tercero Vinculado se la entiende como un tercero acreditado en el CONATEL, relacionado contractual y legalmente con una entidad de certificación de información acreditada, la cual está autorizada para representarla legalmente y prestar servicios de certificación de información y relacionados, a nombre o en representación de la misma.

Dentro de nuestra legislación (Art. 33 Ley de Comercio Electrónico), se faculta a las Entidades de Certificación la posibilidad de brindar los servicios de certificación, de forma total o parcial, por medio de un tercero, previa a demostrar el vínculo contractual que existe entre ambas. De manera complementaria, la Reforma al Reglamento General de la Ley 67 (*Ley de Comercio Electrónico*) establece que su vida jurídica será igual al plazo de

---

<sup>31</sup> HOCSMAN Heriberto Simón; *Negocios en Internet*; Ed. Astrea 2005; p. 373

<sup>32</sup> [http://www.conatel.gov.ec/site\\_conatel/index.php?option=com\\_content&view=article&id=371:resoluciones-octubre-diciembre-2008&catid=134:resoluciones-2008&Itemid=201](http://www.conatel.gov.ec/site_conatel/index.php?option=com_content&view=article&id=371:resoluciones-octubre-diciembre-2008&catid=134:resoluciones-2008&Itemid=201)

duración de la relación contractual con la Entidad de Certificación, adquiriendo esta última la responsabilidad respecto de los servicios prestados.

Sus funciones principales consistirán en la recopilación y custodia de información y documentos de soporte requeridos para la emisión de firmas electrónicas y certificados de firma electrónica; y, la instalación y soporte de aplicaciones relacionadas con el uso y verificación de firmas electrónicas y certificados de firma electrónica.

De esta manera podemos concluir en que el rol que debe cumplir la Entidad de Certificación versa en la ejecución de todas las fases del proceso e incluso administra y expide los certificados y los algoritmos de generación.

Dentro de la ejecución de la fase administrativa, se anida dos obligaciones puntuales de suma importancia; la primera consiste en mantener sistemas de respaldo de la información relativa a los certificados; en la mayoría de normativa internacional a esto se lo conoce como “repositorio”, el cual consiste en una base de datos abierta al público, donde figura el historial de los certificados de firma electrónica que han sido expedidos por parte de la entidad, permitiendo a los usuarios la verificación de vigencia y validez de las firmas electrónicas. “Para que una clave pública y su correspondencia con un firmante específico se pueda utilizar fácilmente en una verificación, el certificado debe publicarse en un repositorio o difundirse por otros medios. Normalmente, los repositorios son bases de datos electrónicas de certificados y de otro tipo de información a los que se puede acceder y que pueden utilizarse para verificar firmas numéricas.”<sup>33</sup>

En segundo lugar, se encuentra el deber de proteger los datos personales obtenidos directa o indirectamente del uso o transmisión de mensajes de datos.

En el artículo noveno de la Ley de Comercio Electrónico, estipula además que “La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.”, de esta manera queda establecido el derecho a la reserva que tiene cada individuo respecto a su correspondencia, siendo además responsabilidad exclusiva del titular, el contenido de los mensajes de datos que este haya enviado, recayendo sobre el suscriptor la obligación de afrontar los cargos legales en caso de ser descubierto información enviada que atente contra las leyes o la seguridad nacional.

---

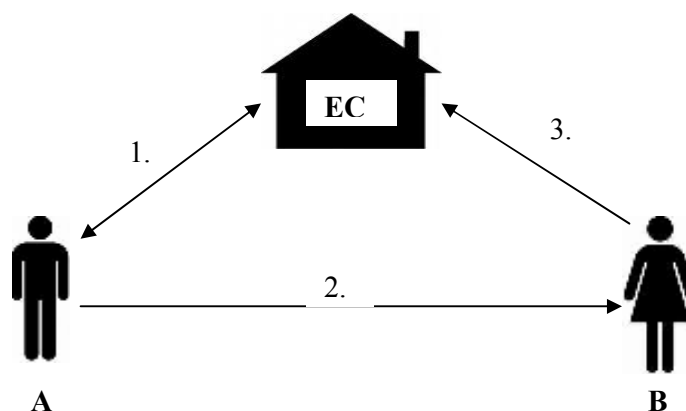
<sup>33</sup> CNUDMI; *Ley Modelo...*; Art. 56; <http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf>

“Los autores J. Dianne Brinson y Mark Radcliffe manifiestan que en la mayoría de las jurisdicciones de los Estados Unidos y en el mundo se reconoce el derecho de todo individuo a tener privacidad. Pero cuando esa privacidad se transmite a una entidad de certificación de firmas electrónicas, esta última debe proteger los datos personales del titular. Pero en caso de que no se dé la correspondiente protección, el titular podrá tomar medidas legales en caso de que la entidad de certificación haya dejado escapar información de los datos personales.”<sup>34</sup> Es por esta razón que el legislador ecuatoriano decretó que las entidades de certificación serán responsables hasta por culpa leve y responderán por los daños y perjuicios que causen a cualquier persona, en el ejercicio de su actividad (Ley Comercio Electrónico Art. 31).

## 2.2 Emisión de Certificados

Una vez definidas las Entidades de Certificación y los Terceros Vinculados, a continuación se grafica la actividad práctica de emisión de certificados de firma electrónica que cumplen ambas; en el primer caso (*gráfico 4*) se establece como único ente a la Entidad de Certificación (EC), mientras en el segundo (*gráfico 5*) aparece la intervención del Tercero Vinculado (3V).

### - *Gráfico 4:*

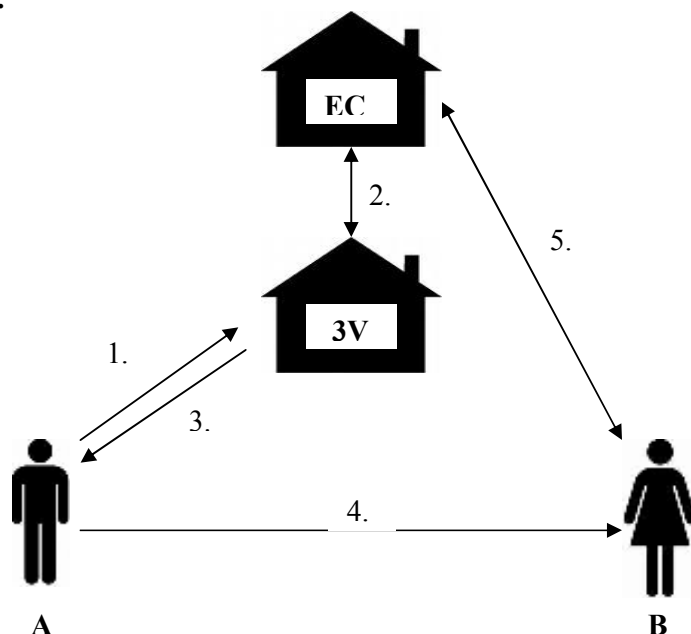


1. A, una vez elaborado el mensaje de datos que desea enviar, solicitará a la Entidad de Certificación que se le expida una certificación de firma electrónica. Inmediatamente EC verificará la identidad de A y emitirá el certificado a nombre del titular con su clave pública.

<sup>34</sup> HERRMANN FERNÁNDEZ Patricia; *Comercio Electrónico...*; p. 141

2. **A** encriptará el mensaje de datos con su clave pública, lo cual dará como resultado una firma electrónica, la cual será enviada conjuntamente con el certificado a **B**, donde este último descifrará la firma electrónica a través de la clave pública de **A**, obteniendo el mensaje original.
3. Opcionalmente **B**, para su mayor seguridad, ingresará al sistema de respaldo de información relativa a los certificados (repositorio) de la **EC**, para verificar la autenticidad del certificado enviado por **A**.

- **Grafico 5:**



1. **A**, solicita la emisión de un certificado de firma electrónica al Tercero Vinculado (**3V**).
2. **3V** previa a la verificación de la identidad del solicitante, pedirá a la Entidad de Certificación (**EC**) que expida el correspondiente certificado. **EC** recibe la solicitud con la identidad verificada del titular, proporcionándole el certificado a **3V**.
3. **3V** procede con la entrega del certificado a **A**, el cual fue emitido por la entidad certificadora.
4. **A** encripta su mensajes de datos y lo envía a **B** conjuntamente con el certificado que recibió de **3V**. **B** descifrará la firma electrónica con la clave pública de **A** obteniendo el mensaje original.
5. De manera facultativa, **B** podrá acceder al repositorio de la **EC**, a fin de verificar la validez de certificado.

### 2.2.1 Clasificación de Procesos de Emisión

Dentro del proceso de emisión de certificados de firma electrónica, ciertas legislaciones y doctrinas internacionales han decidido darle una clasificación especial para cada caso, deviniendo en tres tipos:

- *Certificación Simple*; sucede cuando una Entidad de Certificación única, avala la tecnología y prácticas en todas sus partes, emitiendo también los certificados y pares de claves criptográficas, donde además llevaría un registro de las transacciones que realice.
- *Certificación Cruzada*; generalmente se produce en el reconocimiento de certificados de firma electrónica extranjeros, ya que la clave pública es certificada por varias Entidades de Certificación. “En tales casos es necesario que entidades de certificación sustancialmente equivalentes (o entidades certificadores dispuestas a asumir ciertos riesgos con respecto a los certificados emitidos por otras entidades certificadoras) reconozcan mutuamente los servicios prestados, de forma que los respectivos usuarios puedan comunicarse entre ellos de manera mas eficaz y con mayor confianza en la fiabilidad de los certificados que emitan.”<sup>35</sup>
- *Certificación Jerárquica*; se genera en razón del escalafón de entidades, es decir, cuando uno o varios Terceros Vinculados, situadas bajo una Entidad de Certificación, certifican que la clave pública de un usuario corresponde en realidad a la clave privada del mismo usuario.

### 2.3 Proceso de Acreditación

Dentro del ámbito mundial, por regla general, las entidades de certificación y sus subsidiarias están bajo la regulación y control de entidades gubernamentales, donde cada Estado deberá establecer sus propios lineamientos que se deban cumplir para la acreditación de las entidades. “Los sistemas gubernamentales o privados de certificación se completan con la intervención de una autoridad de control, que depende de algún órgano de gobierno y que vigila el funcionamiento del sistema, pudiendo establecer la necesidad de una autorización previa para que funcionen las autoridades de certificación y estableciendo un registro obligatorio o voluntario de tales entidades.”<sup>36</sup>

---

<sup>35</sup> DEVOTO Mauricio; *Comercio electrónico y firma digital*; p. 174

<sup>36</sup> HOCSMAN Heriberto Simón; *Negocios en Internet*; p. 398

En el caso ecuatoriano existen dos sujetos de derecho público destinados al control y regulación de las entidades de certificación. En primera instancia se encuentra el *Consejo Nacional de Telecomunicaciones (CONATEL)*, organismo encargado de regulación, autorización y registro de las entidades de certificación; dentro de sus funciones substanciales se encuentra el cancelar o suspender la autorización de funcionamiento a las entidades de certificación acreditadas, previo informe motivado de la Superintendencia de Telecomunicaciones, y también el revocar o suspender los certificados de firma electrónica, cuando la entidad de certificación acreditada los emite con inobservancia de las formalidades legales, previo informe motivado de la Superintendencia de Telecomunicaciones.

Por otro lado, la *Superintendencia de Telecomunicaciones (SUPTEL)*, es el organismo delegado al control y fiscalización de las entidades de certificación, contando además con la facultad de imponer sanciones administrativas por incumplimiento de sus obligaciones.

Para poder operar legalmente dentro del Ecuador, los peticionarios deberán entregar a la *Secretaría Nacional de Telecomunicaciones (SENATEL)* los siguientes documentos: a) solicitud dirigida a la SENATEL; b) copia de cédula de ciudadanía y papeleta de votación del representante legal; c) copia certificada e inscrita en el Registro mercantil de la escritura de constitución de la compañía o empresa y del nombramiento del representante legal; d) original del Certificado de Cumplimiento de Obligaciones de la superintendencia a la que corresponda; e) descripción técnica de la infraestructura a ser utilizada y sus recursos; f) descripción de cada servicio propuesto; g) documentos de soporte que confirmen la disposición de mecanismos de seguridad electrónica; h) ubicación geográfica inicial y ubicación de cada *nodo*<sup>37</sup>, incluyendo un diagrama técnico de estos, e; i) documentación que demuestre solvencia económica.

Habiendo solicitado lo anterior, el peticionario requerirá de la *Acreditación*, esto se efectuará por medio de un acto administrativo, en donde la SENATEL deberá en el término de tres días, publicar en su página Web, un extracto de la solicitud. Conjuntamente, contará de 15 días para remitir un informe técnico, legal y económico del solicitante al CONATEL, el cual a su vez, dentro de 15 días término, resolverá sobre el otorgamiento. Dicha resolución será entregada a la SENATEL a fin de que proceda con la

---

<sup>37</sup> Un nodo es un punto de intersección o unión de varios elementos que confluyen en el mismo lugar. Por ejemplo, en una red de ordenadores cada una de las máquinas es un nodo, y si la red es Internet, cada servidor constituye también un nodo.

inscripción en el *Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditados y Terceros Vinculados* (RPNE), el cual se encuentra a su cargo, previo a la consignación del pago de un valor monetario, el cual es determinado por la misma autoridad autorizante, por concepto de derechos de permiso; caso contrario, si el solicitante no cumple con el desembolso en el término de 15 días, el acto administrativo quedará sin efecto procediendo al archivo del trámite.

Según Resolución 480-20/08 emitida por el CONATEL con fecha ocho de octubre de 2008, se estipuló que el valor por acreditación y registro necesarios para el perfeccionamiento del reconocimiento legal será de diez mil dólares de Estados Unidos de América, tanto para las entidades de certificación y terceros vinculados e igualmente se consignará el valor de seis mil dólares americanos para la prestación de servicios de certificación de información y servicios relacionados.

Conjuntamente se depositará una garantía monetaria de cuatrocientos mil dólares (*este valor fue modificado en la Reforma al Reglamento General, siendo anteriormente de un millón de dólares según la Res. 324-17/06*), por concepto de responsabilidad, con el fin de asegurar a los usuarios el pago por posibles daños y perjuicios ocasionados por incumplimiento de obligaciones por parte de la Entidad de Certificación. Este valor variará anualmente según los informes de fiscalización emitidos por la Superintendencia de Telecomunicaciones y en función de un valor base de garantía por certificado, determinado por el CONATEL.

Finalmente se pagará por gastos de administración, el valor de tres mil dólares al CONATEL y SENATEL, y tres mil dólares más a la Superintendencia de Telecomunicaciones por gastos de control.

Tabulando dichos valores, se los entiende de la siguiente manera:

Emisión de Acreditación y Registro	USD 10.000
Prestación de Servicios: <i>emisión de firmas electrónicas, sellado de tiempo, conservación de mensajes de datos y otros servicios relacionados</i>	USD 6.000
CONATEL y SENATEL	USD 3.000
SUPTEL	USD 3.000
<b>TOTAL</b>	<b>USD 22.000</b>

Por lo tanto, teniendo inexcusablemente que realizar una inversión considerable para cumplir con las políticas de solvencia técnica (lo cual considero extremadamente



necesario), se debe disponer de un capital medianamente alto para gastos administrativos, dando como resultado, en el caso de estar interesados en constituir una Entidad de Certificación Acreditada en el Ecuador, la cual cuente con todos los servicios requeridos en el mercado (emisión de firmas electrónicas y certificados, sellado de tiempo y conservación de mensajes de datos), ésta requerirá un capital de cuatrocientos veinte y dos mil dólares americanos.

En lo referente a la garantía de responsabilidad, esta podrá consignarse ya sea mediante una póliza de seguro de responsabilidad (contemplado en el Art. 43 de la Ley General de Seguros) u otorgando una garantía bancaria, conforme a la facultad concedida a las instituciones financieras en el Art. 51 literal c) de la Ley General de Instituciones del Sistema Financiero.

De darse el incumplimiento de obligaciones por parte de la Entidad de Certificación ocasionando daños y perjuicios a un usuario, éste deberá presentar en el término de 15 días, contados desde la ejecución del perjuicio, una solicitud motivada ante la SENATEL, la cual deberá poner en conocimiento del reclamo a la Entidad de Certificación, a fin de que en el término de cinco días reconozca la infracción o presente descargos. Cumplido el plazo, la SENATEL resolverá el reclamo. De ser favorable la resolución para el usuario, deberá disponer a la compañía aseguradora o institución financiera, el desembolso parcial de la garantía.

Ahora bien, el Título Habilitante representa la acreditación y permiso para la prestación de servicios de certificación y servicios relacionados. Este permiso comprende los derechos de instalación, modificación, ampliación y operación de la infraestructura requerida para brindar dichos servicios, cuya vigencia será de diez años, los cuales podrán ser prorrogados por igual tiempo, previa solicitud escrita del interesado, con tres meses de anticipación al vencimiento del plazo original.

Habiendo la SENATEL otorgado la Acreditación al peticionario, éste dispondrá de un plazo de seis meses para iniciar sus operaciones, y será obligación de la Superintendencia de Telecomunicaciones el verificar que se cumpla con este requisito, caso contrario, deberá informar a la SENATEL dicho incumplimiento a fin de que proceda con la extinción del permiso, salvo el caso de que el permisionario haya requerido ampliación en el plazo mediante solicitud motivada ante la SENATEL, la cual contará de 15 días perentorios a fin de que conceda o niegue el requerimiento.

La ampliación no podrá ser por un plazo mayor a 90 días y se otorgará por una sola vez; cabe mencionar que como toda petitoria ante autoridad pública, esta se rige por las normas

generales del silencio administrativo, fallándose favorablemente para el solicitante en caso de no haber respuesta en el término de 15 días.

Una vez cumplidas estas diligencias, el requirente se encuentra facultado legalmente para operar como Entidad de Certificación *Acreditada*, siendo el único beneficiario durante todo el tiempo de ejercicio, ya que por prohibición legal, no podrá ceder ni transferir a un tercero los derechos adquiridos.

### **2.3.1 Acreditación de un Tercero Vinculado**

De forma similar, el trámite de acreditación para un Tercero Vinculado se lo realizará mediante una solicitud ante la SENATEL, en la cual deberá adjuntar los mismos documentos previamente enumerados para las Entidades de Certificación, a excepción de los literales g), h) e i). Adicionalmente, constituye requisito esencial, la presentación de documentos que legitimen la relación contractual con la Entidad de Certificación de Información y Servicios Relacionados Acreditada, donde constará claramente las responsabilidades legales de cada uno de los contratantes respecto de los usuarios y autoridades.

Contando desde la fecha de presentación de la solicitud, la SENATEL dentro de 15 días adjudicará al interesado el certificado de registro. La constancia del mencionado registro gravitará en una razón o marginación efectuada por la Secretaría Nacional de Telecomunicaciones, dentro del *Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditados y Terceros Vinculados*.

### **2.3.1 Acreditación de Entidades Públicas**

Constituyéndose un avance para el Ecuador, en lo concerniente a la práctica de la tecnología informática - como ya se hizo referencia – en sesión 20ª de 2008 del Consejo Nacional de Telecomunicaciones, se autorizó al Banco Central del Ecuador como la primera Entidad de Certificación Acreditada de derecho público, cumpliendo a cabalidad el acto administrativo correspondiente, el cual se efectuó con celeridad y eficiencia, donde las autoridades envueltas en la acreditación supieron respetar los plazos legales establecidos.

Las instituciones públicas que pueden acceder a esta calidad serán los organismos y dependencias de las funciones Legislativa, Ejecutiva y Judicial, así como todas aquellas entidades y organismos creados y contemplados por la Constitución Política o la ley para el ejercicio de la potestad estatal, para la prestación de servicios públicos o para el desarrollo de actividades económicas asumidas por el Estado.

En lo pertinente al proceso de acreditación para entes estatales deviene a ser el mismo que el de las Entidades de Certificación privadas, otorgando dentro del noveno artículo innumerado agregado por el artículo cuarto de la Reforma al Reglamento General a la Ley de Comercio Electrónico, la facultad excluyente para las certificadoras estatales de emitir certificados de firma electrónica para las instituciones públicas.

#### **2.4 Contrato entre Entidad y Usuario**

El contrato que las entidades de certificación o registro suscriban con sus usuarios es de vital importancia por cuanto a través de este instrumento se formaliza la atribución de autoría de todos los mensajes de datos que el consumidor remita a terceros, negándole además cualquier posibilidad de repudio respecto de la información enviada.

De esta manera, todo texto firmado digitalmente alcanzará el nivel jurídico de firma manuscrita, superando el factor de rechazo que tiene la firma autógrafa, por ser un método de presunción de autoría, obligándose al cumplimiento de todo aquello estipulado en el documento.

“Una firma (*electrónica*) podía constituir un testimonio de la intención de una parte de considerarse vinculada por el contenido de un contrato firmado, de la intención de una persona de respaldar la autoría de un texto (manifestando así su conciencia de que del acto de la firma podrían derivarse consecuencias jurídicas), de la intención de una persona de asociarse al contenido de un documento escrito por otra persona, y del hecho de que una persona estuviera en un lugar determinado en un momento determinado.”<sup>38</sup>

Dentro del presente contrato, cada interviniente posee dos obligaciones primordiales que deberán cumplir:

- *Entidad de Certificación*; 1. Deberá certificar la identidad de su consumidor; 2. Emitir el correspondiente certificado de firma electrónica, el cual deberá contar con acceso informático.

---

<sup>38</sup> CNUDMI; *Ley Modelo...*; p. 23

- *Usuario*; 1. Mantener reserva respecto de su clave privada; 2. Notificar de manera oportuna, si existe el hecho presunto o fehaciente de que un tercero tenga conocimiento de dicha clave, a fin de que la Entidad proceda a suspender o revocar los certificados de firma electrónica.

A más de lo estipulado, constituye requisito esencial de la Entidad de Certificación, el determinar el plazo de vigencia de los certificados que se emitan.

Dentro de la legislación ecuatoriana se articula la necesidad de la aprobación por parte del CONATEL respecto de estos contratos, conservando además la facultad de consentir cualquier tipo de modificación ulterior que se realice; debiendo estos contratos ser emitidos dentro del territorio ecuatoriano, en idioma castellano y estar sometidos a la jurisdicción y a las leyes ecuatorianas.

### **3. INFRAESTRUCTURA DE CLAVE PÚBLICA**

Como ya se mencionó la infraestructura de clave pública o *Public Key Infrastructure (PKI)* la constituyen los programas y equipos, sistemas de información, redes electrónicas de información, políticas y procedimientos cuya finalidad es soportar la operación de los servicios de certificación de información y servicios relacionados, “ello tienen como objetivo brindar la mayor seguridad posible y generar la consecuente confiabilidad para los usuarios.”<sup>39</sup>

Dicha infraestructura es de existencia imperante dentro del funcionamiento pleno de la firma electrónica ya que abarca, a parte de los sistemas y políticas de operación, a los sujetos jerárquicamente superiores e inferiores de las entidades de certificación.

De esta manera, la estructura de clave pública comprende determinadas garantías y servicios a sus involucrados:

- *Servicios*; 1) emisión de firmas electrónicas y sus certificados; 2) Certificación electrónica; 3) Conservación de Mensajes de datos; 4) Comprobación de la identidad de los usuarios; 5) publicación de repositorio, entre otros.
- *Garantías*; 1) No alteración de las claves públicas y vinculación inequívoca con el usuario; 2) sistemas que garanticen la confiabilidad en la transferencia de mensaje de datos; 3) técnicas fiables de encriptación.

---

<sup>39</sup> SARRA Andrea; *Comercio electrónico y derecho*; p. 392

### 3.1 Jerarquía Estructural

En base a lo mencionado, nace un escalafón dentro de la infraestructura de clave pública, el cual consta según las funciones e importancia de los miembros que abarcan el universo práctico de la firma electrónica.

- *Entidad de Fiscalización y Control*; Esta entidad se encarga del control y observancia de las políticas generales de funcionamiento, debiendo además realizar auditorías técnicas de las entidades de certificación y emitir informes motivados. En el Ecuador esta función está a cargo de la Superintendencia de Telecomunicaciones (SUPTEL).
- *Entidad de Inscripción y Acreditación*; Ésta estará delegada a la aprobación, suspensión y cancelación de las autorizaciones de funcionamiento de las Entidades de Certificación, de la Acreditación de funcionamiento y además estará obligada de llevar un registro de todas las Entidades de Certificación.

En algunas legislaciones, como es el caso de Ecuador o España, se dividen las funciones de inscripción y acreditación en entidades distintas. La inscripción abarca la autorización, registro y regulación de las entidades, lo cual está a cargo del CONATEL. Mientras que la acreditación, que se realiza a través de la Acreditación legal, la cumple la SENATEL.

Esta distinción es facultativa ya que el cumplimiento de estas obligaciones las puede realizar una sola autoridad.

- *Entidad de Certificación*; Es el tercero de confianza constituido por una persona jurídica, pública o privada, cuya función principal es la de emitir certificados de firma electrónica permitiendo de esta manera, la vinculación del suscriptor con la firma y determinando la identidad del mismo.

Dentro de algunos países, por razones de orden público, estas entidades únicamente podrán ser sujetos de derecho público.

- *Tercero Vinculado*; Como ya revisamos, estas son jerárquicamente inferiores que las de certificación y cumplen con funciones específicas como la recepción de datos, verificación y entrega de los certificados que son emitidos por la Entidad de Certificación.
- *Usuarios*; Son personas naturales o jurídicas, nacionales o extranjeras, titulares de un par de claves (pública y privada), cuya actividad radica en solicitar certificados de firma electrónica y custodia de su clave privada.
- *Organismo de Promoción*; Esta entidad se encuentra contemplada dentro del artículo 36 de la Ley de Comercio Electrónico, cuya finalidad consiste en promover y difundir

los servicios electrónicos, el comercio electrónico y el uso de las firmas electrónicas respecto a la ejecución de inversiones y comercio electrónico. La presente actividad estará a cargo del *Consejo de Comercio Electrónico e Inversiones* (COMEXI).

En esencia, el COMEXI está conformado por representantes de los sectores público y privado, donde su función radica en establecer un nexo entre esos sectores, buscando la apertura de mercados mediante el comercio exterior y dedicándose también a alentar la modernización del Estado.

A la presente estructura jerárquica la podemos entender gráficamente de la siguiente manera:

- Gráfico 6:

