# LA FIRMA ELECTRÓNICA DESDE LA ÓPTICA DE LA LEY Nº 18.600

## ASPECTOS JURÍDICOS Y TECNOLÓGICOS

**Ing. Santiago Paz**[(*)]

**Dra. Esc. María José Viega**[(**)]

## 1. INTRODUCCIÓN

La historia del Derecho, manifiesta el Profesor Losano, "está condicionada por las tres revoluciones de la escritura, de la imprenta y de la ordenación electrónica de datos. En las tres revoluciones el Derecho es afectado a través del Lenguaje. En la primera se pasa de la expresión oral a la escrita; en la segunda, de la escritura manual a la impresa y en la tercera de la escritura tipológica, impresa o mecánica al lenguaje tratado electrónicamente"[1].

Y este lenguaje electrónico, que constituye la forma de comunicación en el ciberespacio, está signado por el cambio de tres elementos que son: el tiempo, el espacio y el acceso. El tiempo, debido a la inmediatez de las comunicaciones, a los diferentes usos horarios, el "ahora" es el tiempo presente en todas partes. El espacio telemático está signado por la inexistencia de fronteras geográficas y por la internacionalidad de los fenómenos. Y el acceso se convierte en la herramienta más poderosa en este proceso de cambios, donde pierde importancia la propiedad y se torna relevante "tener acceso a"[2].

La importancia del acceso se debe al fenómeno de la desmaterialización y éste "responde a la necesidad de cambio y adaptación que va a implicar para el desarrollo de la telemática a un concepto filosófico –antes que jurídico-. En efecto, es físicamente palpable por nuestros sentidos una gradual e ineludible desmaterialización de la realidad. Se observa con nostalgia, o satisfacción para

---

(*) Ingeniero en Telecomunicaciones. Director de Seguridad de la Información de la Agencia para el desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC).

(**) Doctora en Derecho y Ciencias Sociales y Escribana Pública por la Universidad Mayor de la República Oriental del Uruguay (UDELAR). Directora de Derechos Ciudadanos de la Agencia para el desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC). Directora del Instituto de Derecho Informático de la Facultad de Derecho (UDELAR). Profesora de Informática Jurídica, Derecho Informático y Derecho Telemático (UDELAR).

[1] CARRASCOSA LOPEZ Valentín. "Valor Probatorio del Documento electrónico". Revista Informática y Derecho. Volumen 8. UNED Centro Regional de Extremadura, 1995. Página 133.

[2] VIEGA RODRÍGUEZ María José y RODRÍGUEZ ACOSTA Beatriz. "Documento electrónico y firma digital. Cuestiones de seguridad en las nuevas formas documentales". E-book editado por Viega & Asociados. Montevideo, Mayo 2005.

algunos, el derrumbe de lo físico (…) y de lo ético o valorativo lo cual hace recordar la frase del pensador decimonónico: “todo lo sólido se desvanece en el aire”. El fenómeno evolutivo de la desmaterialización al decir de Illescas Ortiz resulta equiparable a una alteración contractual de similar importancia a la que se produjo con la sustitución de la tabla o tablilla de piedra o barro por el papiro y la del pergamino por el papel”[3].

En un mundo en que hoy nos vinculamos, contratamos con personas que no conocemos personalmente, estudiamos en universidades extranjeras desde nuestra casa, nos relacionamos en forma electrónica con las entidades estatales, necesitamos una serie de garantías para estas relaciones telemáticas.

Frente a los desafíos a los que el ciberespacio nos enfrenta, surgen entre otras, las siguientes preguntas: ¿cómo se puede verificar la identidad de las partes en una transacción electrónica?, ¿cómo se puede evitar el repudio de las consecuencias legales de un acto o negocio?, ¿cómo establecer que un documento o mensaje no ha sido alterado?,. Estas son algunas de las cuestiones que la Ley Nº 18.600 de 21 de setiembre de 2009 viene a solucionar.

## 2. EL DOCUMENTO ELECTRÓNICO

Desde un punto de vista funcional, dice Carnelutti que el documento es “una cosa que sirve para representar a otra”[4]. Se hace énfasis entonces en el aspecto probatorio del documento.

Podemos decir que un documento tiene las siguientes características: ocupa un lugar en el espacio, se ubica en un tiempo específico, tiene relación entre el autor y lo querido y expresado por éste, y tiene un valor probatorio (propio del documento jurídico).

Giannantonio define el documento electrónico, distinguiendo:

*En sentido estricto*: el que queda almacenado en la memoria del computador y no puede llegar a conocimiento del hombre sino mediante el empleo de tecnología informática.

*En sentido amplio*: el que es procesado por el computador por medio de periféricos de salida y se torna así susceptible de conocimiento por el hombre.

Pero el punto crucial es el origen del documento. Tenemos que tener en cuenta si el mismo ha sido generado por el hombre y almacenado posteriormente, si se

[3] HERNÁNDEZ AGUILAR Álvaro. “Comercio y contratación electrónica”. IX Congreso Iberoamericano de Derecho e Informática. Costa Rica, 2002.
[4] CARNELUTTI, Francesco, “Sistema de derecho procesal civil”. Buenos Aires (1944), tomo II, página 414.

reproduce por intermedio del ordenador o si se admite que el propio computador genere el contenido del documento a partir de alguna combinación de la información disponible con ciertas instrucciones que operan en su sistema.

Un documento electrónico tiene las siguientes características:[5]: es generado o emitido a través de un computador, sólo puede hacerse público mediante tecnología informática, es inmaterial y para que tenga valor deberá estar sujeto a medidas técnicas de seguridad.

La Ley Nº 18.600 define al "Documento electrónico o documento digital": como la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo.

## 3. LA FIRMA ELECTRÓNICA Y LA FIRMA ELECTRÓNICA AVANZADA

Según el Dr. Eduardo Couture en su "Vocabulario Jurídico", firma es: "el trazado gráfico, conteniendo habitualmente el nombre, apellido y rúbrica de una persona, con el cual se suscriben los documentos para darle autoría y obligarse con lo que en ellos se dice"[6]. Cuando una persona "firma" un documento en papel está manifestando su voluntad y lo que hace es dibujar sobre él una serie de símbolos que lo identifican.

La firma en este caso cumple diversas funciones, lo cual dependerá de la naturaleza del documento: establecer la autoría del propio texto, aceptar las obligaciones que surgen de un texto, adherir a lo expresado por otro y determinar la presencia del mismo.

Dice Palazzi[7] que: "Si se encuentra un medio que reemplace a la firma ológrafa en ambientes digitales, éste nuevo medio deberá cumplir con las funciones tradicionales de la firma. Estas son: (i) indicativa: informa acerca de la identidad de un autor; (ii) declarativa: se refiere al acuerdo respecto al contenido del acto; (iii) probatoria: permite vincular al autor con el signatario".

Consagrándose aquí el criterio de la "equivalencia funcional".

La Ley Nº 18.600 define a la "Firma electrónica" como: los datos en forma electrónica anexos a otros datos electrónicos o asociados de manera lógica con el mismo, utilizados por el firmante como medio de identificación.

---

[5] VIEGA, María José. "Connotaciones jurídicas de la firma electrónica y digital". Primer Congreso Internacional de Derecho Informático y Tecnológico del Paraguay. Asunción, 24 y 25 de octubre de 2005.

[6] COUTURE, Eduardo J.. "Vocabulario Jurídico". Ediciones Depalma, Buenos Aires, 1983.

[7] PALAZZI, Pablo. "Firma digital y comercio electrónico en Internet". Ob. Cit.

La firma electrónica a su vez puede tener diferentes técnicas para firmar un documento, así tenemos las siguientes:

Código secreto o de ingreso: es la necesidad de una combinación determinada de números o letras, que son sólo conocidas por el dueño del documento, o lo que todos usamos, por ejemplo en los cajeros automáticos, es el famoso PIN (Personal Identification Number);

Métodos basados en la Biometría: se realiza el acceso al documento mediante mecanismos de identificación física o biológica del usuario o dueño del documento.

La Biometría es la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos. Realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas. La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona por lo que es (manos, ojos, huellas digitales y voz)[8].

En el perfeccionamiento del cifrado de mensajes, llegamos a lo que se conoce como criptografía. La criptografía es la ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones. Esta consiste en un sistema de codificación de un texto con claves de carácter confidencial y procesos matemáticos complejos, de manera que para el tercero resulta incomprensible el documento si desconoce la clave decodificadora, que permite ver el documento en su forma original. De ahí es que surgen dos tipos de criptografía:

1. de clave secreta o simétrica: las partes en los dos procesos de cifrado y descifrado comparten una clave común previamente acordada. Debe ser conocida solamente por ambas partes para evitar que un tercero ajeno a la operación pueda descifrar el mensaje transmitido. Esta tiene como desventaja que si se realiza en redes abiertas (Internet) puede ser interceptada por un tercero y además no sirve si el tercero que deba participar no tiene la clave.

2. de clave pública o asimétrica: este sistema fue creado en 1976 en Estados Unidos y consiste en que ambas partes deben tener un par de claves que no son iguales sino que son asociadas; es decir, una clave privada en poder del titular, conocida sólo por él, y una clave pública, que

[8] BORGHELLO Cristian Fabián. "Seguridad Informática. Sus implicancias e implementación". Tesis Licenciatura en Sistemas. Universidad Tecnológica Nacional. Setiembre de 2001. Capítulo 2, página 11. www.cfbsoft.com.ar

se relaciona matemáticamente con la clave privada, y que puede estar tranquilo que sólo el destinatario va a poder descifrar su mensaje.

La Ley Nº 18.600 distingue la firma electrónica de la firma electrónica avanzada, otorgándole diferente valor jurídico. La firma electrónica avanzada debe cumplir una serie de requisitos:

1) requerir información de exclusivo conocimiento del firmante, permitiendo su identificación unívoca;

2) ser creada por medios que el firmante pueda mantener bajo su exclusivo control;

3) ser susceptible de verificación por terceros;

4) estar vinculada a un documento electrónico de tal modo que cualquier alteración subsiguiente en el mismo sea detectable; y

5) haber sido creada utilizando un dispositivo de creación de firma técnicamente seguro y confiable, y estar basada en un certificado reconocido válido al momento de la firma.

Esto significa que la firma electrónica avanzada es la emitida por un prestador de servicios de certificación acreditado.

## 4. LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

La ley establece que los prestadores de servicios de certificación no están sujetos a autorización previa y que su actividad se realizará en régimen de libre competencia.

El artículo 2 literal M) define al prestador de servicios de certificación como “la persona física o jurídica, pública o privada, nacional o extranjera, que expida certificados electrónicos o preste otros servicios de certificación en relación con la firma electrónica.

Los prestadores pueden acreditarse ante la Unidad de Certificación Electrónica, por lo que, de acuerdo a lo establecido en el artículo 2 literal N) se consideran prestadores de servicios de certificación acreditados, emitiendo por tanto

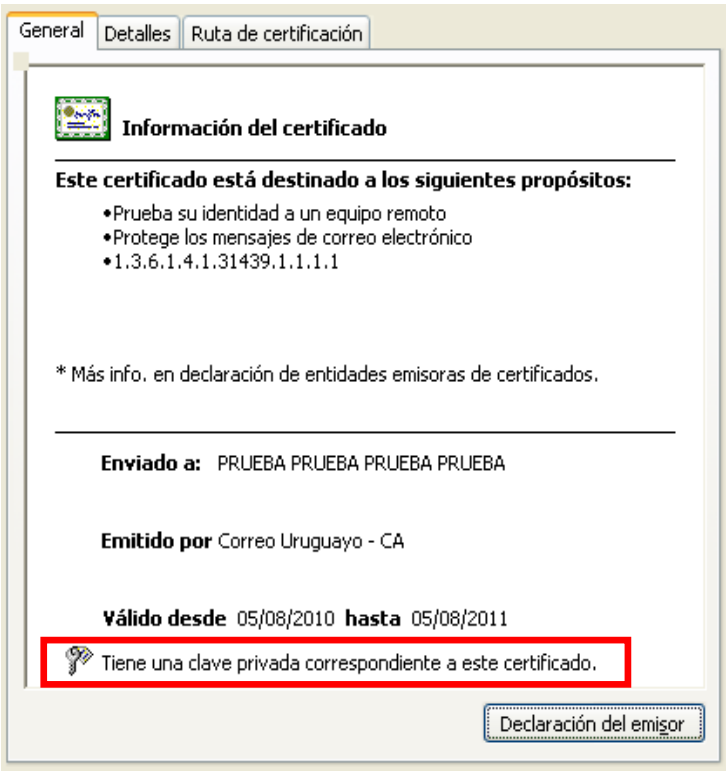
certificados electrónicos reconocidos, que tiene como consecuencia la emisión de firma electrónica avanzada.

## 5. LOS CERTIFICADOS ELECTRÓNICOS

En el contexto de criptografía, uno de los desafíos principales es la distribución de las claves secretas. La criptografía asimétrica soluciona en gran parte ese problema, como se explicó antes, utilizando un par de claves, donde una de ellas es privada y la otra pública.

Sin embargo, se mantiene el problema de determinar qué clave pública pertenece a cada usuario. El poder determinar quién es realmente el que tiene la clave secreta que se corresponde con la clave pública es fundamental para poder garantizar quien es el firmante o quién es el que podrá descifrar el mensaje.

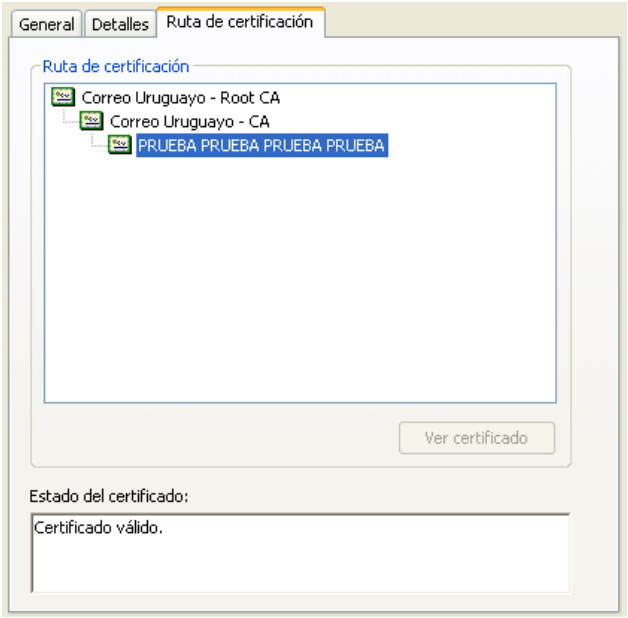
Por ese motivo se crea el concepto del certificado electrónico. Un certificado electrónico es un documento electrónico, firmado electrónicamente, que incluye la clave pública de un usuario vinculado con la identidad del mismo. Quien firma (o emite) este documento es la Autoridad de Certificación, y es quien verifica la veracidad de los datos.



Para emitir un certificado electrónico, una Autoridad de Certificación utiliza un certificado electrónico el cual también está firmado por otra autoridad de certificación, y así sucesivamente. A esto se le llama cadena de confianza.

Esta cadena de confianza comienza en una raíz, que es quien tiene su certificado firmado por sí misma, es decir, la confianza es dada por sí misma, y no por un tercero.

De esta forma, la confianza en las claves públicas y su vinculación con la identidad del firmante recae totalmente en la Autoridad de Certificación Raíz.




## 6. LA INFRAESTRUCTURA NACIONAL DE CERTIFICACIÓN ELECTRÓNICA

Como se mencionó anteriormente, los certificados electrónicos funcionan en un marco de cadena de confianza, en el cual la confianza recae en un punto único conocido como Autoridad de Certificación Raíz.

A partir de la promulgación de la Ley Nº 18.600, en Uruguay existe la Infraestructura Nacional de Certificación Electrónica; Es decir el conjunto de infraestructura tecnológica, de normas y procedimientos necesarios para la gestión de certificados electrónicos reconocidos.

Básicamente, es esta infraestructura quien genera la confianza necesaria para el funcionamiento de la firma electrónica avanzada. Dentro de esta infraestructura se encuentra la Autoridad de Certificación Raíz y los Prestadores de Servicios de Certificación.

## 6.1 La Autoridad de Certificación Raíz Nacional (ACRN)

La Autoridad de Certificación Raíz es el punto de partida para toda la cadena de confianza de la Infraestructura Nacional de Certificación Electrónica.

Se trata de equipamiento tecnológico de primera línea, el cual cumple con altos requerimientos de seguridad. Los procedimientos operativos que aplican a la gestión de dicho sistema, son sumamente exigentes y se adecuan a estándares internacionales.

Dicho sistema se mantiene fuera de línea en una habitación de máxima seguridad, para la cual es necesario acceder siguiendo un protocolo estricto, que requiere la presencia de múltiples personas a la vez.

Cuenta también con un respaldo, guardado bajo las mismas medidas de seguridad.

Cuando este sistema se pone a funcionar, se realiza un procedimiento conocido como Ceremonia de Claves, en el cual se inicializa el sistema y se generan las claves maestras. Dicha ceremonia es verificada por varios actores y organismos de control para verificar que todo se realice de forma controlada.

## 6.2 Unidad de Certificación Electrónica (UCE)

La Unidad de Certificación Electrónica tiene como cometido realizar todas las acciones necesarias para que el sistema en su totalidad funcione de manera correcta.

Dentro de las responsabilidades más destacables están las de fijar los estándares técnicos y operativos que deberán cumplir los prestadores de servicios de certificación, y las de acreditar y controlar a los prestadores de servicio de certificación.

Esta Unidad funciona en la órbita de AGESIC y cuenta con independencia técnica. Esta dirigida por un Consejo Ejecutivo conformado por 3 directores y cuenta con un Consejo Consultivo integrado por representantes de la: Suprema Corte de Justicia, el Banco Central del Uruguay, la Universidad de la República, la Unidad Reguladora de Servicios de Comunicaciones, y la Cámara Nacional de Comercio y Servicios del Uruguay.

# 7. IMPLEMENTACIÓN DE ASPECTOS TÉCNICOS

Un Prestador de Servicios de Certificación Acreditado es una entidad que tiene como cometido expedir Certificados Electrónicos Reconocidos o prestar otros servicios en torno a Firma Electrónica Avanzada.

Por este motivo, deben proporcionar un alto grado de confianza en la Infraestructura Nacional de Certificación Electrónica del Uruguay (INCE).

Dado que la emisión de un Certificado Electrónico implica la validación de la identidad del sujeto del certificado y su futura aceptación por el resto de la cadena (dentro de los ámbitos de uso del certificado), los mecanismos de operación requeridos a estas entidades deben ser exigentes y fuertemente regulados.

Dicha regulación debe abarcar todos los procesos, procedimientos y mecanismos utilizados por el prestador, que intervienen en el ciclo de vida de sus certificados (emisión, renovación, revocación). Se debe tener en cuenta que los requisitos referentes a seguridad de la información cobran alta importancia entre estas exigencias. De este modo se dan las garantías para que terceros puedan confiar en cualquier certificado reconocido emitido dentro de la cadena de confianza de la INCE.

En este sentido se cuenta con estándares internacionales de referencia que son utilizados de guía para definir los requisitos referentes a:

- la escritura de los documentos de políticas y prácticas de certificación del prestador de servicios de certificación (RFC 3647),
- los formatos de los Certificados Electrónicos (ISO/IEC 9594-8),
- los mecanismos de comprobación del estado de dichos certificados (RFC 5280 y RFC 2560),
- el establecimiento de la puesta en marcha y funcionamiento de la Autoridad de Certificación del Prestador de Servicios de Certificación (WebTrust o ETSI 102 042),
- la generación de sellos de tiempo (RFC 3161), y
- el establecimiento de un Sistema de Gestión de la Seguridad de la Información (ISO 27001).

Actualmente la Unidad de Certificación uruguaya se encuentra definiendo las políticas de certificación y evaluando los estándares técnicos que serán aplicables a la INCE y que regirán el correcto funcionamiento de toda la cadena de confianza.

Dicha Unidad también se encarga de definir cuáles son todos los trámites y requisitos administrativos que serán exigidos a los PSC al momento de solicitar

una acreditación de operación dentro de la cadena de certificación. Esto incluye además del proceso de acreditación, la definición e implementación de los mecanismos de verificación y el control del cumplimiento de estos requisitos.