# TEMA 2. NUEVOS DESAFIOS AL DERECHO INFORMÁTICO EN EL NUEVO MILENIO.

## Subtema:

### LA FIRMA DIGITAL Y LA AUTORIDAD CERTIFICANTE EN URUGUAY

***Dra. Esc. María José Viega Rodríguez***

## 1. Introducción.

He presentado a este evento dos ponencias que tienen estrecha relación entre sí, por un lado el análisis de la prueba informática, un tema en el cual la seguridad es de suma importancia, como también lo es, en la contratación electrónica saber con certeza la identidad de la persona con la cual estamos contratando, que ésta existe realmente, que es capaz y que es el titular de los derechos de los cuales está disponiendo.

Como todos sabemos en EEUU se están realizado contrataciones en forma electrónica hace ya un buen tiempo, en forma exitosa entre los distintos Estados. Existen empresas privadas cuyo cometido es certificar la firma de los contratantes, a las cuales se les denomina "Autoridad Certificante", que veremos más adelante.

Pero resulta necesaria la existencia de una persona *"...que fuera entendida en materia jurídica y capaz de redactar cláusulas de un contrato, que fuere imparcial en el negocio jurídico y que además de todo esto diera fe del acuerdo de voluntades y mantuviera bajo su custodia y responsabilidad (copia u original) el negocio jurídico*."[1]

Y advierten que existe un profesional en el ámbito jurídico, que es el Notario u Escribano, en el marco del Notariado Latino, que se adapta a los requerimientos de la contratación electrónica. Es así como surgió el proyecto "Cybernotary", que concluyó con una ley en el Estado de la Florida que concretó el proyecto, creando un profesional del derecho (Abogado), que además tuviera conocimiento del sistema EDI, al cual se lo dotó de la potestad de certificación.

Por lo tanto, la función del escribano es de suma importancia en la contratación electrónica, y sin lugar a dudas va a estar determinando el éxito o fracaso de una negociación.

## 2. Elementos de relevancia para la contratación electrónica:

Cuando realizamos un contrato en forma electrónica es de fundamental importancia que la transferencia de información sea un sistema seguro, para lo cual es importante tener en cuenta los siguientes elementos:

[1] De la Fuente, Juan Angel. "*La intervención notarial en la contratación electrónica*". Libro de Ponencias del VI Congreso Iberoamericanode Derecho e Informática. Montevideo - Uruguay . 1998.

a) Confidencialidad: la comunicación no debe estar expuesta a terceras personas, ni permitir que estas comprendan el mensaje que se está trasmitiendo.

b) Integridad de la transacción: es importante tener la certeza que el mensaje trasmitido y recibido por la otra parte esté completo y no halla sufrido modificación alguna.

c) Identificación de las partes: debemos tener seguridad de quien es la persona con la cual nos estamos comunicando.

d) Seguridad de la transacción: Toda comunicación debe estar firmada, de forma tal que el negocio tenga expresado el consentimiento de forma inequívoca.

## 3. Diferentes tipos de firma.

a) Firma ológrafa o tradicional: 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.

Pablo Palazzi[2] define la firma como "*el trazo particular por el cual el sujeto consigna habitualmente su nombre y apellido, o sólo su apellido, a fin de hacer constar las manifestaciones de su voluntad*".

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.
Determinar la presencia del mismo

Cuando un Escribano certifica una firma lo que está asegurando es que la persona que firma es quien dice ser, que lo hizo libre y conscientemente, que firmó dicho documento en un lugar y día determinado.

Dice Palazzi[3] 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*".

b) Firma electrónica: con relación a las diferentes técnicas utilizadas para firmar electrónicamente un documento, Guillermo Balay[4] describe las siguientes: "*Una técnica disponible es el uso de una tableta sensible y un lápiz magnético*

[2] Palazzi, Pablo Andrés. "*Firma digital y comercio electrónico en Internet*". VI Congreso Iberoamericano de Derecho e Informática. Libro de Ponencias. Montevideo – Uruguay, l998.
[3] Idem cita anterior.

*conectados a un PC donde se registra la presión, velocidad y coordenadas donde el operador apoya el lápiz. Esos datos se combinan matemáticamente para formar la "firma electrónica" de la persona. Posteriormente, se puede comparar esa firma almacenada con otra para verificar si pertenecen a la misma persona.*

*Otra técnica de firma electrónica disponible en el mercado podría ser el registro de la huella digital y de ciertos factores biológicos de la piel que identifican unívocamente a la persona. El dispositivo consiste en un tablero donde la persona coloca su dedo. Allí se digitalizan la huella y los parámetros biológicos del dedo de la persona, de tal forma que es imposible reproducirlos salvo que se obligue a la persona a colocar su dedo en el dispositivo"*.

c) Firma digital: en sí misma es un dato (secuencia de bits) y el peligro radica en que una vez divulgado, cualquiera puede utilizarlo y hacerse pasar por su titular.

Para que esto no suceda, en la firma digital se utiliza lo que se denomina "criptografía de clave pública".

Vayamos por partes. 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. Es una rama de las matemáticas que procura hacer incomprensibles los mensajes, para que no puedan ser leídos por terceros, y luego tornarlos a su estado natural.

Existen dos tipos de criptografía:

* de clave secreta: tanto el que envía el mensaje como el que lo recibe, conocen y utilizan la misma clave. Es una forma conocida también como simétrica. El peligro que acarrea es que normalmente las personas no se conocen personalmente, por lo tanto el canal para el envío de la clave debe ser un canal seguro.

* de clave pública: es un sistema asimétrico, y fue creado en Estados Unidos en el año 1976. No es necesario en esta caso un canal seguro porque cada persona dispone de dos claves, un pública (conocida por todos) y otra privada (conocida únicamente por el titular). Para encriptar el mensaje el remitente utiliza la clave pública del destinatario, de tal manera que solo el destinatario pueda descencriptarlo con su clave privada. Con relación a la seguridad de este sistema el P/S Guillermo Balay[5] dice que: "*Ambas claves de un mismo usuario están relacionadas matemáticamente, pero es casi imposible calcular la clave privada a partir de la pública, aún conociendo el algoritmo empleado para construirlas*".

Este es el sistema utilizado en la firma digital, el emisor cifra el mensaje con la clave pública del receptor, y firma el mensaje aplicando su clave privada; el receptor del mensaje utiliza su clave privada para descifrar el mensaje y la clave pública del emisor para verificar la firma digital.

---

[4] Balay, Guillermo. "*Enfoque informático del Decreto N° 65/998*". Procedimiento administrativo electrónico. Presidencia de la República. Oficina Nacional del Servicio Civil. 1998.

[5] Idem cita anterior.

## 4. Firma electrónica y digital en nuestro derecho.

Nuestro derecho incorporó la firma digital para el Procedimiento Administrativo en la Administración Central por **Ley 16.736** en el artículo 695, el cual equipara los medios informáticos a los convencionales, reconoce su validez jurídica y les otorga el mismo valor probatorio. El inciso final de este artículo consagra expresamente la firma electrónica digital.

El **Decreto 65/998** reglamentario de la ley 16.736, en su artículo 1 inciso final establece: "*Cuando la substanciación de las actuaciones administrativas se realice por medios informáticos, las firmas autógrafas que la misma requiera podrán ser sustituidas por contraseñas o signos informáticos adecuados*".

Este artículo es de una gran amplitud, ya que no establece que tipo de firma sustituirá a la firma autógrafa. Sin embargo en los artículos 18 y 19 definirá la firma electrónica y digital, diferenciándolas.

El artículo 18 define la **firma electrónica**, y dice que es "*el resultado de obtener por medio de mecanismos o dispositivos un patrón que se asocie biunívocamente a un individuo y a su voluntad de firmar*."

Comentando este artículo dice el Dr. Ruben Correa Freitas[6] que "*Esto es lo que comúnmente en informática se conoce como el "password" o contraseña, que es la clave informática que tiene una persona y que solamente ella la puede usar*".

Y el artículo 19 define la **firma digital** como: "*un patrón creado mediante criptografía, debiendo utilizarse sistemas critográficos "de clave pública" o "asimétricos", o los que determine la evolución de la tecnología*". Me parece de suma importancia que el artículo deja una puerta abierta a los avances tecnológicos.

## 5. Autoridad Certificante.

Es un tercero imparcial, confiable para ambas partes y para la sociedad toda, dotado de poderes de certificación. Las autoridades certificantes están autorizadas a emitir certificados digitales, que detallaremos más adelante.

Las funciones de la autoridad certificante son las siguientes:

a) publicar las claves públicas,
b) realizar la identificación física antes de entregar las claves y posteriormente controlar si la clave pública pertenece a la persona que dice ser su titular,
c) certificar el procedimiento de identificación,

[6] Correa Freitas, Ruben. "*Principios del Procedimiento Administratico Electrónico. Decreto del Pode5r Ejecutivo N° 65/998 de 10/III/98*". Procedimiento Administrativo Electrónico. Publicación de la Oficina Nacional del Servicio Civil. Presidencia de la República.

d) publicar siempre que se dé una situación de suspensión, revocación, extinción o modificación de la clave pública.

## 6. Autoridad Certificante en Uruguay.

El art. 2 de la Ley 16736 de 1995 establece: "*La Administración Nacional de Correos tendrá a su cargo la prestación de servicios postales, esto es la admisión, transporte, o distribución y entrega de envíos de correspondencia, giros postales, y productos postales en general*".

Se entiende la correspondencia electrónica como un tipo especial de correspondencia, ya que la diferencia está en el soporte que contiene la información y en la forma de transferirla, por lo que la certificación está dentro de sus cometidos.

A través de la **"Recomendación de la Comisión Nacional de Informática de fecha 25 de setiembre de 1998"**: se autoriza a la Administración Nacional de Correos a prestar servicios de Autoridad de Certificación en todo el país.

Establece la Administración Nacional de Correos[7]: "*La importancia de una Autoridad de Certificación en el contexto de las comunicaciones globales está dada no solamente por su confidencialidad y respeto nacional, sino también por su reconocimiento internacional. A este respecto corresponde destacar que la Administración Nacional de Correos integra la Unión Postal Universal (UPU) y la Unión Postal para las Américas, España y Portugal (UPAEP), organismos internacionales que tienden al incremento mundial de las comunicaciones postales. Los correos más importantes del mundo se han posicionado ya como Autoridad de Certificación Nacional en sus respectivos países, lo que constituye una verdadera Red Internacional con sólido respaldo y trayectoria.*"

## 7. Certificados emitidos por el CORREO:

1. **Certificados Personales (Identificación segura)**: para personas que desean realizar transacciones electrónicas a título personal.
   Requisitos: 18 años de edad y documento de identidad o pasaporte.

2. **Certificados Empresa (Empresa segura)**: son emitidos para personas que van a representar a una Empresa.
   Requisitos: persona mayor de 18 años, se verifica la identidad de la persona y de la empresa y documentación que habilite a actuar en representación de la misma.

3. **Certificados para servidores (Sitio seguro):** "*generalmente servidores de publicación de páginas Web. Estos certificados permiten la habilitación del*

[7] Página de la Administración Nacional de Correo publicada en Internet: www.correo.com.uy

*protocolo SSL (https://) para el acceso seguro a la información publicada, dando garantías a los clientes de estar accediendo al servidor correcto. En este caso se verifica con la autoridad responsable correspondiente que el nombre de dominio solicitado corresponda a la empresa solicitante y se verifica la identidad del servidor."*[8]

Las claves y el certificado se entrega al titular, no quedando copia de las claves en los servicios de Certificación de la A.N.C. El medio en que se entrega puede ser un disquete o una tarjeta Smart Card.

## 8. Conclusiones.

En un trabajo realizado por la Comisión de Informática y Seguridad Jurídica de la Unión Internacional del Notariado Latino "*El notario y las transacciones jurídicas electrónicas*"[9] al referirse a la autoridad certificante manifiesta: "*Esta infraestructura de certificación crea nuevas posibilidades para el notariado, que podrá proponerse como garante de la procedencia de actos públicos de un estado a otro, brindando a la función notarial la plenitud y prestigio que ha gozado en la era papel*".

En nuestro país, si bien se consagró a la Administración Nacional de Correos como la autoridad certificante, la misma se limita a emitir los certificados que hemos vistos, no estamos ante el tercero imparcial que redactara el negocio, que recabara los consentimientos, que tuviera conocimientos jurídicos para asesorar a las partes y que además certificara su firma. Por lo tanto, elaborar un proyecto de ley sobre firma digital se impone, la calidad certificadora es nuestra tarea por naturaleza y debe seguir siéndolo en el mundo digital.

Esto nos demuestra, que lejos de las visiones apocalípticas del notariado para este siglo, como consecuencia de los adelantos tecnológicos, estamos preparados para continuar desarrollando nuestra función, que materialmente tendrá sin lugar a dudas cambios de importancia, pero siempre basado en los principios que nos rigen desde los orígenes, dando transparencia y certeza al negocio jurídico

### Bibliografía


1. Página de la Administración Nacional de Correo publicada en Internet: www.correo.com.uy
2. Correa Freitas, Ruben. "*Principios del Procedimiento Administratico Electrónico. Decreto del Pode5r Ejecutivo N° 65/998 de 10/III/98*". Procedimiento Administrativo Electrónico. Publicación de la Oficina Nacional del Servicio Civil. Presidencia de la República.


[8] Página de la Administración Nacional de Correo publicada en Internet: www.correo.com.uy

[9] Comisión de Informática y Seguridad Jurídica de la Unión Internacional del Notariado Latino "*El notario y las transacciones jurídicas electrónicas*", publicada www.colegio-escribanos.org.ar/ediciones.htm

3. De la Fuente, Juan Angel. "*La intervención notarial en la contratación electrónica*". Libro de Ponencias del VI Congreso Iberoamericanode Derecho e Informática. Montevideo - Uruguay . 1998.
4. Palazzi, Pablo Andrés. "*Firma digital y comercio electrónico en Internet*". VI Congreso Iberoamericano de Derecho e Informática. Libro de Ponencias. Montevideo – Uruguay, l998.
5. Balay, Guillermo. "*Enfoque informático del Decreto N° 65/998*". Procedimiento administrativo electrónico. Presidencia de la República. Oficina Nacional del Servicio Civil. 1998.
6. Comisión de Informática y Seguridad Jurídica de la Unión Internacional del Notariado Latino "*El notario y las transacciones jurídicas electrónicas*", publicada www.colegio-escribanos.org.ar/ediciones.htm

**RESUMEN**

Este trabajo pretende dar una conceptualización del tema firma digital, así como la importancia de la misma en la contratación electrónica.

Además, hemos analizado las normas que regulan la temática en el derecho uruguayo en el ámbito administrativo, así como también la designación de la Administración Nacional de Correos como Autoridad Certificante.

También ha sido nuestro objetivo destacar la importancia de la existencia del notario o escribano, dejando de lado las visiones apocalípticas acerca de nuestra profesión como consecuencia del avance de la tecnología.

**Nombre**: Dra. Esc. María José Viega Rodríguez

**Nacionalidad**: Uruguaya

**Dirección**: Calle 25 de Mayo 477 Esc. 46 Montevideo Uruguay.

**Teléfono**: 915 41 90 – 099 19 34 78

**Fax**: 915 41 90

**Email**: mjviega@adinet.com.uy

**Curriculum**:

- Doctora en Derecho y Ciencias Sociales.

- Escribana Pública.
- Integrante de la Comisión de Derecho Informático y Tecnológico de la Asociación de Escribanos del Uruguay.
- Aspirante a la materia Informática Jurídica en la Universidad de la República.