Universidad Católica Ntra. Sra. de la Asunción
Sede Regional Asunción

"Firma Digital"

*

Daniel Bonhaure Falcón

**

—54771—

***

2010.
Asunción — Paraguay.

---

*Trabajo Práctico presentado a la Cátedra de Teoría y Aplicación de la Informática 2.
**Autor: Alumno del quinto año de la Carrera Ingeniería Informática.
*** Matricula del Autor.

Introducción.

A principio de semestre, en la cátedra Teoría y Aplicación de la Informática 2, se me dijo que tendría que realizar un trabajo monográfico sobre alguno de los diferentes temas presentados por el profesor, Juan Urraza.

Al inspeccionar el listado de temas, uno de ellos despertó en mí un especial interés; **"La Firma Digital"**, debido fundamentalmente a mi desconocimiento del tema y a que en los días previos, este había sido muy mencionado por la prensa ya que luego de cuatro años de discusión el congreso había remitió al Ejecutivo para su promulgación un proyecto de ley por el cuál se instrumentan o crean la firma digital y la firma electrónica.

El gran destaque que tuvo este hecho en la prensa es a consecuencia de que nuestro país, Paraguay, es el único de la región, que todavía no cuenta con una legislación que reglamente el uso y validez jurídica de la Firma Digital. Lo que al entender de la mayoría es una desventaja considerable para el país, principalmente en lo referente al campo tecnológico ya la ausencia de esta legislación disminuye las posibilidades del país de interactuar en todos los niveles de relacionamiento electrónico entre gobiernos y con los ciudadanos a nivel mundial, impidiendo la dinamización del comercio, la economía y el combate a la corrupción.

Creo que a esta altura es bueno aclarar al lector, que este va a ser un trabajo, más bien descriptivo e informativo, ya que tan solo me voy a avocar a describir, en primer término, todo lo relativo a la transmisión segura de información, definiendo y explicando ciertos conceptos que hacen a la materia, desarrollando las ventajas que ofrece la firma digital, los aspectos técnicos de la misma y explicando la necesidad de su legislación y las inconveniencias que acarrea esta para nuestro sistema jurídico; también veremos como la definen y tratan las legislaciones de otros países, particularmente en EEUU, Alemania y las Naciones Unidas, para luego ver el tratamiento que le da la legislación de nuestro país.

Con todo lo antedicho, no queda más que decir que, este es un trabajo que tan solo busca brindar, a aquellas personas que, como yo en un principio, no conocen nada acerca de la firma digital y todo lo que ella significa, una visión general de la misma para que puedan comprender que es lo que ella significa y lo provechoso de su uso, como así también todo lo relativo a su legislación y uso en nuestro país.

La Firma Digital.

El concepto de firma digital nació como una oferta tecnológica para acercar la operatoria social usual de la firma hológrafa (manuscrita) al marco de lo que se ha dado en llamar el ciber-espacio o el trabajo en redes.

Las transacciones comerciales y el hecho de tener que interactuar masiva y habitualmente por intermedio de redes de computadoras dieron lugar al concepto.

Pero, sólo después que los especialistas en seguridad y los juristas comenzaran a depurarlo alcanzó un marco de situación como para ocupar un lugar en las actuaciones entre personas, ya sean jurídicas o reales.

El fin, de la firma digital, es el mismo que el de la firma hológrafa: dar asentimiento y compromiso con el documento firmado; y es por eso que a través de la legislación, se intenta acercarla, exigiéndose ciertos requisitos de validez.

En la firma hológrafa el papel es el medio de almacenamiento, y el mecanismo es alguno de los tipos de impresión posibles (tinta, láser, manuscrito, etc.). Esta cualidad física le da entidad al documento, contiene sus términos, conceptos y sentidos de una manera perdurable, y al ser un elemento físico cualquier alteración dejará "señales" identificables.

Pero, los papeles ocupan lugar y pesan demasiado, resulta complejo y molesto buscar información en ellos (requiriendo de la acción humana ya sea al archivarlos y/o al rescatarlos), y el compartir los documentos también resulta inconveniente, lo que se podría evitar con un sistema de computación.

Ventajas ofrecidas por la Firma Digital

Gracias a la firma digital, los ciudadanos podrán realizar transacciones de comercio electrónico seguras y relacionarse con la Administración con la máxima eficacia jurídica, abriéndose por fin las puertas a la posibilidad de obtener documentos como la cédula de identidad, carnet de conducir, pasaporte, certificados de nacimiento, o votar en los próximos comicios cómodamente desde su casa.

En la vida cotidiana se presentan muchas situaciones en las que los ciudadanos deben acreditar fehacientemente su identidad, por ejemplo, a la hora de pagar las compras con una tarjeta de crédito en un establecimiento comercial, para votar en los

colegios electorales, con el fin de identificarse en el mostrador de una empresa, al firmar documentos notariales, etc.

En estos casos, la identificación se realiza fundamentalmente mediante la presentación de documentos acreditativos como el DNI, el pasaporte o el carnet de conducir, que contienen una serie de datos significativos vinculados al individuo que los presenta, como:

- Nombre del titular del documento.
- Número de serie que identifica el documento.
- Período de validez: fecha de expedición y de caducidad del documento, más allá de cuyos límites éste pierde validez.
- Fotografía del titular.
- Firma manuscrita del titular.
- Otros datos demográficos, como sexo, dirección, etc.

En algunos casos en los que la autenticación de la persona resulta importante, como en el pago con tarjeta de crédito, se puede exigir incluso que estampe una firma, que será comparada con la que aparece en la tarjeta y sobre su documento de identificación. En el mundo físico se produce la verificación de la identidad de la persona comparando la fotografía del documento con su propia fisonomía y en casos especialmente delicados incluso comparando su firma manuscrita con la estampada en el documento acreditativo que porta. En otras situaciones, no se requiere el DNI o pasaporte, pero sí la firma, para que el documento goce de la validez legal (cheques, cartas, etc.), ya que ésta vincula al signatario con el documento por él firmado.

Ahora bien, en un contexto electrónico, en el que no existe contacto directo entre las partes, ¿resulta posible que los usuarios de un servicio puedan presentar un documento digital que ofrezca las mismas funcionalidades que los documentos físicos, pero sin perder la seguridad y confianza de que estos últimos están dotados? La respuesta, por fortuna, es afirmativa, ya que el uso de la **firma digital** va a satisfacer los siguientes aspectos de seguridad:

Integridad de la información: la integridad del documento es una protección contra la modificación de los datos en forma intencional o accidental. El emisor protege el documento, incorporándole a ese un valor de control de integridad, que corresponde a un valor único, calculado a partir del contenido del mensaje al momento de su creación. El receptor deberá efectuar el mismo cálculo sobre el documento recibido y comparar el valor calculado con el enviado por el emisor. De coincidir, se concluye que el documento no ha sido modificado durante la transferencia.

Autenticidad del origen del mensaje: este aspecto de seguridad protege al receptor del documento, garantizándole que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo, no pudiendo alguna otra entidad suplantar a un usuario del sistema. Esto se logra mediante la inclusión en el documento transmitido de un valor de autenticación (MAC, Message autentication code). El valor depende tanto del contenido del documento como de la clave secreta en poder del emisor.

No repudio del origen: el no repudio de origen protege al receptor del documento de la negación del emisor de haberlo enviado. Este aspecto de seguridad es más fuerte que los anteriores ya que el emisor no puede negar bajo ninguna circunstancia que ha generado dicho mensaje, transformándose en un medio de prueba inequívoco respecto de la responsabilidad del usuario del sistema.

Imposibilidad de suplantación: el hecho de que la firma haya sido creada por el signatario mediante medios que mantiene bajo su propio control (su clave privada protegida, por ejemplo, por una contraseña, una tarjeta inteligente, etc.) asegura, además, la imposibilidad de su suplantación por otro individuo.

Auditabilidad: permite identificar y rastrear las operaciones llevadas a cabo por el usuario dentro de un sistema informático cuyo acceso se realiza mediante la presentación de certificados..

El acuerdo de claves secretas: garantiza la confidencialidad de la información intercambiada entre las partes, esté firmada o no, como por ejemplo en las transacciones seguras realizadas a través de SSL.

¿Qué es una firma digital?

A diferencia de la firma manuscrita, que es un trazo sobre un papel, la firma digital consiste en el agregado de un apéndice al texto original, siendo este apéndice, en definitiva, la firma digital; al conjunto formado por el documento original más la firma digital se lo denominará mensaje.

Este apéndice o firma digital es el resultado de un cálculo que se realiza sobre la cadena binaria del texto original.

En este cálculo están involucrados el documento mismo y una clave privada (que, generalmente, pertenece al sistema de clave pública-privada o sistema asimétrico) la cual es conocida sólo por el emisor o autor del mensaje, lo que da como resultado que para cada mensaje se obtenga una firma distinta, es decir, a diferencia de la firma tradicional, la firma digital cambia cada vez con cada mensaje, porque la cadena binaria de cada documento será distinta de acuerdo a su contenido.

A través de este sistema podemos garantizar completamente las siguientes propiedades de la firma tradicional:

1. Quien firma reconoce el contenido del documento, que no puede modificarse con posterioridad (integridad).

2. Quien lo recibe verifica con certeza que el documento procede del firmante. No es posible modificar la firma (autenticidad).

3. El documento firmado tiene fuerza legal. Nadie puede desconocer haber firmado un documento ante la evidencia de la firma (no repudio).

Una **firma digital** es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje. La firma digital no implica que el mensaje esté encriptado, es decir, que este no pueda ser leído por otras personas; al igual que cuando se firma un documento holográficamente este sí puede ser visualizado por otras personas.

El procedimiento utilizado para firmar digitalmente un mensaje es el siguiente: el firmante genera mediante una función matemática una huella digital del mensaje. Esta huella digital se encripta con la **clave privada** del firmante, y el resultado es lo que se denomina **firma digital** la cual se enviará adjunta al mensaje original. De esta manera el firmante va a estar adjuntando al documento una marca que es única para ese documento y que sólo él es capaz de producir.

El receptor del mensaje podrá comprobar que el mensaje no fue modificado desde su creación y que el firmante es quién dice ser a través del siguiente procedimiento: en primer término generará la huella digital del mensaje recibido, luego desencriptará la firma digital del mensaje utilizando la **clave pública** del firmante y obtendrá de esa forma la huella digital del mensaje original; si ambas huellas digitales coinciden, significa que el mensaje no fue alterado y que el firmante es quien dice ser.

La **firma digital** hace referencia, en la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, a un método criptográfico que asocia la *identidad* de una persona o de un equipo informático al mensaje o documento.

Los términos de **firma digital y firma electrónica** se utilizan con frecuencia como sinónimos, pero este uso en realidad es incorrecto.

Mientras que firma digital hace referencia a una serie de métodos criptográficos, la firma electrónica es un término de naturaleza fundamentalmente legal y más amplio desde un punto de vista técnico, ya que puede contemplar métodos no criptográficos.

Una firma electrónica es una firma digital que se ha almacenado en un soporte de hardware; mientras que la firma digital se puede almacenar tanto en soportes de hardware como de software. La firma electrónica reconocida tiene el mismo valor legal que la firma manuscrita.

De hecho, se podría decir que una firma electrónica es una firma digital contenida o almacenada en un contenedor electrónico, normalmente un chip de ROM. Su principal **característica diferenciadora** con la firma digital es su cualidad de ser inmodificable (que no es lo mismo que inviolable). No se debe confundir el almacenamiento en hardware, como por ejemplo, en un chip, con el almacenamiento de la firma digital en soportes físicos; es posible almacenar una firma digital en una memoria flash, pero al ser esta del tipo RAM y no ROM, no se consideraría una firma electrónica sino una firma digital contenida en un soporte físico.

¿Cómo se ve una firma digital?

A la vista, una firma digital se representa por una extensa e indescifrable cadena de caracteres, esta cadena representa en realidad un número que es el resultado de un procedimiento matemático aplicado al documento.

La criptografía como base de la firma digital

La firma digital se basa en la **utilización combinada de dos técnicas** distintas, que son la **criptografía asimétrica** o de clave pública para cifrar mensajes y el uso de las llamadas **funciones hash o funciones resumen**.

El diccionario de la Real Academia Española de la Lengua define la **criptografía** como "el arte de escribir con clave secreta o de forma enigmática". La criptografía es un conjunto de técnicas que mediante la utilización de algoritmos y métodos matemáticos sirven para cifrar y descifrar mensajes.

La criptografía es tan antigua como la escritura. Se dice que las primeras civilizaciones que usaron la criptografía fueron la Egipcia, la Mesopotámica, la India y la China. Pero a quien se atribuye el primer método de encriptado con su debida documentación es al general romano Julio César, quien creó un sistema simple de sustitución de letras, que consistía en escribir el documento codificado con la tercera letra que siguiera a la que realmente correspondía. La A era sustituida por la D, la B por la E y así sucesivamente.

Tradicionalmente se ha hablado de **dos tipos** de sistemas criptográficos: los simétricos o de clave privada y los asimétricos o de clave pública.

Los llamados **sistemas criptográficos simétricos** son aquellos en los que dos personas (A y B), que van a intercambiarse mensajes entre sí, utilizan ambos la misma clave para cifrar y descifrar el mensaje. Así, el emisor del mensaje (A), lo cifra utilizando una determinada clave, y una vez cifrado, lo envía a B. Recibido el mensaje, B lo descifra utilizando la misma clave que usó A para cifrarlo. Los sistemas criptográficos simétricos más utilizados son los conocidos con los nombres de DES, TDES y AES.

Los principales **inconvenientes** del sistema simétrico son los siguientes:

- La necesidad de que A (emisor) y B (receptor) se intercambien previamente por un medio seguro la clave que ambos van a utilizar para cifrar y descifrar los mensajes.
- La necesidad de que exista una clave para cada par de personas que vayan a intercambiarse mensajes cifrados entre sí.

Las dos dificultades apuntadas determinan que los sistemas de cifrado simétricos no sean aptos para ser utilizados en redes abiertas como internet, en las que confluyen una pluralidad indeterminada de personas que se desconocen entre sí y que en la mayoría de los casos no podrán intercambiarse previamente claves de cifrado por ningún medio seguro.

Los **sistemas criptográficos asimétricos o de clave pública** se basan en el cifrado de mensajes mediante la utilización de un par de claves diferentes (privada y pública), de ahí el nombre de asimétricos, que se atribuyen a una persona determinada y que tienen las siguientes características:

- Una de las claves, la privada, permanece secreta y es conocida únicamente por la persona a quien se ha atribuido el par de claves y que la va a utilizar para cifrar mensajes. La segunda clave, la pública, es o puede ser conocida por cualquiera y se utiliza para descifrar los mensajes.

- A partir de la clave pública, que es conocida o puede ser conocida por cualquiera, no se puede deducir ni obtener matemáticamente la clave privada, ya que si partiendo de la clave pública, que es puede o ser conocida por cualquier persona, se pudiese obtener la clave privada, el sistema carecería de seguridad dado que cualquiera podría utilizar la clave privada atribuida a otra persona pero obtenida ilícitamente por un tercero partiendo de la clave pública.

Este dato se basa en una característica de los números primos y en el llamado **problema de la factorización**. El problema de la factorización es la obtención a partir de un determinado producto de los factores cuya multiplicación ha dado como resultado ese producto. Los números primos (números enteros que no admiten otro divisor que no sea el 1 o ellos mismos), incluidos los números primos grandes, se caracterizan porque si se multiplica un número primo por otro número primo, da como resultado un tercer número primo a partir del cual es imposible averiguar y deducir los factores.

El criptosistema de clave pública más utilizado en la actualidad es el llamado RSA, creado en 1978 y que debe su nombre a sus tres creadores (Rivest, Shamir y Adleman).

La utilización del par de claves (privada y pública) implica que A (emisor) cifra un mensaje utilizando para ello su clave privada y, una vez cifrado, lo envía a B (receptor). B descifra el mensaje recibido utilizando la clave pública de A. Si el mensaje descifrado es legible e inteligible significa necesariamente que ese mensaje ha sido cifrado con la clave privada de A (es decir, que proviene de A) y que no ha sufrido ninguna alteración durante la transmisión de A hacia B, porque si hubiera sido alterado por un tercero, el mensaje descifrado por B con la clave pública de A no sería legible ni inteligible. Así se cumplen dos de los requisitos fundamentales, que son la **integridad** (certeza de que el mensaje no ha sido alterado) y **no repudiación** en origen (imposibilidad de que A niegue que el mensaje recibido por B ha sido cifrado por A con la clave privada de éste). El tercer requisito (identidad del emisor del mensaje) se obtiene mediante la utilización de los certificados digitales, que se analizan en otro apartado de esta guía.

Las funciones Hash

Junto a la criptografía asimétrica se utilizan en la firma digital las llamadas **funciones hash** o funciones resumen. Los mensajes que se intercambian pueden tener un gran tamaño, hecho éste que dificulta el proceso de cifrado. Por ello, no se cifra el mensaje entero sino un resumen del mismo obtenido aplicando al mensaje una función hash.

Partiendo de un mensaje determinado que puede tener cualquier tamaño, dicho mensaje se convierte mediante la función hash en un mensaje con una dimensión fija (generalmente de 160 bits). Para ello, el mensaje originario se divide en varias partes cada una de las cuales tendrá ese tamaño de 160 bits, y una vez dividido se combinan elementos tomados de cada una de las partes resultantes de la división para formar el mensaje-resumen o hash, que también tendrá una dimensión fija y constante de 160 bits. Este resumen de dimensión fija es el que se cifrará utilizando la clave privada del emisor del mensaje.

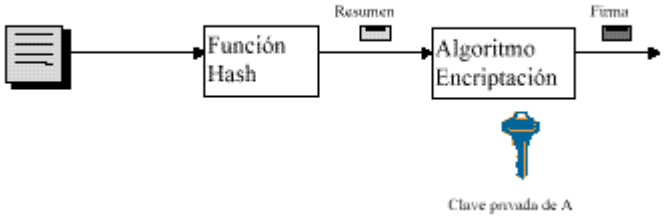
Los sellos temporales

Finalmente, en el proceso de intercambio de mensajes electrónicos es importante que, además de los elementos o requisitos anteriormente analizados, pueda saberse y establecerse con certeza la fecha exacta en la que los mensajes han sido enviados. Esta característica se consigue mediante los llamados **sellos temporales** o "time stamping", que es aquella función atribuida generalmente a los Prestadores de Servicios de Certificación mediante la cual se fija la fecha de los mensajes electrónicos firmados digitalmente.

Funcionamiento de la Firma Digital

La firma digital de un documento no es un passwords, es el resultado de aplicar cierto algoritmo matemático, denominado función hash, al contenido. Esta función asocia un valor dentro de un conjunto finito (generalmente los números naturales) a su entrada.

Cuando la entrada es un documento, el resultado de la función es un número que identifica casi unívocamente al texto. Si se adjunta este número al texto, el destinatario puede aplicar de nuevo la función y comprobar su resultado con el que ha recibido.



Numerando

Para poder realizar una firma digital, es necesario primero convertir el mensaje en un Número. Este Número es entregado a la función de *Hash*, que produce el resumen del mensaje. Esta función convierte un número grande (el mensaje) en un número pequeño (el resumen).

Para que esto funcione, no debería ser sencillo encontrar dos mensajes que produjeran el mismo resumen. Si se pudiera hacer, podrías cambiar el mensaje correspondiente a una firma, como aquel banco que cambió páginas internas del contrato.

El número pequeño del resumen suele tener una longitud de 128 bits (MD5·), o de 160 bits (SHA-1·). Cada BIT puede ser tanto un "0" como un "1". Por lo tanto existen 2 elevado a 128 posibles resúmenes de 128 bits de largo, o 2 elevado a 160 resúmenes de 160 bits.

Ahora bien, el proceso de obtención del resumen a partir del mensaje debe ser determinístico. Debe ser repetible. El mismo mensaje siempre debe dar el mismo resumen. Si no, el proceso de verificación no funcionaría.

Pero, al mismo tiempo, la salida de la función de *hash* debe parecer aleatoria. Debería resultar imposible obtener el mensaje a partir del resumen. De otra manera, alguien podría obtener varios mensajes que tendrían el mismo resumen.

Para que una función de *hash* sea buena, debe ser una función unidireccional. Debe funcionar en un sentido, pero no en el contrario. Además debe ser muy difícil encontrar dos mensajes diferentes que produzcan el mismo resumen.

Cuando ya dispone del resumen del mensaje, el número pequeño, debe firmarlo (cifrarlo). Esto también involucra una transformación matemática.

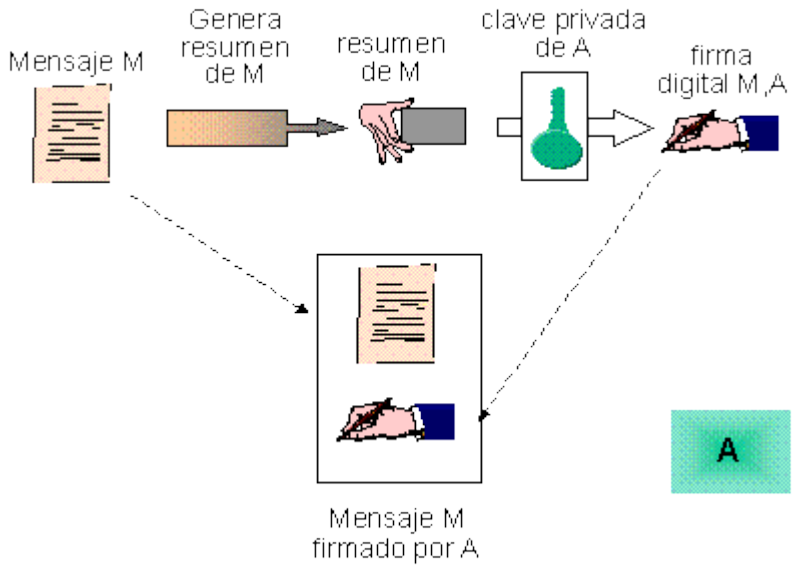
Un algoritmo efectivo debe hacer uso de un sistema de clave pública para cifrar sólo la firma. En particular, el valor "hash" se cifra mediante el uso de la clave privada del firmante, de modo que cualquiera pueda comprobar la firma usando la clave pública correspondiente. El documento firmado se puede enviar usando cualquier otro algoritmo de cifrado, o incluso ninguno si es un documento público.

El Digital Signature Algorithm es un algoritmo de firmado de clave pública que funciona como hemos descrito. DSA es el algoritmo principal de firmado que se usa en GnuPG.

El proceso de firma es el siguiente:

- El usuario prepara el mensaje a enviar.
- El usuario utiliza una función hash segura para producir un resumen del mensaje.
- El remitente encripta el resumen con su clave privada. La clave privada es aplicada al texto del resumen usando un algoritmo matemático. La firma digital consiste en la encriptación del resumen.
- El remitente une su firma digital a los datos.
- El remitente envía electrónicamente la firma digital y el mensaje original al destinatario. El mensaje puede estar encriptado, pero esto es independiente del proceso de firma.

- El destinatario usa la clave pública del remitente para verificar la firma digital, es decir para desencriptar el resumen adosado al mensaje.
- El destinatario realiza un resumen del mensaje utilizando la misma función resumen segura.
- El destinatario compara los dos resúmenes. Si los dos son exactamente iguales el destinatario sabe que los datos no han sido alterados desde que fueron firmados.



¿Dónde puede obtener una persona el par de claves?

La generación del par de claves (pública y privada) es un proceso sencillo, pero que requiere de precauciones especiales. Cuando se crea el par, una de las claves, que es en realidad una secuencia muy larga de números, es designada como clave privada, o sea la que en el futuro se empleará para firmar los mensajes, por ello su almacenamiento requiere máxima seguridad debido a que no debe ser conocida ni utilizada por nadie, excepto por su titular (quien la generó). En consecuencia, la clave privada se encripta y protege mediante una contraseña y se la guarda en un disco, diskette o, idealmente, en una tarjeta inteligente.

La clave pública, en cambio, debe ser conocida por todos por tal motivo es enviada a una **Autoridad Certificante** (que actúa como tercera parte confiable), quien la incluye en un **certificado digital**.

Un **certificado digital** es un archivo electrónico que tiene un tamaño máximo de 2 Kilobytes y que contiene los datos de identificación personal del emisor de los mensajes, la clave pública de este y la firma privada del propio Prestador de Servicios de Certificación. Ese archivo electrónico es cifrado por la entidad Prestadora de Servicios de Certificación con la clave privada de ésta.

Los certificados digitales tienen una **duración determinada**, transcurrida la cual deben ser renovados, y pueden ser revocados anticipadamente en ciertos supuestos (por ejemplo, en el caso de que la clave privada, que debe permanecer secreta, haya pasado a ser conocida por terceras personas no autorizadas para usarla).

Gracias al certificado digital, el par de claves obtenido por una persona estará siempre vinculado a una determinada identidad personal, y si sabemos que el mensaje ha sido cifrado con la clave privada de esa persona, sabremos también quién es la persona titular de esa clave privada.

Como podemos ver, a diferencia de la firma autógrafa, que es de libre creación por cada individuo y no necesita ser autorizada por nadie ni registrada en ninguna parte para ser utilizada, la firma digital, y más concretamente el par de claves que se utilizan para firmar digitalmente los mensajes, no pueden ser creados libremente por cada individuo.

En principio, cualquier persona puede dirigirse a una empresa informática que cuente con los dispositivos necesarios para generar el par de claves y solicitar la creación de dicho par de claves, o incluso puede generar ella misma el par de claves, si cuenta con los dispositivos necesarios. Posteriormente, con el par de claves creado para una persona determinada, ésta se dirigiría a un Prestador de Servicios de Certificación para obtener el certificado digital correspondiente a ese par de claves.

Sin embargo, en la práctica los Prestadores de Servicios de Certificación cumplen ambas funciones: crean el par de claves (pública y privada) para una persona y expiden el certificado digital correspondiente a ese par de claves.

En resumen, ¿cómo obtengo el dispositivo para firmar digitalmente un mensaje?

El **proceso de obtención** de los elementos que necesito para firmar digitalmente mensajes (par de claves y certificado digital) es el siguiente:

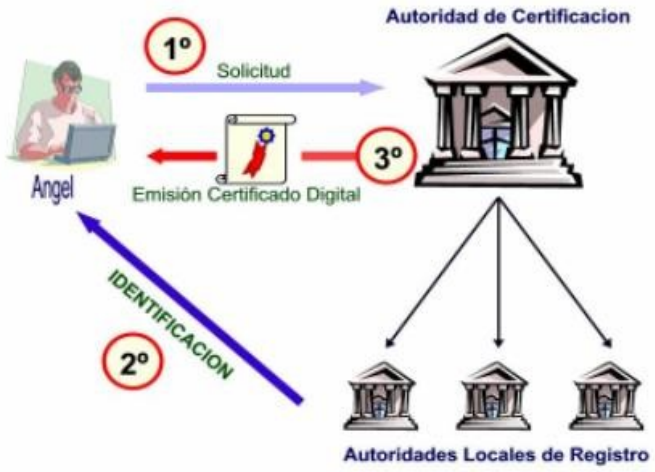
1º).- Me dirijo a una empresa o entidad que tenga el carácter de Prestador de Servicios de Certificación y solicito de ellos el par de claves y el certificado digital correspondiente a las mismas. Generalmente, podré acudir a dicha entidad bien personalmente o por medio de internet utilizando la página web del Prestador de Servicios de Certificación.

2º).- El prestador de Servicios de Certificación comprobará mi identidad, bien directamente o por medio de entidades colaboradoras (Autoridades Locales de Registro), para lo cual deberé exhibirle mi D.N.I. y si soy el representante de una sociedad (administrador, apoderado, etc.) o de cualquier otra persona jurídica, deberé acreditar documentalmente mi cargo y mis facultades.

3º).- El prestador de Servicios de Certificación crea con los dispositivos técnicos adecuados el par de claves pública y privada y genera el certificado digital correspondiente a esas claves.

4º).- El prestador de Servicios de Certificación me entrega una tarjeta semejante a una tarjeta de crédito que tiene una banda magnética en la que están gravados tanto el par de claves como el certificado digital. El acceso al par de claves y al certificado digital gravados en la tarjeta está protegido mediante una clave como las que se utilizan en las tarjetas de crédito o en las tarjetas de cajero automático. En otras ocasiones, en lugar de la tarjeta el Prestador de Servicios de Certificación deja almacenado el certificado digital en su propia página web, a fin de que el destinatario copie el archivo y lo instale en su ordenador.

5º).- Con esa tarjeta magnética y un lector de bandas magnéticas adecuado conectado a mi ordenador personal, podré leer y utilizar la información gravada en la tarjeta para firmar digitalmente los mensajes electrónicos que envíe a otras personas.



Un ejemplo práctico de cómo usar la Firma Digital:

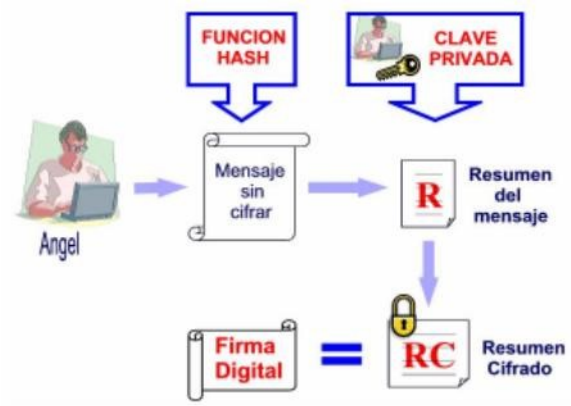
El proceso de firma digital de un mensaje electrónico comprende en realidad dos procesos sucesivos: la firma del mensaje por el emisor del mismo y la verificación de la firma por el receptor del mensaje. Esos dos procesos tienen lugar de la manera que se expresa a continuación, en la que el emisor del mensaje es designado como **Angel** y el receptor del mensaje es designado como **Blanca**:

Firma digital de un mensaje electrónico

1º.- Angel (emisor) crea o **redacta un mensaje** electrónico determinado (por ejemplo, una propuesta comercial).

2º.- El emisor (Angel) aplica a ese mensaje electrónico una **función hash** (algoritmo), mediante la cual obtiene un resumen de ese mensaje.

3º.- El emisor (Angel) **cifra ese mensaje-resumen** utilizando su clave privada.



4º.- Angel envía a **Blanca** (receptor) un correo electrónico que contiene los siguientes elementos:

- El **cuerpo** del mensaje, que es el mensaje en claro (es decir, sin cifrar). Si se desea mantener la confidencialidad del mensaje, éste se cifra también pero utilizando la clave pública de Blanca (receptor).

- La **firma** del mensaje, que a su vez se compone de dos elementos:
    - El hash o mensaje-resumen cifrado con la clave privada de Angel.

- El certificado digital de Angel, que contiene sus datos personales y su clave pública, y que está cifrado con la clave privada del Prestador de Servicios de Certificación.

Verificación por el receptor de la firma digital del mensaje

1º.- Blanca (receptor) recibe el correo electrónico que contiene todos los elementos mencionados anteriormente.

2º.- Blanca en primer lugar **descifra el certificado digital** de Angel, incluido en el correo electrónico, utilizando para ello la clave pública del Prestador de Servicios de Certificación que ha expedido dicho certificado. Esa clave pública la tomará Blanca, por ejemplo, de la página web del Prestador de Servicios de Certificación en la que existirá depositada dicha clave pública a disposición de todos los interesados.

3º.- Una vez descifrado el certificado, Blanca podrá acceder a la clave pública de Angel, que era uno de los elementos contenidos en dicho certificado. Además podrá saber a quién corresponde dicha clave pública, dado que los datos personales del titular de la clave (Angel) constan también en el certificado.

4º.- Blanca utilizará la clave pública del emisor (Angel) obtenida del certificado digital para **descifrar el hash** o mensaje-resumen creado por **Angel**.

5º.- Blanca **aplicará al cuerpo del mensaje**, que aparece en claro o no cifrado, que también figura en el correo electrónico recibido, la misma **función hash** que utilizó **Angel** con anterioridad, obteniendo igualmente **Blanca** un mensaje-resumen. Si el cuerpo del mensaje también ha sido cifrado para garantizar la confidencialidad del mismo, previamente **Blanca** deberá descifrarlo utilizando para ello su propia clave

privada (recordemos que el cuerpo del mensaje había sido cifrado con la clave pública de **Blanca**)

6º.- Blanca comparará el mensaje-resumen o hash recibido de **Angel** con el mensaje-resumen o hash obtenido por ellal misma. Si ambos mensajes-resumen o hash coinciden totalmente significa lo siguiente:

- El mensaje no ha sufrido alteración durante su transmisión, es decir, es íntegro o auténtico.
- El mensaje-resumen descifrado por Blanca con la clave pública de Angel ha sido necesariamente cifrado con la clave privada de Angel y, por tanto, proviene necesariamente de Angel.
- Como el certificado digital nos dice quién es Angel, podemos concluir que el mensaje ha sido firmado digitalmente por Angel, siendo Angel una persona con identidad determinada y conocida.

Por el contrario, si los mensajes-resumen no coinciden quiere decir que el mensaje ha sido alterado por un tercero durante el proceso de transmisión, y si el mensaje-resumen descifrado por Blanca es ininteligible quiere decir que no ha sido cifrado con la clave privada de Angel. En resumen, que el mensaje no es auténtico o que el mensaje no ha sido firmado por Angel sino por otra persona.

Finalmente, hay que tener en cuenta que las distintas fases del proceso de firma y verificación de una firma digital que han sido descritas no se producen de manera manual sino automática e instantánea, por el simple hecho de introducir la correspondiente tarjeta magnética en el lector de tarjetas de nuestro ordenador y activar el procedimiento.

Aplicaciones de la Firma Digital

La firma digital se puede aplicar en las siguientes situaciones:

a). E-mail,

¿Cómo firmar un correo electrónico? :

Si ya posee un certificado y desea firmar digitalmente un correo electrónico, proceda de la siguiente forma (de lo contrario, debe contactarse para gestionarlo con una Autoridad Certificante):

1. Abra el programa que utiliza para enviar sus correos electrónicos. Siga el procedimiento habitual para escribir el mensaje que desea enviar. A continuación, efectúe los pasos que se indican según el cliente de correo que Ud. utilice:

Si utiliza Netscape Navigator:	Si utiliza Outlook Express:
Presione el botón de Opciones (Options) y haga click en la casilla de verificación Firmado (Signed).	En el extremo derecho de la segunda fila de instrucciones observará dos iconos similares. Haga un click en el que representa un sobre con una "cinta roja" o se puede ir al menú de Herramientas (Tools) y luego ir a Firmar mensaje digitalmente (Digitally Sign).

2. Presione el botón Enviar (Send)
3. Por último, ingrese su palabra clave a fin de firmar el mensaje y luego haga un click en Aceptar (OK) para enviar el mensaje firmado.

b). Contratos electrónicos

c). Procesos de aplicaciones electrónicos

d). Formas de procesamiento automatizado

e). Transacciones realizadas desde financieras alejadas

f). Transferencia en sistemas electrónicos, por ejemplo si se quiere enviar un mensaje para transferir $100.000 de una cuenta a otra. Si el mensaje se quiere pasar sobre una red no protegida, es muy posible que algún adversario quiera alterar el mensaje tratando de cambiar los $100.000 por 1.000.000, con esta información adicional no se podrá verificar la firma lo cual indicará que ha sido alterada y por lo tanto se denegará la transacción

g). En aplicaciones de negocios, un ejemplo es el Electronic Data Interchange (EDI) intercambio electrónico de datos de computadora a computadora intercambiando mensajes que representan documentos de negocios

h). En sistemas legislativos, es a menudo necesario poner un grupo fecha / hora a un documento para indicar la fecha y la hora en las cuales el documento fue ejecutado o llegó a ser eficaz. Un grupo fecha / hora electrónico se podría poner a los documentos en forma electrónica y entonces firmado usando al DSA o al RSA. Aplicando cualquiera de los dos algoritmos al documento protegería y verificaría la integridad del documento y de su grupo fecha / hora.

Situación en algunos Países:

1. Firma Digital en Alemania

En Alemania la firma digital es un sello integrado en datos digitales, creado con una clave privada que permite identificar al propietario de la firma y comprobar que los datos no han sido alterados.

El marco común de firma electrónica de la Unión Europea

El mercado interior de la Unión Europea implica un espacio sin fronteras interiores en el que está garantizada la libre circulación de mercancías. Deben satisfacerse los requisitos esenciales específicos de los productos de firma electrónica a fin de garantizar la libre circulación en el mercado interior y fomentar la confianza en la firma electrónica.

En ese sentido la Directiva 1999/93/CE sienta un marco común para la firma electrónica que se concretó con la transposición de la Directiva a las diferentes legislaciones nacionales de los países miembros.

2. Firma Digital en Naciones Unidas

En las Naciones Unidas una firma digital o numérica es un valor numérico que se consigna en un mensaje de datos y que, gracias al empleo de un procedimiento matemático conocido y vinculado a la clave criptográfica privada del originante, logra identificar que dicho valor se ha obtenido exclusivamente con la clave privada de iniciador del mensaje.

Los procedimientos matemáticos utilizados para generar firmas numéricas autorizadas, se basan en el cifrado de la clave pública. Estos procedimientos aplicados a un mensaje de datos, operan una transformación del mensaje a fin que el receptor del mensaje y poseedor de la clave pública del originante pueda establecer:

- Si la transformación se efectuó utilizando la clave criptográfica privada que corresponde a la clave pública que él tiene como válida.
- Si el mensaje inicial ha sido modificado.

3. Firma Digital en E.E.U.U.

En los Estados Unidos podemos observar la sanción de diferentes leyes relativas a la firma digital, para la creación de una infraestructura de firma digital que asegure la integridad y autenticidad de las transacciones efectuadas en el ámbito gubernamental y en su relación con el sector privado:

- Iniciativa del Gobierno Federal:

- Proyecto "Gatekeeper": Prevé la creación de una autoridad pública que administre dicha infraestructura y acredite a los certificadores de clave pública;

- En el área de telecomunicaciones: Régimen voluntario de declaración previa para los certificadores de clave pública;

- Ley de certificadores de clave pública relacionados con la firma digital;

- Proyecto de Ley sobre la utilización de la firma digital en los ámbitos de la seguridad social y la salud pública;

- Ley sobre creación, archivo y utilización de documentos electrónicos;

- Ley sobre intercambio electrónico de datos en la administración y los procedimientos judiciales administrativos;

- Iniciativa sobre la creación de una infraestructura de clave pública para el comercio electrónico;

- Ley que autoriza la utilización de documentación electrónica en la comunicación entre las agencias gubernamentales y los ciudadanos, otorgando a la firma digital igual validez que la firma manuscrita. (Ley Gubernamental de Reducción de la Utilización de Papel - "Government Paperwork Elimination Act");

- Ley que promueve la utilización de documentación electrónica para la remisión de declaraciones del impuesto a las ganancias;

- Proyecto piloto del IRS (Dirección de Rentas - "Internal Revenue Service") para promover la utilización de la firma digital en las declaraciones impositivas;

- Proyecto de Ley de Firma Digital y Autenticación Electrónica para facilitar el uso de tecnologías de autenticación electrónica por instituciones financieras;

- Proyecto de Ley que promueve el reconocimiento de técnicas de autenticación electrónica como alternativa válida en toda comunicación electrónica en el ámbito público o privado;

- Resolución de la Reserva Federal regulando las transferencias electrónicas de fondos;

- Resolución de la FDA (Administración de Alimentos y Medicamentos - "Food and Drug Administration") reconociendo la validez de la utilización de la firma electrónica como equivalente a la firma manuscrita;

- Iniciativa del Departamento de Salud proponiendo la utilización de la firma digital en la transmisión electrónica de datos en su jurisdicción;

- Iniciativa del Departamento del Tesoro aceptando la recepción de solicitudes de compra de bonos del gobierno firmadas digitalmente;

- Iniciativas de los Gobiernos Estatales:

- Casi todos los estados tienen legislación, aprobada o en Proyecto, referida a la firma digital. En algunos casos, las regulaciones se extienden a cualquier comunicación electrónica pública o privada. En otros, se limitan a algunos actos internos de la administración estatal o a algunas comunicaciones con los ciudadanos.

- Se destaca la Ley de Firma Digital del Estado de Utah, que fue el primer estado en legislar el uso comercial de la firma digital. Regula la utilización de criptografía asimétrica y fue diseñada para ser compatible con varios estándares internacionales. Prevé la creación de certificadores de clave pública licenciados por el Departamento de Comercio del estado. Además, protege la propiedad exclusiva de la clave privada del suscriptor del certificado, por lo que su uso no autorizado queda sujeto a responsabilidades civiles y criminales.

- Proyecto piloto de desarrollo de infraestructura de firma digital;

- Normativa fiscal que prevé la presentación digital de la declaración de ingresos.

4. Firma Digital en Argentina

El 24 de marzo de 1997 se publica en el Boletín Oficial, la resolución No. 45/97 de la Secretaría de la Función Pública, que constituye la primera norma nacional que introdujo en el derecho argentino un marco normativo para la incorporación de la tecnología de firma digital en los procesos de información del sector público.

Esta norma tiene por finalidad contemplar estándares tecnológicos de mínima que aseguren la determinación de la autoría de la firma digital y la inalterabilidad del contenido del documento digital suscrito. Esto se logra mediante el cumplimiento de una serie de requisitos, que establece, y que deben ser entendidos como pautas o guías para el caso que se decida dictar una regulación que contemple esta tecnología.

5. Ley sobre firma electrónica en Chile

Se publica el 15 de septiembre del año 2003 por el Ministerio Secretaría General de la Presidencia, la Ley 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma, reconoce que los órganos del Estado podrán

ejecutar o realizar actos, celebrar contratos y expedir cualquier documento, dentro de su ámbito de competencia, suscribiéndolos por medio de firma electrónica simple. Igualmente señala que estos actos, contratos y documentos, suscritos mediante firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los expedidos en soporte de papel.

6. Firma Digital en Costa Rica

En Costa Rica, la Ley de Certificados, Firmas Digitales y Documentos Electrónicos (Ley 8454) es firmada el 22 de agosto del 2005. Esta Ley faculta la posibilidad de vincular jurídicamente a los actores que participan en transacciones electrónicas, lo que permite llevar al mundo virtual transacciones o procesos que anteriormente requerían el uso de documentos físicos para tener validez jurídica, bajo el precepto de presunción de autoría y responsabilidad, además lo anterior sin demérito del cumplimiento de los requisitos de las formalidades legales según negocio jurídico.

7. La ley de firma electrónica en España

En España existe la Ley 59/2003, de Firma electrónica, que define tres tipos de firma:

- **Simple**. Datos que puedan ser usados para identificar al firmante (autenticidad)

- **Avanzada**. Además de identificar al firmante permite garantizar la integridad del documento y la integridad de la clave usada, utilizando para ello un DSCF (dispositivo seguro de creación de firma, el DNI electrónico). Se emplean técnicas de PKI.

- **Reconocida**. Es la firma avanzada y amparada por un certificado reconocido (certificado que se otorga tras la verificación presencial de la identidad del firmante). En ocasiones, esta firma se denomina *cualificada* por traducción del término inglés *qualified* que aparece en la Directiva Europea de Firma Electrónica.

8. Firma Electrónica en Guatemala

En Guatemala, la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas (Decreto 47-2008), fue publicada en el diario oficial el 23 de septiembre de 2008. El Ministerio de Economía de ese país tiene bajo su responsabilidad el regular este tema, y abrió en el mes de Junio de 2009 el Registro de Prestadores de Servicios de Certificación, publicando su sitio web con copia de la ley e información importante sobre el tema.

9. Firma Digital en Nicaragua

El 2 de julio de 2010 se aprobó en Nicaragua la Ley de Firma Electrónica[5] , siendo la Dirección General de Tecnología, adscrita al Ministerio de Hacienda y Crédito Público, la entidad acreditadora de la firma electrónica.

10. La Ley de firma digital en Perú

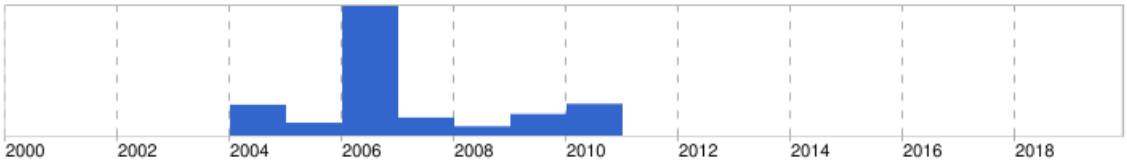
En el Perú se ha dictado la Ley de Firmas y Certificados Digitales (Ley 27269), la cual regula la utilización de la firma electrónica, otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.

Situación de la Firma Digital en el Paraguay:

Con la explosión de Internet en el mundo, a principios de los años 90 comenzó una revolución en la forma de comunicación entre personas, entidades, etc. Se hizo palpable el fin de la era Industrial, comenzó otra, la era de la Información, la era del conocimiento. Internet, al ser un medio de fácil y creciente uso para todo tipo de comunicación se utiliza inclusive para las transacciones comerciales digitales. Esto llevó a diversos países a generar nuevas estructuras legales o al menos a actualizarlas.

Desde finales de la década de los 90, países como EEUU, (a la cabeza), comenzaron este proceso. Nuestro país no estuvo al margen aunque entre 5 y 8 años atrás. En el año 2003 con la ley 2051/03 que establece el Sistema de Contrataciones del Sector Público se le otorga a la nueva dependencia la responsabilidad de crear, operar y mantener un sistema de certificación de medios de identificación electrónica. Con esto la entonces UCNT, hoy DNCP; tuvo el respaldo legal para operar un sistema de certificados digitales. Esto se hizo realidad a finales del 2007. Este esfuerzo no se desarrolló completamente, no se amplió el espectro de influencia del sistema, por la falta de una ley marco que reglamente la firma electrónica y la firma digital.

Fíjense en esta búsqueda en google;



En noticias y/o eventos sobre este tema en sitios paraguayos vemos que las primeras referencias sobre firma digital aparecen en el año 2004, aunque el estamento técnico ya tenía noción desde mediados de los 90. Desde ese año se crearon diversas iniciativas que apuntaban a plantear un anteproyecto de ley, varias instituciones plantearon estos anteproyectos, motivados por un grupo de abogados. Inclusive en el 2006 se tuvo un primer anteproyecto de ley de firma digital con media sanción por parte de diputados, pero no llegó al senado porque algunos senadores creían que la firma digital era la firma física scaneada. Analfabetos digitales dirigiendo nuestros destinos.

El último y más nuevo de todos es un anteproyecto generado a partir de una iniciativa del Ministerio de Industria y Comercio (Proyecto de ley Nº 4017), con el cual inclusive se abrió un debate con diversos actores sociales interesados en la creación de esta ley. Se incluyó a los escribanos en este debate, estamento que en todos los países de la región fue reticente a la sanción de este tipo de ley que reglamente el uso de este tipo de tecnología.

Un anteproyecto muy parecido es introducido a la comisión de Ciencia y Tecnología por un representante del ala más retrógrada de diputados. Realismo mágico en acción al estilo Paraguay.

El resultado de todo este proceso es el decreto 4711 del 15 de julio de este año que veta totalmente el proyecto de ley No. 4017.

El punto crítico es quién la administrará. En la Ley aprobada por el congreso colocan como ariete al **INTN** y en el veto del ejecutivo esgrimen que el **MIC** debe hacer ese trabajo sucio, en el proyecto original estaba así, con el MIC a la cabeza pero senadores lo modificó. En los países serios, lo hacen organismos puntuales y no administraciones con grandes estructuras que lo único que harán será inyectar burocracia innecesaria a la logística diaria.

Finalmente, **Industria y Comercio tendrá a su cargo aplicar la firma digital la normativa volverá a su curso original para su promulgación definitiva.**

La Cámara de Diputados decidió rechazar por unanimidad el veto total del Ejecutivo al proyecto de ley que otorga validez jurídica a la firma digital, los mensajes de datos y el expediente electrónico.

"Estamos trabajando de común acuerdo con el Ejecutivo y acordamos levantar el veto. El compromiso es corregir la autoridad de aplicación e inmediatamente sancionar la ley", indicó el diputado oviedista David Ocampos, uno de los patrocinadores de la normativa Nº 4.017/10.

El parlamentario sostuvo que el MIC será la autoridad de aplicación encargada (con la ratificación hecha del proyecto original).

La función que cumplirá entonces la cartera de Industria y Comercio será la de dictar las normas reglamentarias y de aplicación de la presente ley: establecer los estándares tecnológicos y operativos de la implementación; autorizar, conforme a la reglamentación expedida por el Poder Ejecutivo, la operación de entidades de certificación en el territorio nacional, entre otros aspectos.

APLICACIONES

Con la firma digital se logra la validez jurídica a la rúbrica electrónica, mensajes de datos y expedientes remitidos vía internet en las gestiones de distintas naturalezas (bancarias, personales, judiciales, institucionales, compras, ventas, etc.).

Según la Cámara Paraguaya de Internet (Capadi), el nivel de seguridad es igual al de las tarjetas de créditos, débitos y de datos biométricos con lector láser. Es como un password o PIN (contraseña) que se hace hoy en día con las tarjetas. Este proceso "va a forzar a la banca electrónica a ajustar lo que es el e-comercio para las transacciones desde un SMS, un correo electrónico u otra plataforma electrónica", según su presidente, Rubén Irala.

Por su parte, el diputado Sebastián Acha expresó que los parlamentarios no pueden permitirse no impulsar un adelanto tan importante como la utilización de las firmas y los expedientes digitales que serán de uso gradual y optativo.

El documento indica que la ley reconoce la validez jurídica de la firma digital, los mensajes de datos, el expediente electrónico y regula la utilización de los mismos, las empresas certificadoras, su habilitación y la prestación de los servicios de certificación. Igualmente indica que los datos de creación de firma digital son los datos únicos que el firmante utiliza para crearla y están contenidos en una clave privada que es generada por un proceso matemático.

1. Leyes Vigentes.

Ley 2051/03 que establece el Sistema de Contrataciones del Sector Público otorga a esta nueva dependencia la responsabilidad de crear, operar y mantener un sistema de certificación de medios de identificación electrónica.

Esta ley fue aprobada en 2003. Con esto la entonces UCNT, hoy DNCP; tuvo el respaldo legal para operar un sistema de certificados digitales. Esto se hizo realidad a finales del 2007. Este esfuerzo no se desarrolló completamente, no se amplió el espectro de influencia del sistema, por la falta de una ley marco que reglamente la firma electrónica y la firma digital; La cual actualmente se encuentra a pasos de ser aprobada.

2. Leyes en tratamiento.

Como se podrá observar más adelante, actualmente se encuentran en tratamiento tan solo tres proyectos de ley referentes a La Firma Digital. Y de estos tres; dos, el item 1 y el item 3 (ver tabla siguiente), se encuentran en etapas muy prematuras por lo que su aprobación sin duda requerirá de al menos un año más.

El único proyecto de ley que se encontraba en una etapa bien avanzada, el item 2 “DE VALIDEZ JURIDICA DE LA FIRMA DIGITAL, LOS MENSAJES DE DATOS Y LOS EXPEDIENTES ELECTRONICOS” (ver tabla siguiente) , fue aprobado tanto por la Cámara de Senadores como por la Cámara de Diputados (donde se produjo la iniciativa) y ya nada más requería, para su promulgación, de la aprobación del Poder Ejecutivo.

Sin embargo esto no ocurrió; El Presidente de la República por medio del decreto 4711 (que también se encuentra entre los documentos adjuntos), veto este proyecto de Ley devolviéndolo al Poder Legislativo.

A pesar de esto la Ley todavía puede llegar a ser promulgada pero solamente logrando ¾ de los votos tanto en Cámara de Senadores como en Cámara de Diputados. Si esto no ocurre el Proyecto de Ley no puede volver a ser tratado hasta el año siguiente.

Y finalmente esto es lo que, aparentemente va a suceder ya que según el diputado oviedista David Ocampos, uno de los patrocinadores de la normativa Nº 4.017/10: La Cámara de Diputados esta trabajando de común acuerdo con el Ejecutivo, con el cual se acordó levantar el veto. El compromiso es corregir la autoridad de aplicación e inmediatamente sancionar la ley, con esto, el Ministerio de Industria y

Comercio (MIC) tendrá a su cargo aplicar la firma digital la normativa volverá a su curso original para su promulgación definitiva .

Item	Fecha	Expediente	Acápite	Etapa / Subetapa
1.	11/02/2010	S-107470	Proyecto de Ley: "Que autoriza el uso del expediente digital, la firma digital y las notificaciones electrónicas en todos los procesos promovidos ante el Poder Judicial", presentado por el Poder Judicial - Corte Suprema de Justicia, según nota N° 273 de fecha 10 de febrero de 2010.	**Primer trámite constitucional** Dictamen de comision .
2.	21/05/2009	D-0913467	DE VALIDEZ JURIDICA DE LA FIRMA DIGITAL, LOS MENSAJES DE DATOS Y LOS EXPEDIENTES ELECTRONICOS	**Discusion Veto Total en CO** Discusion Plenario (Veto Total en CO) .
3.	02/05/2005	50175	Mensaje Nº 252 del Poder Ejecutivo, vía Ministerio de Hacienda, de fecha 29 de abril del 2005, por el cual remite el Proyecto de Ley *De Firma Digital(El Proyecto tiene como objetivo transparentar y agilizar los trámites en los procesos de contrataciones del Estado - Unidad Central Normativa y Técnica UCNT).Estado - Unidad Central Normativa y Técnica UCNT).	**Primer trámite constitucional** Discusion plenario .

1. Datos del Proyecto

Cámara:	CAMARA DE SENADORES
Tipo de Proyecto:	Proyecto de ley
Iniciativa:	Corte Suprema
Expediente:	S-107470
Fecha:	11/02/2010
Nro. Mensaje:	
Acápite:	Proyecto de Ley: "Que autoriza el uso del expediente digital, la firma digital y las notificaciones electrónicas en todos los procesos promovidos ante el Poder Judicial", presentado por el Poder Judicial - Corte Suprema de Justicia, según nota N° 273 de fecha 10 de febrero de 2010.
Iniciativa:	Archivo adjunto: Proyecto3277

1. Etapa de la Tramitación

Etapa:	1. Primer trámite constitucional
Subetapa:	3. Dictamen de comision

2. Datos del Proyecto

Cámara:	CAMARA DE DIPUTADOS
Tipo de Proyecto:	Proyecto de ley
Iniciativa:	Parlamentaria
Expediente:	D-0913467
Fecha:	21/05/2009
Nro. Mensaje:	
Acápite:	DE VALIDEZ JURIDICA DE LA FIRMA DIGITAL, LOS MENSAJES DE DATOS Y LOS EXPEDIENTES ELECTRONICOS
Iniciativa:	Archivo adjunto: ProyectoResuelto2677

2.Etapa de la Tramitación

Etapa:	17. Discusion Veto Total en CO
Subetapa:	33. Discusion Plenario (Veto Total en CO)

3. Datos del Proyecto

Cámara:	CAMARA DE SENADORES
Tipo de Proyecto:	Proyecto de ley
Iniciativa:	Poder Ejecutivo
Expediente:	50175
Fecha:	02/05/2005
Nro. Mensaje:	
Acápite:	Mensaje Nº 252 del Poder Ejecutivo, vía Ministerio de Hacienda, de fecha 29 de abril del 2005, por el cual remite el Proyecto de Ley *De Firma Digital*. (El Proyecto tiene como objetivo transparentar y agilizar los trámites en los procesos de contrataciones del Estado - Unidad Central Normativa y Técnica UCNT).
Iniciativa:	**Archivo adjunto: Proyecto217**

3. Etapa de la Tramitación

Etapa:	1. Primer trámite constitucional
Subetapa:	4. Discusion plenario

Seguimiento al Proyecto de ley 4017/03: DE VALIDEZ JURIDICA DE LA FIRMA DIGITAL, LOS MENSAJES DE DATOS Y LOS EXPEDIENTES ELECTRONICOS

Tramitación

Sesión	Fecha	Etapa	SubEtapa	Documento
	21/05/09	Primer trámite constitucional C.Diputados	Ingreso de proyecto ----------	
54	28/05/09	Primer trámite constitucional C.Diputados	Entrada de proyecto Pasa a Comisión Asuntos Constitucionales, a Comisión Ciencia y Tecnología y a Comisión Legislación y Codificación ----------	
60	24/06/09	Primer trámite constitucional C.Diputados	Dictamen de comision Ciencia y Tecnología ->Aprueba ---------- - González Segovia ,Jorge Dario - Ocampos Negreiros ,Hector David - Ortega ,Dionisio - Oviedo Verdún ,Cesar Ariel - Retamozo Ortíz ,Andres - Rios Ojeda ,Victor	
65	16/07/09	Primer trámite constitucional C.Diputados	Discusion plenario Aprobado ----------	
	30/07/09	Primer trámite constitucional C.Diputados	Media sancion ----------	Res. Proy. Msg.
57	30/07/09	Segundo trámite constitucional Senado	Entrada de proyecto Pasa a Comisión Hacienda, Presupuesto y Cuentas y a Comisión Legislación, Codificación, Justicia y Trabajo ----------	
	20/10/09	Segundo trámite constitucional Senado	Dictamen de comision Hacienda, Presupuesto y Cuentas ->Modifica ---------- - Jaeggli Caballero ,Alfredo Luís - González Safstrand ,Marcial	

			- Gómez Verlangieri ,Ramón - Denis Sánchez ,Amancio Oscar	
	21/10/09	Segundo trámite constitucional Senado	Dictamen de comision Legislación, Codificación, Justicia y Trabajo ->Modifica ---------- - Duarte Manzoni ,Marcelo Alberto Diego - Estigarribia Gutierrez ,Hugo Esteban - Fonseca Legal ,Blanca Beatríz - Guastella Capello ,José Abel	
72	22/10/09	Segundo trámite constitucional Senado	Discusion plenario Aprobado con modificaciones ----------	
	22/10/09	Segundo trámite constitucional Senado	Mensaje de modificaciones a Camara de Origen ----------	Res. Proy. Msg.
86	03/11/09	Tercer trámite constitucional C.Diputados	Entrada sancion con modificaciones de Camara Revisora Pasa a Comisión Asuntos Constitucionales, a Comisión Ciencia y Tecnología y a Comisión Legislación y Codificación ----------	
	09/12/09	Tercer trámite constitucional C.Diputados	Dictamen de Comision (3T) - Modificaciones Legislación y Codificación ->Ratifica sanción ---------- - Tuma Bogado ,Oscar Luis - Avalos Mariño ,Jorge Ramón - Ortega ,Dionisio - Garcete Molinari ,Cesar Marcelino - López Benitez ,Cesar - Barrios Monges ,Clemente Ramón	
95	09/12/09	Tercer trámite constitucional C.Diputados	Entrada de Dictamen de Comision (3T) - Modificaciones ----------	
	16/12/09	Tercer trámite C.Diputados	Dictamen de Comision (3T) - Modificaciones Ciencia y Tecnología ->Parte Aprueba/Parte Ratifica	

			---------- - Retamozo Ortíz ,Andres - Ortega ,Dionisio - González Segovia ,Jorge Dario - Rios Ojeda ,Victor	
98	17/12/09	Tercer trámite constitucional C.Diputados	Entrada de Dictamen de Comision (3T) - Modificaciones ----------	
106	08/04/10	Tercer trámite constitucional C.Diputados	Discusion Plenario (3T) - Modificaciones Rechazadas las modificaciones ----------	
	15/04/10	Tercer trámite constitucional C.Diputados	Resolucion rechazo modificaciones a Camara Revisora ----------	Res. Proy. Msg.
92	15/04/10	Cuarto trámite constitucional Senado	Entrada resolucion rechazo a modificaciones Pasa a Comisión Hacienda, Presupuesto y Cuentas y a Comisión Legislación, Codificación, Justicia y Trabajo ----------	
	27/04/10	Cuarto trámite constitucional Senado	Dictamen de Comision - (4T) - Rechazo Hacienda, Presupuesto y Cuentas ->Otra recomendación ---------- - Monges Espínola ,Juan Darío - González Quintana ,Enrique - González Safstrand ,Marcial - Jaeggli Caballero ,Alfredo Luís - Chiola Villagra ,Martín Antonio - Céspedes Colmán ,Jorge Antonio	
95	29/04/10	Cuarto trámite constitucional Senado	Entrada de Dictamen de Comision (4T) - Rechazo ----------	
	26/05/10	Cuarto trámite constitucional Senado	Dictamen de Comision - (4T) - Rechazo Legislación, Codificación, Justicia y Trabajo ->Ratifica sanción ---------- - Duarte Manzoni ,Marcelo Alberto Diego - Estigarribia Gutierrez ,Hugo Esteban	

			- Fonseca Legal ,Blanca Beatríz - Guastella Capello ,José Abel	
99	27/05/10	Cuarto trámite constitucional Senado	Entrada de Dictamen de Comision (4T) - Rechazo ----------	
101	03/06/10	Cuarto trámite constitucional Senado	Discusion Plenario (4T) - Rechazo Se ratifica ----------	
	03/06/10	Cuarto trámite constitucional Senado	Resolucion Sancionado segun CR ----------	Res. Proy. Msg.
128	20/07/10	Discusion Veto Total en CO C.Diputados	Entrada de Veto del Ejecutivo (Veto Total en CO) Pasa a Comisión Asuntos Constitucionales, a Comisión Ciencia y Tecnología y a Comisión Legislación y Codificación ----------	Veto.
	11/08/10	Discusion Veto Total en CO C.Diputados	Dictamen de Comision (Veto Total en CO) Asuntos Constitucionales ->Rechaza ---------- - Acha Mendoza ,Carlos Sebastian - Avalos Mariño ,Jorge Ramón - Silvero Alvarez ,Oscar Ismael - Barrios Monges ,Clemente Ramón - Tuma Bogado ,Oscar Luis - Liseras Osorio ,Carlos Augusto	
	25/08/10	Discusion Veto Total en CO C.Diputados	Dictamen de Comision (Veto Total en CO) Legislación y Codificación ->Rechaza ---------- - Acha Mendoza ,Carlos Sebastian - Avalos Mariño ,Jorge Ramón - Barrios Monges ,Clemente Ramón - Tuma Bogado ,Oscar Luis - López Benitez ,Cesar	
136	26/08/10	Discusion Veto Total en CO C.Diputados	Entrada de Dictamen de Comision (Veto Total en CO) ----------	
139	09/09/	Discusion Veto	Discusion Plenario (Veto Total en CO)	

	10	Total en CO C.Diputados	Rechazado ----------	
	16/09/10	Discusion Veto Total en CO C.Diputados	Resolucion Rechazo Veto Total (Veto Total en CO) ----------	Res. Proy. Msg.
115	21/09/10	Discusion Veto Total en CR Senado	Entrada de Mensaje de Rechazo de Veto Total en CO Pasa a Comisión Asuntos Constitucionales, Defensa Nacional y Fuerza Pública, a Comisión Hacienda, Presupuesto y Cuentas y a Comisión Legislación, Codificación, Justicia y Trabajo ----------	

Conclusión:

Un corto tecleo en la computadora, un gran paso para el Paraguay. Esta podría ser la frase más completa para dimensionar la importancia de la creación de la firma digital. La herramienta permitirá al país potenciar su relacionamiento nacional e internacional, en todos los ámbitos.

La promulgación de una ley por la cuál se instrumenten y se creen la firma digital y la firma electrónica será un gran paso del Gobierno en el campo tecnológico y permitirá al país interactuar en todos los niveles de relacionamiento electrónico entre gobiernos y con los ciudadanos a nivel mundial, dinamizando el comercio, la economía y combatiendo la corrupción.

La firma digital no es una rubricación al estilo físico u holográfico sobre una pantalla de diseño o algo así, sino es la asignación de un código y una contraseña de alta seguridad que identificarán a cada una de las personas, físicas o jurídicas, que estarán certificadas por un organismo oficial y que las habilitarán para realizar todo tipo de operaciones por medios digitales.

Es el resultado de aplicar cierto algoritmo matemático, denominado función hash (método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc.), a su contenido y, seguidamente, aplicar el algoritmo de firma (en el que se emplea una clave privada) al resultado de la operación anterior, generando la firma electrónica o digital.

Esta herramienta podrá ser utilizada en transacciones comerciales, bancarias, de cambio, importación, exportación, gestión de documentos oficiales, remisión de documentos formales, concreción de negocios, firma de contratos, todo lo que se pueda imaginar y desarrollar en la nube digital.

Tendrá igual fuerza y contundencia que una rúbrica a tinta sobre cualquier certificado de depósito, testamento, transferencia o pasaporte. Igualmente obligará al ciudadano a responder a todas las responsabilidades que ella implica ante la ley, nacional o internacional.

Consultado por medios de prensa sobre la posible promulgación de la ley 4017/10, Roberto Fernández, titular de la Unidad Técnica para la Modernización de la Administración Pública (UTMAP), que lleva adelante la iniciativa de gobierno electrónico en nuestro país calificó como un gran paso, muy importante, pues es uno de los soportes fundamentales de un gobierno electrónico, ya que identificará plenamente al ciudadano (físico o jurídico) para interactuar con la administración de gobierno, en forma ágil, directa, no física, sin intermediarios, lo que redundará en beneficio del país en términos económicos por ahorro de tiempo y los gastos que significan hoy hacer gestiones en dependencias estatales y la producción de un documento en forma física. Destacó también su característica de herramienta contra la corrupción, pues elimina el contacto físico entre el ciudadano y el funcionario, interacción que conlleva un alto porcentaje de posibles hechos ilegales.

Bibliografía:

- **http://www.leyes.com.py/todas_disposiciones/2003/leyes/ley_2051_03.php**
- **http://www.firmadigital.gba.gov.ar/html/concepto.html**
- **http://es.wikipedia.org/wiki/Firma_digital**
- **http://www.tuguialegal.com/firmadigital.htm**
- **http://www.deltaasesores.com/terminos/d-g/2681-firma-digital**
- **http://ca.sgp.gov.ar/faq.html**
- **http://www.monografias.com/trabajos11/infor/infor.shtml**
- **http://www.consumer.es/web/es/tecnologia/internet/2004/01/23/94524.php**
- **http://www.fooros.com/tutoriales_manuales/404-como_crear_tu_propia_firma_digital.html**
- **http://www.lanacion.com.py/noticias-325623-2010-09-10.htm**
- **http://www.clubrichdad.com/foros/269-firma-digital-comercio-electronico-e-commerce-en-el-mercosur-asuncion-paraguay.html**
- **http://www.presidencia.gov.py/v1/?p=30573**
- **http://www.paraguay.com/nacionales/experto-destaca-aprobacion-de-ley-que-da-validez-a-la-firma-digital-28972**
- **http://www.pylinks.com/tecnologia/proyecto-de-firma-digital-vuelve-al-congreso-%7C-2010-07-16/**
- **http://www.congreso.gov.py/**
- **http://www.hacienda.gov.py/sseaf/index.php?c=204**
- **http://www.diputados.gov.py/**
- **http://www.senado.gov.py/**

Anexos:

Sesión de la Honorable Cámara de Diputados del 8 de abril de 2010:

SECRETARIO*(Administrativo):Consideración del Proyecto de Ley,* ***"DE VALIDEZ JURIDICA DE LA FIRMA ELECTRONICA, LA FIRMA DIGITAL, LOS MENSAJES DE DATOS Y EL EXPEDIENTE ELECTRONICO"****, aprobado con modificaciones por el Senado y remito con Mensaje N° 483, dictaminado por la Comisión de Legislación y Codificación en mayoría y de Asuntos Constitucionales que aconseja ratificarse en el texto inicialmente aprobado por la Cámara de Diputados y de Ciencias y Tecnología que aconseja en mayoría aceptar algunas de las modificaciones introducidas por el Senado y ratificarse en otros artículos, tiene moción de preferencia.*

SEÑOR PRESIDENTE: *A consideración.*

Tiene la palabra el Diputado Nacional Héctor David Ocampos.

SEÑOR DIPUTADO HECTOR DAVID OCAMPOS NEGREIROS: *Gracias, señor Presidente.*

Este es un proyecto que si bien tuvo leves modificaciones en el Senado, pero prácticamente inofensivas por que son de forma y si no fuera por la modificación de la autoridad de la aplicación que cambiaron de ser el Ministerio de Industria y Comercio pusieron que sea una institución de rango muy inferior y sin la suficiente capacidad de gerenciar un proyecto de esto como una institución o como una autoridad más de segundo piso como podría ser un Ministerio.

Por otro lado también esto fue la autoridad de la elección del Ministerio de Industria y Comercio también fue fruto poco de un trabajo conjunto a nivel MERCOSUR, digamos que la políticas relacionadas a la parte progresista del comercio electrónico a través del subgrupo de trabajo N° 13 del MERCOSUR lo gerencia y el Ministerio de Industria y Comercio así como los ministerio también hermanos de los países de bloque, entonces, para rectificar eso y las otras que poco y nada tienen incidencia al fondo del proyecto.

Solicito el acompañamiento del dictamen de las comisiones de Legislación y Asuntos Constitucionales por la ratificación de la versión original de Diputados.

Muchas gracias.

SEÑOR PRESIDENTE: *Gracias, señor Diputado.*

Tiene la palabra el Diputado Nacional Jorge Ávalos.

SEÑOR DIPUTADO JORGE RAMON AVALOS MARIÑO: *Gracias, señor Presidente.*

En el mismo sentido del preopinante ya me libero de cualquier argumentación.

Así es que acompañamos plenamente la moción de ratificar el proyecto aprobado por Diputados.

Muchas gracias.

SEÑOR PRESIDENTE: *Gracias, señor Diputado.*

Por lo tanto hay que pasar a votar por la ratificación, teniendo en cuenta que hay 3 dictámenes pero se allanan y se necesita un 41 votos.

Los que estén de acuerdo por la ratificación, se servirán votar positivo y los que estén en contra, votarán negativo.

A votación.

Teniendo en cuenta que reúne los votos requeridos.

Vuelve al Senado.

Siguiente punto del orden del día.

<u>Sesión de la Honorable Cámara de Senadores del 3 de junio del 2010</u> (luego de ser aprobada por en esta sesión la ley contó con la aprobación tanto de diputados como de senadores y fue elevada al Poder Ejecutivo)

Tercer punto del orden del día. Proyecto de Ley: "De validez Jurídica de la firma Digital, los mensajes de datos y los expedientes electrónicos".

SECRETARIO GENERAL: Asunción, 26 de mayo del 2010. Honorable Cámara de Senadores: Vuestra Comisión de Legislación, Codificación, Justicia y Trabajo, os aconseja ratificarse en su dedición anterior de fecha 22 de octubre de 2009, con relación a la Resolución Nro. 647, "Que ratifica la sanción inicial acordada del proyecto de Ley: De validez Jurídica de la firma Digital, los mensajes de datos y los expedientes electrónicos", remitida por la H. Cámara de Diputados, según Mensaje Nro. 729.

En ocasión de su estudio, miembros de esta Comisión. Ampliarán los fundamentos del presente dictamen.

Firman: Hugo Estigarribia G., Marcelo Duarte Manzoni, Blanca Fonseca, José Abel Guastella, Alberto Grillón.

Asunción, 27 de abril del 2010. Honorable Cámara de Senadores: Vuestra Comisión de Hacienda, Presupuesto y Cuentas, os aconseja la ratificación en la sanción anterior respecto al proyecto de Ley: "De validez Jurídica de la firma Digital, los mensajes de datos y los expedientes electrónicos", remitido por la Cámara de Diputados según Mensaje Nro. 729 de fecha 15 de abril de 2010.

En ocasión de su tratamiento en plenaria, el vocero de la Comisión fundamentará el presente dictamen.

Os saluda con distinguida consideración.

Firman: Juan Darío Monges, Alfredo Luís Jaeggli, Marcial González Safstrand, Martín Chiola, Enrique González Quintana.

SEÑOR PRESIDENTE: Tiene la palabra el señor Senador Marcelo Duarte.

SEÑOR SENADOR MARCELO DUARTE: Gracias Presidente, efectivamente, este es un proyecto de Ley, que tuvo origen en la Cámara de Diputados, y cuya media sanción fue modificada por esta Cámara, en aspectos de forma en líneas generales y en un aspecto de fondo en relación al organismo de ejecución de la autoridad mejor de ejecución y haciendo una revisión comparativa de las diferencias entre un proyecto y otro, es indudable la conveniencia de que este Senado se ratifique en su sanción original, puesto que se adecua a lo que hoy se está aplicando en nuestro país, al igual que en la mayoría de los países que ya tienen implementado este sistema.

Eso es todo señor Presidente, reitero la recomendación de la Comisión es por la ratificación de la sanción de este Senado, al proyecto de Ley que tuvo su origen en la Cámara de Diputados, es todo. Muchas gracias.

SEÑOR PRESIDENTE: Se necesitan 23 votos, no hay nadie por la Comisión de Hacienda, tiene el uso de la palabra el señor Senador Hugo Estigarribia.

SEÑOR SENADOR HUGO E. ESTIGARRIBIA G.: Señor Presidente, nada más que para aportar algo, que las modificaciones que hicimos nosotros en el Senado, refieren a ajustar la legislación a la Ley modelo, de las Naciones Unidas, que rigen en varios países, y que hace que el Instituto al órgano de aplicación también, Paraguay sea el Instituto Nacional de Tecnología y Normalización, por ser el instituto acorde y he hablado con el proyectista el día de hoy, y le he manifestado que en el mismo sentido que él había proyectado un instituto de propiedad intelectual.

Porque dentro del Ministerio no se puede manejar el tema propiedad intelectual, en ese mismo sentido nosotros planteamos que este tema se haga a través del instituto adecuado, y no a través del Ministerio de Industria y Comercio, o sea que la modificación nuestra, va a mejorar la implementación de la Ley y va a ser acorde al modelo standard internacional que rige en varios países, vamos a tener una armonización legislativa, por eso sugerimos ratificarnos en el texto de senadores por mejorar el proyecto original, gracias.

SEÑOR PRESIDENTE: Estamos 27 senadores en la sala y necesitamos 23 votos, les ruego su atención por favor para ratificarnos en la sanción inicial del Senado. A consideración a votación. Suficiente mayoría.

APROBADA

Queda ratificado, se sanciona el texto de la Cámara de Senadores.

Cuarto punto del orden del día. Proyecto de Ley: “De Educación en una cultura de Paz”.

SECRETARIO GENERAL: Asunción, 12 de mayo de 2010. Honorable Cámara de Senadores: Vuestra Comisión de Legislación, Codificación, Justicia y Trabajo, os aconseja ratificarse en el rechazo, con relación a la Resolución N° 586: “Que ratifica la sanción inicial acordada al proyecto de Ley, Educación en una cultura de Paz”, remitido por la H. Cámara de Diputados según mensaje Nro. 683 de fecha 15 de marzo del 2010.

En ocasión de su estudio, miembros de esta Comisión, ampliarán los fundamentos del presente dictamen.

Firman: Hugo Estigarribia G., Marcelo Duarte Manzoni, Juan Darío Monges, Blanca Fonseca.

Asunción, 26 de mayo de 2010. Honorable Cámara de Senadores: Vuestra Comisión de Cultura, Educación, Culto y Deportes, os aconseja la ratificarse en la sanción inicial del Senado en el sentido de rechazar el Proyecto de Ley: “De Educación en una cultura de Paz”, remitido por Mensaje Nro. 683 de fecha 15 de marzo del 2010.

Firma: Iris Rocío González.

SEÑOR PRESIDENTE: Esto requiere de 30 votos. Tiene el uso de la palabra el señor Senador Marcelo Duarte.

SEÑOR SENADOR MARCELO DUARTE: Señor Presidente, necesitamos dos tercios, mociono el aplazamiento del proyecto de Ley, para cuando la Mesa Directiva lo disponga.

SEÑOR PRESIDENTE: Si señor Senador, no nos da más que para por ocho días, porque después ya va a tener sanción ficta. Tiene el uso de la palabra el señor Senador Carlos Filizzola.
SEÑOR SENADOR CARLOS FILIZZOLA: Si señor Presidente, en el mismo sentido, no vamos a tener los 30 votos necesarios, entonces aplazar para el jueves próximo señor Presidente, gracias.

SEÑOR PRESIDENTE: A consideración a votación, por la postergación suficiente mayoría.

APROBADA

OBS:

Las diarios de las sesiones posteriores al veto presidencial todavía no se han publicado.

Repercusiones de la ley de firmas digitales

- El poder ejecutivo veto la ley “De validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico” (16 de Julio)

- La Camara de Diputados rechaza el veto del Poder Ejecutivo. (9 de septiembre)

- El Diputado David Ocampos (UNACE)

- Poder Judicial.
- La digitalización de los expedientes.
- **"El expediente electrónico reduce cinco veces el tiempo del juicio"**

JUEZ BRASILEÑO SÉRGIO RENATO TEJADA GARCÍA

Otros entes con proyectos que utilizarían la ley

- Subsecretaria de Tributación (proyecto para recaudar impuestos)
- El Banco Central del Paraguay.
- Aduanas.
- Contrataciones Publicas.

Referencias

- http://eleccionesparaguay2013.com/2010/09/10/la-modernidad-digital-del-paraguay-esta-de-nuevo-a-la-vuelta-de-la-esquina/
- http://www.ultimahora.com/notas/362309-El-expediente-electronico-reduce-cinco-veces-el-tiempo-del-juicio
- http://www.lanacion.com.py/noticias-325623-2010-09-10.htm