UNIVERSIDAD DEL ACONCAGUA
FACULTAD DE CIENCIAS ECONÓMICAS Y JURIDICAS
CONTADOR PÚBLICO NACIONAL

Romina Daniela Cortez

Año de cursado: 2010

Director: Dr. Osvaldo DRIBAN

Tema: **“Operatividad e Implementación de la Firma Digital”**

Mendoza, Diciembre 2011

OPERATIVIDAD E IMPLEMENTACIÓN DE LA FIRMA DIGITAL

INDICE ANALÍTICO **Página**

Introducción

Este trabajo tiene como objeto de estudio a la firma digital, me voy a avocar a describir, 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 Alemania y las Naciones Unidas, para luego ver el tratamiento que le da la legislación de nuestro país, desde los antecedentes legislativos hasta la actual ley 25.506 y su decreto reglamentario de fecha 19 de diciembre del 2002.

Este es un tema que, a la hora de su análisis, es en realidad bastante simple, porque no se han presentado, en torno a él, posturas encontradas, que pudieran significar un verdadero inconveniente para nuestro derecho; tan solo se podría citar, como uno, la concepción que el código civil tiene de la firma ológrafa, un inconveniente que como se verá a lo largo de este trabajo ha sido perfectamente subsanado por la Ley 25.506.

Con todo lo antedicho, no queda más que decir que, este es un trabajo busca brindar, a aquellas personas que, 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.

A. Transmisión segura de información: La firma digital

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

Consiste en la transformación de un mensaje utilizando un sistema de cifrado asimétrico de manera que la persona que posee el mensaje original y la clave pública del firmante, pueda establecer de forma segura, que dicha transformación se efectuó utilizando la clave privada correspondiente a la pública del firmante, y si el mensaje es el original o fue alterado desde su concepción [1]

Las transacciones comerciales y el hecho de tener que interactuar masiva y habitualmente por intermedio de redes de computadoras le dio 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 de la firma ológrafa: 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.

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.

---

[1] Lorenzetti, Ricardo Luis, 2002. "La ley Argentina de firma digital", Ed. Abeledo Perrot. Pág 70-102 (cantidad páginas 340)

B. 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 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.

- 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. [2]

- 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

---

[2] MENDIVIL Ignacio, “El ABC de los Documentos Electrónicos Seguros”, pág. 1-10 (cantidad de páginas 30)

- 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 ente las partes, esté firmada o no, como por ejemplo en las transacciones seguras realizadas a través de SSL.

C. Firma digital: Definición, objetivo y terminología

Las firmas digitales son una de estas cosas de las que todo el mundo ha oído hablar pero muchos no saben exactamente que son.

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.

La seguridad es uno de los elementos clave en el desarrollo positivo de las redes de información mundial y particularmente en el comercio electrónico, ésta genera confianza, y hace que los usuarios al depositar sus datos en la red, estén seguros de que no serán alterados ni desviados a usuarios no autorizados. Las firmas digitales se utilizan comúnmente para la distribución de software, transacciones financieras y en otras áreas donde es importante detectar la falsificación y la manipulación.

La firma digital es la transmisión de mensajes telemáticos, un método criptográfico· que asegura su integridad así como la autenticidad del remitente. Consiste en un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje.

¿Tiene el mismo valor que la firma hológrafa?

En nuestro país, el Decreto Nº 427/98 ha otorgado a la firma digital similar valor jurídico que la firma hológrafa para aquellos actos internos de la Administración Pública Nacional que no produzcan efectos jurídicos hacia terceros.

Las firmas tradicionales (escritas) no indican el acuerdo que tiene una persona con los términos de un contrato, o documento en general, esa firma es única y autentica, basadas en la forma física en que la persona firma su nombre. Pero pueden ser fácilmente falsificadas.

Las firmas digitales realizan la misma función pero en documentos electrónicos, utilizando diversas tecnologías que permitan al receptor del documento tener la certeza de la identidad de la persona que envía el documento. Si se cambia siquiera una letra del mensaje original, ya no podrá verificar la firma del mensaje.

Las firmas digitales se basan en la criptografía de clave pública. Este tipo de sistemas criptográficos utiliza dos "claves. Una de esas claves es "publica". Todo el mundo conoce esa clave --o puede obtenerla, como si fuera un número de teléfono. La otra clave es "privada". Solo uno conoce su clave privada. Al firmar (cifrar) algo con tu clave privada, se está poniendo su sello personal. Nadie más puede hacerlo, ya que el resto no conoce la clave privada. Lo que se firma, entones, es el resumen del mensaje. El usuario firma el resumen del mensaje con su clave privada. Cualquiera puede descifrar el resumen del mensaje utilizando la clave pública del Firmante.

Terminología

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, "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. Existe entonces una relación de género especie entre ambos conceptos, teniendo por ende "firma electrónica" un significado más extenso que el de "firma digital".

La Firma Electrónica es cualquier tipo de método que se utilice con la intención de firmar algún dato electrónico, y la Firma Digital es aquella Firma Electrónica que utiliza la criptografía asimétrica para firmar datos electrónicos.

FIRMA ELECTRÓNICA: Es aquella firma que se verifica mediante algoritmos criptográficos que usan un par de llaves únicas para cada persona: una privada (para crear una firma digital) y otra pública (para verificar la firma digital). Consiste en dos procesos: uno de firma y otro de verificación de la firma. Con la verificación de la firma entre ambas llaves, se verifica igualmente la autenticidad de la misma.

La Ley Modelo UNCITRAL (United Nations Commission on International Trade Law/ CNUDMI: Comisión de las Naciones Unidas para el Derecho Mercantil Internacional) la define como datos en forma electrónica consignados en un mensaje de datos o adjuntados o lógicamente asociados al mismo y que pueden ser utilizados para identificar al titular de la firma y aprueba la información contenida en el mensaje de datos.

FIRMA DIGITAL

"La firma digital es una firma electrónica que por su avanzada técnica confiere mayor seguridad, al ser creada a partir del uso del sistema de criptografía asimétrica o clave pública que fue desarrollada por Diffie y Hellman en los años sesenta.

La denominada firma o rúbrica digital es una versión legal de una firma, basada en algoritmos matemáticos. No hay dos iguales. No existen dos firmas iguales.

La Firma Electrónica es más amplia, es el género; la Firma Digital es una especie de Firma Electrónica.

D. Aspectos técnicos

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:

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

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

El concepto de criptografía de clave pública fue introducido por Whitfield Diffie y Martin Hellman a fin de solucionar la distribución de claves secretas de los sistemas tradicionales, mediante un canal inseguro.

Este sistema utiliza dos claves diferentes: una para cifrar y otra para descifrar. Una es la clave pública, que efectivamente se publica y puede ser conocida por cualquier persona; otra, denominada clave privada, se mantiene en absoluto secreto ya que no existe motivo para que nadie más que el autor necesite conocerla y aquí es donde reside la seguridad del sistema.

Ambas claves son generadas al mismo tiempo con un algoritmo matemático y guardan una relación tal entre ellas que algo que es encriptado con la privada, solo puede ser desencriptado por la clave pública.

Resumiendo, la clave privada es imprescindible para descifrar criptogramas y para firmar digitalmente, mientras que la clave pública debe usarse para encriptar mensajes dirigidos al propietario de la clave privada y para verificar su firma.

Si bien no se trata de un tema estrictamente técnico, es conveniente aclarar que en tiempo de generación de cada par de claves, pública y privada, podría intervenir otra clave que es la de la Autoridad Certificante, que provee la garantía de autenticidad del par de claves generadas, así como también, su pertenencia a la persona cuya propiedad se atribuye [3]

Este esquema se utiliza en intercambios entre entidades cuando se trata de transferencias electrónicas de dinero, órdenes de pago, etc. donde es indispensable que las transacciones cumplan con los requisitos de seguridad enunciados anteriormente (integridad, autenticidad, no repudio del origen, imposibilidad de suplantación, auditabilidad y acuerdo de claves secretas), pero no se satisface el concepto de confidencialidad de la información (secreto).

---

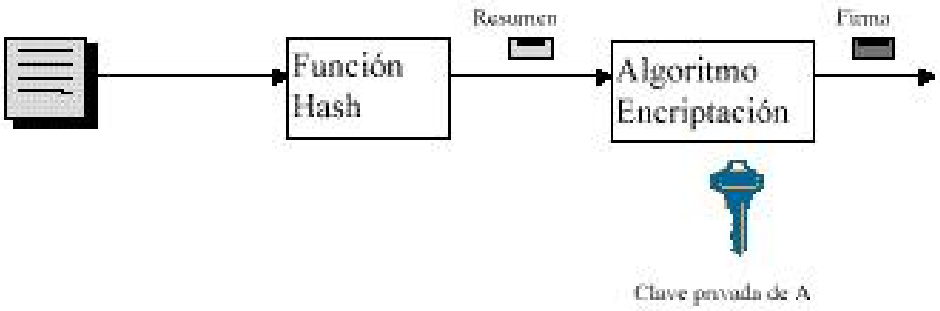
[3] REYES Krafft Alfredo, La Firma Electrónica y las Entidades de Certificación, Editorial Porrúa, pág. 152-214 (cantidad de páginas 260).

Desarrollo

1. Funcionamiento

A. Firma digital. Funcionamiento.

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.



La firma electrónica, como la firma hológrafa (autógrafa, manuscrita), puede vincularse a un documento para identificar al autor, para señalar conformidad (o disconformidad) con el contenido, para indicar que se ha leído y, en su defecto mostrar el tipo de firma y garantizar que no se pueda modificar su contenido.

El software de firma digital debe además efectuar varias validaciones, entre las cuales podemos mencionar:

Vigencia del certificado digital del firmante,

Revocación del certificado digital del firmante (puede ser por OCSP o CRL).

Inclusión de sello de tiempo.

La función hash es un algoritmo matemático que permite calcular un valor resumen de los datos a ser firmados digitalmente. Funciona en una sola dirección, es decir, no es posible, a partir del valor resumen, calcular los datos originales. Cuando la entrada es un documento, el resultado de la función es un número que identifica inequívocamente 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. Ello no obstante, este tipo de operaciones no están pensadas para que las lleve a cabo el usuario, sino que se utiliza software que automatiza tanto la función de calcular el valor hash como su verificación posterior.

Las posibilidades de red

Para que sea de utilidad, una función hash debe satisfacer dos importantes requisitos:

1. debe ser imposible encontrar dos documentos cuyo valor para la función hash sea idéntico.

2. dado uno de estos valores, debe ser imposible producir un documento con sentido que de lugar a ese hash.

Existen funciones hash específicamente designadas para satisfacer estas dos importantes propiedades. SHA y MD5 son dos ejemplos de este tipo de algoritmos.

Algunos sistemas de cifrado de clave pública se pueden usar para firmar documentos. El firmante cifra el hash calculado de un documento con su clave privada y cualquiera que quiera comprobar la firma y ver el documento, no tiene más que usar la clave pública del firmante para descifrar el hash, y comprobar que es el que corresponde al documento.

La solución.

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. Si el documento se modifica, la comprobación de la firma fallará, pero esto es precisamente lo que la verificación se supone que debe descubrir.

B. Criptografía: esquema simétrico y asimétrico.

El fundamento de las firmas electrónicas es la criptografía, disciplina matemática que no sólo se encarga del cifrado de textos para lograr su confidencialidad, protegiéndolos de ojos indiscretos, sino que también proporciona mecanismos para asegurar la integridad de los datos y la identidad de los participantes en una transacción.

El cifrado consiste en transformar un texto en claro (inteligible por todos) mediante un algoritmo en un texto cifrado, gracias a una información secreta o clave de cifrado, que resulta ininteligible para todos excepto el legítimo destinatario del mismo. Se distinguen dos métodos generales de cifrado:

• Cifrado simétrico: cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el criptosistema es simétrico o de clave secreta. Estos sistemas son mucho más rápidos que los de clave pública, y resultan apropiados para el cifrado de grandes volúmenes de datos. Ésta es la opción utilizada para cifrar el cuerpo de los mensajes en el correo electrónico o los datos intercambiados en las comunicaciones digitales. Para ello se emplean algoritmos como IDEA, RC5, DES, TRIPLE DES, etc.

• Cifrado asimétrico: cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el criptosistema es asimétrico o de clave pública. Una clave, la privada, se mantiene secreta, mientras que la segunda clave, la pública, es conocida por todos. De forma general, las claves públicas se utilizan para cifrar y las privadas, para descifrar. El sistema posee la propiedad de que a partir del conocimiento de la clave pública no es posible determinar la clave privada ni descifrar el texto con ella cifrado. Los cripto-sistemas de clave pública, aunque más lentos que los simétricos, resultan adecuados para los servicios de autenticación, distribución de claves de sesión y firmas digitales. Se utilizan los algoritmos de RSA, Diffie-Hellman, etc.

En general, el cifrado asimétrico se emplea para cifrar las claves de sesión utilizadas para cifrar el documento, de modo que puedan ser transmitidas sin peligro a través

de la Red junto con el documento cifrado, para que en recepción éste pueda ser descifrado. La clave de sesión se cifra con la clave pública del destinatario del mensaje, que aparecerá normalmente en una libreta de claves públicas. El cifrado asimétrico se emplea también para firmar documentos y autenticar entidades. En principio, bastaría con cifrar un documento con la clave privada para obtener una firma digital segura, puesto que nadie excepto el poseedor de la clave privada puede hacerlo. Posteriormente, cualquier persona podría descifrarlo con su clave pública, demostrándose así la identidad del firmante.

Algunos conceptos:

1.- CRIPTOGRAFÍA: Es el arte o ciencia de la escritura secreta. Es un sistema cifrado de mensajes para mantener un determinado nivel de privacidad. Se define también como el conjunto de técnicas (entre algoritmos y métodos matemáticos) que resuelven problemas de autenticidad, privacidad, integridad y no rechazo en la transmisión de información.

2.- SISTEMA CRIPTOGRÁFICO ASIMÉTRICO: Es aquel sistema que utiliza dos claves diferentes para cada usuario, una para cifrar que se llama clave pública y otra para descifrar denominada clave privada.

3.- SISTEMA CRIPTOGRÁFICO SIMÉTRICO: Es aquel sistema de cifrado basado en claves privadas. Se emplea la misma clave para encriptar y desencriptar el mensaje o los datos. La simetría se refiere a que las partes tienen la misma llave (clave) tanto para cifrar como descifrar.

4.- ALGORITMO: Conjunto final de reglas determinadas tendientes a resolver un problema a medida de un número específico de operaciones.

C. Esquema general de firma: procedimiento

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.

¿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 el cual es el resultado de un procedimiento matemático aplicado al documento.

D. Necesidad de utilización de certificados

Un elemento importante en este proceso es un intermediario llamado "Autoridad certificadora", cuya labor es establecer la liga entre el firmante y las llaves utilizadas para crear la firma digital. En esencia, la autoridad certificadora revisa los documentos de identificador del firmante, como licencia, pasaporte, o cualquier documento que ratifique su persona y posteriormente certifica que la persona que está utilizando la llave sea realmente la persona que dice ser. Cualquiera que desee verificar una firma digital debe de confiar en la autoridad de certificación en lugar de personalmente revisar los documentos de identificación del firmante.

¿Cómo se usan los certificados con el objeto de verificar una firma digital?

Generalmente los certificados se usan para generar confianza en la legitimidad de una clave pública. Esencialmente son documentos digitales que protegen a las claves públicas del fraude, de la falsa representación o de la alteración. Un uso seguro de la autenticación implica adjuntar uno o más certificados con cada mensaje firmado. El receptor del mismo verificará el certificado usando la clave pública de la Autoridad Certificante, y a continuación, asegurada su confianza en la clave pública del remitente, verificará la firma del mensaje.

Finalmente, en la cúspide de una jerarquía de certificados, se tiene a una Autoridad Certificante de más alto nivel, en la que se confía sin necesidad de ninguna otra certificación probatoria.

Cuanto mayor sea la certeza que el receptor tenga de que la clave pública es realmente del emisor, menor es la necesidad de adjuntar y verificar certificados.

E. Certificados de claves públicas

a. Organismo Licenciante:

Es la Autoridad Certificante Raíz que emite certificados de clave pública a favor de aquellos organismos o dependencias del Sector Público Nacional que deseen actuar como Autoridades Certificantes Licenciadas, es decir como emisores de certificados de clave pública para sus funcionarios y agentes.

Estas deben abstenerse de acceder, absolutamente, a la clave privada de cualquier suscriptor de los certificados que emitan.

Dentro del marco creado por dicho decreto, las funciones de Autoridad de Aplicación y de Organismo Licenciante son asumidas por la Subsecretaría de la Gestión Pública, SGP.

En cumplimiento de esa responsabilidad, se ha dispuesto la asignación de los recursos materiales y humanos, incluyendo la adquisición de equipamiento de última generación. Además, se ha elaborado una serie de documentos - que se encuentran en proceso permanente de revisión - y que servirán como base para el funcionamiento de Autoridades Certificantes que se licencien.

La Infraestructura del Organismo Licenciante ha sido instalada en la sede de la Subsecretaría de la Gestión Pública (Roque Sáenz Peña 511 - 5º piso - Buenos Aires).

b. Organismo Auditante:

Es el órgano de control, tanto para el Organismo Licenciante como para las Autoridades Certificantes Licenciadas.

Este control lo realiza mediante la auditación de estos, evaluando la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos.

Según lo establecido por el artículo 61 de la Ley Nº 25.237, el rol del Organismo Auditante dentro de la Infraestructura de Firma Digital para el Sector Público Nacional es cumplido por la Sindicatura General de la Nación (SIGEN).

c. Autoridades Certificantes Licenciadas:

Son aquellos organismos o dependencias del Sector Público Nacional que soliciten y obtengan la autorización, por parte del Organismo Licenciante, para actuar como Autoridades Certificantes de sus propios agentes. Es decir que, cumplidos los recaudos exigidos por el Decreto mencionado, podrán emitir certificados de clave pública a favor de sus dependientes.

Dentro de dichos recaudos encontramos que, debe abstenerse de acceder a las claves privadas de los suscriptores y además debe utilizar sistemas generadores de claves técnicamente confiables.

d. Suscriptor de certificado de clave pública:

Debe proveer a la Autoridad Certificante Licenciada todos los datos requeridos por esta, mantener el control de su clave privada e impedir su divulgación.

Certificados de clave pública:

Enumera los datos que deben contener los Certificados de Clave Pública.

Pasos:

1) Licenciamiento:

El licenciamiento es el procedimiento por el cual el Organismo Licenciante emite un certificado de clave pública a favor de un organismo público (quien adquiere la calidad de Autoridad Certificante Licenciada), quedando éste habilitado para emitir certificados a favor de sus dependientes.

Para obtener dicha licencia, el postulante debe completar un formulario de solicitud y adjuntar un requerimiento de certificado PKCS#10 en formato PEM.

2) Revocación:

La revocación es el procedimiento por el cual el Organismo Licenciante cancela la autorización otorgada a la Autoridad Certificante Licenciada para emitir certificados.

Esta cancelación puede efectuarse a solicitud de esta última o bien por decisión del Organismo Licenciante, según las pautas establecidas en la Política de Certificación.

Si una Autoridad Certificante Licenciada desea pedir al Organismo Licenciante la revocación de su certificado, puede utilizar un formulario de solicitud de revocación.

3) Comprobación de la identidad del firmante y de la integridad del mensaje:

En primer término el receptor 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 serlo.

Las firmas digitales dependen de un par de algoritmos matemáticos, denominados clave, que utilizan el remitente y el destinatario del mensaje.

Estas claves se encargan de establecer la correspondencia que permite a la computadora del destinatario reconocer la computadora del remitente y certificar la autenticidad de un mensaje.

Una de las claves, la clave privada de la persona, está alojada en la PC o registrada en una tarjeta inteligente, e identifica que un mensaje ha sido enviado por la persona.

La segunda es una clave pública, que puede ser empleada por cualquiera que desee autenticar documentos que la persona firme. La clave pública 'lee' la firma digital creada por la clave privada de la persona y verifica la autenticidad de los documentos creados con la misma.

La clave privada de la persona se desbloquea mediante una contraseña. En el futuro, para mayor seguridad aún, este sistema de clave y contraseña podría ser reemplazado por tecnologías biométricas, que miden características del cuerpo humano, como la retina, una huella digital o un rostro asociado con un registro de identidad.

4) Obtención de una firma digital:

Para enviar una firma digital, se requiere en primer lugar registrarse en una autoridad de certificados y solicitar el certificado de identidad digital, que hace de la firma un instrumento único.

La mayoría de las autoridades de certificados también proporcionan el software necesario y ofrece asesoría al usuario en el proceso de obtención, instalación y utilización de la firma digital. La persona debe llenar un formulario de solicitud y suministrar pruebas de identidad para obtener el certificado.

La firma digital se anexa a un mensaje de E-mail de manera muy similar al de los archivos.

Este es el certificado Raíz de la Infraestructura de Firma Digital del Sector Público Nacional.

(Su instalación implica la aceptación de los términos y políticas establecidos por el Organismo Licenciante):

Versión	V3
Numero de Serie	3828 65C7
Algoritmo de Firma	sha1RSA
Válido Desde	Martes 9 de Noviembre de 1999 15:20:39
Válido Hasta	Viernes 6 de Noviembre de 2009 15:20:39
Asunto	CN = Organismo Licenciante OU = Autoridad Certificante Raíz de la IFDAPN OU = Política de Certificación en ol.pki.gov.ar/politica O = Administración Publica Nacional C = AR
Restricciones Básicas	Tipo de asunto=CA
Restricción de longitud de ruta	1
Algoritmo de identificación	sha1
Huella digital	5DD7 0846 0AE2 0909 6D2E 041D F8E4 D05C 7C37 7E93

F. Estándares tecnológicos

Las firmas digitales, así como los certificados que permiten su verificación, son herramientas fundamentales a la hora de otorgar validez a los documentos electrónicos. Por ello, la tecnología que viabiliza su utilización requiere de especial cuidado y atención.

Este cuidado se vincula fundamentalmente a la utilización de estándares tecnológicos basados en normas y protocolos internacionalmente aceptados. Esto último asegura no sólo el correcto funcionamiento de Infraestructura de Firma Digital, sino también la interoperabilidad de las aplicaciones y entre Certificadores Licenciados nacionales con las infraestructuras de Claves Públicas de otros países.

Frente a cualquier transacción que involucre el uso de una firma digital o de un certificado digital, la adopción de estándares tecnológicos internacionalmente aceptados permite asegurar un proceso efectivo de verificación de dichas firmas, otorgando seguridad técnica y legal a las transacciones electrónicas.

En este marco, la **Infraestructura de Firma Digital de la República Argentina (IFDRA)** ha adoptado los siguientes estándares tecnológicos:

- Para el formato de los certificados y de las listas de certificados revocados: **ITU–T X509**.
- Para la generación de las claves: **RSA, DSA o ECDSA**.
- Para la protección de las claves privadas de certificadores y suscriptores: **FIPS 140**.
- Para las políticas de certificación: **RFC 5280 y 3739**.

El listado completo de los estándares aprobados para la IFDRA, así como las condiciones bajo las cuales deben ser utilizados, se encuentra descripto en la Decisión Administrativa Nº 6/2007 (Anexo 3).

2. Aplicaciones

A. Principales usos

La firma digital se puede aplicar en las siguientes situaciones:

- Correo seguro
- Mensajes con autenticidad asegurada
- Contratos comerciales electrónicos
- Factura _ electrónica
- Desmaterialización de documentos
- Transacciones comerciales electrónicas
- Invitación electrónica
- Dinero electrónico
- Notificaciones judiciales electrónicas
- Voto electrónico
- Decretos ejecutivos (gobierno)
- Créditos de seguridad social
- Contratación pública
- Sellado de tiempo
- 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
- 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
- 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.

Correo seguro

No hay nada más fácil que leer los correos de otras personas, ya que viajan desnudos por la Red. Valga la siguiente analogía, un correo electrónico normal es como una tarjeta postal sin sobre, que puede leer todo el que tenga interés. Por consiguiente, la mejor manera de preservar la intimidad en los mensajes de correo electrónico es recurrir a la criptografía. Por medio de potentes técnicas criptográficas, el contenido del mensaje puede ser enviado cifrado, permitiendo así que sólo el destinatario legítimo del correo sea capaz de leerlo. Con este mecanismo se garantiza la confidencialidad del correo. Sin embargo, los modernos sistemas de seguridad del correo, como PGP y otros, no se limitan a cifrar el contenido de los mensajes intercambiados, sino que también añaden otros servicios, como la integridad, que garantiza que el contenido del mensaje no ha sido alterado por el camino; la autenticación, que asegura la identidad del remitente del correo, de manera que podemos estar seguros de que fue escrito por quien lo envió y no ha sido falsificado; y el no repudio, que nos protege frente a que posteriormente el que envió el correo (o lo recibió de nosotros) alegue posteriormente no haberlo enviado (o recibido sí era el destinatario). Estos últimos servicios se prestan mediante las firmas digitales.

¿Cómo hago para 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).

Abra el programa que utiliza para enviar sus correos electrónicos. Siga el procedimiento habitual para escribir el mensaje que desea enviar.

Presione el botón de Enviar (Send).

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.

Factura electrónica

La factura electrónica es un tipo de fichero que recoge la información relativa a una transacción comercial y sus obligaciones de pago y de liquidación de impuestos.

La factura electrónica es enviada por el vendedor al comprador a través de un medio de comunicación a distancia para documentar la venta o la provisión del servicio. Está sometida a ciertos requisitos legales por las autoridades tributarias de cada país, de forma que no siempre es posible remitir electrónicamente las facturas, y, en ese caso, se envía la factura impresa, por correo o mensajería.

Los requisitos legales respecto al contenido, afectan tanto a las facturas electrónicas como a las de papel. Los requisitos legales respecto a la forma imponen determinado tratamiento en aras a garantizar la integridad y la autenticidad.

La factura electrónica es un caso especial de factura. La factura es el justificante fiscal de la entrega de un producto o de la provisión de un servicio, que afecta al obligado tributario emisor (el vendedor) y al obligado tributario receptor (el comprador). Tradicionalmente, es un documento en papel, cuyo original debe ser archivado por el receptor de la factura. Habitualmente el emisor de la factura conserva una copia o la matriz en la que se registra su emisión. [4]

La factura electrónica fomenta que las instituciones dejen atrás las facturas en papel y las reemplacen por una versión electrónica de un documento tributario generado electrónicamente, que tiene la misma validez tributaria que la tradicional y registra las operaciones. Todo el ciclo de la facturación puede ser administrado en forma electrónica, en toda Factura también se debe agregar el impuesto al valor agregado (IVA), en aquellos países en los que se usa esta forma de impuesto.

---

[4] SOLIS García, José Julio. FACTURA Y FIRMA ELECTRONICA AVANZADA. Editorial Gasca. Pág. 85-120 (páginas totales 167)

Entre los países que disponen de normativa de factura electrónica cabe citar los siguientes:

- Todos los europeos, en función de la transposición de la Directiva 2001/115
- España, en función del Real decreto 1496/2003
- Argentina
- Chile
- México

¿Cuáles son los beneficios?

Dependiendo del volumen de las empresas, el ahorro por concepto de administración de facturas (recepción, almacenaje, búsqueda, firma, devolución, pago, envío, etc.) puede fluctuar entre el 40% y el 80%. Entre los motivos que hacen esto posible este ahorro se encuentran:

- Oportunidad en la información, tanto en la recepción como en el envío.
- Ahorro en el gasto de papelería.
- Facilidad en los procesos de auditoría.
- Mayor seguridad en el resguardo de los documentos.
- Menor probabilidad de falsificación.
- Agilidad en la localización de información.
- Eliminación de bodegas para almacenar documentos históricos.
- Procesos administrativos más rápidos y eficientes.

Voto electrónico

El voto electrónico, es un conjunto de datos o registro informático, que procesado convenientemente, una autoridad electoral puede conocer el resultado de la elección de un ciudadano sin poder identificar al elector y por parte del elector en cualquier momento posterior a su sufragio poder verificar su elección.

¿Cómo funciona el sistema de voto electrónico?

Este proceso que basado en algún método criptográfico y de las denominadas "pruebas de conocimiento cero", el sistema de "voto electrónico" propuesto, funciona de la siguiente manera:

1. El elector, en primer lugar configurará su cuenta de "empadronamiento electrónico" y establecerá sus claves para realizar la transacción.

2. Se instala un servidor con el "padrón electrónico" electoral, obtenido del proceso de empadronamiento, este servidor será accesible ya sea por una Intranet o por la Internet, o mediante una red privada como la de los bancos con sus cajeros automáticos, o bien un teléfono celular que soporte el protocolo "WAP".

3. El elector ejerce el sufragio y esta información es enviada a la autoridad electoral (el contenido del sufragio únicamente será descifrado por la autoridad electoral, o por el votante en el momento de una posterior verificación).

4. Si el elector quiere verificar su elección, posterior a la emisión de su "voto electrónico", una vez que ingrese a su "cuenta de empadronamiento", se descifrará de la "base de datos" los resultados procesados por la autoridad electoral y obtendremos su elección, en esta fase solo el votante puede realizar esta operación y garantizar que su decisión no ha sido cambiada, tampoco el votante puede cambiar la información ya registrada.

El principal problema a resolver en la "Ciberdemocracia", y uno de los principales en el "Comercio Electrónico", el que presupone "la unicidad y autenticación de la información", en otras palabras, saber que "Juan Pérez" que se registró y se ha dado de alta en el "padrón electrónico" es efectivamente "Juan Pérez"; encontrado el sistema para garantizar este principio, provocamos lo que conocemos como "no repudiabilidad de la transacción", por tanto es necesario crear una "base de datos relacional", en donde interactuarán dos bases de datos principales, la de "empadronamiento", en donde, deberán de constar al menos los siguientes campos:

• Número de Documento de Identidad.

• Apellidos y Nombres.

• Fecha de nacimiento.

• Identificación Dactilar. (Imagen obtenida con un dispositivo de captura o escaneo de la huella dactilar y su correspondiente código identificatorio único, para la primera sesión de empadronamiento este código será el impreso o la información guardada en su documento de identidad).

• "Clave privada" del elector. (Campo a calcularse el momento de terminar el proceso de empadronamiento electrónico)

• Provincia o Estado donde vive.

• Ciudad donde vive.

• Dirección domiciliaria.

• Pregunta secreta 1 y su respuesta.

• Pregunta secreta 2 y su respuesta.

• Pregunta secreta 3 y su respuesta.

• Pregunta secreta 4 y su respuesta.

• Dirección de "correo electrónico".

Y, la "base de datos" del "padrón electrónico" como tal, con los siguientes campos de los datos obtenidos:

• Número de Documento de Identidad.

• Apellidos y Nombres.

• Identificación Dactilar (Imagen obtenida con un dispositivo de captura o escaneo de la huella dactilar y su correspondiente código identificatorio único)

• "Clave pública" del elector. (Campo a calcularse el momento de terminar el proceso de empadronamiento electrónico)

• Campo para la "firma digital" del elector. (Campo a ser calculado el momento de la votación)

La votación

El proceso de registro de los votos seguiría el siguiente esquema:

1. El elector ingresa mediante la Intranet de la Autoridad Electoral, o la Internet, o mediante su celular con capacidad "wap" o a través de la red de cajeros automáticos, a su cuenta de "empadronamiento electrónico".

2. Escoge la opción "ejercer sufragio", y se abrirá una sesión segura bajo el protocolo SSL para esta transacción.

3. Se desplegará la papeleta electoral y podrá elegir al(los) candidato(s) de su preferencia mediante un simple "clic" en la casilla correspondiente, o número de opción si lo hace a través de un cajero automático o teléfono celular.

4. Esta información, construirá la trama de selección y se la estructurará conforme el siguiente diseño:

• Número de transacción.

• "Firma digital de la Autoridad Electoral", aplicada al "hash" resultante de la concatenación de los siguientes tres datos: la respuesta expresada en la papeleta llena del elector, el número de transacción, y la clave de sesión; esta firma se la hará con la "clave privada" de la Autoridad Electoral, esta firma a su vez se la cifrará con la "clave pública" del elector.

• "Firma digital del elector", aplicada al "hash" resultante de la concatenación hecha en el paso anterior, esta firma se la hará con la "clave privada" del elector, esta firma a su vez se la cifrará con la "clave pública" de la Autoridad Electoral.

• Clave de sesión cifrada con la "clave pública" de la Autoridad Electoral. (Esta clave de sesión es calculada en el proceso de comunicación por parte de lo equipos que intervienen)

• Clave de sesión cifrada con la "clave pública" del elector.

• Papeleta llena, cifrada con la clave de sesión, para este proceso se utilizará cualquier algoritmo de "criptografía simétrica", considerado seguro por parte de la comunidad criptográfica internacional.

• CRC calculado, para validación del registro.

5. Transmitida la trama que constituye el "voto electrónico", se grabará en el registro de votación que tiene la Autoridad Electoral, y los que a petición de los veedores quieran tener una copia de esta información, es decir será enviada a cada partido o movimiento político, a los observadores designados de los países amigos u organismos internacionales invitados,

etc., está transmisión se hará al mismo tiempo de la emisión del "voto electrónico" y "certificado de votación", por parte de la Autoridad Electoral.

6. Con la "clave privada" de la Autoridad Electoral, de la trama recibida, se descifrará la clave de sesión, y con ella se obtendrá el campo de la papeleta llena, procediendo a alimentar los acumuladores correspondientes a los resultados.

7. La "firma digital" del elector será grabada en el "padrón electrónico", y la misma será impresa en el "certificado de votación" construido al momento de la elección, este certificado será enviado mediante correo electrónico a la dirección que el votante haya configurado en su "cuenta de empadronamiento", e impreso si posee una impresora al momento de realizar la elección, también puede imprimirlo posteriormente, para validar la firma, solo la Autoridad Electoral puede "certificar" si es original o no el certificado impreso.

8. Se termina la "sesión SSL" y finaliza el proceso, enviando el "voto electrónico" a los veedores del proceso electoral.

9. Al cerrar el proceso electoral se grabará la "firma digital" calculada de la "base de datos" con los registros de los "votos electrónicos", este proceso se lo hará con la "clave privada" de la Autoridad Electoral, esta "firma" será enviada a cada observador, que calculada sobre los registros que cada uno posee, esta respuesta debe confirmar que no existe variación en la información recibida.

El escrutinio

En el proceso de "escrutinio", se hará la siguiente verificación con los resultados de los acumuladores obtenidos en el proceso de votación:

1. Se verificará la integridad de la "base de datos" creada, con la "firma digital" que la Autoridad Electoral grabó al momento de cerrar el proceso de elecciones.

2. Se procesarán del registro de "votos electrónicos", todas y cada una de las tramas que se han guardado, procediendo a descifrar la información con la "clave privada" de la Autoridad Electoral, y recontando las papeletas llenas.

3. Se cuentan los resultados y se compara con los acumuladores del proceso de votación, esta información debe ser igual, caso contrario se pedirá a cada observador que se realice este proceso sobre los registros que cada uno posee, los resultados no pueden variar.

4. Se publican los resultados obtenidos.

En cuanto a la tecnología utilizada para el llamado "voto electrónico" se puede decir lo siguiente:

1. Puede el ciudadano, ejercer su derecho al sufragio en cualquier parte del mundo, inclusive dentro del país en que vive, a través de la Internet o algún dispositivo que le dé acceso a la misma.

2. No se necesita de equipos especiales que no se pueda conseguir libremente en el mercado o alquilar su servicio (Cajeros automáticos de los bancos, cyber cafés, teléfonos celulares, etc.)

3. Se garantiza la privacidad y secreto de la elección, y lo más importante que la misma no puede ser manipulada.

4. En cualquier momento el ciudadano puede verificar su elección.

5. En ningún momento, así exista una impugnación legal, la autoridad electoral puede conocer la elección del ciudadano que ha enviado su voto electrónico.

6. La obtención y publicación de los resultados oficiales a pocas horas de cerrado el proceso electoral.

7. Se ahorra ingentes cantidades de dinero, ya que no es necesario imprimir por parte de la Autoridad Electoral, las papeletas de elección y los certificados respectivos, se constituyen menos "mesas electorales", se despliega menor logística por parte de los miembros de la Fuerza Pública.

8. El elector ahorra, aunque parezca irrisorio, el costo de movilización, si este se encuentra empadronado fuera de su recinto de residencia.

9. El elector en el exterior, podrá sufragar sin el temor de que las autoridades migratorias de los respectivos países de residencia, estén al acecho de los "ilegales", y este hecho no se constituya en discriminatorio y atente a lo que estipula las leyes electorales, y en el mejor de los casos, el emigrante "legal", que reside en el exterior, no tendría que asumir el costo de movilización desde el lugar de residencia hasta el consulado del país respectivo.

10. Como verdadero sistema, que recoge de manera inmediata y a bajo costo, la decisión de un pueblo, los gobiernos podría realizar las consultas populares necesarias, en un modelo de democracia participativa, en cualquier momento y lugar.

Máquina de voto electrónico usada en Brasil

Sellado de tiempo

El sellado de tiempo (Timestamping) es un mecanismo on-line que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo.

Una Autoridad de Sellado de Tiempo actúa como tercera parte de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora concretos.

B. Situación en otros países

a. 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.

b. 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.

c. 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.

C. Situación actual en la Argentina

En la Argentina la firma digital es el resultado de una transformación de un documento digital empleando un criptosistema asimétrico y un digestoseguro, de forma tal que una persona que posea el documento digital inicial y la clave pública del firmante pueda establecer, con exactitud:

Primero, si la transformación se llevó a cabo utilizando la clave privada que corresponde a la clave pública del originante, lo que impide su repudio.

Y después, si el documento digital ha sido modificado desde que se efectuó su transformación, lo que garantiza su integridad.

Uso de documentos digitales en la Administración Pública Nacional

El primer antecedente que autorizó el uso de documentos digitales dentro de la Administración Pública Nacional es el art. 30 de la ley 24.624 (Boletín Oficial 29/12/95) reglamentado posteriormente por la Decisión Administrativa No. 43/96 (Boletín Oficial 7/5/96).

Mediante esta normativa se autorizó al Archivo General de la Administración a transformar sus documentos originales a soporte electrónico u óptico indeleble, mediante el procedimiento que se establece en la respectiva reglamentación.

Con esta reforma se abrió la posibilidad de digitalizar la documentación administrativa del Estado, pero sólo con fines de archivo. No existía hasta la fecha una normativa de carácter general que regulara el procedimiento administrativo informatizado, permitiendo prescindir del expediente tradicional (en papel) y reemplazarlo por mensajes electrónicos.

Fue así como se formó un comité en el ámbito de la Secretaría de la Función Pública que se dedicó al estudio de la implementación de la firma digital dentro de la administración pública.

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 nuestro derecho 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.

Los requisitos o guías son:

- Documentos digitales oponibles a terceros: esto implica que el documento digital requiere que la firma digital permita la identificación del emisor o autor y la integridad de su contenido.
- Equiparación de la firma digital a la firma ológrafa: este punto constituye la esencia de la normativa al permitir que quienes opten por utilizar documentos digitales suscritos digitalmente obtengan garantías legales similares a las que brinda la firma ológrafa sobre el soporte de papel.
- La firma ológrafa permite, simultáneamente, identificar a su autor así como imputarle la autoría del texto que la precede.
- Uso de la criptografía asimétrica como medio para instrumentar la firma digital: la criptografía asimétrica o de clave pública constituye el único método actualmente capaz de implementar la firma digital, pues cumple con las características esenciales de la firma ológrafa, es decir, que permite simultáneamente identificar en forma inequívoca al autor y verificar sin lugar a dudas que el mensaje no ha sido alterado desde el momento de su firma. Este mecanismo es el único que no requiere la divulgación de la clave privada (secreta) utilizada por el firmante para suscribir el documento.
- Autoridades certificantes de claves públicas y privadas: esta autoridad certifica la correspondencia entre una clave pública y la persona física o jurídica titular de la misma. En forma similar a lo que ocurre con las entidades verificadoras de dominios en Internet, sería posible acudir a las autoridades certificantes para saber de manera inequívoca si una clave pública corresponde a quien debería.

El Anexo de la Resolución 45/97 concluye que la firma digital permitirá:

La digitalización de cualquier circuito de la información, incluyendo documentos legales que normalmente requieren firmas y sellos convencionales.

La generalización de la utilización de firma digital a través de la adopción de pautas uniformes que permitan verificar la autenticidad e integridad de los documentos digitales que requieran firma para su validez.

Un menor riesgo de fraude en los documentos digitales suscritos digitalmente.

El martes 21 de abril de 1998 se publicó en el Boletín Oficial el decreto 427/98, que fija el "Régimen al que se ajustará el empleo de la firma digital en la instrumentación de los actos internos, que no produzcan efectos jurídicos individuales en forma directa, que tendrá los mismos efectos de la firma ológrafa. Autoridad de aplicación".

Basándose en la normativa que ya había sido dictada y aplicada anteriormente, los objetivos de este decreto son:

Eliminar el uso del papel y automatizar los circuitos administrativos mediante la introducción de tecnología de última generación incluyendo el uso de la firma digital que posee la misma o superior garantía de confianza que la firma ológrafa.

Designar a la Secretaría de la Función Pública como Autoridad de aplicación para, entre otras cosas, dictar los manuales de procedimiento de las Autoridades Certificantes Licenciadas y de los Organismos Auditante y Licenciante, la fijación de los estándares tecnológicos aplicables a las claves. Debiendo cumplir esta tarea en un plazo de seis meses a partir de la fecha de publicación.

D. Organismos que utilizan firma digital

- Subsecretaría de Gestión Pública Descripción: Autenticación del ingreso a bases de datos de la Coordinación de Emergencias en Redes Teleinformáticas para la Administración Pública Nacional.

Usuarios: Organismos Públicos

Inicio de Operaciones: 08/1999

- Ministerio de Economía

Descripción: Incorpora la firma digital en el intercambio de información entre las Unidades Operativas de Compras de los organismos y la Oficina Nacional de Contrataciones.

Cantidad de Usuarios: 300 aprox.

Inicio de Operaciones: 03/2001

- Comisión Nacional de Valores

Descripción: Proyecto desarrollado con el objetivo de recibir y publicar por Internet, a beneficio del público inversor nacional e internacional, la información financiera de las principales empresas del país que cotizan sus acciones y obligaciones negociables en el ámbito bursátil. Algunos ejemplos de información firmada digitalmente recibida por la AIF son: estados contables, prospectos informativos de emisión de acciones y de obligaciones negociables, estatutos, actas de asamblea, calificaciones de riesgo de títulos valores, notificaciones de eventos económicos significativos.

Usuarios: 120 Agentes CNV; 200 Empresas Cotizantes; 12 Calificadores de Riesgo; 200 Fondos Comunes de Inversión.

Inicio de Operaciones: 04/1999

- Comisión Nacional de Energía Atómica

Descripción: Circuito de comunicaciones a través de correo electrónico firmado dentro del organismo.

3. Marco normativo

A. Normativa específica

*Resolución JGM Nº 176/2002

Habilita en Mesa de Entradas de la Subsecretaría de la Gestión Pública el Sistema de Tramitación Electrónica para la recepción, emisión y archivo de documentación digital firmada digitalmente.

*Resolución SGP Nº 17/2002

Establece el procedimiento para solicitar la certificación exigida al Registro del Personal acogido al Sistema de Retiro Voluntario, habilitando la modalidad de tramitación mediante el empleo de documentación digital firmada digitalmente.

*Decreto Nº 1023/2001

En su artículo 21 permite la realización de las contrataciones comprendidas en el Régimen en formato digital firmado digitalmente.

*Decreto Nº 889/2001

Aprueba la estructura organizativa de la Secretaría para la Modernización del Estado en el ámbito de la Subsecretaría de la Gestión Pública, creando la Oficina Nacional de Tecnologías de la Información y otorgándole competencias en materia de firma digital.

*Decreto Nº 677/2001

Otorga a los documentos digitales firmados digitalmente remitidos a la Comisión Nacional de Valores de acuerdo a las reglamentaciones dictadas por ese organismo, similar validez y eficacia que los firmados en soporte papel.

*Decreto Nº 673/2001

Crea la Secretaría para la Modernización del Estado en el ámbito de la Jefatura de Gabinete de Ministros, asignándole competencia para actuar como Autoridad de Aplicación del régimen normativo que establece la Infraestructura de Firma Digital para el Sector Público

Nacional y para la aplicación de nuevas tecnologías informáticas en la Administración Pública Nacional.

*Ley Nº 25.237

Establece en el artículo 61 que la SINDICATURA GENERAL DE LA NACION ejercerá las funciones de Organismo Auditante en el régimen de empleo de la firma digital en la instrumentación de los actos internos del Sector Público Nacional.

*Resolución SFP Nº 212/98

Establece la Política de Certificación del Organismo Licenciante, en la cual se fijan los criterios para el licenciamiento de las Autoridades Certificantes de la Administración Pública Nacional.

*Decreto Nº 427/98

Autoriza la utilización de la firma digital en la instrumentación de los actos internos del Sector Público Nacional, otorgándole los mismos efectos que la firma ológrafa y estableciendo las bases para la creación de la Infraestructura de Firma Digital para el Sector Público Nacional.

*Resolución SFP Nº 45/97

Establece pautas técnicas para elaborar una normativa sobre firma digital que permita la difusión de esta tecnología en el ámbito de la Administración Pública Nacional.

Normativa sobre Aplicaciones:

*Resolución SAFJP Nº 293/97

Implementa en el ámbito de la Superintendencia de Administradoras de Fondos de Jubilaciones y Pensiones el sistema de Telecomunicaciones de la SAFJP con el fin de establecer un correo electrónico entre las Administradoras de Fondos de Jubilaciones y Pensiones y este Organismo

Normativa Específica sobre Tecnología:

*Resolución Nº 178/2001

Aprueba las aperturas inferiores del primer nivel operativo de la estructura organizativa de la Secretaría para la Modernización del Estado de la Jefatura de Gabinete de Ministros.

*Decreto Nº 889/2001

Aprueba la estructura organizativa de la Secretaría para la Modernización del Estado en el ámbito de la Subsecretaría de la Gestión Pública, creando la Oficina Nacional de Tecnologías de la Información y otorgándole competencias en materia de firma digital.

*Decreto Nº 673/2001

Crea la Secretaría para la Modernización del Estado en el ámbito de la Jefatura de Gabinete de Ministros, asignándole competencia para actuar como Autoridad de Aplicación del régimen normativo que establece la Infraestructura de Firma Digital para el Sector Público Nacional y para la aplicación de nuevas tecnologías informáticas en la Administración Pública Nacional.

Procedimientos Administrativos:

*Decisión Administrativa N° 118/2001

Crea el Proyecto de Simplificación e Informatización de Procedimientos Administrativos (PRO-SIPA), en el contexto del Plan Nacional de Modernización y en el ámbito de la Jefatura de Gabinete de Ministros.

La Digitalización en el Proyecto de Unificación de 1998

Como podremos ver, a continuación, este proyecto amplia la concepción de nuestro actual código, que muchas veces es un obstáculo a la hora de intentar implementar en nuestro país tecnologías modernas, como es la firma digital, introduciendo al documento electrónico como un documento válido, además de aceptar, también, a la firma digital como firma válida y estableciendo en torno a estos una gran cantidad de normas, que los hace de más fácil aplicación.

Estas normas son: *De los hechos y actos jurídicos*.

ART.42- Donde se prevén importantes modificaciones es en el tratamiento de los instrumentos. Se mantiene la regla de libertad de formas y se prevé la forma convenida que es obligatoria para las partes bajo pena de invalidez del negocio jurídico.

Se reconocen los instrumentos públicos, los instrumentos privados y los instrumentos particulares que son los no firmados.

Lo relevante es que se amplía la noción de escrito, de modo que puede considerarse expresión escrita la que se produce, consta o lee a través de medios electrónicos.

Se define la firma y se considera satisfecho el requisito de la firma cuando en los documentos electrónicos se sigue un método que asegure razonablemente la autoría e inalterabilidad del documento.

Se prevé expresamente la posibilidad de que existan instrumentos públicos digitales. En este sentido el Código se abre a la realidad abrumadora de los documentos electrónicos, aunque con fórmulas abiertas y flexibles y sin vinculación a la tecnología actual, de modo de evitar su rápido envejecimiento que se produciría por la previsible permanente superación de esas tecnologías.

ART.43- En las escrituras públicas se incorporan dos reglas novedosas. La primera relativa a la justificación de la identidad, que sustituye a la fe de conocimiento; se prevé incluso la posibilidad de insertar la impresión digital del compareciente no conocido por el notario.

La segunda es la reglamentación de las actas, a las que sólo se asigna valor probatorio cuando son protocolares.

ART.44- En materia de instrumentos privados, se elimina el requisito del doble ejemplar.

Con ello se sigue el criterio definido por el Proyecto de Código Único de 1987, que había contado con el aval de la doctrina que lo comentó.

Lo relevante es que se regula expresamente el valor probatorio del documento electrónico, que se vincula a los usos, a las relaciones preexistentes de las partes y a la confiabilidad de los métodos usados para asegurar la inalterabilidad del texto. Cabe apuntar que en cuanto a la noción de firma y de valor probatorio, se han tenido especialmente en consideración la ley modelo de comercio electrónico elaborada por UNCITRAL, el Código de Québec y las tentativas de reforma del Código Civil francés en materia de prueba.

ART.46- La contabilidad y estados contables tienen un tratamiento con numerosas novedades.

En esta materia se siguen los pasos de los Proyectos de Código Único de 1987 y los de 1993 (el de la Comisión Federal y el de la Comisión designada por decreto 468/92). El sistema propuesto prevé que el interesado pueda llevar el sistema de registración mediante métodos mecánicos, electrónicos o libros.

Forma y prueba de los actos jurídicos.

ART. 260. - Libertad de formas. Si la ley no designa una forma determinada para un acto jurídico, las partes pueden usar las formas que juzguen convenientes

ART. 261. - Forma impuesta. Sanción. Si la ley impone una forma para la validez del acto éste es inválido si la forma exigida no ha sido satisfecha.

Si la ley no impone una forma determinada, ésta constituye sólo un medio de prueba del otorgamiento del acto.

ART. 262. - Forma convenida. Si las partes convienen por escrito la forma a que han de sujetar la conclusión de un acto jurídico futuro, entiéndase que sólo quedarán vinculadas por la forma convenida.

ART. 263. - Expresión escrita. La expresión escrita puede tener lugar por instrumentos públicos o por instrumentos particulares firmados o no firmado, salvo los casos en que determinada forma de instrumento sea exclusivamente impuesta. Puede hacerse constar en cualquier soporte siempre que su contenido pueda ser representado como texto inteligible aunque para su lectura se requiera la intervención de medios técnicos.

ART. 264. - Instrumentos particulares. Son instrumentos particulares, si no están firmados, los impresos, los registros visuales o auditivos de cosas o hechos y, cualquiera que sea el medio empleado, los registros de la palabra y de información, y en general todo escrito no firmado.

ART. 265. - Instrumentos privados. Son instrumentos privados los instrumentos particulares firmados.

ART.266.- Firma. La firma prueba la declaración de voluntad expresada en el texto al cual corresponde. Debe ser manuscrita y consistir en el nombre del firmante, o en un signo, escritos del modo en que habitualmente lo hace a tal efecto.

En los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho si se utiliza un método para identificarla; y ese método asegura razonablemente la autoría e inalterabilidad del instrumento.

ART. 268. - Requisitos. Son recaudos de validez del instrumento público:

e) Que el instrumento conste en el soporte exigido por la ley o las reglamentaciones. Los instrumentos generados por medios electrónicos deben asegurar la autenticidad, integridad e inalterabilidad del contenido del instrumento y la identificación del oficial público.

ART.269.- Validez como instrumento privado. El instrumento que no reúne los recaudos del artículo precedente, vale como instrumento privado si lo han firmado los comparecientes

Escrituras públicas y actas.

ART.277.- Requisitos. El escribano debe recibir por sí mismo las declaraciones de los comparecientes. Las escrituras públicas, que deben extenderse en un único acto, pueden ser manuscritas o mecanografiadas, pudiendo utilizarse mecanismos electrónicos de procesamiento de textos, siempre que en definitiva el texto resulte estampado en el soporte exigido por las reglamentaciones, con caracteres fácilmente legibles.

En los casos de pluralidad de otorgantes en los que no haya entrega de dinero, títulos valores o cosas en presencia del escribano, los interesados pueden suscribir la escritura en distintas horas del mismo día de su otorgamiento, dejándose constancia de ello en el protocolo. Este procedimiento puede usarse siempre que no se modifique el texto definitivo después de la primera firma.

Luego de este vistazo al proyecto de código civil argentino, podemos decir que este ha adoptado una postura de "Tecnología Neutra", en esta materia, sin definir específicamente el método que asegure efectivamente la autoría e inalterabilidad del documento.

La utilización de una "Tecnología Neutra", no impide que en algún momento se opte por otra o varias tecnologías a legislar, pero así, se evita que el paso del tiempo vuelva obsoleto al código.

B. Análisis de la ley Argentina de firma digital (Ley 25.506)

Con la puesta en común de varios proyectos que tenían trámite parlamentario, el Congreso de la Nación Argentina dio sanción a la Ley de Firma Digital.

Una de las cuestiones más debatidas en cuanto a la política legislativa en el derecho comparado ha sido referida a si la Ley de Firma Digital debe ser una ley de principios generales o bien una disposición que imponga tecnologías específicas, como la criptografía asincrónica.

La ley Argentina se inclina por seguir el modelo de principios y reglas generales, ya que el modelo utilizado para la elaboración de esta ley ha sido "La Ley Modelo aprobada por la Comisión de las Naciones unidas para el derecho mercantil internacional, Uncitral".

*Objetivos del legislador

El objetivo de la ley argentina (Art. 1) es reconocer "el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley".

El texto se refiere a las fuentes de legitimación de la firma, que naturalmente surge de un acuerdo de partes, al que la norma reconoce y da eficacia en cuanto a su oponibilidad ínter partes y frente a terceros.

También es posible extraer de esta norma objetivos generales:

- Dar eficacia jurídica a la firma digital

- Dar eficacia jurídica a la firma electrónica

- Dar eficacia jurídica al documento electrónico.

A fin de facilitar el comercio electrónico internacional, se reconoce la validez de certificados digitales emitidos por certificadores extranjeros cuando los mismos reúnan las condiciones que establece la ley.

Para promover la masificación del uso de esta herramienta e impulsar la despapelización del sector público nacional, el artículo 48 establece un plazo máximo de

cinco años para que se aplique la tecnología de firma digital a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanadas de las respectivas jurisdicciones.

*Distingo entre la firma y la tecnología utilizada para firmar

En las relaciones jurídicas por medios electrónicos surge un problema de recognoscibilidad: en qué condiciones existe un documento y cuando es atribuible a su autor.

En el mundo de los átomos y de la escritura es posible realizar una comparación entre el documento original y el falso para deducir la autenticidad; es factible la prueba empírica respecto de la firma consignada en el documento.

En el mundo virtual no es posible, el documento original puede ser igual que el falso porque no hay bits falsos, un bits hará una copia exacta de otro bits original.

En cuanto a la firma, no hay una obra de la mano del autor, no hay una firma en el sentido que se le da a la palabra en la cultura escrita. La firma es un medio para vincular un documento con su autor.

En la cultura escrita se utilizó la grafía del autor en toda una serie de garantías de autenticidad para ese acto, según la importancia del mismo (ejemplo: para casarse hay un oficial público, para transferir un inmueble hay un notario y si es para obligarse a pagar un cupón de una tarjeta de crédito, es suficiente su sola presencia).

En la tarjeta de crédito, como en otros supuestos similares se ha llegado a prescindir de la firma, siendo suficiente el envío de los datos de identificación y una clave.

En el mundo digital se avanza en este sentido: se permite que el medio para vincular un documento a su autor sea una clave y no la firma ológrafa.

En un sentido amplio, la firma es cualquier método o símbolo utilizado por una parte con la intención de vincularse o autenticar un documento.

Las técnicas pueden ser muy diferentes: desde la firma ológrafa hasta la clave en la criptografía. La diferencia entre todos estos sistemas técnicos es la seguridad que ofrecen y por ello la criptografía en doble clave es el mejor para el medio electrónico, pero nada impide que en un futuro no muy lejano exista otro medio mejor y, en ese caso caerían en desuso las leyes diseñadas en virtud de esta asimilación.

La ley Argentina para evitar los riegos de la caducidad tecnológica no se ha inclinado por regular una técnica específica de firma digital.

*Distingo entre firma electrónica y firma digital

La firma electrónica es un género, caracterizado por el soporte: todo modo de identificación de auditoría basado en medios electrónicos es firma; luego vienen las especies, que en general, se caracterizan por agregar elementos de seguridad que la sola firma electrónica no posee.

Las legislaciones reconocen el género de la firma electrónica y luego eligen una especie que denominan "firma electrónica avanzada" o "firma digital", que es la que utiliza un sistema, generalmente criptográfico, que da seguridad.

La gran diferencia está en que cuando se utiliza la firma digital se aplican presunciones iuris tantum sobre la identidad del firmante y la integridad del documento que firmó.

*Elementos de la firma digital

Independientemente de la criptografía, la firma digital se caracteriza por los siguientes elementos:

- **Elemento objetivo-soporte:** en un sentido negativo, el soporte no es escrito y no hay una elaboración manual del autor. En un sentido positivo, la firma es cualquier símbolo o procedimiento de seguridad usado por una persona que incluye medios electrónicos, digitales, magnéticos, ópticos o similares. Puede advertirse, entonces, que la firma electrónica no necesariamente debe ir anexa a un documento, como ocurre en el caso de la firma ológrafa.

- **Elemento subjetivo:** los símbolos asentados en medios electrónicos tienen un propósito específico: se hacen para identificar a la persona e indicar su aprobación del contenido de un mensaje electrónico.

Con estos dos elementos hay firma electrónica pero no firma digital, pues para que se le asigne los efectos de presunción se requiere más seguridad:

Esfera de control del titular: siendo un elemento de imputación de autoría, es lógico que se requiera que esté bajo el control del titular, ya que sólo él es quien decide que

declaraciones de voluntad son suyas. Por ello, es necesario que la firma pertenezca únicamente a su titular y se encuentre bajo su control exclusivo.

Derechos de verificación del receptor: es necesario que los sistemas utilizados puedan ser verificados por el receptor para asegurarse de la autoría.

*Noción de firma digital en la ley

La ley define a la firma digital (Art. 2) diciendo que es el "... **resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.**

Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes".

De acuerdo con la norma, los elementos de calificación de la firma digital son:

- Debe existir un documento digital;
- Se debe aplicar sobre dicho documento un procedimiento matemático que requiere información de exclusivo conocimiento del firmante;
- Debe existir un absoluto control del firmante sobre esa información;
- Debe permitir una verificación por parte de los terceros respecto de la identidad del firmante y de cualquier alteración del documento digital con posterioridad a su firma;
- El procedimiento de verificación debe ser determinado por la autoridad de aplicación.

La ley define a la firma electrónica (Art. 5) como el "**... conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez".**

De modo que la diferencia entre una firma digital y una firma electrónica es simplemente que a la segunda le falta alguno de los requisitos legales de la primera.

*Requisitos de validez

La ley establece (Art. 9) que: "Una firma digital es válida si cumple con los siguientes requisitos:

a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante;

b) Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente;

c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado".

*Equiparación de los efectos jurídicos y ámbitos de aplicación

El artículo 3 dice: "Del requerimiento de firma. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia".

El primer párrafo prevé el principio de no-discriminación, lo que significa que cuando la ley establece el requerimiento de firma, tanto puede cumplirse con la modalidad manuscrita como con la digital.

El segundo párrafo limita estos efectos, excluyendo los casos en que existe una obligación de firmar o se establecen consecuencias jurídicas derivadas de la ausencia de firma. Esta segunda regla es una excepción respecto de la regla general de la equiparación de los efectos y se complementa con el Art. 4, que establece:

"Exclusiones. Las disposiciones de esta ley no son aplicables:

a) A las disposiciones por causa de muerte;

b) A los actos jurídicos del derecho de familia;

c) A los actos personalismos en general;

d) A los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes".

*Documento digital

El documento digital es (Art.6): "la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura".

El documento digital tiene como principal efecto el dar por cumplido el requisito de forma escrita, cuando la ley así lo requiere y con las excepciones ya mencionadas.

La ley establece que (Art. 7): "Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma".

Esta norma se complementa con el Art. 10 que dice: "Remitente. Presunción. Cuando un documento digital sea enviado en forma automática por un dispositivo programado y lleve la firma digital del remitente se presumirá, salvo prueba en contrario, que el documento firmado proviene del remitente".

La ley dispone (Art. 8) que: "Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma".

*Documento electrónico original, duplicado y falsificado

La ley dice al respecto en su Art. 11: "Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación".

El documento electrónico puede ser firmado o no y, en ambos casos, puede haber un original y un duplicado; este último puede ser legítimamente emitido por el autor o por un tercero, o bien ser una falsificación ilegitima.

Como hemos señalado anteriormente la dificultad que ofrece el documento electrónico reside en que el original es igual al duplicado, ya que los bites son idénticos, por lo que no son aplicables los procedimientos legales elaborados con relación a la duplicación y falsificación del documento escrito.

El concepto de documento original y duplicado no tiene base empírica, sino que deberá surgir de una definición de las partes en el contrato o del legislador; en este último caso, la tendencia se orienta a tomar en cuenta el criterio de la "primera generación", en el sentido de "primera elaboración", y la segunda para referirse al duplicado.

*Conservación

La ley dice en el Art. 12: "La exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción".

Uno de los problemas relevantes es el de la conservación, ya que existe la impresión generalizada de que el documento electrónico puede desaparecer en un instante y ofrece menos seguridades que el escrito. Paradójicamente, el documento electrónico se ha ido transformando en la principal fuente de archivo de la cultura escrita, ya que por razones de espacio, los documento escritos se traducen en bites para su conservación. La realidad es que puede ser mucho más seguro y conservable que la forma escrita.

En una relación jurídica, las partes tienen la opción de utilizar la tecnología digital para guardar los documentos que emiten, o para hacerlos desaparecer, ya sea que esto sea decidido por una de ellas para perjudicar a la otra, o por ambas para eludir a terceros. Consecuentemente el problema no reside en la tecnología, sino en las obligaciones de conservación que las partes deben asumir.

Una vez decidida la conservación deviene otro problema: se ha creado una base de datos que interesa a las partes, pero también a terceros. Por ello debe establecerse que la guarda de datos tenga una forma fiable y sea accesible.

*Certificados digitales

El certificado digital tiene por función básica la de autorizar la comprobación de la identidad del firmante, pero además debe permitir que el titular los reconozca indubitablemente, conocer su período de vigencia, determinar que no ha sido revocado, reconocer claramente la inclusión de información no verificada, especificar tal información, contemplar la información necesaria, para la verificación de la firma, identificar claramente al emisor del certificado digital.

La ley 25.506 en su artículo 13 dice que: **"Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular".**

Para ser válidos, los certificados deben cumplir, según el Art. 14, con los siguientes requisitos:

a) Ser emitidos por un certificador licenciado por el ente licenciante;

b) Responder a formatos estándares reconocidos internacionalmente, fijados por la autoridad de aplicación, y contener, como mínimo, los datos que permitan:

1. Identificar indubitablemente a su titular y al certificador licenciado que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única;

2. Ser susceptible de verificación respecto de su estado de revocación;

3. Diferenciar claramente la información verificada de la no-verificada incluidas en el certificado;

4. Contemplar la información necesaria para la verificación de la firma;

5. Identificar la política de certificación bajo la cual fue emitido.

El certificado tiene un período de vigencia (Art. 15) y "... es válido únicamente dentro del período de vigencia, que comienza en la fecha de inicio y finaliza en su fecha de vencimiento, debiendo ambas ser indicadas en el certificado digital, o su revocación si fuere revocado.

La fecha de vencimiento del certificado digital referido en el párrafo anterior en ningún caso puede ser posterior a la del vencimiento del certificado digital del certificador licenciado que lo emitió.

La Autoridad de Aplicación podrá establecer mayores exigencias respecto de la determinación exacta del momento de emisión, revocación y vencimiento de los certificados digitales".

La ley en el artículo 16 establece: "Los certificados digitales emitidos por certificadores extranjeros podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley y sus normas reglamentarias cuando:

a) Reúnan las condiciones que establece la presente ley y la reglamentación correspondiente para los certificados emitidos por certificadores nacionales y se encuentre vigente un acuerdo de reciprocidad firmado por la República Argentina y el país de origen del certificador extranjero, o

b) Tales certificados sean reconocidos por un certificador licenciado en el país, que garantice su validez y vigencia conforme a la presente ley. A fin de tener efectos, este reconocimiento deberá ser validado por la autoridad de aplicación".

*El certificador licenciado

Conforme al artículo 17, "Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante.

La actividad de los certificadores licenciados no pertenecientes al sector público se prestará en régimen de competencia. El arancel de los servicios prestados por los certificadores licenciados será establecido libremente por éstos".

Las funciones del certificador licenciado, según el artículo 19 son las siguientes:

"a) Recibir una solicitud de emisión de certificado digital, firmada digitalmente con los correspondientes datos de verificación de firma digital del solicitante;

b) Emitir certificados digitales de acuerdo a lo establecido en sus políticas de certificación, y a las condiciones que la autoridad de aplicación indique en la reglamentación de la presente ley;

c) Identificar inequívocamente los certificados digitales emitidos;

d) Mantener copia de todos los certificados digitales emitidos, consignando su fecha de emisión y de vencimiento si correspondiere, y de sus correspondientes solicitudes de emisión;

e) Revocar los certificados digitales por él emitidos en los siguientes casos, entre otros que serán determinados por la reglamentación:

1) A solicitud del titular del certificado digital.

2) Si determinara que un certificado digital fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación.

3) Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.

4) Por condiciones especiales definidas en su política de certificación.

5) Por resolución judicial o de la autoridad de aplicación.

f) Informar públicamente el estado de los certificados digitales por él emitidos. Los certificados digitales revocados deben ser incluidos en una lista de certificados revocados indicando fecha y hora de la revocación. La validez y autoría de dicha lista de certificados revocados deben ser garantizadas".

El certificador debe obtener una licencia (Art. 20) para lo cual "... debe cumplir con los requisitos establecidos por la ley y tramitar la solicitud respectiva ante el ente licenciante, el que otorgará la licencia previo dictamen legal y técnico que acredite la aptitud para cumplir con sus funciones y obligaciones. Estas licencias son intransferibles".

*Organización institucional

La firma digital requiere un marco institucional que produzca confianza.

Evidentemente puede haber una firma de este tipo mediante un acuerdo celebrado entre dos partes, las cuales se obligan a reconocerla según los criterios que los contratantes fijen, y ello no ofrece ninguna dificultad.

Sin embargo, el costo de negociar estos acuerdos es alto entre las partes que no se conocen o que están situados en lugares lejanos y no tienen referencias; por ello, para que exista un uso difundido y rápido, se utiliza un tercero que certifica.

La figura del tercero otorga confianza y disminuye los costos de la transacción. El problema es quién es ese tercero, que hace y con qué extensión.

En la práctica negocial han surgido organizaciones que proveen de certificados y que se hacen confiables por su conducta y el apoyo que van logrando en la comunidad. La expansión de estos procedimientos de adhesión voluntaria se produce, generalmente, en grupos cerrados o que reconocen algún límite, pero es difícil para ellos lograr un reconocimiento generalizado de su actuación.

Por esta razón, muchas legislaciones regulan un sistema institucional que requiere del registro público de las autoridades certificantes.

La ley Argentina organiza una serie de instituciones para afianzar la confiabilidad del certificado.

*Auditoria

Además de la emisión por parte de un certificador licenciado (Art. 26) se establece un sistema auditoria (Art. 27), en los siguientes términos: "La autoridad de aplicación, con el concurso de la Comisión Asesora para la Infraestructura de Firma Digital, diseñará un sistema de auditoría para evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, así como también el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y de contingencia aprobados por el ente licenciante".

Los sujetos a auditar (Art. 33) son el ente licenciante y los certificadores licenciados.

La autoridad de aplicación podrá implementar el sistema de auditoría por sí o por terceros habilitados a tal efecto.

Asimismo se establece en el artículo 34 que:" Podrán ser terceros habilitados para efectuar las auditorias las Universidades y organismos científicos y/o tecnológicos nacionales o provinciales, los Colegios y Consejos profesionales que acrediten experiencia profesional acorde en la materia".

*Comisión asesora

También se establece (Art. 28) una comisión asesora para la infraestructura de firma digital.

La comisión asesora (Art. 35) "... estará integrada multidisciplinariamente por un máximo de 7 (siete) profesionales de carreras afines a la actividad de reconocida trayectoria y experiencia, provenientes de Organismos del Estado nacional, Universidades Nacionales y Provinciales, Cámaras, Colegios u otros entes representativos de profesionales.

Los integrantes serán designados por el Poder Ejecutivo por un período de cinco (5) años renovables por única vez.

Se reunirá como mínimo trimestralmente. Deberá expedirse prontamente a solicitud de la autoridad de aplicación y sus recomendaciones y disidencias se incluirán en las actas de la Comisión.

Consultará periódicamente mediante audiencias públicas con las cámaras empresarias, los usuarios y las asociaciones de consumidores y mantendrá a la autoridad de aplicación regularmente informada de los resultados de dichas consultas".

Son sus funciones según el artículo 36: "...emitir recomendaciones por iniciativa propia o a solicitud de la autoridad de aplicación, sobre los siguientes aspectos:

a) Estándares tecnológicos;

b) Sistema de registro de toda la información relativa a la emisión de certificados digitales;

c) Requisitos mínimos de información que se debe suministrar a los potenciales titulares de certificados digitales de los términos de las políticas de certificación;

d) Metodología y requerimiento del resguardo físico de la información;

e) Otros que le sean requeridos por la autoridad de aplicación".

*Autoridad de aplicación

Finalmente se dispone que la autoridad de aplicación será la jefatura de gabinete de ministros (Art. 29). Sus funciones son (Art. 30):

"a) Dictar las normas reglamentarias y de aplicación de la presente;

b) Establecer, previa recomendación de la Comisión Asesora para la Infraestructura de la Firma Digital, los estándares tecnológicos y operativos de la Infraestructura de Firma Digital;

c) Determinar los efectos de la revocación de los certificados de los certificadores licenciados o del ente licenciante;

d) Instrumentar acuerdos nacionales e internacionales a fin de otorgar validez jurídica a las firmas digitales creadas sobre la base de certificados emitidos por certificadores de otros países;

e) Determinar las pautas de auditoría, incluyendo los dictámenes tipo que deban emitirse como conclusión de las revisiones;

f) Actualizar los valores monetarios previstos en el régimen de sanciones de la presente ley;

g) Determinar los niveles de licenciamiento;

h) Otorgar o revocar las licencias a los certificadores licenciados y supervisar su actividad, según las exigencias instituidas por la reglamentación;

i) Fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los certificadores licenciados;

j) Homologar los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la reglamentación;

k) Aplicar las sanciones previstas en la presente ley".

Se establecen las siguientes obligaciones en el artículo 31:

"a) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder, bajo ninguna circunstancia, a los datos utilizados para generar la firma digital de los certificadores licenciados;

b) Mantener el control exclusivo de los datos utilizados para generar su propia firma digital e impedir su divulgación;

c) Revocar su propio certificado frente al compromiso de la privacidad de los datos de creación de firma digital;

d) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, números telefónicos y direcciones de Internet tanto de los certificadores licenciados como los propios y su certificado digital;

e) Supervisar la ejecución del plan de cese de actividades de los certificadores licenciados que discontinúan sus funciones".

La autoridad de aplicación, según el artículo 32, podrá cobrar un arancel de licenciamiento para cubrir sus costos operativos y de las auditorías realizadas por sí o por terceros contratados a tal efecto.

*Responsabilidad

En la legislación de la Unión Europea se prevé un sistema de responsabilidad por culpa que será contractual frente a las partes y extracontractual frente a los terceros.

El sistema de la ley Argentina es el siguiente:

- Responsabilidad contractual (Art. 37):

"La relación entre el certificador licenciado que emita un certificado digital y el titular de ese certificado se rige por el contrato que celebren entre ellos, sin perjuicio de las previsiones de la presente ley, y demás legislación vigente".

- Responsabilidad extracontractual (Arts. 38 y 39):

"El certificador que emita un certificado digital o lo reconozca en los términos del artículo 16 de la presente ley, es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de ésta, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos, en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá al prestador del servicio demostrar que actuó con la debida diligencia".

Los certificadores licenciados no serán responsables en los siguientes casos:

"a) Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstos en la ley;

b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;

c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el certificador pueda demostrar que ha tomado todas las medidas razonables".

- Responsabilidad administrativa:

El ente licenciante puede aplicar sanciones conforme a la ley 19.549 de procedimientos administrativos y sus normas reglamentarias, las que pueden consistir en lo siguiente (Art. 41):

"a) Apercibimiento;

b) Multa de pesos diez mil ($ 10.000) a pesos quinientos mil ($ 500.000);

c) Caducidad de la licencia.

*El tecnolenguaje

Como todas las leyes de este tipo, se introduce un anexo con el tecnolenguaje, explicando el significado de los elementos técnicos. El anexo de la ley 25.506 dice lo siguiente:

- "Información: conocimiento adquirido acerca de algo o alguien.
- Procedimiento de verificación: proceso utilizado para determinar la validez de una firma digital. Dicho proceso debe considerar al menos:

- que dicha firma digital ha sido creada durante el período de validez del certificado digital del firmante;

- que dicha firma digital ha sido creada utilizando los datos de creación de firma digital correspondientes a los datos de verificación de firma digital indicados en el certificado del firmante;

- la verificación de la autenticidad y la validez de los certificados involucrados.

- Datos de creación de firma digital: datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear su firma digital.

- Datos de verificación de firma digital: datos únicos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma digital, la integridad del documento digital y la identidad del firmante.

- Dispositivo de creación de firma digital: dispositivo de hardware o software técnicamente confiable que permite firmar digitalmente.

- Dispositivo de verificación de firma digital: dispositivo de hardware o software técnicamente confiable que permite verificar la integridad del documento digital y la identidad del firmante.

- Políticas de certificación: reglas en las que se establecen los criterios de emisión y utilización de los certificados digitales.

- Técnicamente confiable: cualidad del conjunto de equipos de computación, software, protocolos de comunicación y de seguridad y procedimientos administrativos relacionados que cumplan los siguientes requisitos:

  - Resguardar contra la posibilidad de intrusión y/o uso no autorizado;

  - Asegurar la disponibilidad, confiabilidad, confidencialidad y correcto funcionamiento;

  - Ser apto para el desempeño de sus funciones específicas;

  - Cumplir las normas de seguridad apropiadas, acordes a estándares internacionales en la materia;

  - Cumplir con los estándares técnicos y de auditoría que establezca la Autoridad de Aplicación.

- Clave criptográfica privada: En un criptosistema asimétrico, es aquella que se utiliza para firmar digitalmente.

- Clave criptográfica pública: En un criptosistema asimétrico, es aquella que se utiliza para verificar una firma digital.

- Integridad: Condición que permite verificar que una información no ha sido alterada por medios desconocidos o no autorizados.

C. Reglamentación de la ley de firma digital

El 19 de diciembre del año 2002, se sancionó el decreto reglamentario de la ley de Firma Digital, el cual, dentro de sus considerandos, va a destacar la importancia que tiene la firma digital para el comercio en nuestro país, diciendo "Que la.....firma digital representa un avance significativo para la inserción, de nuestro país en la sociedad de la información y en la economía digital, brindando una oportunidad para el desarrollo del sector productivo vinculado a las nuevas tecnologías."

Además va a destacar la importancia que tiene la misma para la despapelización del estado, la importancia que tiene la ley de Firma Digital, tanto en el ámbito nacional como en el internacional, para la gestión del estado, entre otros.

El decreto establece lo siguiente:

- Consideraciones generales

En el artículo 1°, establece cual es el objeto, del decreto y dice "...la presente reglamentación regula el empleo de la firma electrónica y de la firma digital y su eficacia jurídica. En los casos contemplados por los artículos 3°, 4° y 5° de la Ley N° 25.506 podrán utilizarse los siguientes sistemas de comprobación de autoría e integridad:

- Firma electrónica
- Firma digital basada en certificados digitales emitidos por certificadores no licenciados en el marco de la presente reglamentación,
- Firma digital basada en certificados digitales emitidos por certificadores licenciados en el marco de la presente reglamentación,
- Firma digital basada en certificados digitales emitidos por certificadores extranjeros que hayan sido reconocidos en los siguientes casos:

1. En virtud de la existencia de acuerdos de reciprocidad entre la República Argentina y el país de origen del certificador extranjero.

2. Por un certificador licenciado en el país en el marco de la presente reglamentación y validado por la Autoridad de Aplicación."

En cuanto a la validez de los certificados (Art. 2°), nos dice "...Los certificados digitales emitidos por certificadores no licenciados serán válidos para producir los efectos jurídicos que la ley otorga a la firma electrónica."

En cuanto a la conservación de los documentos electrónicos el Art. 5°, nos dice "... El cumplimiento de la exigencia legal de conservar documentos, registros o datos, conforme a la legislación vigente a la materia, podrá quedar satisfecha con la conservación de los correspondientes, documentos digitales firmados digitalmente. Los documentos, registros o datos electrónicos, deberán ser almacenados por los intervinientes o por terceros confiables aceptados por los intervinientes, durante los plazos establecidos en las normas específicas. Se podrán obtener copias autenticadas a partir de los originales en formato digital firmado digitalmente. La certificación de autenticidad se hará de conformidad a los procedimientos legales, vigentes para el acto de que se trate, identificando el soporte que procede la copia."

Según el artículo 6°, se faculta a la JEFATURA DE GABINETE DE MINISTROS a establecer:

Los estándares tecnológicos y de seguridad aplicables en consonancia con estándares internacionales.

Los procedimientos de firma y verificación en consonancia con los estándares tecnológicos definidos conforme el inciso precedente.

Las condiciones mínimas de emisión de certificados digitales.

Los casos en los cuales deben revocarse los certificados digitales

Los datos considerados públicos contenidos en los certificados digitales.

Los mecanismos que garantizarán la validez y autoría de las listas de certificados revocados.

La información que los certificadores licenciados deberán publicar por internet.

La información que los certificadores licenciados deberán publicar en el Boletín Oficial.

Los procedimientos mínimos de revocación de certificados digitales cualquiera que sea la fuente de emisión, y los procedimientos mínimos de conservación de la documentación de

respaldo de la operatoria de los certificadores licenciados, en el caso que éstos cesen su actividad.

El sistema de auditoría, incluyendo las modalidades de difusión de los informes de auditoría y los requisitos de habilitación para efectuar auditorias.

Las condiciones y procedimientos para el otorgamiento y revocación de las licencias.

Las normas y procedimientos para la homologación de los dispositivos de creación y verificación de firmas digitales.

El reglamento de funcionamiento de la Comisión Asesora para la Infraestructura de Firma Digital.

El procedimiento de instrucción sumarial y la gradación de sanciones previstas en la Ley N° 25.506, en virtud de reincidencia y/u oportunidad.

Los procedimientos aplicables para el reconocimiento de certificados extranjeros

Las condiciones de aplicación de la presente ley en el Sector Público Nacional, incluyendo la autorización para prestar servicios de certificación digital para las entidades y jurisdicciones de la Administración Pública Nacional.

Los contenidos mínimos de las políticas de certificación de acuerdo con los estándares nacionales e internacionales y las condiciones mínimas que deberán cumplirse en el caso de cese de actividades de un certificador licenciado.

Los niveles de licenciamiento.

Reglamentar el uso y los alcances de los certificados de firma digital emitidos por los Registros Públicos de Contratos.

Exigir las garantías y seguros necesarios para prestar el servicio previsto.

Las condiciones de prestación de otros servicios en relación con la firma digital y otros temas cubiertos en la ley."

- <u>De la comisión asesora para la infraestructura de firma digital</u>

Según el Articulo 7°, "..... En el ámbito de la JEFATURA DE GABINETE DE MINISTROS funcionará la Comisión Asesora para la Infraestructura de Firma Digital, que se constituirá de acuerdo a lo dispuesto por el artículo 35 de la Ley N° 25.506."

Según el Articulo 8° "..... La Comisión Asesora para la Infraestructura de Firma Digital estará integrada multidisciplinariamente por profesionales de carreras afines a la actividad, de reconocida trayectoria y experiencia, provenientes de organismos del Estado Nacional, Universidades, Cámaras, Colegios u otros entes representativos profesionales. Para integrar la Comisión Asesora para la Infraestructura de Firma Digital se deberán reunir los siguientes requisitos:

Poseer título universitario, expedido por Universidad Nacional o privada reconocida por el Estado, correspondiente a carrera profesional de duración no inferior a CUATRO (4) años, con incumbencias relacionadas con la materia.

- Del ente administrador de firma digital

En el artículo 11°, se crea el Ente Administrador de Firma Digital y se determinan sus funciones y según el artículo 12° el ente estará constituido por".....por un Directorio integrado por TRES (3) miembros, designados por el JEFE DE GABINETE DE MINISTROS, previo concurso.....uno de los cuales ocupará el cargo de Presidente del Ente. El gerenciamiento del Ente estará a cargo del Coordinador Ejecutivo designado por el JEFE DE GABINETE DE MINISTROS."

Según el artículo 13°, "Son funciones del Ente Administrador:

- Otorgar las licencias habilitantes para acreditar a los certificadores en las condiciones que fijen el presente decreto y las normas reglamentarias, modificatorias o de aplicación que se dicten en el futuro.
- Fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los certificadores licenciados.
- Denegar las solicitudes de licencia a los prestadores de servicios de certificación que no cumplan con los requisitos establecidos, para su licenciamiento.
- Revocar las licencias otorgadas a los Certificadores licenciados que dejen de cumplir con los requisitos establecidos para su licenciamiento.
- Aprobar las políticas de certificación, el manual de procedimiento, el plan de seguridad, de cese de actividades y el plan de contingencia, presentado por los certificadores solicitantes de la licencia o licenciados.

- Solicitar los informes de auditoría en los casos que correspondiere.
- Realizar inspecciones a los certificadores licenciados por sí o por terceros.
- Homologar los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la presente reglamentación.
- Disponer la instrucción sumarial, la aplicación de sanciones e inhabilitar en forma temporal o permanente a todo certificador o licenciado que no respetare o incumpliere los requerimientos y disposiciones de la Ley N° 25.506, el presente decreto y las normas complementarias.
- Dictar las normas tendientes a asegurar el régimen de libre competencia, equilibrio de participación en el mercado de los prestadores y protección de los usuarios."

Y según el articulo 14°, "..... El Ente Administrador tiene idénticas obligaciones que los titulares, de certificados y que los Certificadores Licenciados, en su caso, y además debe:

- Permitir el acceso público permanente a la nómina actualizada de certificadores licenciados con los datos correspondientes.
- Supervisar la ejecución del plan de cese de actividades de los Certificadores licenciados que discontinúan sus funciones;
- Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas.
- Supervisar la ejecución de planes de contingencia de los certificadores licenciados.
- Efectuar las tareas de control del cumplimiento de las recomendaciones formuladas por el Ente Administrador para determinar si se han tomado las acciones correctivas correspondientes.
- Recibir, evaluar y resolver los reclamos de los usuarios de certificados digitales relativos a la prestación del servicio por parte de certificadores licenciados."

En cuanto a los recursos para cubrir sus costos, según el artículo 16 "....Los recursos propios del Ente Administrador se integrarán con:

a) Los importes provenientes de los aranceles que se abonen por la provisión de los siguientes servicios:

1.Servicios de certificación digital,

2.Servicios de certificación digital de fecha y hora,

3.Servicios de almacenamiento seguro de documentos electrónicos,

4.Servicios prestados por autoridades de registro,

5.Servicios prestados por terceras partes confiables,

6.Servicios de certificación de documentos electrónicos firmados digitalmente

7.Otros servicios o actividades relacionados a la firma digital.

b) Los importes provenientes de los aranceles de homologación de dispositivos de creación y verificación de firmas digitales.

c) Los importes provenientes de los aranceles de certificación de sistemas que utilizan firma digital.

d) Los importes provenientes de los aranceles de administración del sistema de auditoría y las auditorias que el organismo realice por sí o por terceros.

e) Los subsidios, herencias, legados, donaciones o transferencias bajo cualquier título que reciba.

f) El producido de multas.

g) Los importes que se le asignen en el cálculo de recursos de la respectiva ley de presupuesto para la administración nacional.

h) Los demás fondos, bienes, o recursos que puedan serle asignados en virtud de las leyes y reglamentaciones aplicables."

- Del sistema de auditoria

Según el artículo 18°, la JEFATURA DE GABINETE DE MINISTROS, llevará a cabo un concurso público, para la precalificación de entidades de auditoría, en el artículo 19°, se nombra el informe de auditoría, el cual será según lo establecido en el ley 25.506.

En el artículo 20°, trata sobre quienes no pueden ser entidades de auditoría porque estaríamos frente a un conflicto de intereses, con lo cual sería imposible garantizar la imparcialidad de las mismas.

El artículo 21°, trata sobre el deber de confidencialidad que tienen estas entidades, para con la información que ellas recauden en el ejercicio de sus funciones.

- De la revocación de certificados digitales

Según el artículo 23°, "..... Se deberán revocar los certificados digitales emitidos en los siguientes casos:

a) A solicitud del titular del certificado digital

b) Si se determina que un certificado digital fue emitido en base a una información falsa que en el momento de la emisión hubiera sido objeto de verificación.

c) Si se determina que los procedimientos de emisión y/o verificación han dejado de ser seguros.

d) Por condiciones especiales definidas en las Políticas de Certificación

e) Por Resolución Judicial o de la Autoridad de Aplicación debidamente fundada.

f) Por fallecimiento del titular.

g) Por declaración judicial de ausencia con presunción de fallecimiento del titular.

h) Por declaración judicial de incapacidad del titular.

i) Si se determina que la información contenida en el certificado ha dejado de ser válida.

j) Por el cese de la relación de representación respecto de una persona."

- De los certificadores licenciados

Según el artículo 24°, "..... Para obtener una licencia, los proveedores de servicios de certificación deberán particularizar las actividades para las cuales requieren la licencia y acreditar por los medios que este determine ante el Ente Administrador de Firma Digital:

a) Documentación que demuestre:

1.En el caso de personas jurídicas, su personería.

2.En el caso de registro público de contratos, tal condición

3.En el caso de organización pública, la autorización de su máxima autoridad para iniciar el proceso de licenciamiento y la correspondiente aprobación de la JEFATURA DE GABINETE DE MINISTROS, de acuerdo con lo dispuesto en el artículo 41 de la presente reglamentación.

b) El cumplimiento de las condiciones establecidas en la ley; este decreto y las normas complementarias.

c) Las políticas de certificación para las cuales solicita licencia que respaldan la emisión de sus certificados, Manual de Procedimientos, Plan de Seguridad, Plan de Cese de Actividades y Plan de Contingencia satisfactorias de acuerdo con las normas reglamentarias.

d) Toda aquella información o requerimiento, que demande la Autoridad de Aplicación."

Según el artículo 29° ".....La JEFATURA DE GABINETE DE MINISTROS definirá el contenido, mínimo de las políticas de certificación de acuerdo con los estándares nacionales e internacionales vigentes, las que deberán contener al menos la siguiente información:

a) Identificación del certificador licenciado.

b) Política de administración de los certificados y detalles de los servicios arancelados.

c) Obligaciones de la entidad y de los suscriptores de los certificados.

d) Tratamiento de la información suministrada por los suscriptores, y resguardo de la confidencialidad en su caso.

e) Garantías que ofrece para el cumplimiento de las obligaciones que se deriven de sus actividades.

Otro requisito que deberán cumplir el certificador licenciado es el de tener un *seguro* (artículo 30°), el que deberá reunir los siguientes requisitos.

"a) Ser expedidos por una entidad aseguradora autorizada para operar en la República Argentina.

b) Establecer la obligación de la entidad aseguradora de informar previamente al Ente Administrador de la Infraestructura de Firma Digital la terminación del contrato o las modificaciones que reduzcan el alcance o monto de la cobertura. Los certificadores licenciados pertenecientes a entidades y jurisdicciones del sector público quedarán exentos de la obligación de constituir el seguro previsto en el presente artículo."

Según el artículo 31°, "......En ningún caso, la responsabilidad que pueda emanar de una certificación efectuada por un certificador licenciado, público o privado, comprometerá la responsabilidad pecuniaria del Estado en su calidad de Ente Administrador de la Infraestructura de Firma Digital."

Según el artículo 32°, ".....Para el desarrollo adecuado de las *actividades de certificación*, el certificador deberá acreditar que cuenta con un equipo de profesionales, infraestructura física tecnológica y recursos financieros, como así también procedimientos y sistemas de seguridad que permitan:

a) Generar en un ambiente seguro las firmas digitales propias y todos los servicios para los cuales solicite licencia.

b) Cumplir con lo previsto en sus políticas y procedimientos de certificación.

c) Garantizar la confiabilidad de los sistemas de acuerdo con los estándares aprobados por la Autoridad de Aplicación.

d) Expedir certificados que cumplan con:

1.Lo previsto en los artículos 13 y 14 de la Ley N° 25.506.

2.Los estándares tecnológicos aprobados por la JEFATURA DE GABINETE DE MINISTROS.

e) Garantizar la existencia de sistemas de seguridad física y lógica que cumplimenten las normativas vigentes.

f) Proteger el manejo de la clave privada de la entidad mediante un procedimiento de seguridad que impida el acceso a la misma a personal no autorizado.

g) Proteger el acceso y el uso de la clave privada mediante procedimientos que exijan la participación de más de una persona.

h) Registrar las transacciones realizadas, a fin de identificar el autor y el momento de cada una de las operaciones.

i) Utilizar con exclusividad los sistemas que cumplan las funciones de certificación con ese propósito, sin que se les asigne ninguna otra función.

j) Proteger a todos los sistemas utilizados directa o indirectamente en la función de certificación con procedimientos de autenticación y seguridad de alto nivel de protección, que deban ser actualizados de acuerdo a los avances tecnológicos para garantizar la correcta prestación de los servicios de certificación.

k) Garantizar la continuidad de las operaciones mediante un Plan de Contingencia actualizado y aprobado.

I) Disponer de los recursos financieros adecuados al tipo de actividad de certificación que desarrolla, acorde con los niveles de responsabilidad derivados de la misma."

- De las autoridades de registro

Según el artículo 35°, ".....Los Certificadores Licenciados podrán delegar en Autoridades de Registro las funciones de validación de identidad y otros datos de los suscriptores de certificados y de registro de las presentaciones y trámites que les sean formuladas, bajo la responsabilidad del Certificador Licenciado, cumpliendo las normas y procedimientos establecidos por la presente reglamentación. Una autoridad de Registro es una entidad responsable de las siguientes funciones:

a) La recepción de las solicitudes de emisión de certificados.

b) La validación de la identidad y autenticación de los datos de los titulares de certificados.

c) La validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador Licenciado.

d) La remisión de las solicitudes aprobadas al Certificador Licenciado con la que se encuentre operativamente vinculada.

e) La recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento al Certificador Licenciado con el que se vinculen.

f) La identificación y autenticación de los solicitantes de revocación de certificados.

g) El archivo y la conservación de toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el certificador licenciado.

h) El cumplimiento de las normas y recaudos establecidos para la protección de datos personales.

i) El cumplimiento de las disposiciones que establezca la Política de Certificación y el Manual de Procedimientos del Certificador Licenciado con el que se encuentre vinculada, en la parte que resulte aplicable."

Y el articulo 36°, nos dice ".....Una Autoridad de Registro puede constituirse como una única unidad o con varias unidades dependientes jerárquicamente entre sí, pudiendo, delegar su operatoria en otras autoridades de registro, siempre que medie la aprobación del Certificador Licenciado. El Certificador, Licenciado es responsable con los alcances establecidos en la Ley N° 25.506, aún en el caso de que delegue parte de su operatoria en Autoridades de Registro, sin perjuicio del derecho del certificador de reclamar a la Autoridad de Registro las indemnizaciones por los daños y perjuicios que aquél sufriera como consecuencia de los actos y/u omisiones de ésta."

- Disposiciones para la administración pública nacional

En este articulo 37°, despapelización del Estado. Sin perjuicio de la aplicación directa de la ley en lo relativo a la validez jurídica de la firma electrónica, de la firma digital y de los documentos digitales, la implementación de las disposiciones de la ley y del presente decreto para la digitalización de procedimientos y trámites internos de la Administración Pública Nacional, de las Administraciones Públicas Provinciales, y de los Poderes Legislativos y Judiciales del orden nacional y provincial, así como los vinculados a la relación de las mencionadas jurisdicciones y entidades con los administrados, se hará de acuerdo a lo que fijen reglamentariamente cada uno de los Poderes y Administraciones.

Según el artículo 38°, ".....Los organismos de la Administración Pública Nacional que para la tramitación de documentos digitales o la implementación de aplicaciones requieran firma digital, solamente aceptarán certificados digitales emitidos por Certificadores, Licenciados, o certificados digitales emitidos por certificadores extranjeros reconocidos por acuerdos internacionales o por certificadores licenciados del país. Las entidades y jurisdicciones pertenecientes al sector público podrán ser certificadores licenciados y emitir certificados para agentes y funcionarios públicos destinados a las aplicaciones de gestión interna de los organismos públicos a que éstos pertenecieran. Cuando razones de orden público o de interés social lo ameriten y cuenten con la autorización de la JEFATURA DE GABINETE

DE MINISTROS podrán emitir certificados a particulares. En aquellas aplicaciones en las que el Estado interactúe con la comunidad, se deberá admitir la recepción de documentos digitales firmados digitalmente utilizando certificados digitales emitidos por certificadores licenciados privados o públicos, indistintamente."

En el artículo 41°, se establece que, la JEFATURA DE GABINETE DE MINISTROS, dictará las normas de aplicación de la presente reglamentación en la Administración Pública Nacional, que deberán contemplar:

"a) Las acciones tendientes a promover el uso masivo de la firma digital con el fin de posibilitar el trámite de los expedientes en forma simultánea, búsquedas automáticas de información, seguimiento y control por parte de los interesados.

b) Las acciones tendientes a implementar la progresiva despapelización del Estado, a fin de contar en un plazo de CINCO (5) años con la totalidad de la documentación administrativa en formato digital.

c) La interoperabilidad entre aplicaciones.

d) La autorización para solicitar el licenciamiento como certificador ante el Ente Administrador de la Infraestructura de Firma Digital para las entidades y jurisdicciones de la Administración Pública Nacional.

e) La participación del Cuerpo de Administradores Gubernamentales a los fines de difundir el uso de la firma digital y facilitar los procesos de despapelización."

Según el artículo 42°, los organismos de la Administración Pública Nacional, serán los encargados de establecer los mecanismos que garanticen la opción de remisión, recepción, mantenimiento y publicación de información electrónica.

4. Beneficios y estrategias de gestión

A. Uso de documentos digitales en el ámbito privado

Las ventajas que brinda este sistema hace que cada vez haya más entidades que se adhieren al mismo, instrumentando los procedimientos necesarios para la operatoria en un marco legal de Derecho Privado (acuerdo entre las partes).

Se utilizan lo que se denominan VAN (Valued Added Networks) o redes de valor agregado que, sin utilizar Internet, permiten establecer un vínculo seguro con la otra u otras partes.

Por otro lado, los esquemas de encripción, manejo de claves, etc. se hacen siguiendo estándares internacionalmente aceptados que brindan no solo los aspectos de seguridad ya mencionados al comienzo, sino también confidencialidad mediante el uso de encripción del texto completo del mensaje (EDI – Electronic Data Interchange)

Edi: Electronic Data Interchange

EDI es el intercambio Electrónico de Documentos Comerciales en formato estandarizado entre las aplicaciones informáticas de empresas relacionadas comercialmente.

Este formato responde a un estándar internacional (EDIFACT/EANCOM) desarrollado por Naciones Unidas y actualmente utilizado en todo el mundo.

A nivel internacional, EDI es el sistema de intercambio de documentos electrónicos estandarizados mas difundido.

A lo largo de los últimos años ha crecido exponencialmente en los países desarrollados tales como E.E.U.U., Japón y países de Europa. A nivel regional, específicamente en América Latina, recién está dando sus primeros pasos.

A continuación se detalla una lista de algunos de los Documentos Estándar disponibles para establecer la comunicación entre entidades:

PARTIN: Este documento proporcionará la información de las partes.

PRICAT: Catálogos de artículos.

ORDERS: Órdenes de compra.

ORDRSP: Respuesta a la orden de compra.

DESADV: Aviso de despacho.

RECADV: Aviso de recibo

INVOIC: Factura

PAYMUL: Orden de pago

DEBMUL: Aviso de débito

CREMUL: Aviso de crédito

REMADV: Aviso de remesa

Algunos de los beneficios que aporta el comunicarse a través de este estándar son:

- Información rápida y precisa en el lugar indicado.
- Permite un mejor planeamiento de la recepción y el despacho de mensajes.
- Seguridad en el procesamiento de transacciones, se eliminan los errores por el reingreso de información disminuyendo así los problemas generados en la conciliación de facturas y la subsiguiente confección de débitos y créditos.
- Reducción de costos administrativos.
- Disminuye notablemente la cantidad de documentos impresos.
- Fortalece la relación comercial de los "socios del negocio".
- Comunicación permanente las 24 horas los 365 días del año.
- Mejora notablemente la relación comercial de los "socios del negocio".

Los Componentes De Un Sistema EDI

Los tres componentes o estructuras de un sistema EDI son los mensajes estándares, los programas EDI y las (tele) comunicaciones.

Para que las empresas estén en condiciones de operar utilizando un Sistema EDI deberán estar en condiciones de manejar los componentes que a continuación se detallan.

- Mensajes Estándares

EDI y los mensajes estándares han llegado a ser inter-dependientes a medida que el EDI ha progresado desde sistemas propietarios, sistemas cerrados en un entorno único, a sistemas abiertos.

Las distintas aplicaciones que se comunican entre sí necesitan una lengua común con el fin de comprenderse unas con otras.

Este lenguaje común se encuentra en los mensajes estándares EDI y más concretamente en UN/EDIFACT (United Nations Electronic Data Interchange for Administration Commerce and Transport), los mensajes estándar internacionales EDI y la guías de implementación de UN/ EDIFACT tales como EANCOM.

- Programas que soportan EDI

La función básica de los programas que soportan EDI, generalmente conocidos como los convertidores EDI, consiste en la traducción de los mensajes entrantes desde un mensaje estándar tal como EDIFACT/ EANCOM a un formato interno de archivo de una compañía, y el proceso inverso para mensajes que salen de la misma.

Sin embargo, además de la función de convertidor, los paquetes de EDI contienen también otras funciones adicionales, las cuales generalmente incluyen conversión de múltiples mensajes estándares y versiones de mensaje, mantenimiento de perfiles de los socios de negocios, interfaces de aplicación, módulos de comunicaciones para intercambiar información directamente o por medio de una o más redes de valor agregado, información de administración de mensajes salientes y entrantes incluyendo referencias para auditoria; manuales sobre menús referentes a los módulos de recibo de información y seguridad o control de acceso a través de contraseñas.

- Comunicaciones y redes de EDI

Una vez que los datos de una aplicación se han convertido desde un archivo con formato interno al formato de mensaje estándar por medio del software de EDI, los datos deben ser comunicados o físicamente transferidos al receptor del mensaje.

Aunque es posible transferir los datos por medios magnéticos tales como cintas o disquetes, las telecomunicaciones son parte esencial del concepto EDI.

Las comunicaciones de datos requieren algunas normas de disciplina para lograr una transferencia ordenada de información; esto se realiza mediante los protocolos de comunicación. Adicionalmente, habrá varias opciones de telecomunicaciones / redes que tendrán la función de ofrecer medios para la comunicación de datos. Algunas de estas opciones son la comunicación privada punto a punto, utilizando líneas arrendadas, el uso de la red telefónica pública de datos empaquetados o red de servicios de valor agregado ofrecidas por compañías especializadas.

B. Análisis de costo/beneficio del proyecto EDI

Costos del proyecto EDI

Encarar un proyecto de este estilo en una empresa no es una tarea sencilla por cuanto se deben considerar los costos que implica la adopción de este nuevo estilo de trabajo, no solo por los cambios tecnológicos sino por los cambios culturales que implica.

Entre los aspectos más destacados en cuanto costos resaltamos:

- Estratégicos, o aquellos costos que insume el tiempo invertido en el planeamiento de todo lo que tenga que ver con el sistema EDI. Este costo implica el tiempo que se tomará el área Gerencial de la entidad en tomar la decisión de implementar EDI, analizando Políticas de Implementación.
- Desarrollo, el estudio Económico y el Impacto que la nueva tecnología tendrá sobre las operaciones que actualmente se realizan.
- Desarrollo, adquisición de programas EDI, desarrollo y programación de las interfaces de aplicación, mejoramiento del software de aplicación interno para aprovechar todas las ventajas de un EDI integral y las pruebas necesarias para la óptima implementación de la nueva tecnología.
- Educación, este aspecto incluye tanto el entrenamiento del personal interno para redefinir y asumir nuevas responsabilidades en un ambiente de EDI, como así también la educación de los socios de negocios.
- Implementación, incluye el costo del personal del área de Sistemas de Información que asegura la compatibilidad de las aplicaciones internas con los sistemas de los nuevos socios de negocios.
- Intercambios, son los costos asociados con el envío y recibo de mensajes EDI a través de redes privadas o redes de valor agregado. Este costo incluye tanto el Gasto en comunicaciones, como el mantenimiento de todos los elementos que permitan el óptimo funcionamiento de los programas EDI, ya sea Líneas Telefónicas, Cuentas de Usuario en la VAN, Servicio Técnico mensual de los Equipos, etc.

Beneficios del proyecto EDI

Los beneficios de la implementación de EDI se presentan al iniciar el proyecto, y los beneficios son más cualitativos e intangibles que cuantitativos. Los podemos sintetizar en los siguientes puntos:

- Beneficios administrativos y de procesamiento

Estos son probablemente los beneficios más tangibles obtenidos al implementar un sistema EDI. Los estimativos deben realizarse en el número de documento/ítems por línea procesados por año para cada documento en particular. Los costos relativos al procesamiento de tal documento deben incluir papelería preimpresa, sobres, estampillas, telex, teléfono, fax y costos de fotocopias.

Los estimativos deben ser hechos contemplando el tiempo que se gasta en consecución y ordenamiento de los datos, entrada de los mismos, mecanografía, fotocopias, archivo, correo y fax y lo más importante, en el control y corrección de errores de cada ítem por línea. El intercambio directo de datos entre una aplicación y otra eliminará los frecuentes y costosos errores que se producen inevitablemente cuando los datos son manejados e intercambiados manualmente.

- Beneficios por la reducción del ciclo de los negocios.

Un sistema EDI exitoso reducirá substancialmente el tiempo de realización de una transacción, sea del tipo que fuere.

EDI no solamente conducirá a un ciclo de negocios más rápido sino además, a una mejor calidad de la información compartida entre los socios de negocios.

- Beneficios estratégicos

A pesar de que EDI tiene algunos costos y beneficios claros, es antes que todo una forma de hacer negocios, siendo los beneficios estratégicos los más importantes. Estos incluyen aspectos tales como mayor satisfacción del cliente, las mejores relaciones entre empresas y fortalecimiento de las relaciones de negocios.

Otros beneficios estratégicos pueden incluir incrementos sostenidos en la participación en el mercado y ventajas competitivas.

Los beneficios estratégicos son difíciles de cuantificar pero presentan una respuesta a las necesidades del mercado. Aunque puede ser fácil demostrar que EDI conducirá a un incremento en la participación del mercado y cuantificar el valor de este incremento, será difícil predecir que tanto se incrementará esta participación gracias a un sistema EDI.

- Seguridad de la información transmitida.

Como sabemos, en un Sistema de Comunicación de Datos, es de vital importancia asegurar que la Información viaje segura, manteniendo su autenticidad, integridad, confidencialidad y el no repudio de la misma entre otros aspectos.

Estas características solo se pueden asegurar utilizando las Técnicas de Firma Digital Encriptada y la Encripción de Datos. A continuación se realiza un breve comentario sobre métodos de encripción:

Para poder encriptar un dato, se pueden utilizar tres procesos matemáticos diferentes:

Los algoritmos HASH, los simétricos y los asimétricos.

Algoritmo HASH:

Este algoritmo efectúa un cálculo matemático sobre los datos que constituyen el documento y da como resultado un número único llamado MAC. Un mismo documento dará siempre un mismo MAC.

Algoritmos simétricos:

Utilizan una clave con la cual se encripta y desencripta el documento. Todo documento encriptado con una clave, deberá desencriptarse, en el proceso inverso, con la misma clave. Es importante destacar que la clave debería viajar con los datos, lo que hace arriesgada la operación, imposible de utilizar en ambientes donde interactúan varios interlocutores.

Algoritmos asimétricos (Rsa):

Requieren dos claves, una privada (única y personal, solo conocida por su dueño) y la otra llamada Pública, ambas relacionadas por una fórmula matemática compleja imposible de reproducir.

El usuario, ingresando su PIN genera la clave pública y privada necesarias. La clave pública podrá ser distribuida sin ningún inconveniente entre todos los interlocutores. La privada deberá ser celosamente guardada.

Cuando se requiera verificar la autenticidad de un documento enviado por una persona se utiliza la clave pública porque el utilizó su clave privada.

Como ya vimos, este es el sistema que estableció la Ley 25.506, para el uso de la firma digital en la Argentina.

A continuación se muestra un listado con los proveedores con quienes actualmente se puede establecer comunicación mediante la utilización de EDI, que integran la VAN del SEA:

Proxter.

Molinos Río de la Plata

Mastellone hnos.

Sancor s.a.

Lever s.a.

Quilmes.

Budweiser.

Coca Cola.

Pepsico.

Estas empresas proveen, a través de este sistema, el 75% de los productos que comercializa la empresa.

Obviamente existen muchas otras no enumeradas, que podrían incorporarse a la VAN, pero las mencionadas son las que actualmente pueden implementar, y de hecho, ya lo han hecho, con cadenas de supermercados, y están en mejores condiciones técnicas de realizarlo.

En el momento de tomar la decisión, será muy importante seleccionar adecuadamente a los proveedores con quienes se iniciará la implantación.

C. Firma digital y estrategias de gestión

a. En la gestión de empresas privadas

Es importante tener en cuenta en qué áreas de una empresa resultaría más conveniente aplicar primero firma digital, para ello habría que analizar actividades donde la firma digital le aporte mayor beneficio a la empresa [5]

Es recomendable empezar con áreas de gran valor añadido y por aquellas que supongan costos de tiempo o desplazamientos.

Algunos de los usos que podrían darse en una empresa son los siguientes:

- Firma de documentos administrativos: nóminas, contratos, actas, pedidos
- Licitaciones públicas
- Firma de documentos: certificados, calibraciones, visados, etc.
- Identificación frente a terceros (como bancos)
- Email y comunicación cifrada.
- Facturación electrónica

De esta manera, la utilización de la firma digital puede proporcionar las siguientes ventajas:

- Agilidad y ahorro en la contratación electrónica
- Disponibilidad de tiempo
- Reducción de trabajo que no aporta valor y de posibles errores
- Eliminación de desplazamientos
- Reducción de costos

---

[5] PIZZOLO, Calogero, Globalización e Integración. Ensayo de una teoría general, Argentina. EDIAR 2002, pág. 29 - 150 (cantidad de páginas 614)

La automatización e integración de procesos resulta realmente una estrategia de gestión combinada con la firma digital, ya que facilita la administración y nos ahorra tareas.

Es una herramienta que puede mejorar la competitividad de las pymes, trae beneficios de ahorro de tiempo y dinero, es sencilla de utilizar. Por ejemplo, una empresa que emite una gran cantidad de facturas podría exportarlas a formato PDF y después se pueden firmar todas de forma masiva utilizando alguna aplicación de firma digital. A continuación pueden enviarse por email o ponerlas en una extranet o gestor documental.

b. En la Administración Pública

Los sistemas automatizados de control de gestión en las dependencias y entidades de la administración pública proporcionarían los siguientes beneficios:

a) Mejorar la gestión y trámites de los asuntos administrativos mediante el uso de medios electrónicos.
b) Utilizar la firma electrónica avanzada como medio de autenticación del documento electrónico gubernamental y como método alternativo a la firma autógrafa
c) Permitir la intercomunicación entre los sistemas de control de gestión con que cuenten las dependencias y entidades
d) Asegurar la confidencialidad, integridad y resguardo de la información acorde a los ordenamientos legales aplicables.

En el ámbito privado como en el público, la firma digital representa un avance significativo para la inserción, de nuestro país en la sociedad de la información y en la economía digital, brindando una oportunidad para el desarrollo del sector productivo vinculado a las nuevas tecnologías.

Además cabe destacar la importancia que tiene la misma para la despapelización del estado, la importancia que tiene la ley de Firma Digital, tanto en el ámbito nacional como en el internacional, para la gestión del estado, entre otros.

Como se desarrollo anteriormente, el EDI que es el intercambio electrónico de documentos Comerciales en un formato estandarizado entre las aplicaciones informáticas de empresas que se encuentran relacionadas comercialmente, brinda múltiples beneficios que pueden ser ventajosos estratégicamente, como la obtención de información rápida y precisa en

el lugar indicado, permite un mejor planeamiento de la recepción y el despacho de mensajes, seguridad en el procesamiento de transacciones, se eliminan los errores por el reingreso de información disminuyendo así los problemas generados en la conciliación de facturas y la subsiguiente confección de débitos y créditos, reducción de costos administrativos.

Resulta conveniente para nuestro país dado que mejoraría notablemente la relación comercial de los "socios del negocio”.

Conclusión

La firma digital es, a mi entender, un requerimiento de los tiempos que corren y, también, de esta globalización que se viene dando en el mundo, desde hace ya unos años, que acarrea consigo al comercio y el cual, a su vez, le exige al derecho que avance al ritmo de esta; y es por eso que considero, que era necesaria y fue oportuna la legislación sobre este tema.

Por suerte por tratarse de un tema de esta índole, es decir ser un requerimiento actual, y como ya anticipara mi introducción, se podría decir que esta presentó a nuestro derecho, casi, un único inconveniente que está relacionado con la concepción que el código civil tiene de la firma como manifestación de la voluntad, una concepción que se la podría considerar obsoleta en el presente, aunque adecuada para los tiempos del código.

El artículo 1012 del Código Civil Argentino, establece que la firma es condición esencial para la existencia de todo acto bajo forma privada. Y agrega además que la firma es 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.

Al parecer dentro de los términos del citado artículo no cabría la concepción de firma digital y lo que ella significa, ya que esta firma es un conjunto de números y letras encriptadas, donde existe una clave pública y una privada, un concepto muy lejano al que tuvo Vélez Sarsfield, que en su época, ni imagino, que podría haber llegado a existir una firma que no fuera la que surge del puño y letra de un ser humano.

Pero, como se demostró en el desarrollo de este trabajo, esto se encuentra resuelto en la Ley 25.506, ya que esta le da a la firma digital la característica de ser manifestación de la voluntad, igualándola, así, a la firma ológrafa.

La utilización de la firma digital trae beneficios administrativos, competitivos, de procesamiento, debido a que los procesos son más rápidos y eficientes, elimina el uso del papel y automatiza los circuitos administrativos, reduce substancialmente el tiempo de realización de una transacción, sea del tipo que fuere.

Proporciona seguridad de la información transmitida, si se utilizan las técnicas de firma digital encriptada y la encripción de datos y reduce el trabajo que no aporta valor.

La AFIP y Anses aceptan la firma digital y esto se trata de un instrumento que contribuirá a una relación más ágil, eficiente y transparente en la relación entre el ciudadano y el Estado.

Este mecanismo posibilita a las empresas, en particular las Pyme reducir costos, con menor uso de papel y administración de archivos.

Como ya di a entender al inicio de esta conclusión, estoy total mente de acuerdo con la implementación del sistema de la firma digital ya que considero que este significa un gran avance por la influencia que tiene en el comercio para con la Argentina, como de ésta para con el mundo, ya que esta ley coloca nuestra legislación a la par de la legislación de otros países del mundo, como ser Alemania, EE.UU., entre otros, y resulta una conveniente estrategia de gestión que nos permitiría mejorar nuestras relaciones comerciales con esos países y, en la medida de lo posible, acrecentarlas

Índice Bibliográfico

- Decisión Administrativa N° 118/2001
- Decreto Nº 1347/99
- Decreto Nº 673/2001
- Decreto Nº 889/2001
- Decreto Nº 1023/2001
- Ley 25.506 Ley de Firma Digital, publicada en el Boletín Oficial el 14/12/2001.
- Ley Nº 25.237
- LORENZETTI, Ricardo Luis. **"La ley Argentina de firma digital"**, 2002. Ed. Abeledo Perrot.
- MENDIVIL Ignacio, "El ABC de los Documentos Electrónicos Seguros"
- PIZZOLO, Calogero, **"Globalización e Integración".** Ensayo de una teoría general, Argentina. EDIAR 2002
- RAMOS SUAREZ, Fernando. **"Cómo aplicar la nueva normativa sobre firma electrónica"**, Feb. 2000. Revista electrónica de derecho informático Nº 19.
- Recopilación de "Ponencias", del XVIII Jornadas Nacionales de Derecho Civil, Comisión N° 7, "Derecho Internacional Privado. La jurisdicción internacional en el comercio electrónico."
- REYES Krafft Alfredo, La Firma Electrónica y las Entidades de Certificación

  Editorial Porrúa
- SOLIS García, José Julio. FACTURA Y FIRMA ELECTRONICA AVANZADA.-

  Editorial Gasca.
- Resolución JGM Nº 176/2002

- Resolución SAFJP Nº 293/97
- Resolución SFP Nº 212/98
- Resolución SGP Nº 17/2002
- Resolución General CNV Nº 345/99
- Resolución Nº 178/2001
- Resolución SFPNº 97/97
- Para la realización de este trabajo se consultaron los siguientes sitios web:

www.altavista.com.ar

www.infoleg.gov.ar

http://ca.sgp.gov.ar

http://es.wikipedia.org

http://www.iec.csic.es