UNIVERSIDAD NACIONAL DE TUCUMÁN

FACULTAD DE CIENCIAS ECONOMICAS
UNIVERSIDAD NACIONAL TUCUMAN

Firma Electrónica Una Herramienta Informática Segura

Autores: CUCCHIARO, Noelia Romina
GONZA, Rita Janet

Director: C.P.N. GONZALEZ, José Antonio

2010

Trabajo de Seminario: **Contador Público Nacional**

PROLOGO

La evolución tecnológica ha revolucionado a nivel mundial las diferentes áreas del conocimiento y de las actividades humanas, fomentando el surgimiento de nuevas formas de trabajar, aprender, comunicarse y celebrar negocios. Al mismo tiempo ha contribuido a borrar fronteras, comprimir el tiempo y acortar las distancias.

El uso cada vez más cotidiano y difundido de las nuevas tecnologías en materia de transmisión de datos de toda índole, parece mostrar un escenario futuro en el cual los documentos de elaboración electrónica han de reemplazar paulatinamente a los documentos tradicionales o manuales (los creados en soporte "papel"), para gran parte de los actos documentados de la vida cotidiana y en especial en todo ámbito de trabajo que se precie como tal.

No puede desconocerse, sin embargo, la desconfianza que todavía genera en el común de la gente la falta de una firma escrita para celebrar un acto.

Las primitivas formas de pensar, las antiguas fórmulas y dogmas, por estimadas y útiles que nos hayan parecido en el pasado, no se ajustan en la actualidad a esta nueva tecnología.

Con este trabajo se pretende mostrar que hoy en día necesitamos de una herramienta como la firma digital que nos brinde seguridad, y se puede asegurar con certeza, que es una forma adecuada de otorgar autenticidad a la mayoría de los documentos electrónicos.

También se destacará la importancia de esta herramienta en la tarea que actualmente se esta implementando en el Estado, la cual consiste en la despapelización del Sector Público.

Por lo anterior, podemos decir que estamos ante el ocaso de la firma ológrafa, ya que ésta ha demostrado, hasta el momento, ser insuficiente y muy susceptible de falsificación.

Antes de abordar el estudio de esta herramienta tan importante como es la firma digital, creemos necesario efectuar un análisis del documento electrónico, firma manuscrita u ológrafa.

La metodología utilizada en este trabajo de seminario consistió en la utilización de distintas fuentes de información, para ello se realizó una Investigación de fundamentos teóricos a partir de consultas bibliográficas, apuntes de clases e Internet; comenzando con una visión global de la firma digital hasta introducirnos puntualmente en el análisis de digitalización de actas en el Registro Civil.

Agradecemos la colaboración en la confección de este trabajo a nuestro profesor conductor CPN José Antonio González, quien además de brindarnos su tiempo nos ayudó a contactarnos con personas involucradas en este tema en la provincia; al CPN Carlino Bernardo, quien nos permitió el acceso a su bibliografía, ya que la misma no se encontraba disponible en la facultad de Derecho a causa de las remodelaciones; y a todo el personal del Registro Civil del área de digitalización de actas, que desde el primer momento nos atendieron con cordialidad, brindándonos datos para poder confeccionar nuestra tesis de graduación.

INTRODUCCIÓN

En el presente trabajo se comienza describiendo nociones previas a tener en cuenta para introducirnos en el desarrollo del mismo, nociones tales como el documento escrito y la forma en que fue sustituido por el documento electrónico como consecuencia de los modernos medios tecnológicos que han permitido formas de operación y contratación a distancia.

En el Capítulo II exponemos uno de los elementos que le da carácter jurídico a un documento, que es la firma, analizando sus funciones, características y la forma en que ésta se encuentra representada en un documento electrónico, otorgándole validez jurídica al mismo. Seguidamente, en el Capítulo III, nos adentramos en el concepto de firma digital y el tratamiento legal que le otorga la Ley nacional 25506 de Firma Digital, reconociéndole equivalencia funcional con la firma manuscrita, lo que constituye un paso fundamental en la convergencia entre el documento escrito y el documento digital.

En los Capítulos IV y V explicamos la infraestructura de firma digital adoptada por el Sector Público, de acuerdo al marco normativo constituido por la Ley 25506 y decretos reglamentarios. Dicho sistema esta integrado por entidades públicas nacionales que cumplen distintas funciones, desde la emisión de un certificado electrónico que contiene la firma digital, hasta las autoridades de aplicación y auditoría del sistema, las que permiten el uso de los documentos electrónicos en el ámbito de la Administración Pública Nacional.

Finalmente, en el Capítulo VI tratamos sobre la “despapelización” del Sector Público como consecuencia de la aplicación de estas herramientas tecnológicas, como la firma digital y el documento electrónico, incluyendo un trabajo de investigación realizado en el Registro Civil de la Provincia de Tucumán, el cual ejemplifica el nivel de modernización y digitalización en que se encuentra nuestra provincia en la actualidad.

CAPITULO I

DOCUMENTO

Sumario: 1.- Introducción. 2.- Documento. 3.- Documento electrónico. 4.- El documento electrónico como medio de prueba.

1.- Introducción

Cada día que pasa aumenta el uso que se hace de las computadoras en los más variados ámbitos de la vida social. Así, cualquiera de nosotros se encuentra diariamente en situación de tener que utilizar documentos provenientes de un sistema informático.

Es un fenómeno de origen relativamente reciente pero que parece presentar un carácter irreversible y es posible que en un momento no tan lejano, la mayoría, sino la totalidad, de los procedimientos documentarios se lleven a cabo en forma automatizada, salvo casos excepcionales. De esta manera, el documento manual será casi completamente sustituido por el documento electrónico.

El avance de la tecnología informática y de los modernos medios tecnológicos permite formas de operación y contratación a distancias que modifican los usos tradicionales. Lo que debemos analizar son las condiciones para la admisión, en el tráfico jurídico, de los documentos surgidos a distancia y operados a través de computadoras conectadas por algún mecanismo. Esto significa reconocer y apoyar el advenimiento del

comercio electrónico y la aplicación de la firma digital para otorgar seguridad a las transacciones; es decir cómo conformar una estructura informático-jurídica, basándose en la legislación vigente, para la transmisión por computadora de un acto de voluntad ya perfeccionado.

2.- Documento

Palacios define como documento a "todo objeto susceptible de representar una manifestación del pensamiento, con prescindencia de las formas en que esa representación se exterioriza."(1)

Todo documento se compone de dos elementos:

- **El soporte instrumental**, que es el continente del documento (papel: documento escrito) soporte escrito tradicional
- **El contenido**, que es la información que se vuelca en el soporte instrumental

La unión de ambos elementos nos da como resultado el documento en el sentido que lo conocemos.

Las nuevas tecnologías han hecho aparecer el documento, no ya en soporte material, sino en un soporte virtual al que denominamos: documento electrónico.

Cuando en la elaboración de este documento electrónico se emplea algún proceso criptográfico se lo transforma en un documento digital.

Nuestro Código Civil distingue entre:

Instrumentos Públicos: Son aquellos que se otorgan con ciertas formalidades esenciales que garantizan su autenticidad: fundamentalmente la intervención en el acto de un funcionario público que se denomina oficial publico. Son condiciones de validez del instrumento publico las siguientes: la capacidad y la competencia del oficial público, y el cumplimiento ciertas

(1) PALACIOS, Lino Enrique, Manual del Derecho Procesal Civil; 14º edición, (Buenos Aires, s.f.), Pág. 423.

exigencias formales, entre las que se encuentran la escritura papel, la firma y el cumplimiento de alguna formalidad o solemnidad.

Hacen plena fe hasta que sean argüidos de falsos.

Instrumentos Privados: Son los que se realizan entre las partes, sin intervención de oficial publico, y sin ajustarse a formalidades esenciales. El art 1020 del Código Civil establece “para los actos bajo firma privada no hay forma alguna especial. Las partes pueden formarlos en el idioma y con las solemnidades que juzguen más convenientes.”[(2)] Existe la libertad de las formas, pero es necesario que contengan: escritura en papel y firma.

De allí que el documento electrónico y el documento digital no tenían hasta hace poco encuadramiento en nuestra legislación tradicional ni como documento público o privado.

Con la sanción de la Ley N° 25.506 de Firma Digital el 14.11.2001, se ha dado reconocimiento al Documento Electrónico y al Documento Digital y se ha incorporado a la legislación argentina el principio de la equivalencia funcional. Sobre esto trataremos en los capítulos siguientes.

3.- Documento Electrónico

Noción y Especie

El documento electrónico es aquel proveniente de un sistema de elaboración electrónica (certificados de antecedentes, tickets emitidos por cajeros automáticos, etc.), es decir, es la información procesada por computadora, a través de señales electrónicas, plasmadas en un soporte. Aquí se debe distinguir entre el documento electrónico en sentido estricto, que es aquel que está "escrito" en forma magnética u óptica y aquel proveniente de un sistema informatizado, es decir, que ha sido plasmado en papel o llevado a la pantalla del computador con información proveniente de un documento electrónico en sentido estricto.

[(2)] AGLIANO, Humberto, Compendio de Derecho Civil, (año 2002), Pág.74.

Técnicamente, el documento electrónico es un conjunto de impulsos eléctricos que recaen en un soporte de computadora, y que sometidos a un adecuado proceso, a través del computador, permiten su traducción a lenguaje natural a través de una pantalla o de una impresora.

En este punto es necesario detenernos a reflexionar sobre si lo que se lee en la pantalla o lo impreso constituye o no el documento en original o si es solo una copia de este.

Documento electrónico e informático

Del análisis de los trabajos doctrinarios consultados se desprenden grandes diferencias de opinión en cuanto a una conceptualización precisa del documento electrónico. Las razones para ello son fundamentalmente la imprecisión que hay respecto del documento en general y la confusión conceptual que existe respecto de las nuevas tecnologías.

Hay autores que hablan de documento electrónico y otros de documento informático. Nos parece que la primera expresión es la más correcta ya que pone el acento en la diferencia fundamental entre el documento en sentido clásico y el electrónico: el soporte físico.

Concepto

"Bajo documento electrónico se comprenden datos (o bien informaciones) que tienen relevancia jurídica, los cuales son transmitidos o registrados por vía electrónica, especialmente a través del procesamiento electrónico de datos, pero también por medio de simples soportes de sonido".

"El documento electrónico es el que está en la memoria de la máquina y cuyo contenido o texto está en lenguaje de máquina, el que puede ser pasado a lenguaje natural y eventualmente ser impreso para facilitar su utilización y lectura por parte de los usuarios".(3)

---

(3) DESCHKA, Fridolin, El documento electrónico. Revista Internacional del Notariado, N° 87, volumen 42, (Argentina, 1991), Pág.364.

Algunos Conceptos

Para llegar a tener una idea clara de la naturaleza del documento electrónico, debemos primero determinar algunos conceptos que son propios del origen computacional de éste:

a) Programa o software
b) Datos
c) Información o dato elaborado

a) El programa:

Hace funcionar a la computadora, es su "cerebro", y se lo puede definir como: **Un conjunto ordenado de instrucciones que actúan entre si para llegar a un resultado final**. Estas instrucciones son establecidas previamente por el ser humano en su calidad de programador con el fin de llegar a un resultado por él querido.

Este resultado puede ser información, o bien una decisión. Aquí es donde debemos tener muy presente que es el ser humano quien toma la decisión ya que la máquina por si misma nada hace sino cumplir órdenes explícitas y claras.

A modo de ejemplo podemos presentar un caso práctico: Supongamos que dos computadoras se encuentran conectadas entre si, siendo la computadora A la vendedora y la B, la compradora. B tiene la instrucción de comprar acciones de A si estas llegan a un determinado nivel de precio previamente establecido por el programador y a su vez A esta programada para vender estas acciones dentro de ciertos parámetros del mercado, de esta manera se lleva a cabo la compraventa de acciones de un modo totalmente automático sin que aparentemente haya intervenido la mano del hombre.

Sin embargo, esta afirmación es más aparente que real ya que debemos preguntarnos, ¿quien tomó la decisión de comprar o vender en su

caso?, parece evidente que no ha sido la máquina, que sólo se limita a seguir instrucciones, sino el ser humano.

b) Los datos:

Son aquellos elementos que llegan a la computadora por diversos medios y que no son más que la base por medio de la cual llegan a trabajar los diversos programas, convirtiéndolos en información útil.

Estos datos pueden tener su origen en la misma o en otra computadora pero siempre debe tenerse en cuenta que es la mano del hombre la que está detrás.

c) La información:

Es el dato elaborado, es el producto final de la interacción hombre máquina y dicha información puede llegar a plasmarse en una decisión, pero ésta siempre tendrá por origen el intelecto humano.

Requerimientos

Estos instrumentos electrónicos así transmitidos, para ser aceptados tanto en materia civil como en materia comercial, deben cumplir los siguientes requerimientos:

- Deben otorgar certeza para conocer quién es el emisor y quien es el receptor.
- Deben permitir demostrar la existencia de la voluntad jurídica
- Deben configurar prueba fehaciente de la misma, en cualquiera de sus modalidades.

Por lo tanto, se intenta hacer aplicables al documento electrónico todo aquello que en la actual legislación esta previsto para los documentos soportados en papel. En realidad ya son muchas y diversas las transacciones, transferencias bancarias, contrataciones entre empresas, operaciones de bolsa, presentaciones de declaraciones juradas, que

continuamente se ejecutan por vía electrónica con el apoyo de la informática y tecnología."[4]

En la contratación a distancia debe estudiarse la relación existente entre instrumentos jurídicos o documentos, y los nuevos medios tecnológicos. Aquí lo sustancial es la voluntad jurídica que expresa el instrumento, y lo adicional es la forma de creación y su seguridad.

4.- Documento electrónico como medio de prueba

Para los efectos del presente trabajo, las disposiciones que hay que tomar para ponerse en una situación favorable en caso de diferencias con la otra parte en un contrato o con el deudor en una obligación, específicamente nos referimos a la prueba documental.

a) Inconvenientes

1. Inseguridad Informática

Si bien las nuevas tecnologías aseguran una optimización de funciones, los accidentes o interrupciones en el funcionamiento de los equipos pueden producir serios inconvenientes. Así, observamos que las empresas informatizadas no pueden afrontar fallas en sus equipos ya que las imposibilitan para proseguir su trabajo en forma manual.

En la mayoría de los casos las fallas de los sistemas serán imputables a problemas técnicos, desastres naturales o accidentes, aunque la posibilidad de sabotaje también debe tomarse en cuenta.

Podemos concluir que una falla es algo posible. Sin embargo, esto no ha desanimado a los legisladores de diversos países los cuales han creado han tratado de avanzar hacia la informatización de sus sistemas.

2. Dudosa Autenticidad

---

[4] LARDENT, Alberto, Sistema de Información para la Gestión Empresaria: Planeamiento, Tecnología y Calidad, 1º Edición, (Buenos Aires, 2001), Pág. 451.

Una de las características principales que se piden de un documento en la vida jurídica es su autenticidad, y la legislación provee diversos medios para asegurarla.

En este sentido, un documento lo será cuando cumpla con los requisitos legales que tienden a asegurar que el documento no ha sufrido alteraciones y a evitarlas en el futuro.

En el caso del documento electrónico, la falta de autenticidad puede producirse en la etapa de memorización, porque se digitó mal o porque se omitió algún dato; en la etapa de elaboración, como consecuencia de una disfunción debida a un exceso o falta de temperatura o humedad; y, finalmente, en la etapa de transmisión, como consecuencia de la superposición.

Otra fuente de falta de autenticidad del documento electrónico puede deberse a la intervención de personas no autorizadas a ingresar en el sistema. La protección se realiza a través de la entrega a ciertas personas, expresamente autorizadas, de la llave criptográfica y el algoritmo de transformación, además de un registro automático de cualquier operación realizada con el computador y del usuario que la efectuó.

b) Ventajas del documento electrónico como medio de prueba y registro:

El documento electrónico presenta ventajas como una forma de conservar documentos, ya que puede guardar mucha información en un espacio ínfimo, se puede acceder a él con gran facilidad y se puede traspasar vía conexión a otras personas o instituciones interesadas en su examen.

Análisis comparativo

Un documento tradicional se encuentra constituido por un medio de almacenamiento (papel) y un mecanismo de impresión (manuscrito, tinta, tecnología laser, etc.). Cualquier alteración en su contenido será, de acuerdo

con la cultura tradicional, fácilmente detectada. En el caso del documento electrónico, el documento y su medio de almacenamiento están integrados en un solo elemento, y esta es la primera diferenciación: no hay elemento físico que represente el documento (el papel, por el contrario, sí tiene cualidades físicas).

Si nos detenemos en estos antecedentes observamos la dificultad que surge ante el intento de compatibilizar los actuales medios de identificación electrónica (firmas digitales) con la concepción tradicional de firma. Sin embargo, para que el comercio electrónico pueda continuar su desarrollo, alcance y consolidación, es necesario prever y solucionar su principal problema: la inseguridad propia del medio por el que transita la información. Y la firma constituye uno de los elementos fundamentales en este intento de alcanzar seguridad. La firma digital es la llave para habilitar el comercio electrónico, con la condición de que otorgue seguridad y privacidad en la comunicación a distancia. El sistema de firma digital debe constar de dos partes: por un lado un método que haga imposible la alteración de la firma; por el otro verificar que la firma pertenece realmente al firmante. De esta manera la firma digital cumplirá la finalidad que tradicionalmente cumplía la firma ológrafa (manuscrita), pero adaptada al marco del ciberespacio; esto es, la operatoria en redes con documentos transmitidos a distancia.

CAPITULO II

LA FIRMA

Sumario: 1.- Introducción. 2.- Concepto. 3.- Importancia y elementos. 4.- Características. 5.- Funciones. 6.- La firma y el documento electrónico. 7.- Autenticidad, inalterabilidad y seguridad del documento electrónico.

1.- Introducción

El documento escrito se compone de un continente y un contenido, es decir, datos impresos en un soporte. Sin embargo, lo que le procura un carácter jurídico a un documento es, además de otros elementos, la firma.

Es aquí donde se presenta el mayor dilema en el derecho de base romanista, ya que éste gira en torno al requisito fundamental de la firma del emisor. En efecto, desde que se comenzó a usar la firma en el documento escrito, o sus equivalentes como los sellos, ha tenido gran importancia cumpliendo funciones que más adelante detallaremos.

Sin embargo, nos enfrentamos ahora a la problemática del documento electrónico en el cual nos vemos imposibilitados de firmar por las características que le son propias. Ello nos obliga a un estudio más detallado de su naturaleza, funciones y trascendencia con el objeto de encontrar la manera de sustituir sus funciones con otros métodos en los casos en que sea necesario y posible.

2.- Concepto

Etimología

Proviene del latín "firmare" que significa corroborar o confirmar el contenido de un documento, lo cual se hacía poniendo la mano sobre él y después suscribiéndolo.

Definición

Según el Diccionario de la Lengua Española de la Real Academia, la firma es el "Nombre y apellido, o título, que una persona escribe de su propia mano en un documento, para darle autenticidad o para expresar que aprueba su contenido" (5)

Según nuestro Código Civil en su artículo 1012, “la firma es la condición esencial para la existencia de todo acto jurídico bajo forma privada. Ella no puede ser reemplazada por signos ni por iniciales de los nombres o apellidos.” (6) En este sentido es el elemento por el cual su autor hace constar la manifestación de su voluntad o consentimiento, expresado en el documento que sirve de apoyo al acto de referencia. En su concepción tradicional la firma es el trazo peculiar por el cual una persona identifica su nombre y apellido, o sólo su apellido.

Por su parte, de conformidad con lo dispuesto por el art. 1014 del mismo código "ninguna persona puede ser obligada a reconocer un instrumento que esté solo firmado por iniciales o signos; pero si el que así lo hubiese firmado lo reconociera voluntariamente, las iniciales o signos valen como la verdadera firma" (7). Y el art. 1026 dispone que el reconocimiento judicial de la firma sea suficiente para que el cuerpo del instrumento quede también reconocido

---

(5) Diccionario de la Lengua Española. Real Academia Española, Vigésima segunda edición, (Madrid, 2002), Pág. 733.

(6) Código Civil de la Republica Argentina, 8ª edición, (Buenos Aires, 2010), Pág. 214.

(7) AGLIANO, Humberto, Op. Cit., Pág. 80.

Para reafirmar este concepto, en la nota al Art 3639 del Código Civil, se lee que “la firma no es la simple escritura que una persona hace de su nombre o apellido: es el nombre escrito de una manera particular, según el modo habitual seguido por una persona en diversos actos sometidos a esta formalidad.” (8)

Couture define la firma como "trazado gráfico, conteniendo habitualmente el nombre, apellido y rúbrica de una persona, con el cual se suscriben los documentos para darles autoría y obligarse con lo que en ellos se dice". (9)

Para Llambías “la firma es el trazo peculiar mediante el cual el sujeto consigna habitualmente su nombre y apellido, o sólo su apellido, a fin de hacer constar las manifestaciones de su voluntad". (10)

3.- Importancia y elementos

Importancia

Radica en que ella implica la asunción de autoría de una declaración de voluntad por parte del sujeto que suscribe el documento de tal manera que, aun cuando haya redactado íntegramente el texto, no le podrá ser imputado sin que antes haya estampado su firma.

Elementos

De los conceptos antes enunciados podemos establecer que, desde un punto de vista amplio ellos serían:

a) Nombre: Palabra con que se designa a una persona y que antecede al apellido.

b) Apellido: Nombre de familia con que se distinguen las personas.

---

(8) Ibídem, Pág. 83.

(9) COUTURE, Eduardo J., Vocabulario jurídico (Depalma, Buenos Aires, 1976), Pág. 290.

(10) LLAMBÍAS, Jorge Joaquín, Tratado de Derecho Civil Argentino", Parte General, séptima edición actualizada, Editorial Perrot, Buenos Aires, 1878, t. II, N° 1584, Pág. 397.

c) Rúbrica: Rasgo o conjunto de rasgos de figura determinada, que como parte de la firma pone cada cual después de su nombre o título. A veces se coloca la rúbrica sola; esto es, sin que vaya precedida del nombre o título de la persona que rubrica.

Por regla general el nombre y el apellido no están integrados con la rúbrica. Así, las partes se identifican con éstos en la primera parte del documento y al pie estampan su rúbrica que consiste en un "trazo peculiar"[(11)], como dice Llambías.

4.- Características

1. Irregular: La firma de una misma persona nunca es exactamente igual en cada una de las oportunidades en que se estampa.

2. Habitual: Está referida a la intención del que firma en orden a no variarla. Es un importante elemento en la vinculación de la grafía con su autor, ya que el perito se basará en ejemplos anteriores de la firma que sean indubitables, al momento de realizar la pericia.

3. Peculiar: Propia de una persona y de nadie más.

4. Autógrafa: Puesta del puño y letra por el firmante. La manuscripción implica la inmediatez, el contacto directo entre el suscriptor y el documento, y la voluntariedad de la acción y el otorgamiento.

Se presume, en otros términos, que cada persona tiene un modo particular de suscripción, nunca perfectamente reproducible y que los peritos documentales pueden poner en evidencia las diferencias existentes entre una suscripción auténtica y otra falsificada o adulterada. De aquí la necesidad de que la firma sea autógrafa, es decir, impuesta de propio puño por el firmante; puede ser extendida inclusive con letra de imprenta, pero no por medios mecánicos, excepto en situaciones expresamente autorizadas por la legislación (Ej.: billetes, cheques extendidos así por su gran volumen y con previa autorización).

---

(11) Ibídem, Pág. 401.

La firma, a nuestro entender, debe ser autógrafa para ser tal, pero esto no significa que sus funciones no puedan ser cumplidas por otros medios.

5.- Funciones

Estas son, la declarativa, la indicativa y la probatoria, pudiendo conceptuarlas de la siguiente manera:

a) Declarativa

La inscripción de la firma de una persona está indicando que la declaración que hace es suya, si bien muchas veces al firmar no se escribe el nombre, o se estampa media firma o se hacen signos que no son alfabéticos. Es decir, cuando se la asienta en documentos o escritos se está significando conformidad y asentimiento.

b) Indicativa

En nuestra legislación la utilización de la firma es de uso general para identificar a las personas que toman parte en un determinado acto jurídico como autores de él. Sin embargo, a simple vista podemos hacerle a esta función de la firma algunas críticas:

1. La generalidad de las personas no firma con su nombre sino con caracteres ilegibles (una rúbrica) que nada dicen acerca de la persona que los trazó. Su nombre estará generalmente, junto con otros datos relevantes para la identificación, en el contenido del documento.

2. La firma es fácilmente adulterable, y sobre todo la rúbrica hecha con caracteres ilegibles.

3. En la mayoría de los trámites que requieren la identificación de la persona se usará la cédula de identidad u otro medio similar.

c) Probatoria

Esta función esta íntimamente relacionada con la indicativa y ésta, a su vez, con la declarativa. Efectivamente, al establecer que una firma

pertenece a la persona que la estampó (indicativa) estamos probando, en principio, que ella acepta lo que se acordó en el documento (declarativa).

A simple vista este no parece un medio demasiado exacto para probar ya que su adulteración es obviamente fácil de realizar, en todo caso nos remitimos a las críticas enumeradas en el punto anterior.

6.- La firma y el documento electrónico

Crisis de la Firma:

Irti en "Il contratto tra faciendum e factum" expresa que se está ante una crisis de la firma; los contratantes en la economía moderna ya no se comunican mediante cartas firmadas, sino por telex o telefax y el producto es un texto sin firma, o como en el caso del fax, una fotocopia de un texto original firmado, o incluso directa y automáticamente entre sus respectivas computadoras. "Este proceso, que se llamaría la crisis de la suscripción, está destinado a acelerarse y a intensificarse. Los sujetos de la economía moderna ya no se comunican con cartas firmadas por el remitente, sino por medio de signos transmitidos por aparatos mecánicos (telegrama sobre original escrito, telegrama dictado por teléfono, telex, telecopiart, etc). El resultado de la actividad expresiva es siempre un texto escrito, aunque desprovisto de firma autógrafa. El requisito de la suscripción, históricamente ligado al contrato entre personas presentes y al uso social de las cartas misivas, se descubre ahora incompatible con las modernas técnicas de fijación y transmisión de la palabra. Los mensajes escritos quieren liberarse del vínculo de la firma, y por ello solicitan nuevos métodos de imputación, nuevos criterios de referencia a la persona del declarante. Métodos y criterios no ya más ligados a la firma autógrafa, sino al uso exclusivo del aparato técnico: la mencionada exclusividad tomará el lugar de la personalidad de la

suscripción. Una rápida y advertida disciplina legislativa serviría para prevenir las tortuosas calles de la analogía y las temeridades de la jurisprudencia". (12)

Se necesitarán nuevos métodos de imputación o criterios de referencia de la persona del declarante, métodos y criterios que tienen muy poco que ver con la firma autógrafa, existen inclusive computadoras que leen firmas, habiéndose implantado métodos para controlar la autenticidad del documento, los que aparentemente son superiores a la firma. Estudios biométricos (mapa de venas del rostro, huella retinal, huella palmar, huella digital), son medios de control que pueden identificar a la persona y que no pueden ser copiados, existiendo además los códigos de acceso que son personales.

La Suscripción Electrónica

Siguiendo la línea de Couture, para quien la firma no es más que un trazado gráfico podríamos deducir que las claves, los códigos, los signos y los sellos, al ser trazados gráficos, también serían firma y, por ende, obligarían.

Entonces, la función que cumple la firma no sólo puede realizarse con el nombre y apellido puestos de puño y letra, seguidos de la rúbrica; sino que además cabe la posibilidad de que se realicen algunas de sus funciones mediante códigos, claves, sellos u otros elementos identificatorios, pero no podríamos decir que es una firma.

Estos nuevos métodos sólo cumplirán sus funciones, ya que la firma propiamente dicha, tiene características y contenido bien definidos. Por ello creemos que a estos métodos de identificación y consentimiento deberíamos llamarlos "suscripción electrónica", tomando el término suscripción en el sentido que nos indica el Diccionario de la Lengua Española.

---

(12) GIANNANTONIO, Ettore, Valor jurídico del documento electrónico; Informática y Derecho. Aportes de la Doctrina Internacional. Tomo I, Ediciones Depalma, Buenos Aires, 1987, Pág.115, nota al pie n.22

1. Elementos de la Suscripción Electrónica

Debido a la naturaleza misma de la suscripción electrónica, se diferenciará de la firma en que aquella no incluirá la rúbrica, pero deberá llevar el nombre y apellido como complemento necesario de la clave, código de aceptación o sistema de verificación que se utilice.

Tendremos entonces:

a. Nombres y apellidos

b. Clave o código de aceptación:

Esta reemplazaría la función de prueba que cumple la rúbrica en la firma autógrafa. Podemos imaginarnos a las partes contratando a distancia a través de un "centro de suscripción electrónica" que guardaría en sus archivos las claves de aceptación de las partes, dando fe de su consentimiento, lográndose así una total seguridad del sistema para los efectos probatorios, sistema que bien podría estar adscrito al servicio que prestan las notarías.

2. Funciones de la Suscripción Electrónica

Al igual que en la firma, la suscripción electrónica deberá cumplir una función probatoria que le permitiría suplir eficazmente la función declarativa e indicativa, ya que como dijimos son atributos dados por un convencionalismo social y jurídico que es aplicable también a este nuevo método.

3. Seguridad de la Firma Tradicional

Un argumento clásico para sostener el uso del documento papel es el de la aparente dificultad que reviste su falsificación. Pero a diario en nuestro país los hechos demuestran lo contrario. Basta con mirar en noticias, artículos de revistas y expedientes judiciales para que nos demos cuenta de lo fácilmente falsificable que es este tipo de documentos y la cantidad de técnicas que se desarrollan para ello. Títulos universitarios, membretes de

notarías, pasaportes y visas, facturas, boletos para partidos de fútbol, etc.; todo lo cual ha llevado a usar métodos cada vez más sofisticados para evitar estos hechos: papel químico para boletos de entrada a espectáculos deportivos, claves secretas en los billetes, fotos impresas y símbolos visibles sólo por luz ultravioleta. Sin embargo, todo esto ha sido falsificado produciendo un aumento de los costos de estos documentos. En otros simplemente no hay ningún resguardo: ¿qué nos impide falsificar un documento notarial?, aparentemente nada, pues el papel de que está hecho es de lo más corriente, la firma es fácilmente adulterable y que decir de los sellos que pueden ser fabricados en cualquier esquina.

Algunos de estos papeles se utilizan para pedir préstamos en instituciones bancarias y financieras y, sin embargo, su aceptación en general está fuera de cuestión a pesar de que sabemos de la facilidad con que personas inescrupulosas pueden procurárselos.

Con esto no pretendemos decir que ya no tiene utilidad la documentación en papel, sino que la seguridad que muchos pretenden atribuirle no es tal y estas falencias podrían, en algunos casos, ser salvadas mediante métodos de control electrónico. Así, por ejemplo, un abogado de un banco podría pedir directamente al Registro Inmobiliario mediante su computador la historia de un bien raíz sin necesidad de que, por ejemplo, el solicitante de un préstamo con garantía hipotecaria llevara títulos cuya autenticidad no es absolutamente segura. Lo mismo podríamos decir de los registros notariales.

7.- Autenticidad, Inalterabilidad y Seguridad del Documento Electrónico

La autenticidad es la correspondencia entre el autor aparente y el autor real del documento. Dicha correspondencia dependerá, en lo relativo al documento electrónico, de los niveles de estandarización de los sistemas informáticos emisores, los que deberán responder a las reglamentaciones

que se dicten al efecto. La autenticidad e inalterabilidad del documento, dependerá, en última instancia, de la seguridad con que se rodee el proceso de elaboración y emisión del mismo.

CAPITULO III

LA FIRMA DIGITAL

Sumario: 1.- Introducción 2.- Firma digital y firma electrónica 3.- Firma manuscrita y firma digital 4.- Comparación entre las firmas 5.- Procedimiento de firma digital 6.- Criptografía 7.- Consecuencias de la firma digital 8.- Ventajas y desventajas 9.- Aplicaciones. 10.- Validez jurídica del documento electrónico

1.- Introducción

Con la sanción de la ley 25506, denominada de Firma Digital y sancionada por el Congreso de la Nación el 14 de diciembre de 2001, la Argentina se incorpora al elenco de países que ha encarado la regulación normativa de la denominada "sociedad de la información", nacida a partir de la digitalización de las comunicaciones y caracterizada por la facilitación y rapidez de las comunicaciones a lo largo y ancho del planeta, con acceso a una cantidad infinita de información por un idéntico universo de usuarios, a través de la red abierta de Internet.

La ley regula los aspectos tendientes a dotar de seguridad a las declaraciones de voluntad o de ciencia enviadas a través de las redes,

mediante la adopción de métodos que aseguren la autoria e inalterabilidad del documento electrónico.

Ya mencionamos anteriormente que para que las operaciones y el comercio electrónico puedan continuar su desarrollo, es necesario prever y solucionar su principal problema: la inseguridad del medio por el que transita la información; y que es la firma digital sea la llave para otorgar seguridad y privacidad en la comunicación a distancia.

La firma digital es una propuesta de la tecnología informática que intenta cumplir la finalidad que tradicionalmente cumplía la firma manuscrita. En este sentido, los obstáculos que se oponen al reconocimiento del documento electrónico se apoyan en uno de los elementos que integran el documento, que es la firma.

Si tomamos en cuenta las consideraciones efectuadas anteriormente sobre la definición y descripción de firma en la legislación argentina, es imposible asimilarla a un código electrónico por el cual se encripta un documento electrónico. La ley de Firma Digital (en adelante LFD) regula los aspectos jurídicos de la misma, definiendo el grado de validez del resultado de la aplicación de esta nueva tecnología, el reconocimiento legal de los actos amparados por esa aplicación y los derechos u obligaciones emergentes de los mismos.

2.- Firma digital y firma electrónica

La LFD distingue entre firma digital y firma electrónica. Sigue la distinción que las legislaciones, proyectos y doctrina realizan: firma digital, que es el procedimiento técnico que adosado a un documento electrónico asegura ciertos resultados (autenticación y no alteración del documento transmitido), y firma electrónica, el que no asegura estas prestaciones.

Una firma electrónica seria simplemente cualquier método o símbolo basado en medios electrónicos utilizado por una parte con la intención de vincularse a un documento, cumpliendo las funciones

características de una firma manuscrita. En este concepto amplio de firma tendrían cabida técnicas tan simples como un nombre u otro elemento identificativo (por ejemplo la firma manual digitalizada), incluido al final de un documento electrónico, y de tan escasa seguridad que plantean la cuestión de valor probatorio a efectos de autenticación, aparte de su nula aportación respecto de la integridad del mensaje.

Firma digital, en tanto, es “tecnológicamente especifica” pues se crea a través de un sistema de criptografía asimétrica o de clave publica. Estos sistemas permiten, aplicando la clave pública al mensaje cifrado por el firmante mediante su clave privada, la autenticación y la integridad del mensaje y el no rechazo, pudiendo, incluso, mantener la confidencialidad.

En el art. 2º la LFD define: “Firma digital. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose esta 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.”

El art. 5º, en tanto, define: “Firma electrónica. Se entiende por firma electrónica al 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 este sentido la LDF determina cuales serán los requisitos exigibles al procedimiento técnico aplicado al documento electrónico, para considerarlo firma digital, y aplicar sus efectos:

a) que los datos mediante los cuales se crea la firma se mantengan en confidencialidad absoluta del signatario;
b) que la firma pueda ser verificada por terceros (quienes expedirán el certificado correspondiente);

c) que permita identificar al firmante y detectar alteraciones en el documento electrónico;
d) que haya sido creada durante el periodo de vigencia del certificado digital válido del firmante (art. 9º LDF, inc a);
e) que pueda ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente (art. 9º, inc. b);
f) que el certificado haya sido emitido o reconocido por un certificador licenciado, de acuerdo con el régimen de licencias de servicios de certificación determinado por la ley (art. 9º, inc. c).

Si bien en la definición de firma digital la ley pretende mantenerse en un estado de neutralidad respecto de la tecnología a aplicar, es notorio que todo el sistema esta estructurado sobre la base del sistema criptográfico de doble clave simétrica, el cual explicaremos más adelante.

Por lo tanto, lo que diferencia a una firma digital de una electrónica podríamos sintetizarlo de la siguiente manera:

Firma digital = documento digital + procedimiento matemático + requisitos legales.

Firma electrónica = firma digital - requisitos legales.

Dentro de la categoría genérica de firma electrónica, es necesario distinguir entre firma electrónica en general y firma electrónica segura, refrendada o firma digital. Esta distinción tiene su origen en la tecnología que se aplica para poder calificar a la firma como segura o no. Además, tiene repercusiones posteriores, puesto que la legislación prima a las firmas digitales o firmas electrónicas seguras tanto a nivel internacional como comunitario.

La diferencia principal entre ambos tipos de firma, radica en el sistema criptográfico que se ha utilizado: para las firmas electrónicas en

general se utiliza un sistema criptográfico simétrico o de clave secreta; mientras que para la firma digital el método utilizado es asimétrico o de clave publica.

"Una firma digital es una cadena de datos creada a partir de un mensaje, o parte de un mensaje, de forma que sea imposible que quien envía el mensaje reniegue de él (repudio) y que quien recibe el mensaje pueda asegurar que quién dice que lo ha enviado es realmente quien lo hizo, es decir, el receptor de un mensaje digital puede asegurar cual es el origen del mismo (autenticación). Así mismo, las firmas digitales pueden garantizar la integridad de los datos (que no se hayan modificado los datos durante la transmisión)." (13)

3.- Firma manuscrita y firma digital

Es criterio legislativo general que ciertas declaraciones de voluntad deben estar firmadas para ser atribuidas a su autor. El requisito se repite a lo largo y ancho de las legislaciones. La necesidad de firma persigue diversos fines: identificar a una persona, dar certeza a la participación personal de esa persona en el acto de firmar y asociar a esa persona con el contenido de un documento.

Además, se reconoce que la firma puede desempeñar, además, otras funciones: demostrar la intención de una parte contractual de obligarse por el contenido del contrato firmado, de reivindicar la autoria de un texto, la intención de una persona, de asociarse con el contenido de un documento escrito por otra, o el hecho de que esa persona había estado en un lugar determinado, en un momento dado.

Expuestas estas ideas, vemos que es necesario compatibilizar las soluciones ideadas para el antiguo esquema de representación con el nuevo escenario, otorgando carta de ciudadanía definitiva a los documentos

(13) NIEVA CONEJOS, María Isabel; Ponencia: Firmas Digitales, ¿El comercio electrónico esta beneficiado con la reglamentación de la ley 25506?; cátedra de Derecho Comercial II; Facultad de Ciencias económicas de la UNT; AÑO 2007., Pág. 82.

digitales en el mundo jurídico. Ahora bien, para otorgar carta de ciudadanía a estos documentos es necesario, primero, reconocer que un documento electrónico firmado digitalmente es equiparado legalmente a un documento escrito firmado y, segundo, determinar los requisitos para que las nuevas técnicas de firma cumplan funciones iguales a la firma manuscrita.

Con la sanción de la Ley 25506 de Firma Digital se ha dado reconocimiento a la firma Electrónica y Digital y se ha incorporado a la legislación argentina el principio de la equivalencia funcional.

En este sentido, el art. 3º, LDF expresa: “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”

La ley equipara firma manuscrita con firma digital, lo que constituye un paso fundamental en el nuevo camino de convergencia entre lo escrito manuscrito y lo escrito digital, y afirma que dicha equiparación o equivalencia rige tanto cuando la ley establece la obligatoriedad de firmar (exigencia positiva), como cuando la ley prevé una consecuencia en caso de ausencia de firma (exigencia negativa).

Esto es lo que se denomina Criterio de Equivalencia Funcional: se establece con relación a la firma digital una presunción iuris tantum de autoría y de integridad, estableciendo que salvo prueba en contrario se considera que la firma digital pertenece al titular del certificado y que luego de aplicado un procedimiento de verificación a un documento digital corresponde tener al documento por no modificado desde el momento de su firma.

Tal presunción no existe con relación a la firma electrónica ya que el art. 5° in fine establece que en caso de ser la firma electrónica, corresponde a quien la invoca acreditar su validez.

Por otra parte, la LDF en su art. 4º determina en qué actos jurídicos no puede ser utilizada firma digital: en las disposiciones por causa de muerte; en los actos jurídicos de derecho de familia, en los actos personalísimos en general; en 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 entre partes.

En las exclusiones existen supuestos más claros como los testamentos, o el reconocimiento de hijos, y otros que traerán evidentes discusiones. La ley deja abierto el elenco de actos excluidos mediante una formula amplia de “incompatibilidades” con el nuevo medio, difiriendo a la ley su determinación o a la voluntad de las partes intervinientes, quienes pueden exigir mayores formalidades en su resguardo.

4.- Comparación entre las firmas

La firma es un conjunto de letras o signos que identifican a la persona que la estampa. En el concepto tradicional la firma de un documento, ya sea este privado o público, debe efectuarse de manera manuscrita u hológrafa.

La firma electrónica es cualquier método o símbolo basado en medios electrónicos, utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita.

Por su parte la firma digital es una forma específica de firma electrónica en la cual interviene un proceso criptográfico que cumple determinados requisitos, y que da seguridad a quien extiende esta firma.

VS

Parametro	Manuscrita	Digital
Autenticidad	Puede ser falsificada	No puede ser copiada
Integridad	No ayuda	Firma por cada documento
No-repudio	Necesita un grafólogo	Con un computador y la CA

Respecto de la firma digital, para una mejor comprensión de la misma, hacemos las siguientes aclaraciones:

- Equivalente digital a la firma manuscrita.
- NO ES LA IMAGEN ESCANEADA de la firma manuscrita.
- NO ES UN PASSWORD sino el resultado de un procedimiento realizado con una clave numérica llamada clave privada. Es la encriptación (criptografía) con la llave privada del hash (resumen) de un documento.
- Existe una diferente para cada documento.
- Debe constar de por lo menos dos partes:
  1. Método que haga imposible la alteración de la firma.
  2. Verificación que la firma pertenece al firmante.

5.- Procedimiento de firma digital

El procedimiento de firma digital de un mensaje consiste en extraer un “resumen” (o *hash* en inglés) del mensaje, cifrar ese resumen con la clave privada del remitente y añadir el resumen cifrado al final del mensaje. El algoritmo que se utiliza para obtener el resumen del mensaje debe cumplir la propiedad de que cualquier modificación del mensaje original, por pequeña que sea, dé lugar a un resumen diferente. “La firma digital de un usuario no

será siempre la misma secuencia de bits, sino que dependerá del mensaje firmado.” (14)

En forma más detallada explicaremos el proceso:

El usuario prepara el mensaje a enviar:

1- utiliza una función *hash* para producir un resumen del mensaje

2- el remitente encripta el resumen con su clave privada. La clave privada es aplicada al resumen usando un algoritmo matemático. La firma digital consiste en la encriptación del resumen.

3- El remitente une su firma digital a los datos; luego envía electrónicamente la firma digital y el mensaje original al destinatario. El mensaje puede estar encriptado, pero esto es independiente del proceso de firma.

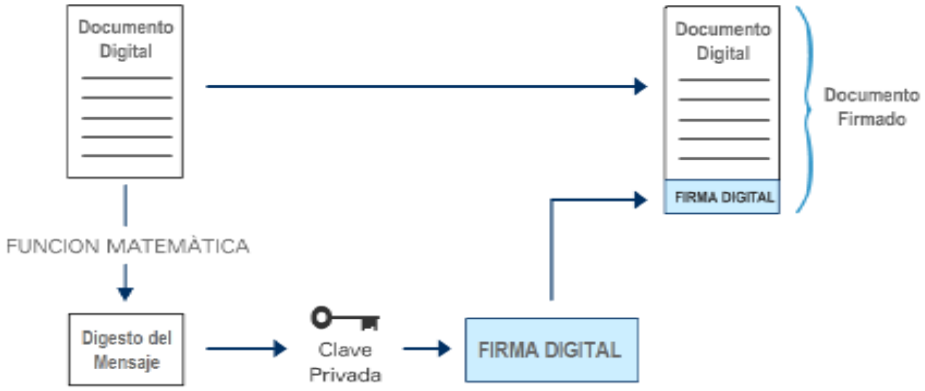
4- El destinatario usa la clave pública del remitente para verificar la firma digital, es decir para desencriptar el resumen adosado al mensaje.

5- El destinatario realiza un resumen del mensaje utilizando la misma función resumen segura.

6- 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.

(14) Ibídem; Pág. 83.

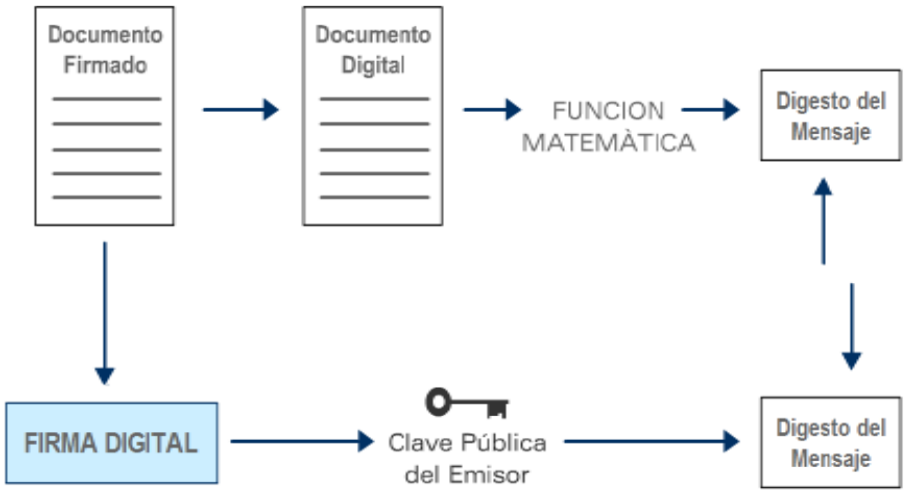
EMISOR



Cuando el destinatario recibe el mensaje, lo descifra con su clave privada y pasa a comprobar la firma. Para ello, hace dos operaciones: por un lado averigua la clave pública del remitente y descifra con ella el resumen que calculó y cifró el remitente. Por otro lado, el destinatario calcula el resumen del mensaje recibido repitiendo el procedimiento que usó el remitente. Si los dos resúmenes (el del remitente descifrado y el calculado ahora por el destinatario) coinciden la firma se considera valida y el destinatario puede estar seguro de la integridad del mensaje; si el mensaje hubiera sido alterado en la red, el resumen calculado por el destinatario no coincididita con el original calculado por el remitente.

Además, el hecho de que el resumen original se haya descifrado con la clave publica del remitente, prueba que solo él pudo cifrarlo con su clave privada. Así el destinatario esta seguro de la procedencia del mensaje (autenticación), y llegado el caso, el remitente no podría negar haberlo enviado (no repudio) ya que solo él conoce su clave secreta.

RECEPTOR



La firma digital es generalmente invisible y va anexada a los documentos en forma de “certificado” encriptado. De imprimirse este certificado se vería como una serie revuelta de letras y números. En realidad el intercambio de llaves se realiza rápidamente, y tanto el remitente como el destinatario deberán contar con un software capaz de desencriptar los certificados y autentificar la identidad del firmante. Para construir la firma digital se recurre a la criptografía.

¿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.

¿Qué consideraciones se deben tener para utilizar una firma digital?

Se necesita contar con un navegador como Internet Explorer 4.0x o Netscape 4.03 o versiones superiores, tener conexión a Internet y poseer

una cuenta de correo electrónico que no sea una Webmail (como Yahoo, uolmail, etc).

6.- Criptografía

El hombre, desde tiempos inmemoriales, siempre ha tratado de proteger la información. Como uno de los recursos mas valiosos que posee, ha buscado defenderlo de sus enemigos. Hay una manera, la que podemos pensar como más lógica, es asegurarla físicamente. De esta manera, se previene que nuestros adversarios o rivales la obtengan. Pero pensemos por un momento, ¿que pasaría si la información cayera en manos de quienes no queremos? (la seguridad perfecta no existe). ¿No sería más práctico que a pesar de ello, la información no pueda ser útil al enemigo? Es aquí donde entra a jugar el concepto de criptografía.

"La criptografía es la ciencia que estudia la ocultación, disimulación o cifrado de la información. La criptografía tradicional se basa en el conocimiento que tienen de una clave secreta tanto quien envía un mensaje como quien lo recibe. De manera que el encriptado es la transformación de datos en signos ilegibles para quien no disponga de la clave secreta para desencripralo. El proceso criptográfico transforma un texto claro y legible en un mensaje cifrado al que se denomina criptograma." (15)

Por lo tanto, el que envía el mensaje utiliza una clave para encriptarlo (codificar su contenido) y el que lo recibe aplica la misma clave para desencriparlo, y así tomar conocimiento del mensaje. La inseguridad de este procedimiento radica en el riesgo de que un tercero también conozca la clave, pudiendo acarrear problemas de confidencialidad, ya que si se utiliza en un entorno multiusuario, ello hace necesario distribuir la clave, quedando en evidencia. Este método se conoce como **criptografía con clave secreta o criptografía simétrica.** En estos sistemas existe una sola clave que sirve tanto para encriptar como para desencriptar.

---

(15) LARDENT, Alberto, Op. Cit., Pág. 460.

Uno de los métodos criptográficos simétricos mas conocidos y utilizado en el mundo es DES (Data Encryption Standard, Estándar de encriptación de datos).

Un método que otorga seguridad y validez a los documentos transmitidos por vía electrónica es el que se apoya en las denominadas "firmas electrónicas mediante **criptografía asimétrica**" o "**criptografía con clave pública**".

La criptografía asimétrica utiliza un software encriptador que se apoya en dos tipos de llaves o claves; las partes contratantes disponen de dos claves que se complementan entre sí: una de ellas (clave pública) es conocida públicamente; la otra (clave privada) es secreta y confidencial.

Encriptación:

Texto Original + Clave de Encriptado = Texto Encriptado

Desencriptacion:

Texto Encriptado + Clave de Desencriptado = Texto Original

"Cada usuario debe generar su propio par de claves por intermedio de un software confiable, o también puede peticionarse por separado a un ente que tenga a su cargo la autoridad de certificar a quién pertenece y las condiciones de vigencia, revistiendo a su vez el carácter de tal por medio de una fuente formal que la autorice. En tales casos, esas personas autorizadas o con licencia para esos fines, se conocen como "Autoridades Certificantes". (16)

Entonces Cada usuario debe poseer dos claves o llaves:

CLAVE PRIVADA: es el conjunto de datos únicos e inalterables generados sobre la base de un procedimiento informático que garantiza su irreproductibilidad y confidencialidad, asignada a una persona física o jurídica

(16) CARLINO, Bernardo P., Firma Digital y derecho Societario; Rubinzal-Culzoni Editores; Buenos Aires, 2004; Pág. 40.

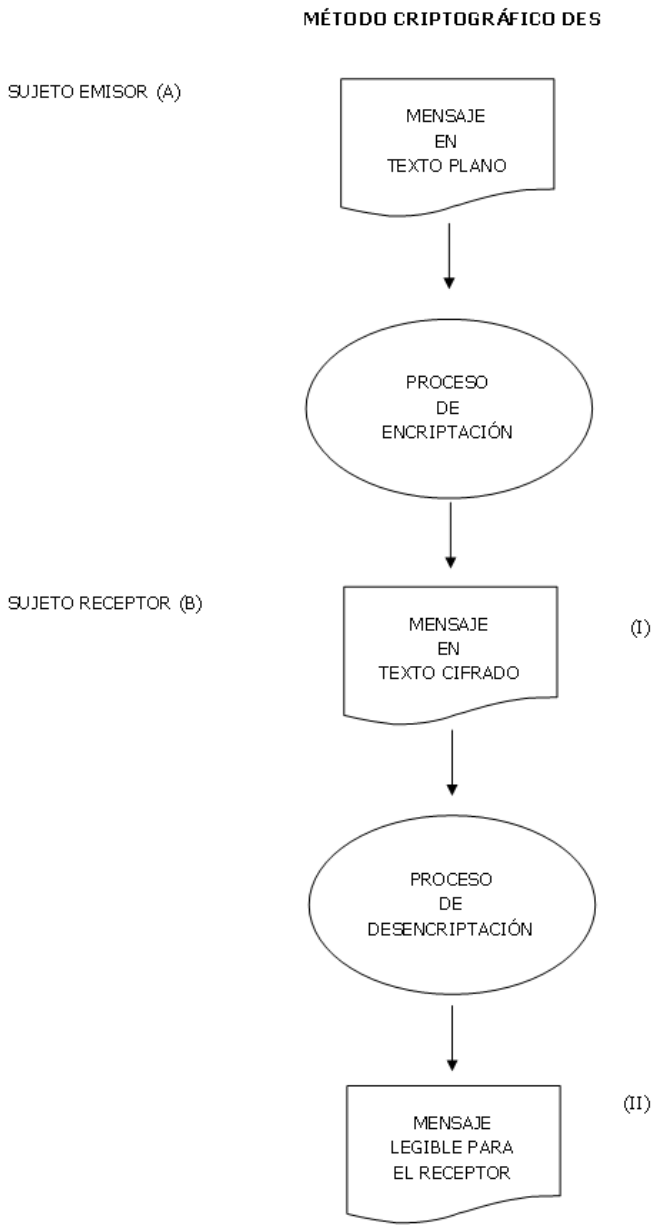
por una autoridad certificadora, y que esta contenido electrónicamente en un medio físico, tal como una tarjeta inteligente.

CLAVE PÚBLICA: es el conjunto de datos únicos e inalterables generados en forma simultánea con la clave privada, que se corresponden unívocamente a los datos contenidos en esta ultima asignado por la autoridad certificadora a la misma persona física o jurídica titular de la clave privada y que es mantenida en un archivo electrónico.

La diferencia entre clave pública y privada reside en que con la pública queda eliminada la necesidad de que un remitente y un receptor compartan la misma clave: las comunicaciones sólo necesitan de la clave pública; entonces la clave privada no se transmite ni comparte.

Las dos claves o llaves están relacionadas matemáticamente entre si y las genera simultáneamente una sola vez el usuario; están vinculadas a un certificado digital.

Debe aclararse, en cuanto a las condiciones de seguridad, que el conocimiento del código de una clave publica no significa que a partir de allí se pueda deducir la clave privada correspondiente.



(I) Se ejecuta a traves de una clave privada de encripación.
(II) Se ejecuta a traves de una clave privada de desencripación (la misma para emisor y receptor).

Si bien la firma digital puede obtenerse de una variedad de protocolos, el que cumple con los atributos de la firma tradicional es el denominado sistema de clave pública o sistema asimétrico, que asegura las siguientes propiedades:

- el emisor que firma un documento electrónico debe reconocer su contenido, debido a que no puede modificárselo después (no repudio)
- el receptor puede verificar la seguridad de la procedencia del documento (confirma la firma del emisor)
- en consecuencia, el documento tiene fuerza legal para las partes

Para describir el funcionamiento de este sistema, debemos dar algunas aclaraciones, este sistema utiliza dos claves por usuario:

- **Una pública**: conocida por todos
  - sirve para encriptar mensajes dirigidos a quien posee la clave privada
  - sirve para constatar la firma
- **Una privada** conocida sólo por su titular
  - sirve para desencriptar mensajes
  - sirve para firmar digitalmente

Recordemos que ambas claves se generan simultáneamente y que tienen la propiedad de que cada una desencripta lo que encripta la otra.

De acuerdo con este criptosistema, el emisor del mensaje o contrato utiliza la clave pública del destinatario para encriptar el contrato dirigido a esa persona, y lo firma electrónicamente con su llave privada. Por su parte, el destinatario utiliza su llave privada para desencriptarlo, verifica la firma del emisor con la clave pública del mismo y luego firma el documento electrónico con su llave privada. Así el receptor desencripta el mensaje recibido con su clave privada, habiendo el emisor encriptado el mensaje enviado con la clave pública del destinatario.

El documento electrónico así elaborado forma un conjunto cerrado de pulsos electrónicos y cualquier alteración que sufriera seria detectada por la computadora, declarándose al documento como no válido, es decir, no auténtico.

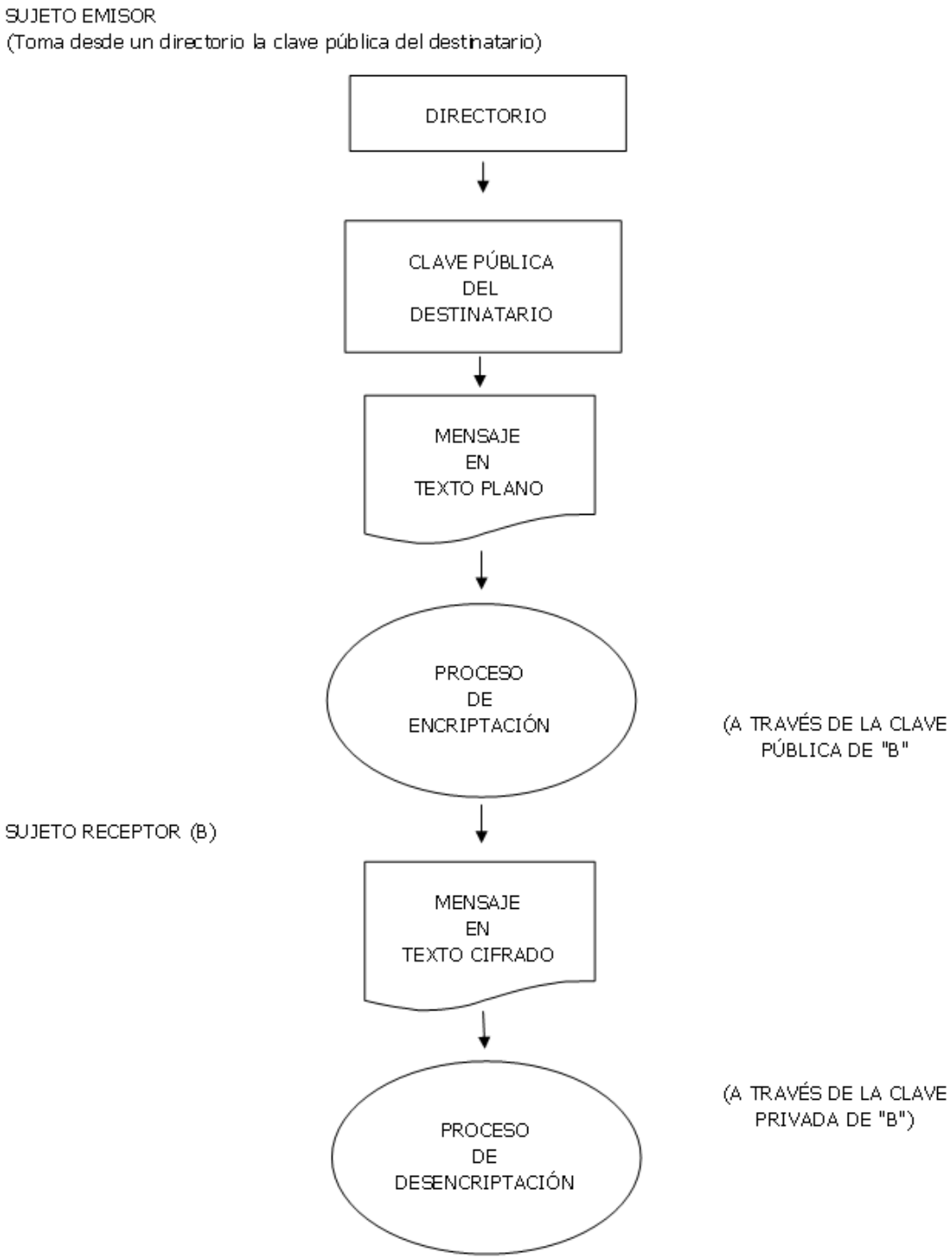
Si se presentara algún conflicto entre las partes como consecuencia de este modo de operación, el mismo seria dirimido por el ente de certificación, que mantiene el resguardo de todas las claves públicas y privadas.

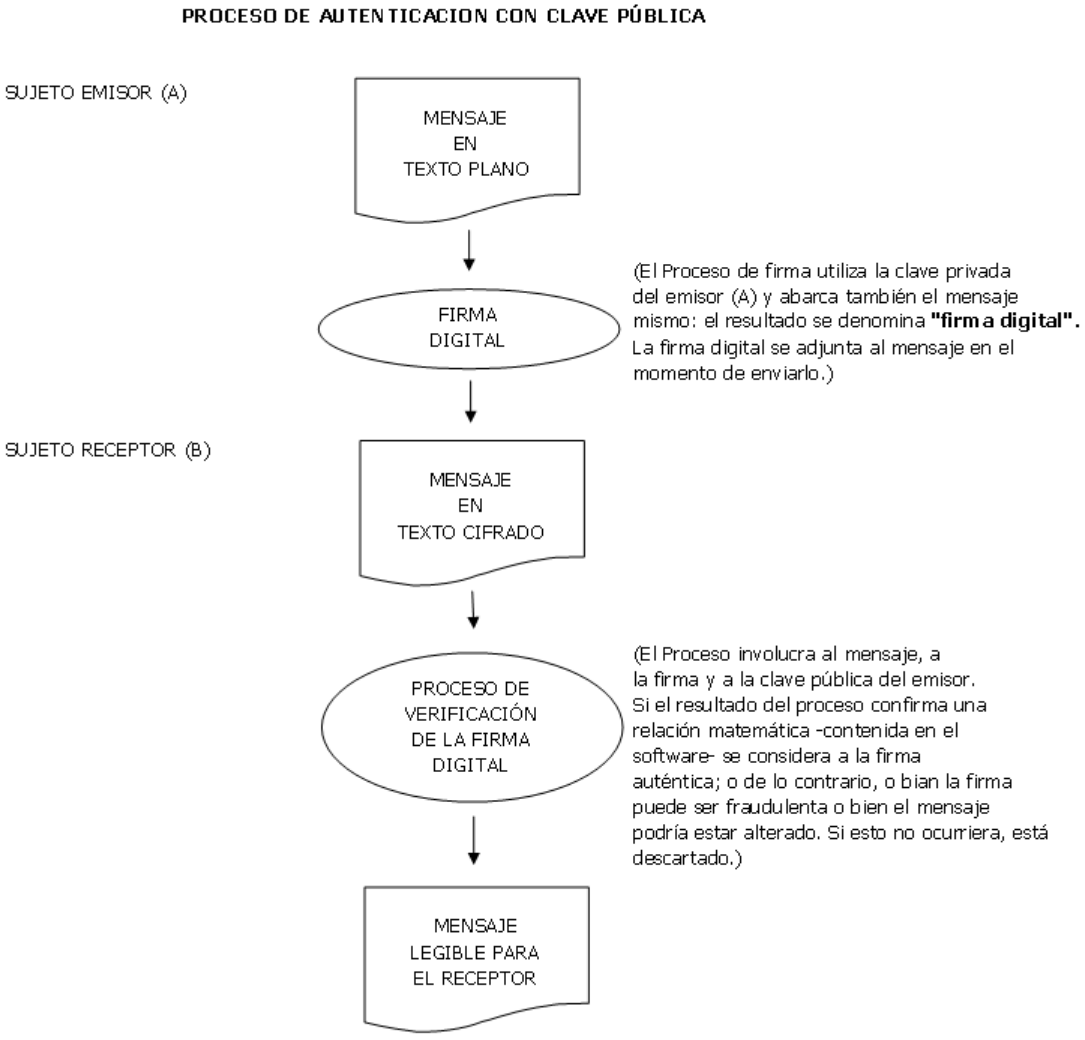
En realidad, en razón de la lentitud del proceso de generación de firma digital, no se aplica el cálculo (algoritmo) sobre el mensaje completo sino sobre una parte reducida de éste, que es una muestra que se obtiene del mensaje, es decir un resumen. Este resumen se calcula mediante la función *hash.*

"Una función *hash* tiene el propósito de reducir mensajes de cualquier longitud a una pequeña dimensión, de un rango de ocho a dieciséis *bytes (string* o serie continua integrada por letras y números). La propiedad que tiene esta función, como ya se explicó, es que si se modifica el mensaje original se modificará su resumen." (17)

(17) LARDENT, Alberto, Op. Cit., Pág. 467.

PROCESO DE ENCRIPTACIÓN CON CLAVE PÚBLICA





La firma digital así generada permite garantizar la integridad del documento durante su transmisión y hasta su destino; posibilita certificar su origen y crea el no repudio.

En cuanto al nivel de seguridad, aunque el mensaje se envíe por un canal inseguro, podemos decir lo siguiente:

Siendo la persona **A** el emisor del mensaje, y **B** el destinatario:

a) Si bien otras personas pueden conocer la clave pública A, debido a que podrían descifrar el mensaje encriptado con la clave privada de éste, solamente B conoce su propia clave privada (la de B), por lo que únicamente B es quien podría

desencriptar el mensaje que recibe de A con la clave privada de B. Esto asegura que sólo la persona B puede conocer el mensaje.

b) Si la firma digital se desencripta con la clave pública de A, ello significa que fue encriptada con la clave privada de A; por lo tanto se garantiza que el mensaje fue generado por la persona A, pues es la única que puede conocer la clave privada de A.

c) Debido a que el canal de transmisión (Internet) es inseguro, una tercera persona podría interceptar el mensaje, ya que puede conocer la clave pública del destinatario y la del emisor (en razón de que estas claves son públicas); pero el intruso al no tener la clave privada no podrá descifrar el contenido del mensaje.

Entre las desventajas de este sistema de criptofrafía de clave pública es que es menos veloz que el de clave privada.

“El software más utilizado es el RSA (Sistema criptografico con clave pública) y es cien veces más lento que el DES (Estandar Simétrico de clave secreta). Pero ambos sistemas pueden combinarse para obtener lo mejor de cada uno: la seguridad de la clave pública y la velocidad de la clave privada.” (18)

El Sistema criptográfico RSA, el más utilizado en la actualidad, si bien no es el único, presenta ventajas debido a que puede ser usado tanto para encriptación como para autenticación de mensajes. Este otorga confianza en los documentos firmados digitalmente, los cuales se pueden intercambiar entre usuarios de distintos países que utilizan diferente software sobre diferentes plataformas.

Una firma digital RSA es más confiable que una firma manuscrita, por las siguientes razones:

---

(18) NIEVA CONEJOS, María Isabel; Op. Cit., Pág. 86.

1. atestigua la identidad del firmante. Si se aplica adecuadamente la función *hash* no es posible “copiar” una firma tomándola de un documento y trasladándola a otro.

2. Asegura el contenido del mensaje. El sistema de autenticación de RSA permite verificar la integridad de un documento firmado. Por lo tanto, es posible detectar si el contenido de un mensaje firmado digitalmente ha sido alterado maliciosamente, aunque haya sido modificado un solo bit.

Los especialistas en el tema, si bien reconocen que la seguridad absoluta es imposible (los hackers existen), afirman que lograr decodificar una clave generada por RSA puede insumir tanto tiempo y dinero que disuade de su intento a cualquier estafador.

7.- Consecuencias de la firma digital

1- Presunción de autoria

El art. 7º de la LDF dispone: “Presunción de autoria. Se presume, salvo pruebo en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma”.

El sistema de firma digital adoptado por la LDF implica la presencia de un tercero, habilitado por el organismo de aplicación de la ley, quien es el encargado de emitir un certificado digital que permitirá la verificación de la firma inserta en el documento digital.

La ley presume que el titular del certificado es quien firmo el documento y, por ende, su autor.

2- Presunción de integridad

El art.8º, LDF expresa: “Presunción de integridad. 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.”

El procedimiento de firma digital debe asegurar la inalterabilidad del documento. Consecuencia lógica es, entonces, que si el destinatario del mensaje ha aplicado el procedimiento de verificación de firma y ha resultado que la firma pertenece al remitente del mensaje, el documento es integro, es decir, no ha sido modificado desde que fue emitido.

8.- Ventajas y desventajas

Las ventajas derivadas de la utilización del sistema de firma digital van desde el aumento de la seguridad en las transacciones hasta la no necesidad de presencia o traslado físico, ventajas éstas que se traducen en celeridad y ahorro de costos.

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.

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, ya que el uso de la firma digital satisface los siguientes aspectos de seguridad:

Integridad de la información: la integridad del documento es una protección contra la modificación de los datos en forma intencional o accidental. El emisor protege el documento, incorporándole a ese un valor de control de integridad, que corresponde a un valor único, calculado a partir del contenido del mensaje al momento de su creación. El receptor deberá

efectuar el mismo cálculo sobre el documento recibido y comparar el valor calculado con el enviado por el emisor. De coincidir, se concluye que el documento no ha sido modificado durante la transferencia.

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

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

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

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

Entre las desventajas podemos mencionar la necesidad de contar con una autoridad certificadora de confianza (tercera parte de confianza) y la responsabilidad que pesa sobre los propios usuarios de generar un entorno adecuado que les permita mantener bajo su exclusivo control los datos de creación de la firma y contar con un dispositivo de creación técnicamente confiable.

9.- Aplicaciones

El abanico de posibilidades de aplicación de la firma digital es muy variado, tan variado como el de aplicación de la firma manuscrita.

A modo de ejemplos enumeramos algunos casos particulares de aplicación a nivel mundial:

- Transacciones bancarias
- Transacciones comerciales
- Declaraciones impositivas
- Documentos relativos a operaciones de seguro
- Factura electrónica
- Dinero electrónico
- Contratos comerciales electrónicos
- Certificación de los actos de gobierno (leyes, resoluciones, dictámenes, sentencias, etcétera)
- Contrataciones públicas (envío y recepción de ofertas, adjudicaciones, etcétera)
- Decretos ejecutivos (gobierno)
- Desmaterialización de documentos
- Notificaciones judiciales electrónicas
- Documento de identidad electrónico (e-DNI)
- Voto electrónico
- Obtención del CUIL
- Solicitud de empleo público
- Historias clínicas
- Invitación electrónica
- Mensajes con autenticidad asegurada y sin posibilidad de repudio
- Correo seguro

10.- Validez jurídica del documento electrónico

Documento Escrito y Documento Digital

Las declaraciones de voluntad (o de ciencia) expresadas por medios digitales o electrónicos deben buscar su reconocimiento legal en un universo de normas dictadas para un modelo escrito en papel. De allí que las legislaciones para los nuevos mundos digitales afirman, a través de sus disposiciones, la igualdad de tratamiento.

El art. 6° de la LFD expresa: “Documento digital. Se entiende por documento digital a 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”.

Si la idea o declaración esta representada digitalmente se considera escrita.

La Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Desarrollo del Derecho Mercantil Internacional (CNUDMI/Uncitral), material tenido en cuenta para la confección de la LDF, contiene disposiciones en igual sentido: “Art. 5°. Reconocimiento jurídico de los mensajes de datos: No se negaran efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos”.

“Art. 6°. Escrito: 1) Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos si la información que éste contiene es accesible para su ulterior consulta. 2) El párrafo 1° será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no conste por escrito”.

Según la Guía para la Incorporación de la Ley Modelo a las legislaciones nacionales (aleccionadora en diferentes aspectos), los objetivos y funciones que persigue la presentación de un escrito consignado en papel son: “ese documento de papel cumple funciones como las siguientes: proporcionar un documento legible para todos; asegurar la inalterabilidad de un documento a lo largo del tiempo; permitir la reproducción de un documento a fin de que cada una de las partes disponga de un ejemplar del mismo escrito; permitir la autenticación de los datos consignados suscribiéndolos con una firma; y proporcionar una forma aceptable para la presentación de un escrito ante las autoridades publicas y los tribunales.

Luego de afirmar que el documento digital, bajo el cumplimiento de ciertas normas técnicas, cumple todas y cada una de las funciones reseñadas, aun con mayor eficacia y seguridad que el mismo papel, expresa que ello no debe llevar a exigir a un documento digital más requisitos que los que se exigiría a un documento en papel.

Expresa la Guía que:”…no se negaran efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensajes de datos. El Art.5° se limita a indicar que la forma en que se haya conservado o sea presentada cierta información no podrá ser aducida como única razón para denegar eficacia jurídica, validez o fuerza ejecutoria a esa información.

El hecho de que se requiera documento “escrito” no equivale a “escrito firmado”, “original firmado” o acto jurídico autenticado”.Éstos serán requisitos adicionales que la ley puede requerir, o no hacerlo, para otorgar otros efectos jurídicos, distintos o gravados, al requisito de la escritura.

En la realidad el requisito de la escritura es el piso mínimo de seguridad exigido a un documento para su inserción en el mundo jurídico, y no más de eso debe pedirse al documento digital para su reconocimiento.

La Ley de Firma Digital no exige ningún requisito al documento digital para su consideración como “escrito”.La ley Uniforme, por contrario, fija un mínimo: el mensaje de datos debe ser “accesible”, esto es, debe poder ser leído e interpretado.

La reglamentación a la Ley de Firma Digital, posiblemente, determinará qué requisitos entiende exigible el legislador nacional para considerar que un mensaje de datos cumple función equivalente a la expresión escrita tradicional.

Entendemos que se debería seguir el criterio amplio de la Ley Uniforme, fijando un piso mínimo (que se accesible, legible), para, luego, determinar estándares más exigentes para dotar al documento digital de otros efectos (para permitir el archivo en forma digital).

Original en papel y original digital

Muchas veces la ley exige que quien pretende oponer una declaración de voluntad presente el original del documento portante de la declaración. También es necesario resolver este problema cuando la declaración se fija en un documento digital.

En realidad, tratándose de documentos digitales, si por “original” se entiende el soporte en el que por primera vez se consigna la información, seria imposible hablar de mensajes de datos “originales”, pues el destinatario de un mensaje de datos recibiría siempre una copia del mismo.

El requerimiento de original del documento es materia corriente en el comercio internacional, pero también las normas de derecho interno lo imponen en diversas oportunidades, a fin de que le sea oponible a la contraparte.

La LFD regula la cuestión en el Art. 11: “*Original.* Los documentos electrónicos 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".

La Ley Modelo, por su parte, propone el siguiente texto para regular este punto:

Art.8°.Original 1) cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedara satisfecho con un mensaje de datos: a) Si existe alguna garantía fidedigna de que se ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma; b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar. "La Ley de Firma Digital reconoce valor de original al documento digital firmado en forma digital y a la reproducción digital de un documento originariamente no digital, siempre que esta reproducción estuviera firmada.

La Ley Modelo no impone que el documento digital este firmado para ser considero original. Fija, en forma mucho más amplia, que se debe garantizar, con grado de fiabilidad, la integridad del documento.

Archivo en papel y archivo digital.

En diversas oportunidades la legislación impone la conservación de documentos a los fines de su utilización como prueba. Así el Código de Comercio Argentino en su Art.67, impone a los comerciantes la conservación de sus libros de comercio y la documentación respaldatoria por un plazo de diez años.

La posibilidad de archivar la documentación en forma digital es una necesidad, por múltiples ventajas (comodidad, inalterabilidad) que acarrea.

Mas es necesario otorgar respaldo legal a esta posibilidad.

La LDF siguiendo los modelos que la anteceden, acomete la cuestión en su Art.12: “*Conservación*. La exigencia legal de conservar la documentación, 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 permita determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción.”

Además determina los requisitos mínimos exigibles a los archivos digitales para cubrir la exigencia legal de conservación de documentos, registros o datos: a) que el documento digital este firmado digitalmente-no basta la firma electrónica-;b) “que el documento sea accesible”; c) que el archivo digital permita determinar, en forma fehaciente, su origen, destino, fecha y hora de generación, envío y/o recepción.

Dable es recalcar que no todos los documentos digitales que luego serán archivados (o conservados, en terminología de la ley) estarán destinados a ser enviados, por lo cual no será necesario determinar el origen o el destino del documento, ni fecha u hora de envío o recepción.

Estos datos del documento serán necesarios cuando se pretenda hacer valer como prueba un documento enviado por una persona a otra, en una controversia entre las mismas.

Cuando se trate de oponer archivos generados por al misma persona que los utiliza como prueba, será necesario poder determinar la fecha y hora de generación del documento y su inalterabilidad, requisitos que se cubrirán mediante la inserción de la firma digital.

Como puede inferirse de la lectura del texto, la LDF determina accesibilidad e integridad.

Beneficios del documento digital

Además de los beneficios legales, existen ventajas de tipo material que brinda la utilización de la firma digital para otorgar seguridad a las operaciones y transacciones con documentos electrónicos:

- Oportunidad en la información, tanto en la recepción como en el envío.
- Ahorro en el gasto de papelería. el ahorro por concepto de administración de facturas (recepción, almacenaje, búsqueda, firma, devolución, pago, envío, etc.) puede fluctuar entre el 40% y el 80%.
- Facilidad en los procesos de auditoria.
- 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.

CAPÍTULO IV

ESTRUCTURA DEL SISTEMA DE FIRMA DIGITAL

Sumario: 1.- Infraestructura de firma digital 2.- Infraestructura del sector público.

1.- Infraestructura de firma digital

Internacionalmente, cuando se habla de firma digital se hace referencia a un conjunto de elementos que es necesario disponer para que esta tecnología sea válida, se encuentre operativa y garantice los aspectos de seguridad que requiere para su correcta aplicación. Estos elementos se sintetizan en la denominada Infraestructura de Clave Pública o Public Key Infrastructure (PKI), que consiste en un sistema de combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas y comunicaciones por Internet. Es un sistema un sistema complejo necesario para la gestión de certificados digitales y aplicaciones de la Firma Digital.

Los actores participes de esta infraestructura son:

a) Organismo o Ente Licenciante (OL)
b) Autoridades Certificantes (o, en inglés, CA, ***C****ertificate* ***A****uthority*): es la encargada de emitir y revocar certificados. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.

c) Autoridades de registro (o, en inglés, RA, ***R****egistration* ***A****uthority*): es la responsable de verificar el enlace entre los certificados (concretamente, entre la clave pública del certificado) y la identidad de sus titulares.
d) Organismo Auditante (OA)
e) Suscriptores titulares de certificados digitales: los que pueden firmar documentos digitales. Los usuarios y entidades finales son aquellos que poseen un par de claves (pública y privada) y un certificado asociado a su clave pública. Utilizan un conjunto de aplicaciones que hacen uso de la tecnología PKI (para validar firmar digitales, cifrar documentos para otros usuarios, etc.)

Una PKI bien construida debe proporcionar:

• **Autenticidad**. La firma digital tendrá la misma validez que la manuscrita.

• **Confidencialidad**, de la información transmitida entre las partes.

• **Integridad**. Debe asegurarse la capacidad de detectar si un documento firmado ha sido manipulado.

• **No Repudio**, de un documento firmado digitalmente.

2.- Infraestructura del sector público

I. Consideraciones previas

Previamente a la exposición de la Estructura del Sector Público Nacional para la Firma Digital, es necesario dejar en claro algunos conceptos sobre el certificado de Clave Pública y la correspondiente Autoridad Certificante que emite dicho certificado.

A.- *Certificado de clave pública*

Firma digital y certificado digital son dos conceptos íntimamente relacionados, a punto tal que los mencionados requisitos de validez, que diferencian a la firma digital de la firma electrónica, tienen todos que ver con los certificados digitales.

Como mencionamos anteriormente, desde el punto de vista técnico, en la firma digital intervienen dos elementos llamados "clave": clave privada empleada para firmar digitalmente y clave pública utilizada para verificar dicha firma digital. Las técnicas indicadas en el capítulo anterior sobre criptografía asimétrica utilizadas para firmar digitalmente un documento electrónico, si bien son técnicamente correctas, implican un grave problema a nivel de seguridad: ¿Cómo se puede asegurar que una clave pública pertenece a un usuario dado? Es necesario poder vincular la clave pública de un usuario con su identidad y para esto surge el concepto de "Certificado Digital o Certificado de Clave Pública".

El **certificado de clave pública** es una especie de "pasaporte", documento electrónico o identificador digital, cuya función es dar fe de la vinculación entre una clave pública determinada y una persona, titular de la clave. Es decir, garantiza la autenticidad de la clave pública del firmante y, como consecuencia de ello, la identidad del firmante (autenticación), que el mensaje no ha sido alterado en el camino (integridad) y que una vez recibido el documento el firmante no pueda negar su emisión (no repudio).

La LDF, en su art. 13º define: "Certificado digital. Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular." Por lo tanto, si una persona requiere verificar la firma digital del firmante de un documento digital, con la clave pública que obtiene de un certificado, puede confiar en que el firmante dispone de su correspondiente clave privada.

Dicho certificado deberá ser extendido por un sistema confiable: una Autoridad Certificante o también denominado Certificador Licenciado.

i. ¿Qué contiene un certificado?

En su forma más simple, los certificados contienen una clave pública y un nombre. Habitualmente, un certificado también contiene una fecha de expiración, el nombre de la Autoridad Certificante que emitió ese certificado, un número de serie, versión, identificador del algoritmo, firma, la dirección de Internet de las condiciones de emisión y utilización del certificado, dirección de Internet del manual de procedimientos y de los informes de auditoria de la autoridad certificante que lo emitió, dirección de Internet de la lista de certificados revocados y alguna otra información. Pero lo más importante es que el certificado propiamente dicho está firmado digitalmente por el emisor del certificado.

El art. 14º LDF establece los requisitos que deben cumplir los certificados digitales para ser válidos:

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.

Esta información se encapsula en un formato estándar, definido por la norma ISO X.509 versión 3. Generalmente existirá una Autoridad de Registro que se encargará de publicar todos los certificados gestionados y podrá ser consultada por otros usuarios que quieran enviar información cifrada o verificar firmas digitales.

Los certificados digitales sólo son válidos durante su período de vigencia (debiendo la fecha de inicio y de vencimiento ser indicadas en el mismo), o con su revocación si fuere revocado. Por su parte, la fecha de vencimiento del certificado digital en ningún caso puede ser posterior a la del vencimiento del certificado digital del certificador licenciado que lo emitió.

La LDF establece los casos en que un certificado digital no es válido: si es utilizado para alguna finalidad diferente a los fines para los cuales fue extendido, para operaciones que superen el valor máximo autorizado cuando corresponda, o una vez revocado.

Respecto de operaciones que se realizan a través de documentos digitales emitidos por personas físicas o jurídicas radicadas en el exterior, el procedimiento de verificación de firma digital es el mismo. La ley contempla esta situación al referirse en su art.16º sobre el reconocimiento de certificados extranjeros:”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: 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 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.”

ii. Cómo se obtiene un certificado digital

Existen dos procesos de registro y se realiza a través de la denominada Autoridad de Certificación o Certificador Licenciado.

• *Registro Clásico*. El solicitante acude en persona a una "Oficina de Registro", donde, tras acreditar su identidad, se le proporciona de forma segura su clave privada y su certificado.

• *Registro Remoto*. El usuario, a través de Internet, realiza una solicitud de certificado. Para esto empleará un software que generará el par de claves y enviará su clave pública a la Autoridad de Registro para que sea firmada por la Autoridad Certificadora y le sea emitido su certificado.

De acuerdo a esta forma de registro, en primer lugar se debe generar el par de claves. Este par de claves es propio, personal, y no se puede repetir para ninguna otra persona. Para ello la persona utiliza un programa especial en su computadora. Las dos claves consistirán en números muy grandes, relacionados matemáticamente entre sí, que se generan simultáneamente. Como aclaramos en el capítulo anterior, el hecho de que ambas claves estén relacionadas no implica que una pueda descifrarse a partir de la otra.

La clave privada que se empleará para firmar los mensajes, debe ser almacenada con la máxima seguridad debido a que no debe ser conocida ni utilizada por nadie, excepto por su titular (quien la generó). En consecuencia, ésta se encripta y protege mediante una contraseña y se la guarda en un disco, diskette o, idealmente, en una tarjeta inteligente.

Los medios de resguardo más comunes de la clave privada son:

- Llaves por puerto USB – Existen dos tipos :
  - Almacenan clave Privada generada en PC.

- Generan la Clave Privada directamente y la almacenan.

➢ Lectores de Tarjetas

- Almacenan clave Privada generada en PC.
- Generan la Clave Privada directamente y la almacenan.

➢ Grabación en Mini CD

La clave pública, en cambio, debe ser conocida por todos por tal motivo es enviada a una Autoridad Certificante o también llamado Certificador Licenciado (que actúa como tercera parte confiable), para que la incluya en un certificado digital: se envía a dicha entidad el archivo binario que contiene la clave pública a certificar, incluyendo cierta información tal como nombre, apellido, domicilio, etc. Una vez que la autoridad certificante verificó la identidad le aplica su propia clave pública, certificando la clave pública del solicitante como válida. Entonces, cualquiera que confíe en la autoridad certificante tendrá como confiable la clave pública firmada.

La validez de la Firma Digital estará condicionada por la calidad del proceso de registro, siendo obligatorio para asegurar la validez legal de la firma, algún tipo de registro "Cara a Cara", ya que es el único que asegura la identidad del solicitante. Por otra parte, la validez de la firma digital también estará condicionada a la firma manuscrita de un "contrato" por el que el solicitante acepta su certificado y las condiciones de uso del mismo.

iii. Cuáles son los distintos fines del certificado, y cómo usarlos con el objeto de verificar una firma

Un certificado puede utilizarse para identificarse en cualquier tipo de transacción o comunicación electrónica, garantizar que un mensaje emitido ha sido enviado por el titular del certificado y que no ha sufrido

ninguna alteración; generan confianza en la legitimidad de una clave pública.

También se puede utilizar un certificado ajeno para extraer la clave pública de alguien y así poder utilizarla para enviarle un mensaje encriptado a esa persona.

Esencialmente protegen a las claves públicas del fraude, de la falsa representación o de la alteración. En consecuencia, la verificación de una firma incluye el chequeo de la validez del certificado de la clave pública en cuestión. El receptor del mensaje verificará el certificado usando la clave pública de la Autoridad Certificante, y a continuación, teniendo confianza en la clave pública del remitente, verificará la firma del mensaje.

Puede haber más de un certificado con el mensaje, formando una cadena jerárquica de certificados, donde cada uno da fe de la autenticidad del certificado previo. Al final de una jerarquía de certificados, se tiene a una Autoridad Certificante de más alto nivel, en la que se confía sin un certificado de ninguna otra Autoridad Certificante. La clave pública de una Autoridad Certificante raíz debe ser conocida independientemente, por ejemplo, publicándola ampliamente.

iv. ¿Qué hacer si se desea que el certificado no siga vigente?

Se debe revocar el certificado, esto es anular su validez antes de la fecha de caducidad que consta en el mismo. La revocación puede ser solicitada a la Autoridad Certificante que emitió el certificado en cualquier momento, y en especial, cuando el titular crea que su clave privada es conocida por otro.

La revocación tiene efectos a partir de la fecha efectiva de revocación que consta junto al número de serie del certificado revocado, en un documento firmado y publicado por la Autoridad Certificante que se denomina Lista de Certificados Revocados. Cualquier firma digital realizada

con la clave privada asociada a ese certificado con posterioridad a la fecha efectiva de revocación no tendrá validez.

Tipos de certificados

Existen diferentes tipos de certificado digital, en función de la información que contiene cada uno y a nombre de quién se emite el certificado:

- **Certificado personal**, que acredita la identidad del titular.
- **Certificado de pertenencia a empresa**, que además de la identidad del titular acredita su vinculación con la entidad para la que trabaja.
- **Certificado de representante**, que además de la pertenencia a la empresa acredita también los poderes de representación que el titular tiene sobre la misma.
- **Certificado de persona jurídica**, que identifica una empresa o sociedad como tal a la hora de realizar trámites ante las administraciones o instituciones.
- **Certificado de atributo**, el cual permite identificar una cualidad, estado o situación. Este tipo de certificado va asociado al certificado personal. (p.ej. Médico, Director, Casado, Apoderado de..., etc.).

Además, existen otros tipos de certificado digital utilizados en entornos más técnicos:

- **Certificado de servidor seguro**, utilizado en los servidores web que quieren proteger ante terceros el intercambio de información con los usuarios.
- **Certificado de firma de código**, para garantizar la autoría y la no modificación del código de aplicaciones informáticas.

B.- *Certificador Licenciado*

La Autoridad Certificadora (CA) o también denominada Certificador Licenciado, es la entidad que emite certificados digitales para su uso por terceros y que, por sí misma o mediante la intervención de una Autoridad de Registro, verifica la identidad del solicitante de un certificado antes de su expedición.

Estas entidades disponen de sus propios certificados públicos, cuyas claves privadas asociadas son empleadas para firmar los certificados que emiten.

La LDF define: “Certificador Licenciado: 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 art. 18 indica que las entidades que controlan la matrícula, en relación a la prestación de servicios profesionales, podrán emitir certificados digitales en lo referido a esta función, con igual validez y alcance jurídico que las efectuadas en forma manuscrita.

Entre las tareas que un Certificador Licenciado tiene encontramos:

- Recibir las solicitudes de emisión de certificado digital, firmadas digitalmente con los correspondientes datos de verificación de firma digital del solicitante;
- Emitir certificados digitales; identificar inequívocamente los certificados digitales emitidos;
- Revocar los certificados digitales por él emitidos en los siguientes casos: a solicitud del titular del certificado digital si determinara que un certificado digital fue emitido en base a una información falsa; si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguro; por pérdida de la clave privada que posibilita la firma; cuando

el usuario ya no desee utilizar ese certificado; por resolución judicial o de la Autoridad de Aplicación. Los certificados digitales revocados deben ser incluidos en una lista de certificados revocados (CRL) indicando fecha y hora de la revocación.

- Gestionar la caducidad y renovación de certificados.

Para obtener una licencia el certificador debe tramitar la solicitud respectiva ante un 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.

De acuerdo a la estructura establecida en la LDF, los Certificadores Licenciados deben cumplir ciertas obligaciones para garantizar el correcto funcionamiento del sistema. En el art. 21º, encontramos:

- Informar a quien solicita un certificado las condiciones precisas de utilización del certificado digital;
- Abstenerse de tomar conocimiento o acceder a los datos de creación de firma digital de los titulares de certificados; mantener la documentación respaldatoria de los certificados digitales emitidos, por DIEZ (10) años a partir de su fecha de vencimiento o revocación;
- Operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la Autoridad de Aplicación;
- Publicar en Internet la lista de certificados digitales revocados, las políticas de certificación, la información relevante de los informes de la última auditoria de que hubiera sido objeto, su manual de procedimientos y toda información que determine la Autoridad de Aplicación;
- Solicitar inmediatamente al Ente Licenciante la revocación de su certificado, cuando los datos de creación de firma digital que utiliza hubiesen sido comprometidos o cuando los

procedimientos de verificación de firma digital hayan dejado de ser seguros;

- Permitir el ingreso de los funcionarios autorizados de la Autoridad de Aplicación, del Ente Licenciante o de los auditores, a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso; emplear personal idóneo.

Vemos que la Autoridad Certificante es un elemento importante en el proceso de firma digital, cuya labor es establecer la liga entre el firmante y las claves utilizadas para crear la firma digital. 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.

Certificadores Licenciados públicos y privados

"Respecto del termino "Autoridad Certificante" es necesario aclarar que no necesariamente se trata de la habilitación de una repartición publica, o de conceder por licencia el carácter de autoridad publica a una persona, ya que en esencia se trata de la denominación técnica que utiliza el sistema para validar y autenticar la integridad del contenido y la autoría del mensaje, y puede estar incluido en el mismo software, por lo que no debe tomarse en su significado etimológico excluyente." (19)

Una CA puede ser o bien publica o bien privada. Las CAs públicas emiten los certificados para la población en general (aunque a veces están focalizadas hacia algún colectivo en concreto) y además firman CAs de otras organizaciones.

Pueden constituirse en autoridades competentes tanto las empresas que certifican las claves públicas de sus empleados, los bancos que certifican la de sus clientes, los escribanos o los nuevos organismos creados con tal fin. Lo ideal es que toda entidad certificante se organice

(19) CARLINO, Bernardo P., Op. Cit., Pág. 51.

dentro de una estructura de certificación mutua para que su propia clave pública esté avalada por una autoridad diferente. Por ejemplo la clave pública de una sociedad podría ser avalada por la Inspección General de Justicia, la Comisión Nacional de Valores, etc.

II. Organización Institucional del Sector Público Nacional

La LDF y un conjunto de normas complementarias(capítulo 5) representan el marco regulatorio para el empleo de la Firma Digital en la instrumentación de los actos internos del Sector Público Nacional, que no produzcan efectos jurídicos individuales en forma directa, otorgándole a esta nueva tecnología similares efectos que a la firma ológrafa.

La Infraestructura de Firma Digital de la República Argentina, esta integrada por las siguientes entidades:

a. Ente Licenciante: Es la Autoridad Certificante Raíz de la Infraestructura de Firma Digital del Sector Público 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.

"El organismo que actúa como Ente Licenciante es la Oficina Nacional de Tecnologías de Información (ONTI), dependiente de la Secretaría de la Gestión Pública en la Jefatura de Gabinete de Ministros del Gobierno Nacional. La ONTI es el órgano rector en materia de empleo de tecnologías informáticas de la Administración Pública Nacional, participa activamente en la implementación de la Infraestructura Nacional de Firma Digital,

impulsando el uso de la certificación digital en el Estado y actuando como Autoridad de Certificación Raíz.” [20]

Funciones de la ONTI

Dentro de las numerosas funciones asignadas a la Oficina Nacional de Tecnologías de Información, se destacan las siguientes en el campo de la firma digital:

- ✓ Asistir en el proceso de licenciamiento de certificadores, en el marco de la Ley 25.506. Otorgar licencias habilitantes a las autoridades o entes certificadores, emitir los certificados de clave pública, revocar las licencias otorgadas.
- ✓ Actuar como Autoridad Certificante para el Sector Público.
- ✓ Impulsar el desarrollo de aplicaciones en el Estado.
- ✓ Difundir y capacitar sobre aspectos técnicos y legales de esta herramienta y su utilización en nuestro país.
- ✓ Controlar la aplicación de sistemas técnicamente confiables.
- ✓ Analizar y aprobar el manual de procedimientos y el plan de seguridad formulados por las autoridades certificantes.

En cuanto su participación en el proceso de licenciamiento, la ONTI lleva adelante el mantenimiento de la

[20] Consultas a bases de información, en Internet: www.pki.gov.ar, (Abril de 2010).

instalación de la Autoridad Certificante Raíz de la República Argentina, siendo además responsable de la organización de las ceremonias de emisión o revocación de los certificados digitales emitidos a favor de los certificadores licenciados y de las listas de certificados revocados.

Brinda además, asistencia en el análisis de las solicitudes de licenciamiento, atiende consultas de otras entidades interesadas en conocer los pasos a seguir para ser certificadores licenciados y lleva adelante tareas de difusión, participando en congresos y eventos.

Con relación a su actuación como Autoridad Certificante, viene cumpliendo esta función desde al año 2001. A la fecha, lleva emitidos más de diez mil certificados digitales para agentes y funcionarios públicos y para magistrados y empleados de la Justicia.

Esta última función se lleva delante de acuerdo a lo establecido en el Convenio de Comunicación Electrónica Interjurisdiccional, firmado por los Superiores Tribunales Provinciales y otros organismos del ámbito judicial en el año 2001.

En este marco, cuenta sesenta Autoridades de Registro, de las cuales treinta y tres se encuentran en Organismos públicos nacionales, nueve en Gobiernos provinciales y dieciocho en Superiores Tribunales de Justicia.

La ONTI también lleva adelante una importante tarea de asistencia para la incorporación de la tecnología de firma digital en los sistemas de organismos públicos, sean estos desarrollos nuevos o ya existentes.

b. Autoridad de Aplicación: “su función está a cargo de la Subsecretaría de la Gestión Pública, actuará como autoridad de

aplicación del régimen normativo que establece la infraestructura de firma digital establecida en la Ley N° 25.506 y en las funciones de entidad licenciante de certificadores, supervisando su accionar. Cuenta con una Comisión Asesora para la Infraestructura de Firma Digital". (21)

Algunas de sus funciones son: dictar las normas reglamentarias y de aplicación de la presente; establecer los estándares tecnológicos y operativos de la Infraestructura de Firma Digital; 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; determinar las pautas de auditoria, incluyendo los dictámenes tipo que deba emitirse como conclusión de las revisiones; aplicar las sanciones previstas en la presente ley.

La Decisión Administrativa N° 06/2007 define los mecanismos que la Subsecretaría de la Gestión Pública utilizará para otorgar y revocar las licencias. Dicha entidad, además de Entidad Licenciante, actúa como Autoridad Certificante Raíz, otorgando y revocando licencias a las entidades públicas y privadas que deseen operar como Certificadores Licenciados.

c. Comisión Asesora para la Infraestructura de Firma Digital: integrada por un máximo de siete profesionales, de reconocida trayectoria en la materia, de carreras afines a la actividad (8provenientes de Organismos del Estado Nacional, Universidades Nacionales y Provinciales, Cámaras, Colegios u otros entes representativos de Profesionales) que emite recomendaciones sobre los aspectos técnicos referidos al funcionamiento de la Infraestructura de Firma Digital.

---

(21) Consultas a bases de información, en Internet: www.sgp.gov.ar, (Abril de 2010).

Se reunirá como mínimo trimestralmente. Deberá expedirse prontamente a solicitud de la Autoridad de Aplicación

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

Este control lo realiza mediante la auditoria periódica de estos, evaluando su actuación de acuerdo con los estándares que a tal efecto establezca la Autoridad de Aplicación, como así también la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos.

La LDF indica que la Autoridad de Aplicación, con el concurso de la Comisión Asesora para la Infraestructura de Firma Digital, es quien debe diseñar un sistema de auditoria, un manual de procedimientos y los planes de seguridad y de contingencia aprobados por el Ente Licenciante.

La Autoridad de Aplicación puede implementar el sistema de auditoria por sí o por terceros habilitados a tal efecto. Por lo tanto es la Autoridad de Aplicación quien establece la entidad que ejercerá la función de auditoria.

El Decreto2628/02 establece que el Jefe de Gabinete de Ministros debe convocar a concurso público para la precalificación de entidades de auditoria entre las universidades y organismos científicos y tecnológicos nacionales y provinciales, los colegios y consejos de profesionales, que acrediten experiencia profesional en la materia.

e. Autoridades de Registro: Son entidades que tienen a su cargo las funciones de validación de la identidad y otros datos de los suscriptores de certificados. Dichas funciones son delegadas por el certificador licenciado.

Es una parte de la Autoridad Certificante que realiza la autenticación de la identidad y de la condición del solicitante de un certificado digital. La condición se refiere a requisitos que establece la Política de Certificación para la emisión de certificados, como por ejemplo, ser empleado público, pertenecer a un determinado colegio profesional que acredite la matrícula, etc.

f. Autoridad Certificante licenciada o Entidades Certificantes:

Son aquellos organismos o dependencias del Sector Público Nacional que soliciten y obtengan la autorización, por parte del Ente Licenciante, para actuar como Autoridades Certificantes de sus propios agentes. Deben cumplir ciertos recaudos para poder emitir certificados de clave pública a favor de sus dependientes, entre los cuales encontramos que, debe abstenerse de acceder a las claves privadas de los suscriptores y además debe utilizar sistemas generadores de claves técnicamente confiables.

Entre ellas encontramos entes como la Bolsa de Valores, Comisión de Energía Atómica, Ministerio de Justicia, etc. Sus funciones son:

- ✓ Emitir los certificados de clave pública (los cuales se consideran válidos mientras no expire su plazo ni sean revocados).
- ✓ Firmar digitalmente los certificados, con identificación del algoritmo utilizado para ello.

Los Certificadores Licenciados vigentes en Argentina son AFIP - Administración Federal de Ingresos Públicos y ANSES - Administración Nacional de la Seguridad Social, que en diciembre de 2008 fueron los dos primeros organismos en obtener su licencia como Certificadores Licenciados de Firma Digital

La Política de Certificación de la primera institución, aprobada por Resolución SGGP Nº 88/2008, tiene el siguiente alcance:

a. Los documentos electrónicos de carácter tributario, aduanero, fiscal y administrativo, firmados digitalmente que se intercambien entre los contribuyentes y la AFIP. Por ejemplo Formulario F780- para fines fiscales- Presentación electrónica.

b. Los documentos electrónicos de carácter tributario, aduanero, fiscal y administrativo, firmados digitalmente que se intercambien entre los contribuyentes y los organismos recaudadores provinciales y municipales, que adopten la utilización de certificados digitales emitidos por la AFIP para sus sistemas de información.

c. Los documentos electrónicos firmados digitalmente presentados por personas físicas ante organismos de la Administración Pública Nacional, que adopten la utilización de certificados digitales emitidos por la Autoridad Certificante de la AFIP para sus sistemas de información.

La Política de Certificación de la ANSES, por su parte, fue aprobada por Resolución SGGP Nº 87/2008, tiene la siguiente aplicabilidad:

a. Las comunicaciones internas de ANSES, realizadas a través del correo electrónico institucional.

b. Las comunicaciones de la ANSES con otros organismos nacionales o internacionales, tanto privados como públicos, a través de correo electrónico institucional.

c. La firma de actos administrativos y documentación de incumbencia de la ANSES, tales como Resoluciones, Disposiciones, Notas, Circulares, etc.

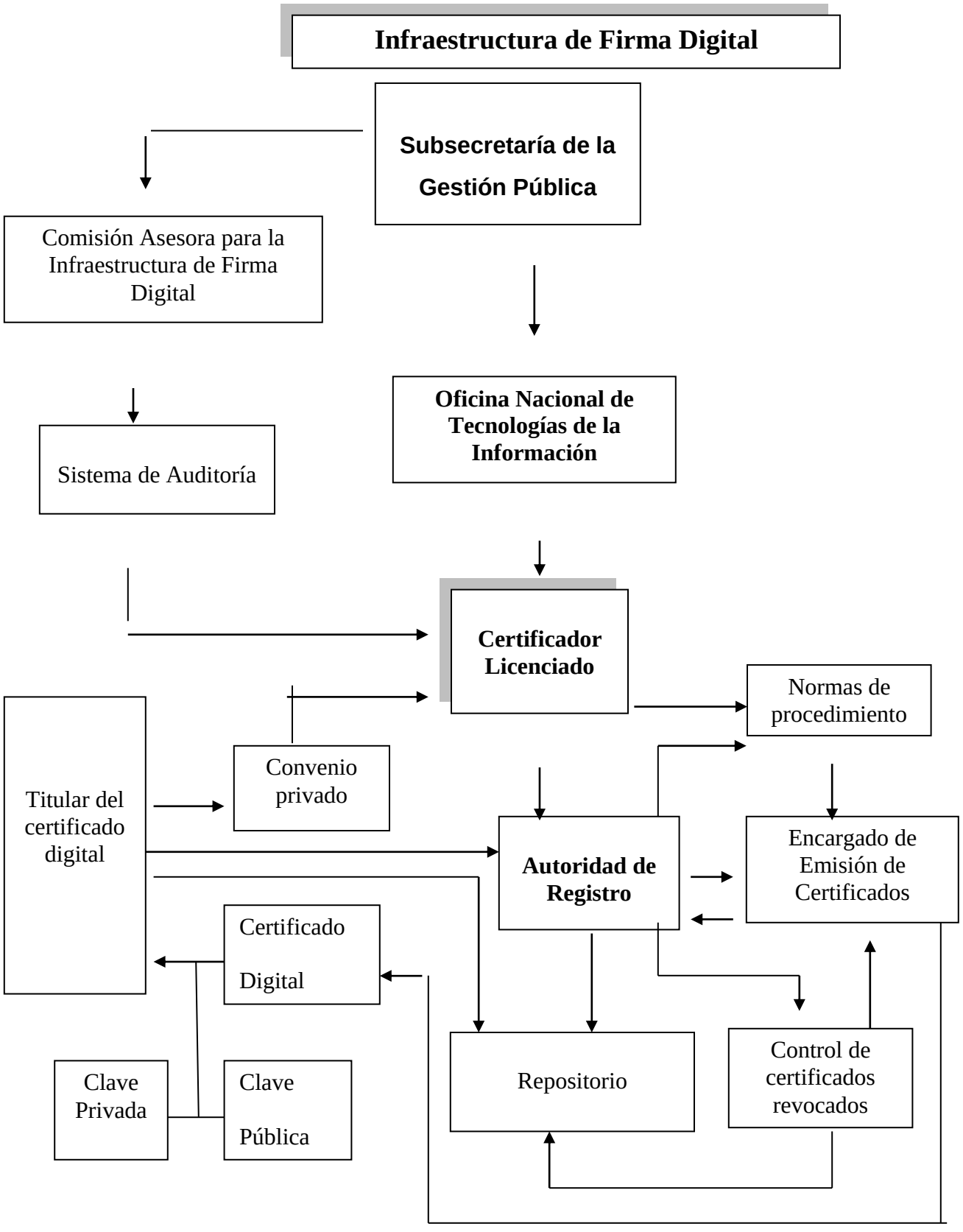
d. La Firma de convenios y Acuerdos con otras instituciones.

"Según una entrevista realizada en el acto de otorgamiento de las licencias efectuado el 09/03/2009, el Director Ejecutivo de ANSES, especificó la importancia que la Firma Digital tiene para el organismo a su cargo y, en ese sentido, señaló que "la firma digital es muy importante para que el Estado y los contribuyentes tengan que hacer menos trámites, por ejemplo, cualquier ciudadano del MERCOSUR que haya trabajado en diferentes países de la región y quien antes tardaba mucho tiempo en juntar los antecedentes para su jubilación, ahora podrá realizar los trámites en apenas tres días. También se agilizarán los trámites judiciales que los jubilados tengan con el Estado. El licenciamiento de AFIP y ANSES habilita la efectiva utilización de la Firma Digital en nuestro país ya que estos organismos podrán emitir Certificados Digitales en sus respectivos ámbitos de aplicación." (22)

g. 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.

(22) Consultas a bases de información, en Internet: www.clarín.com.ar, (Marzo de 2010).


Infraestructura de Firma Digital
Subsecretaría de la Gestión Pública
Comisión Asesora para la Infraestructura de Firma Digital
Oficina Nacional de Tecnologías de la Información
Sistema de Auditoría
Certificador Licenciado
Normas de procedimiento
Titular del certificado digital
Convenio privado
Autoridad de Registro
Encargado de Emisión de Certificados
Certificado Digital
Clave Privada
Clave Pública
Repositorio
Control de certificados revocados

CAPÍTULO V

MARCO NORMATIVO

Sumario: 1.- Introducción; 2.- Marco Normativo sobre Firma Digital: Alcance y Estructura; 3.- Objetivos de la Ley; 4.- El Decreto Reglamentario 2628/2002; 5.- Infraestructura de Firma Digital; 6.- Resumen de Legislación Vigente sobre Firma Digital; 7.- Otras normas específica sobre Firma Digital; 8.- Adhesión en las Provincias; 9.- Estado y Firma Digital: Normativa sobre Firma Digital específica para el Sector Público; 10.- Normativa sobre aplicaciones en el Sector Público; 11.- Antecedentes legales internacionales de la firma digital.

1.- Introducción

Dado que el comercio electrónico esta basado en el Electronic Data Interchange (Intercambio Electrónico de Datos) y que para que haya confianza jurídica es básico que los documentos digitales tengan los mismos atributos que los documentos de papel, desde hace algún tiempo los juristas se han abocado a este arduo problema.

Ello nos lleva a tratar la validez jurídica del documento almacenado mediante diversos medios tecnológicos y el empleo de técnicas de firma digital como medio de autenticación o identificación de esos documentos.

En este capitulo trataremos la recopilación de los antecedentes jurídicos y legales relativos a la firma digital en la República Argentina incluyendo también el estado de avance en este tema en otros países del mundo.

2.- Marco Normativo sobre Firma Digital

El marco normativo de la República Argentina en materia de Firma Digital está constituido por la Ley Nº 25.506 (B.O. 14/12/2001), el Decreto Nº 2628/02 (B.O. 20/12/2002), el Decreto N° 724/06 modificatorio del anterior (B.O. 13/06/06) y un conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos.

La legislación argentina emplea el término "Firma Digital" en equivalencia al término "Firma Electrónica Avanzada" o "Firma Electrónica Reconocida" utilizado por la Comunidad Europea o "Firma Electrónica" utilizado en otros países como Brasil o Chile.

Alcance y Estructura

La ley de firma digital se desarrolla sobre la base de once capítulos y un anexo que es el glosario de términos técnicos-jurídicos, con la finalidad de dar una explicación clara y abreviada a aquellos términos de difícil comprensión o que pueden resultar desconocidos para los lectores, dado lo innovador del impacto de las Nuevas Tecnologías en el ámbito del derecho.

3.- Objetivos de la Ley

La finalidad que la presente ley busca cumplir es crear el marco legal adecuado- que era inexistente hasta su sanción y posterior reglamentación- para el desarrollo del Comercio Electrónico, y las transacciones que se llevan a cabo en entornos de redes abiertas como Internet, tratando de brindar un ámbito seguro que facilite el avance del mismo y la confianza de los usuarios, poniéndonos a la altura de todos los países que hayan legislado sobre la materia.

El art.1 de la ley, expresa que se reconoce el empleo de firma digital y su eficacia jurídica en las condiciones que establece la normativa. Los artículos siguientes determinan cuales son los requisitos para que la firma digital tenga plena eficacia que la ley reconoce.

A pesar del ámbito de alcance que parecería derivar de este articulo introductorio, la ley avanza sobe algunas cuestiones no incluidas en este objetivo, tal como el reconocimiento de validez del documento digital no firmado (art 6 LDF).

El informe de las Comisiones de Comunicaciones e Informática y de Legislación General manifiesta que “las nuevas tecnologías exigen poder identificar en forma fehaciente a las personas de modo tal de permitirles realizar todo tipo de transacciones que van desde el comercio electrónico, efectuar gestiones ante distintos organismos del Estado, trabajar en forma remota y hasta ejercer el derecho democrático de votar.” (23)

El artículo y el informe se alinean en el objetivo reconocido a la firma digital de aventar los riesgos e inseguridades derivados de la utilización de mensajes digitales a través de redes abiertas. Las comunicaciones por redes abiertas están sujetas a ciertos riesgos: que el autor y fuente del mensaje haya sido suplantado; la alteración, provocada o accidental, del mensaje trasmitido; el repudio del mensaje, tanto por parte del emisor cuanto por parte del receptor; la intercepción del mensaje por persona no autorizada.

Es necesario, entonces, implementar métodos tecnológicos que permitan asegurar que el mensaje proviene de quien dice enviarlo, que no haya sido alterado desde su envío, el no repudio o rechazo respecto del envío y a la recepción del mensaje y la confidencialidad.

4.- El Decreto Reglamentario 2628/2002

El 19 de diciembre del año 2002, se sancionó el decreto reglamentario de la ley de Firma Digital, el cual, dentro de sus considerándos, 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

(23) Consultas a bases de información, en Internet: www.pki.gov.ar, Mayo 2010.

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.

Su estructura se basa en diez capítulos sobre distintos rubros y un glosario anexo de términos técnicos-jurídicos.

5.- Infraestructura de Firma Digital

Este conjunto normativo conforma una Infraestructura de Firma Digital de alcance federal. Si bien este tema fue desarrollado en el capítulo IV, creemos que es importante agregar la normativa bajo la cual funcionan las distintas entidades que conforman dicha infraestructura en el ámbito del Sector Público Nacional:

Autoridad de Aplicación: Según el Decreto N° 409/2005, la Subsecretaría de la Gestión Pública actuará como autoridad de aplicación del régimen normativo que establece la infraestructura de firma digital establecida en la Ley N° 25.506 y en las funciones de entidad licenciante de certificadores, supervisando su accionar.

Comisión Asesora para la Infraestructura de Firma Digital: Funciona en el ámbito de la Subsecretaría de la Gestión Pública, emitiendo recomendaciones sobre los aspectos técnicos referidos al funcionamiento de la Infraestructura de Firma Digital.

A través del Decreto N° 160/2004, el Poder Ejecutivo Nacional ha designado a los integrantes de la Comisión Asesora para la Infraestructura Nacional de Firma Digital, en cumplimiento de lo dispuesto en la Ley N° 25.506.

Ente Licenciante: Es el órgano técnico-administrativo encargado de otorgar las licencias a los certificadores y de supervisar su actividad.

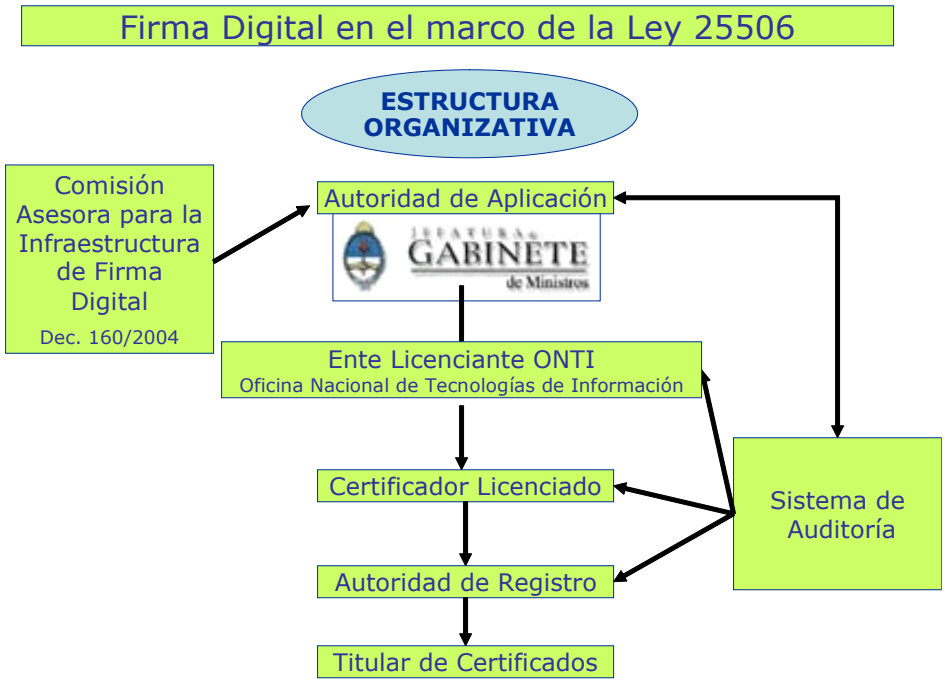
Esta función ha sido asignada a la Oficina Nacional de Tecnologías de Información (ONTI) por el Decreto Nº 1028/03, el cual establece como una de sus responsabilidades primarias "Asistir al Subsecretario de la Gestión Pública actuando como Autoridad Certificante en los organismos del Sector Público Nacional" y dentro de sus acciones "Entender, asistir y supervisar en los aspectos relativos a la seguridad y la privacidad de la información digitalizada y electrónica del Sector Público Nacional".

Certificadores licenciados: Son aquellas personas de existencia ideal, registro público de contratos u organismo público que obtengan una licencia emitida por el ente licenciante para actuar como proveedores de servicios de certificación en los términos de la Ley Nº 25.506 y su normativa complementaria.

Autoridades de Registro: Son entidades que tienen a su cargo las funciones de validación de la identidad y otros datos de los suscriptores de certificados. Dichas funciones son delegadas por el certificador licenciado.

Sistema de Auditoría: Será establecido por la autoridad de aplicación, a fin de evaluar la confiabilidad y calidad de los sistemas utilizados por los certificadores licenciados.

Este marco normativo deroga el Decreto Nº 427/98, cuya aplicación era específica para el Sector Público, por cuanto cubre sus objetivos y alcance.



6.- Resumen de Legislación Vigente sobre Firma Digital

A continuación se detallan las normas que constituyen el régimen normativo vigente en materia de Firma Digital en la República Argentina:

- Decisión Administrativa JGM Nº 6/2007

Establece el marco normativo de firma digital aplicable al otorgamiento y revocación de las licencias a las entidades públicas y privadas que quieran convertirse en certificadores licenciados

- Decreto N° 724/2006 Modifica el Decreto N° 2628/02 reglamentario de la Ley de Firma Digital.

- Decreto N° 409/2005

Establece que la Subsecretaría de la Gestión Pública actuará como autoridad de aplicación del régimen normativo que establece la infraestructura de firma digital establecida en la Ley N° 25.506 y en las funciones de entidad licenciante de certificadores, supervisando su accionar.

- Resolución JGM Nº 435/2004

Aprueba el Reglamento de funcionamiento de la Comisión Asesora para la Infraestructura de Firma Digital, que fuera creada por la Ley N° 25.506 y cuyos miembros fueran designados por Decreto N° 160/04 del Poder Ejecutivo Nacional.

- Decreto Nº 160/2004

Designa a los integrantes de la Comisión Asesora para la Infraestructura Nacional de Firma Digital, en cumplimiento de lo dispuesto en la Ley N° 25.506.

- Decreto Nº 1028/2003

Disuelve el Ente Administrador de Firma Digital, creado por el artículo 11 del Decreto N° 2628/02, cuyo accionar será llevado a cabo por la Oficina Nacional de Tecnologías de Información de la Subsecretaría de la Gestión Pública.

- Decreto Nº 152/2003

Otorga competencia a la Subsecretaría de la Gestión Pública para licenciar a los certificadores, supervisar su actividad y dictar normas tendientes a asegurar el régimen de libre competencia en el mercado de los prestadores y protección de los usuarios de firma digital.

- Decreto Nº 283/2003

Autoriza con carácter transitorio a la Oficina Nacional de Tecnologías de Información a proveer certificados digitales para su utilización en aquellos circuitos de la Administración Pública Nacional que requieran firma digital, de acuerdo a la Política de Certificación vigente.

- Decreto Nº 2628/2002

Reglamenta la Ley N° 25.506 de firma digital. Crea el Ente Administrador de Firmas Digitales.

- Ley Nº 25.506

Ley de de Firma Digital - Boletín Oficial del 14/12/2001

- Decreto Nº 1023/2001

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

- Resolución SFPNº 194/98

Establece los estándares sobre tecnología de firma digital para la Administración Pública Nacional.

7.- Otras normas específica sobre Firma Digital

- Disposición Nº 5 AC-ONTI

Documentación técnica de la Autoridad Certificante de la ONTI (Oficina Nacional de Tecnología Informática).

- 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 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.

- Decisión JGM Nº 43/96

Reglamenta los archivos digitales. Establece como órgano rector a la Contaduría Gral. de la Nación.

- Ley Nº 24.624 Artículo 30

Autoriza el archivo y conservación en soporte electrónico u óptico indeleble de la documentación financiera, de persona y de control de la Administración Pública Nacional.

8.- Adhesión en las Provincias

Las siguientes provincias poseen iniciativas de adhesión y puesta en operatividad del régimen establecido por la Ley N° 25.506 de firma digital.

- La Pampa (Ley N° 2073 – B.O. 31/10/2003)
- Tucumán (Ley N° 7291 – B.O. 07/11/2003)
- Mendoza (Ley N° 7234 - B.O. 04/08/2004)
- Tierra del Fuego (Ley N° 633 - B.O. 04/08/2004)
- San Luis (Ley N° 5540 de Procedimientos Administrativos Art. 59 - B.O. 19/05/2004)
- Formosa (Ley N° 1454 - sancionada 26/08/2004)
- Jujuy (Ley N° 5425 - B.O. 22/09/2004)
- Río Negro (Ley N° 3997 - B.O. 20/10/2005)
- Santa Fé (Ley N° 12.491 - BO 21/12/2005)
- Buenos Aires (Ley N° 13.366 – B.O. 15/05/2007)
- Neuquén (Ley N° 2578 - sancionada 24/04/2008)

Municipios:

- Municipalidad de Allen - Provincia de Rio Negro (Ordenanza Municipal N° 019/07)

9.- Estado y Firma Digital

Hace ya varios años aun antes de la sanción de la ley de firma digital (2001), se ha venido trabajando en la implementación de iniciativas relativas a la digitalización en el Sector Público Argentino, iniciativas relativas a la digitalización de sus circuitos administrativos y a la utilización de la firma digital para dotar de seguridad a las comunicaciones internas.

A partir de la promulgación, en diciembre de 2001, de la Ley N° 25.506 de Firma Digital, este proceso se ha consolidado. La legislación mencionada establece como obligación del Estado Nacional la utilización de esta tecnología en su ámbito interno y en sus relaciones con los administrados, estableciendo un plazo máximo de cinco años para que la misma sea aplicada a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanadas del Sector Público Nacional (Ley N° 25.506, arts. 47 y 48).

A fin de fortalecer y apoyar a los organismos del Sector Público Nacional, la Oficina Nacional de Tecnologías de Información participa activamente en las iniciativas de despapelización, proveyendo certificados digitales a agentes y funcionarios públicos actuando como Autoridad Certificante.

Estos certificados digitales son administrados de manera centralizada por la ONTI, la cual delega en las jurisdicciones respectivas las funciones de Autoridad de Registro.

De este modo se logra mayor eficiencia en el proceso de emisión y administración de los certificados ya que el procedimiento de validación de identidad de los suscriptores se realiza directamente en cada organismo, evitando desplazamientos y demoras.

Sector público provincial: muchas provincias argentinas han adherido a la ley nacional y, bajo la supervisión de la ONTI, están llevando a cabo el proceso de implementación de la firma digital.

Puede consultarse el grado de avance de la implementación del sistema de firma digital en el sitio de la ONTI. (http://www.sgp.gov.ar/sitio/firma_digital.htm o http://www.pki.gov.ar/).

Normativa sobre Firma Digital específica para el Sector Público

En el caso particular de la Administración Pública Nacional, se encuentra vigente el Decreto N° 283/03, que autoriza con carácter transitorio

a la Oficina Nacional de Tecnologías de Información a proveer certificados digitales para su utilización en aquellos circuitos de la Administración Pública Nacional que requieran firma digital, de acuerdo a la política de certificación vigente.

Este decreto es de aplicación transitoria hasta tanto se encuentre la Administración Pública Nacional en condiciones de emitir certificados digitales en los términos previstos en la Ley N° 25.506 y establece además un puente entre el marco normativo creado por el Decreto Nº 427/98 (derogado por el Decreto Nº 2628/02) y el marco normativo establecido por la citada Ley.

A continuación se detallan las normas que constituyeron el régimen normativo vigente para el Sector Público:

- Decisión Administrativa JGM Nº 6/2007

Establece el marco normativo de firma digital aplicable al otorgamiento y revocación de las licencias a los certificadores que así lo soliciten.

- Decreto N° 724/2006

Modifica el Decreto N° 2628/02 reglamentario de la Ley de Firma Digital.

- Decreto Nº 160/2004

Designa a los integrantes de la Comisión Asesora para la Infraestructura Nacional de Firma Digital, en cumplimiento de lo dispuesto en la Ley N° 25.506.

- Decreto Nº 1028/2003

Disuelve el Ente Administrador de Firma Digital, creado por el artículo 11 del Decreto N° 2628/02, cuyo accionar será llevado a cabo por la Oficina Nacional de Tecnologías de Información de la Subsecretaría de la Gestión Pública.

- Decreto Nº 624/2003

Aprueba la estructura organizativa de primer nivel operativo de la Jefatura de Gabinete de Ministros.

- Decreto Nº 152/2003

Otorga competencia a la Subsecretaría de la Gestión Pública para licenciar a los certificadores, supervisar su actividad y dictar normas tendientes a asegurar el régimen de libre competencia en el mercado de los prestadores y protección de los usuarios de firma digital.

- Decreto Nº 283/2003

Autoriza con carácter transitorio a la Oficina Nacional de Tecnologías de Información a proveer certificados digitales para su utilización en aquellos circuitos de la Administración Pública Nacional que requieran firma digital, de acuerdo a la Política de Certificación vigente.

- Decreto Nº 2628/2002

Reglamenta la Ley N° 25.506 de firma digital y crea el Ente Administrador de Firmas Digitales.

- Ley Nº 25.506

Ley de de Firma Digital - Boletín Oficial del 14/12/2001.

- Decreto Nº 1023/2001

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

- Resolución SFP Nº 194/98

Establece los estándares sobre tecnología de firma digital para la Administración Pública Nacional.

10.- Normativa sobre aplicaciones en el Sector Público

Independientemente del marco normativo general existente para el Sector Público, distintos organismos han establecido procedimientos o aplicaciones específicas para sus operaciones internas, o para las comunicaciones que establecen con sus administrados que habilitan el uso de documentos electrónicos y firmas digitales.

A continuación se detallan algunas normas relacionadas con la utilización de Documentos Electrónicos y Firma Digital en el Sector Público:

- Circular 48/2007 - STJ Santa Fe

Resuelve la utilización obligatoria de la firma digital y/o electrónica para diversas comunicaciones electrónicas internas

- Resolución N° 48/2008 Secretaria de Gabinete y Gestión Pública

Establece que las entidades detalladas en el Anexo I del Convenio Colectivo de Trabajo General para la Administración Pública Nacional deberán informar los datos de las personas contratadas a plazo fijo y eventual. La información requerida podrá ser remitida a través de correo electrónico utilizando firma digital.

- Resolución N° 1050/2005 ANSES

Dispone a partir del 1° de noviembre de 2005 el empleo de la firma digital, según la Ley N° 25.506 y sus Decretos y Resoluciones reglamentarias, en el ámbito de la Administración Nacional de la Seguridad Social. Crea el Registro de Firma Digital de la Seguridad Social.

- Resolución N° 398/2005 STJ de Río Negro

Habilita en forma gradual, permanente y obligatoria el uso de la firma digital en el Poder Judicial de la Provincia, de acuerdo a los términos de la Ley N° 25.506.

- Acordada STJ Jujuy N° 70/2002

Autoriza el uso de la firma digital para comunicaciones que materialicen trámites judiciales entre organismos jurisdiccionales provinciales y trámites administrativos y judiciales entre organismos jurisdiccionales provinciales y los de otras provincias.

- Resolución Administrativa STJ Chubut N° 508/02

Autoriza la realización de una experiencia piloto de notificación por cédula en dirección de correo electrónico constituida al efecto, mediante cédula emitida a través de correo electrónico, y firmada digitalmente.

- Decreto Nº 1023/2001

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

- 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.

11.- Antecedentes legales internacionales de la firma digital

- Naciones Unidas - UNCITRAL - Ley Modelo de Firma Digital.
- Directiva de Firma Digital de la Comisión Europea del 13 de diciembre de 1999.
- Ley de Firma Digital de la República Federal Alemana.
- Ley Reglamentaria de Firma Digital de la República Federal Alemana.
- Ley de Firma Digital de la República Francesa.
- Ley de Firma Digital de Hong Kong.
- Ley de Firma Digital del Perú.
- Ley de Firma Digital del Estado de Utah, EE.UU.
- Ley de Firma Digital de los EE.UU.
- Normativa de Firma Digital de la ABA, American Bar Association (Asociación Americana de Abogados) -

Sección de Ciencia y Tecnología, Comité de Seguridad en la Información.

CAPITULO VI

DESPAPELIZACION DEL SECTOR PÚBLICO

Sumario: 1.- Introducción; 2.- Deficiencias en el uso del papel como soporte de información; 3.- Despapelización de la administración pública: Implicancias del proceso; 4.- Herramientas tecnológicas necesarias; 5.- Cambio de paradigmas; 6.- Posibilidades a futuro que ofrece la firma digital: Aplicaciones en el Sector Público, 7.- Situación en la Provincia de Tucumán.

1.- Introducción

En la actualidad, el papel se ha transformado en un elemento costoso no sólo para la registración, almacenamiento y transmisión de información, sino también en términos de preservación de medio ambiente. Por ello, se hace necesario evaluar nuevas alternativas que sustituyan al papel en esta tarea.

Con mayor o menor velocidad todas las sociedades se encuentran expuestas al cambio permanente y está en la habilidad de sus gobiernos y en la voluntad de su gente tomar las medidas necesarias para que esos cambios los afecten de la mejor manera posible o los daños que les causen sean los mínimos.

En la actualidad muchos países y regiones están dejando de lado el uso del papel como soporte para realizar sus tramitaciones tanto en el ámbito local como en el internacional. En su reemplazo comenzaron a utilizar

herramientas más sofisticadas que aseguran una mayor eficiencia en sus procesos y un menor tiempo de respuesta, lo que se traduce en intercambios de información mucho más dinámicos. Este pasaje de la “sociedad del papel” hacia la “sociedad digital” pone en escena a las tecnologías de la información y comunicación, con el documento electrónico y la firma digital a la cabeza.

Este capitulo tiene como objetivo analizar las implicancias que tendría la utilización de herramientas tecnológicas y, puntualmente la firma digital, en la gestión de la información dentro de la Administración Pública. Al mismo tiempo, se propone indagar sobre las implicancias que el proceso de despapelización tendría, cuales serían los recursos necesarios para su implementación y los beneficios que traería aparejados.

2.- Deficiencias en el uso del papel como soporte de información

Al utilizar el papel como medio de registro y transmisión de datos es factible que se presenten deficiencias en las siguientes áreas:

- **Almacenamiento:**
  - Necesidad de contar con espacio físico destinado a archivo de los documentos.
  - Gastos en administración y vigilancia del archivo.
  - Diseño de normas de seguridad alineadas con la legislación vigente.
- **Manipulación:**
  - Dificultades para su traslado o remisión.
  - Medio de soporte débil para proteger la integridad de los datos.
- **Accesibilidad:**
  - Dificultades de acceso para usuarios de la organización como para los externos.

- Lento acceso a la información requerida.
- Eventual necesidad de trasladarse para acceder a la información.

- **Procesamiento:**
  - Dificultades para procesar la información
  - Dificultades para actualizar la información
- **Toma de decisiones:**
  - Imposibilidad de aplicar software diseñado para la toma de decisiones.
- **Seguridad:**
  - Alta exposición al fraude.
  - Problemas para brindar confidencialidad.
  - Ineficiencias para crear backup de la información.

3.- Despapelización de la administración pública

Podemos definir la despapelización del Sector Público como la disminución del uso del papel en los trámites de la Administración Pública, procurando conseguir beneficios tales como la disminución del espacio ocupado para almacenar la documentación histórica generada y la disminución en los tiempos de búsqueda de ésta.

La despapelización en el Sector Público es uno de los principios básicos en los que se sustenta la idea de Gobierno Electrónico con el objetivo de alcanzar la simplificación de los trámites y reducción de costos de la gestión administrativa, la estandarización de los procesos y normativas de la Administración Pública y fomentar los procesos de transparencia.

"La idea de Gobierno Electrónico del Estado Nacional pretende delinear el marco adecuado para impulsar el uso intensivo de estas nuevas tecnologías, a fin de optimizar así la gestión pública de manera permanente, con el propósito de ofrecer mejores servicios al ciudadano, garantizar la transparencia de los actos de gobierno, generar nuevos espacios de

participación, digitalizar con validez legal la documentación pública y permitir el intercambio de información entre el Estado y los particulares mediante canales alternativos al papel, reducir la brecha digital incluyendo a personas, empresas y comunidades menos favorecidas y propiciar la integración de la producción nacional al mercado global.

El resultado de este propósito se vio reflejado en la aprobación del Decreto Nº 378/2005 el día 27/04/2005, en virtud del cual se aprobaron los lineamientos estratégicos que han de regir el Plan Nacional de Gobierno Electrónico y los Planes Sectoriales para el uso intensivo de las TICs (Tecnologías de la Información y las Comunicaciones) en los organismos de la Administración Pública Nacional (APN)." [(24)]

Según el Decreto Nº 21/07 se determinó que la Secretaria de la Gestión Pública, debe entender en la planificación e implementación del Plan Nacional de Gobierno Electrónico, que tiene como principal objetivo que las tecnologías de la información y la comunicación, y en especial Internet y el correo electrónico, faciliten la comunicación entre los agentes y funcionarios públicos y entre éstos y la población y las organizaciones no gubernamentales.

Lo cual se conseguiría, entre otras tareas, con la publicación de los números telefónicos y las direcciones de correo electrónico y postales de todos los organismos que componen la Administración Pública Nacional y de sus responsables, facilitando a los ciudadanos la comunicación con los mismos, fomentando la transparencia y accesibilidad con la gestión de gobierno.

Implicancias del proceso de despapelización

[(24)] Consultas a bases de información, en Internet: www.argentina.gov.ar, Mayo 2010.

El papel es costoso así como los procesos ligados a su utilización, transporte y conservación. Los documentos digitales, en comparación, son baratos, fáciles de utilizar, conservar, transportar y comunicar.

Existen pocos estudios respecto al ahorro que pueda resultar del reemplazo total de los documentos en papel por aplicaciones informáticas; pero donde se ha intentado calcularlo, los resultados fueron sorprendentes. Según una publicación reciente de la ANSeS, dicho organismo manifiesta tener un gasto anual en papel e insumos estimados en $23 millones, que equivalen a un total de 150 millones de hojas impresas.

Considerando las deficiencias descriptas que acarrea el uso del papel y el entorno digital en el que nos encontramos, continuar con su utilización, en procesos que puedan implementarse tecnológicamente deviene en una barrera para el desarrollo tecnológico. Por ello, contar con una administración sin papeles y orientada al uso de Tecnologías de la información se torna de vital importancia dado el rol que ocupan actualmente estas herramientas en la vida cotidiana, no solo del Sector Público sino también de empresas e individuos.

La misma tiende a favorecer la eficientización y transparencia en los trámites de la Administración Pública. Pero para que la despapelización del Sector Público pueda materializarse resulta imprescindible disponer de una serie de herramientas tecnológicas y promover un cambio de paradigmas en cuanto a “la forma de hacer las cosas” en el sector.

4.- Herramientas tecnológicas necesarias

El reemplazo del papel por el soporte digital para la gestión de trámites en la Administración Pública, requiere el uso de tecnologías de la información tales como el documento electrónico, la firma digital y otras herramientas en materia de seguridad informática pertinentes. A continuación detallaremos algunos de estas herramientas:

i. Documento Electrónico

A los efectos de su utilización en el Sector Público, se entiende por documento electrónico a toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogida en cualquier tipo de soporte material, incluso los soportes informáticos, con eficacia probatoria o cualquier otro tipo de relevancia jurídica.

Documento electrónico en el sector público

Como se explicó en el capítulo anterior, existe tanto a nivel nacional como provincial normativa referida al uso y condiciones que debe reunir un documento electrónico para su aplicación en el ámbito de la Administración Pública. Entre éstas reencuentran la Ley Nacional N° 25.506 “Ley de Firma digital” y la Resolución DGCC 175/06 de la Provincia de Misiones que establece, entre otras cuestiones, que el formato de codificación de los documentos electrónicos utilizados en la administración pública de la provincia deberá ser del tipo abierto “OpenDocument” en línea con las especificaciones establecidas en las normas ISO/IEC 26300. Esta estandarización de formato facilita la utilización de software para la decodificación de los documentos.

Beneficios en el uso del documento electrónico

La utilización del documento electrónico como soporte sustituto del papel supone beneficios múltiples tales como:

- Aumento de la eficiencia en el tratamiento de los procesos: Se reducen los tiempos en el ingreso a las bases de datos y en la autenticación y control de integridad de la información. Se facilita el seguimiento de las tramitaciones pudiéndose determinar su ubicación y estado fácilmente. Además, se minimiza la posibilidad de errores en la información suministrada dada la existencia de pruebas de validación y consistencia de la misma.

- Ahorro de recursos: el incremento en la eficiencia de los procesos genera reducción en los tiempos de tramitación y respuesta a las solicitudes. Adicionalmente, se producen ahorros de dinero derivados de un menor costo de captura y mantenimiento de la información.
- Mayor confidencialidad de la información contenida en los documentos: se ofrece mayor control en cuanto a los accesos permitidos a los datos.
- Mejora las condiciones de trabajo de los empleados: producto de procesos ágiles y facilitados.
- Perdurabilidad de los documentos: por su naturaleza digital y la seguridad que puede rodearlos, los documentos electrónicos se encuentran expuestos a una menor cantidad de factores que puedan dañarlos o destruirlos.
- Preservación del medio ambiente: el menor consumo de papel supone una menor demanda de recursos naturales para su elaboración y un menor consumo eléctrico producto del menor uso de fotocopiadoras e impresoras.

ii. Firma Digital

Remitimos al capítulo III de este trabajo en el cual se explicó los distintos aspectos de la firma digital según la LDF 25506:"…es el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante (clave privada), encontrándose ésta bajo su absoluto control…"

Con esta Ley se propuso rodear al documento digital de las mayores seguridades jurídicas, para constituirlo así en una herramienta útil y eficaz para la celebración de negocios jurídicos.

Se puede decir que el documento digital firmado digitalmente ofrece garantías adicionales, que no las brinda la firma ológrafa en un documento

en soporte papel, y que marcan una fuerte ventaja de la firma digital en orden a la seguridad de las relaciones jurídicas.

Firma Digital en la Administración Pública

La Ley de Firma Digital, que entró en vigencia a partir de diciembre del año 2001, asimiló, con escasas excepciones, la firma digital a la firma manuscrita, lo que abría la posibilidad de ser usada en los más diversos ámbitos. El art. 48 de esa ley establecía que en el plazo máximo de 5 años, a contar desde su entrada en vigencia, los organismos del Estado Nacional debían aplicar sistemas informáticos con firma digital a tal punto de hacer desaparecer el papel de casi todos los organismos públicos.

Hacia fines de 2008, la situación de esta herramienta resultaba un tanto diferente a la planeada al momento de sancionar la Ley. Prueba de ello era un informe realizado por la Auditoria General de la Nación (AGN), donde el organismo manifestaba que la firma digital sólo había logrado un avance inferior al 5%. Una de las principales causas de este retraso, según AGN, era la inexistencia de certificadores licenciados, lo que derivaba en el atraso de la infraestructura de clave pública.

Finalmente, la Subsecretaría de Gestión Pública dio el último paso para instrumentación de la firma digital, cuando firmó una resolución por la cual se autoriza a la AFIP y la ANSeS a operar como certificadores del sistema, un rol clave si se tiene en cuenta que esos organismos tendrán la responsabilidad de garantizar la identidad de los que "firmen" digitalmente los documentos.

De todos modos, al menos en un principio, la firma digital no estará disponible para todos sino sólo para algunos usuarios de los organismos certificadores, funcionarios, beneficiarios de la seguridad social, las entidades bancarias y las mutuales. La explicación por la cual la firma digital no estará disponible en forma masiva para individuos y empresas obedece, en principio, a que la emisión de los certificados digitales tiene un costo, lo

que se tornaría un impedimento para su mayor expansión. Los certificados digitales más baratos, para uso personal, cuestan $ 30 anuales, mientras que los más caros, alcanzan los US$ 2.000. La variación del precio de un certificado tiene que ver con el uso que se le dará.

En principio, sólo los documentos electrónicos certificados por la AFIP y la ANSeS tendrán el mismo valor legal que los de papel.

Beneficios brindados por el uso de la firma digital

Sumado a los beneficios brindados por el documento electrónico, la firma digital favorece significativamente el proceso de despapelización del sector público. Brinda garantía de autoría e integridad de los documentos electrónicos, bajando la tasa de repudio. Adicionalmente, otorga validez legal a la documentación electrónica y contribuye a la introducción de estándares de seguridad en las transacciones electrónicas.

iii. Otras herramientas de seguridad informática

Como mencionamos anteriormente el proceso de despapelización implica pasar de un esquema de trabajo apoyado en soporte papel a un esquema digital donde la tecnología utilizada ocupa un rol central. Sin embargo, no debe perderse de vista que la tecnología a utilizarse no sólo debe apuntar a la captura y transmisión del dato sino también a su conservación y protección. Es en estas últimas fases donde el diseño de la arquitectura de seguridad de la información es relevante.

La seguridad informática deberá asegurar que los recursos del sistema de información (material informático o programas) de la organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible para las personas que se encuentren acreditadas y dentro de los límites de su autorización.

La seguridad informática deberá centrarse en cuatro características:

- Integridad: La información sólo puede ser modificada por quien está autorizado y de manera controlada.
- Confidencialidad: La información sólo debe ser legible para los autorizados.
- Disponibilidad: Debe estar disponible cuando se necesita.
- Irrefutabilidad (No repudio): El uso o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

Dependiendo de las fuentes de amenaza, la seguridad podrá dividirse en seguridad física, seguridad ambiental y/o seguridad lógica.

5.- Cambio de paradigmas

La firma digital no es una herramienta informática más. Su aplicación constituye una transformación integral en el modo de trabajar en las organizaciones. Hasta hoy, los sistemas informáticos debían conservar la mayoría de los documentos en papel porque sólo de esta forma se aseguraba su efecto legal y probatorio, característica no dada aún por el documento digital. Esto no sólo provocó la duplicación de los sistemas sino que sus mismas configuraciones y características se vieron determinadas por la “organización del papel”.

La posibilidad de contar con un sistema informático verdaderamente autónomo, con plena validez legal, facilita el camino para un desarrollo creativo, más eficiente que el actual. No se trata de una nueva tecnología para hacer lo mismo sino para generar formas diferentes de organización en el ámbito de la gestión de instituciones. En otras palabras, la firma digital implica repensar el modo en el que se desarrollan las tareas enfocándose hacia procedimientos mucho más dinámicos y eficientes.

No obstante, la incorporación de la firma digital y otras tecnologías de la información y comunicación a los procesos de las organizaciones por sí mismas son insuficientes para el desarrollo de las organizaciones si su

implementación no está acompañada por un cambio de paradigmas en cuanto al desarrollo de procesos y procedimientos.

La puesta en marcha del proceso de despapelización en cualquier dependencia de la administración pública requiere del compromiso de todos los funcionarios que la conforman. Si bien al inicio es lógico pensar en una fuerte resistencia al cambio, sobre todo de parte de las áreas que gestionan las tramitaciones, es fundamental en esta etapa, el rol de las áreas encargadas de asistencia al personal y capacitación sobre el uso de la herramienta para aminorar esta resistencia y allanar el camino hacia su aceptación.

Por otra parte, aún cuando el cambio actitudinal en el personal de la Administración Pública es imprescindible, la necesidad de generar cambios no se agota allí. Por el contrario, ese es sólo el punto de partida hacia una nueva forma de gestión del Sector Público que necesitará de cambios en áreas tales como:

- Costos: luego de la inversión inicial requerida la digitalización de los procesos genera la reducción de costos en lo referido a captura, administración, mantenimiento y archivo de la información.
- Manejo de la información: Se hace más eficiente la administración de la información en cuantos a los tiempos que ella demanda, principalmente apoyado en el creciente uso de internet para la gestión de trámites.
- La digitalización de la información brinda ventajas en materia de acceso a los datos por lo que es importante desarrollar una cultura de compartir la información entre las distintas áreas del organismo.
- Resguardo de la información: Se debe tender a minimizar los riesgos de pérdida de información en un nuevo ámbito que ya no es físico sino tecnológico. Para ello, es necesario adoptar medidas en cuanto a la seguridad y confidencialidad que rodea a los datos, previniéndolos de

accesos de personas no autorizadas y factores que puedan afectar la integridad de los mismos. Asimismo, es imprescindible la adopción de prácticas como el back up de la información, en el caso que los sistemas de seguridad previstos fallen.

- Orientación al cliente/ usuario: Los trámites realizados en formato papel implican un contacto personal con las personas, lo que en ocasiones puede generar demoras en los tiempos que demanda la gestión. La despapelización conlleva, con frecuencia, un trato más de tipo virtual con las personas disminuyendo la burocracia generada por el papelerío, un mejor diseño de los formularios requeridos, un menor tiempo de respuesta en las actuaciones y la posibilidad de que el usuario pueda realizar el seguimiento de su tramitación en todo momento de forma online, lo que provoca la buena aceptación del usuario hacia este proceso.

6.- Posibilidades a futuro que ofrece la firma digital

La firma digital conjuntamente con otras tecnologías de la información y comunicación brindan infinitas prestaciones en materia comunicacional, las que, en no mucho tiempo, implicarán una verdadera revolución en la forma de celebrar los negocios jurídicos. Pero también están generando una modificación sustancial en los métodos de archivo y transmisión de la información, tanto en el ámbito privado como en el público.
Con respecto a las posibilidades de aplicación en forma uniforme a todas las dependencias de la Administración Pública, se cree que previamente es necesario realizar una evaluación de razonabilidad desde el punto de vista operativa. Las tecnologías de la información y comunicación, como el documento electrónico, la firma digital y la estructura de seguridad informática que se requiere son herramientas que demandan una inversión inicial considerable, por ello, es necesario realizar una evaluación de razonabilidad sobre las áreas o procedimientos en los que se va a aplicar. El objetivo de esta evaluación deberá tender a evitar la implementación del

proceso de despapelización cuando los beneficios que se deriven de ello fueran menores a sus costos.

Aplicaciones en el Sector Público

A continuación se listan algunas aplicaciones de la tecnología de certificación digital en el ámbito público. Si bien algunas de ellas no constituyen una firma digital propiamente dicha, en los términos dispuestos por la normativa vigente, representan el aprovechamiento de las ventajas de esta herramienta, con las mismas seguridades desde la perspectiva técnica.

A.- *Aplicación a la Central de Balances del Banco Central de la República Argentina.*

Entre las posibilidades que brinda la firma digital podemos citar algunos de los usos que el Banco Central de la República Argentina prevé hacer de ella. Este organismo desarrollo un proyecto denominado “Central de Balances”. Este proyecto tiene por objetivo concentrar información económico-financiera sobre empresas y distribuir reportes multiusuarios de carácter individual y agregado. Esta información será de utilidad para la evaluación del riesgo de crédito, para la toma de decisiones económico-financieras y monetarias y deberá propender a la reducción del costo del crédito.

El desarrollo de la firma digital en el país sería una herramienta fundamental en la implementación de esta Central ya que aseguraría la autenticidad de los datos recibidos, las empresas informantes podrían remitir los datos electrónicamente con la firma digital de sus autoridades. Además, la firma digital ofrecería seguridad en cuanto a la confidencialidad e integridad de los datos suministrados y celeridad en el envío de la información.

B.- *La a.f.i.p como autoridad certificante*

Como Autoridad Certificante tiene como objetivo emitir certificados digitales para aquellas entidades del Sector Público y Privado que soliciten y obtengan autorización para operar como certificadores licenciados.

A continuación se listan algunas de las aplicaciones para las cuales se aplicará la firma digital en el ámbito de esta entidad: se permitirá a los ciudadanos hacer el seguimiento de sus trámites en la administración nacional, llenar formularios (Formulario Valor, Documentación para Desaduanamiento, Certificado de Origen digital) y pagar impuestos con el objetivo de reducir el papel en los documentos oficiales públicos y privado; enviar reclamos on-line a cualquier funcionario, notas internas y dictámenes jurídicos;buscar todo tipo de datos, agilizar habilitaciones de sus negocios y vender mercancías al Estado , presentación de declaraciones juradas mediante transferencia electrónica de datos a través de la página "web" (Resolución General AFIP Nº 2239/2007) y pueden notificarse actos administrativos como: liquidaciones de la Ley N° 11.683; citaciones, notificaciones, emplazamientos e intimaciones por falta de presentación de declaraciones juradas y/o de pago (Resolución General AFIP Nº 1995/2006)

C.- *ANSES como autoridad certificante*

“A partir del Decreto 378/2005 sobre el Plan de Gobierno Electrónico, han surgido iniciativas en distintas áreas del Estado, entre las que encontramos la Resolución 574/ 2007 suscripta por la Administración Nacional de la Seguridad Social (ANSES), dependiente del Ministerio de Trabajo y Seguridad Social, referida al Programa de Digitalización y Despapelización de Documentación.

Este proyecto consiste en la digitalización de más de 150 millones de documentos y formularios que anualmente la entidad tiene que imprimir, lo que permitirá ahorrar costos, garantizar la seguridad de los documentos y mejorar los procesos internos del trabajo cotidiano a través del uso de la firma digital, permitiendo la mejora de la calidad de servicio que presta

ANSES a la sociedad. Según los cálculos realizados en el organismo, que maneja el mayor presupuesto de la Administración Pública Nacional, actualmente gastan $10 millones por año en impresiones. La normativa insta a todas las dependencias de ANSES a definir e implementar la tramitación electrónica de expedientes, con la tecnología necesaria para la conversión de documentos a imágenes digitales, permitiendo la captura, conversión, almacenamiento, resguardo y posibilidad de recuperación de los mismos. Estas definiciones deben asegurar que los archivos digitalizados no pierdan validez ni interoperabilidad.

Asimismo, la normativa establece la posibilidad de digitalizar la documentación pública con validez legal, brindar servicios digitales de apoyo a la gestión como la Biblioteca Digital y desarrollar la "Interoperabilidad" con los organismos que componen su "Comunidad de Información" (todos los organismos de la Administración Pública que comparten intereses de información con ANSES),

Otras Aplicaciones en el Sector Público

✓ **Registro de Reincidencias y Estadística Criminal del Ministerio de Justicia, Derechos Humanos y Seguridad** – Emisión del Certificado de Antecedentes Penales (para los casos en que no se registran antecedentes.)

✓ **Oficina Nacional de Empleo Público** - Sistema de Retiro Voluntario – Se logró disminuir el tiempo promedio de respuesta: de 5 días a 2 horas

✓ **PAMI** – A la fecha se ha logrado digitalizar y firmar usando certificados digitales más de 11.000 Resoluciones y 4.000 dictámenes

✓ **Comisión Nacional de Valores –** Una de las experiencias más antiguas en el Estado, la Autopista de la Información Financiera lleva más de 35.000 documentos recibidos de empresas controladas por el organismo

✓ **Procuración General de la Nación –** Se la utiliza para la notificación de resoluciones a las 15 Fiscalías Generales del interior del país y a los Magistrados y Jefes de Área.

✓ **Ministerio de Economía y Finanzas:** altas de usuarios sistemas de administracion financiera de la Administracion Publica Nacional (SLU – UEPEX)

✓ **Sistemas de la SGGP –** Varios sistemas del organismo vienen utilizando esta tecnología. Entre ellos, el SIREPEVA (Sistema de Registro del Personal SINAPA), SECOP (Sistema Electrónico de Compras Públicas), Remisión de informes de Diagnóstico de Gobierno Electrónico, Informe sobre contratados, Acceso a las Bases de Datos confidenciales de ArCERT (Proyecto de Seguridad Informática de la ONTI).

✓ **DNI electrónico:** este proyecto del Estado Nacional consiste de una nueva tecnología para identificación de personas, que trata de una tarjeta de policarbonato, parecida a las de crédito, pero de alta seguridad que garantiza la identificación del portador, y tiene incorporado un chip electrónico que incluye certificados digitales de identidad, como datos biométricos (huella dactilar), iris, fotografía digital, y firma electrónica, imposible de alterar.

Dentro de las ventajas que brindaría el DNI electrónico aparecen su alta seguridad, la agilización de trámites administrativos, como el acceso al registro civil y partidas de nacimiento, y el comercio electrónico seguro, gracias al certificado de identidad y la firma electrónica incorporados en el microprocesador de alta seguridad, acreditando electrónicamente la identidad de los ciudadanos. Toda la información estaría encriptada en una clave emitida por la Policía al Ministerio del Interior, que aseguraría la inviolabilidad de estos.

7.- <u>Situación en la provincia de Tucumán</u>

A.- Digitalización e informatización en diversas áreas

"La Dirección de Modernización, Planificación y control de Gestión de la Administración publica provincial, dependiente de la Secretaria de Estado de Planeamiento de la Provincia tiene como misión diseñar, implementar y monitorear políticas de consulta documental a través de digitalización e informatización a reparticiones de la Administración Pública Provincial, con el objeto de lograr una mejor conservación de documentos originales, optimizar el tiempo de búsqueda de información, reducir costos y facilitar la toma de decisiones.

Bajo diferentes programas implementados por dicha repartición se realizaron distintos trabajos en la provincia:

- Digitalización de Prontuarios en la División de Antecedentes Personales.
- Digitalización de Padrones de Contribuyentes en el Instituto Provincial de Lucha contra el Alcoholismo (IPLA).
- Digitalización de Juicios en la Caja Popular de Ahorros.
- Digitalización de Actas en el Registro Civil de la Provincia.
- Digitalización de Legajos en la Secretaría de Estado de Niñez, Adolescencia Y Familia. (En proceso)
- Digitalización de Dictámenes en Fiscalía de Estado. (En proceso)
- Digitalización de Leyes y Decretos en la Dirección de Leyes y Decretos. (En proceso)" [25]

B.- Registro civil de la provincia: digitalización de actas

Hemos efectuado una entrevista con el coordinador del Proyecto de Digitalización de Actas del Registro Civil, Alejandro Miranda. Si bien este programa no representa actualmente una aplicación de la firma digital

[25] Consultas a bases de información, en Internet: www.tucuman.gov.ar, Abril 2010.

propiamente dicha, representan el aprovechamiento de las ventajas de esta herramienta y de la tecnología, brindando beneficios a toda la comunidad:

Este proyecto tuvo inicio en la ciudad de La Plata, Provincia de Buenos Aires, siendo el Registro Civil de dicha ciudad el primero que se involucro con el mismo, a través de una prueba piloto.

Hoy hay más de 15 provincias adheridas. La Provincia De Tucumán es una de las cuatro mejores, debido a que se preocuparon por que la calidad de las actas sea la mejor, ya que de nada sirve un acta ilegible.

El proyecto arranco en el año 2008 como resultado de un relevamiento a las necesidades de la gente. Todo inicio como un convenio entre S.I.N.T.Y.S, Secretaria de Planeamiento de Tucumán, UTN de Bs. As, UTN de Tucumán y Registro Civil.

En este momento el convenio solo involucra a cuatro reparticiones. Planeamiento dejo de asistir al convenio en el mes de febrero de 2009, desde entonces esta S.I.N.T.Y.S, UTN de Bs. As, UTN de Tucumán y Registro Civil.

Las actas que se cargan son:

- Nacimiento: se carga nacido, padre y madre.
- Matrimonio: se cargan a los dos contrayentes.
- Defunción: se carga al difunto.

Las Funciones que se cumplen con este proyecto son:

Sección escaneo: consiste en sacar una foto al acta para tener un soporte magnético.

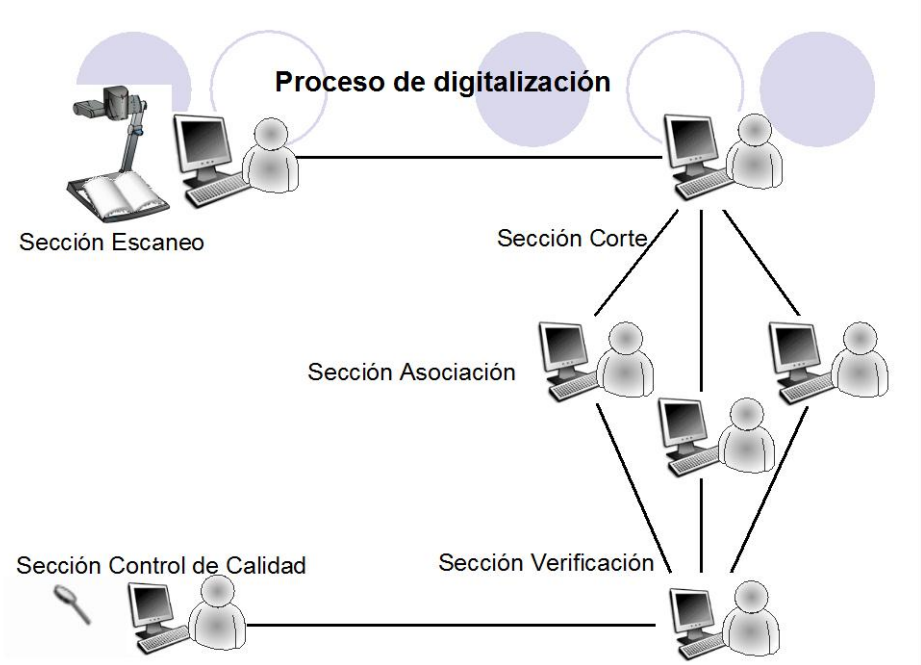
Sección Corte: corta las actas en 2 o 4 dependiendo la necesidad, cada libro cuenta con 200 o 400 folios y a la vez cada folio puede contar con 1 o 2 actas.

Sección Asociación: se encarga de cargar los datos, los mismos reciben el nombre de vinculadotes.

No se deben cargar: Sin DNI – Acta de Reconocimiento – F25 – CI Prov –DNI Extr. – No son Actas.

Sección Verificación: se controla los datos cargados por los vinculadores, es decir se corrobora que los datos estén correctamente cargados: Apellido y Nombre, DNI, ROL, Fecha de Nac, Sexo. Esta sección debe informar a control de calidad a través de un cuadro de observaciones lo que no se tuvo en cuenta

Sección Control de Calidad: es la única persona autorizada a realizar cambios en el acta. Una vez terminada esta etapa el acta esta en condiciones de ser expedida, sin embargo todavía no se esta realizando.



El Señor Alejandro Miranda durante la entrevista realizada estableció, que prevé que se estaría terminando con este proceso en el plazo de uno o dos años.

En este proyecto se encuentran trabajando 33 personas, la mayoría de ellos, eran empleados de la cooperadora del registro civil, los mismos

tuvieron una capacitación previa, en la cual se explicó la importancia de su tarea.

La *cantidad* de RRHH se encuentra distribuida de la siguiente manera:

3 en control de calidad
2 en catalogo
2 en corte
2 en escaneo
26 en verificación

Las actas que se cargaron fueron desde el año 1968 en adelante; por lo general, esto se debió a que desde ese año todos los nacimientos tienen documento y para poder cargar es necesario el mismo.

Se cargan actas tanto de la provincia como del interior.

El registro Civil cuenta con una base de datos cruzada con la base del padrón electoral. Esto facilita la tarea de carga de datos, ya que si una persona votó alguna vez se tiene la información de esa base; en caso contrario es necesario cargar todos los datos.

Sin embargo antes de empezar con la expedición es necesario un convenio entre el Registro Civil y Archivo General de la Provincia, porque los dos expiden actas. Esto generaría un problema económico debido a que sus ingresos esta dado por entrega de actas.

Ventajas de la digitalización de Actas:

- Velocidad en la expedición, la cual demoraría entre 5 a 10 minutos. Comparado con el proceso manual hoy implementado, el cual demora entre 2 a 4 hs. aproximadamente o más.
- Soporte Magnético, el cual agiliza la tarea del personal del registro civil, ya que no es necesario realizar búsquedas manuales.
- Mayor Seguridad de la información.
- Contar con una base actualizada de datos.

- Poder expedirse un acta de una persona proveniente de otra provincia, en la cual el Registro Civil también tenga implementado el sistema de digitalización de actas.

Desventajas de la digitalización de Actas:

- Riesgo de ruptura del back-up
- Peligro de que las personas involucradas en este proceso no tengan en cuenta la importancia de su trabajo y se tenga por resultado actas ilegibles, que no sirvan al interesado.
- Que el vinculador y el verificador sean la misma persona, entonces no seria posible detectar errores de los datos cargados.

Apéndice

REPORTE DE PRODUCCION

1. CANTIDAD DE ACTAS ESCANEADAS Y CORTADAS

1.1. Cantidad de Actas escaneadas y cortadas actualmente:

UNIVERSO COMPLETO							
REPARTICION	**REGISTRO CIVIL**			**ARCHIVO GRAL DE LA PROVINCIA**			**REESCENO**
Tipo de Actas	*Nacimiento*	*Defunciones*	*Matrimonio*	*Nacimiento*	*Defunciones*	*Matrimonio*	
Total discriminado por Tipo de Acta	620.141	213.189	77.427	682.639	127.570	124.139	Actas Reescaneadas (libros 400)
Sub- Total discriminado por Repartición	**910.757**			**934.348**			**187.100**
	1.845.105						
TOTAL	**2.032.205**						

2. CANTIDAD DE ACTAS VINCULADAS Y PRODUCTIVIDAD ALCANZADA

2.1. Cantidad de Actas Asociadas desde 03 de octubre del 2008, hasta el 31 de Mayo de 2010.

Detalle	Total Actas Vinculadas
Oct-08	23.591
Nov-08	31.777
Dic-08	30.568
Ene-09	17.438
Feb-09	40.698
Mar-09	38.306
Abr-09	43.590
May-09	47.388
Jun-09	52.013
Jul-09	55.489
Ago-09	54.890
Sep-09	68.958
Oct-09	71.861
Nov-09	56.960
Dic-09	67.782
Ene-10	34.229
Feb-10	47.383

Mar-10	64.971
Abr-10	50.016
May-10	1.097
TOTAL	**899.005**

2.2. Cantidad de actas asociadas respecto al total de actas escaneadas y cortadas:

Detalles	Cantidad	Porcentaje
Cantidad de Actas Escaneadas	1.845.105	**100**
Actas Asociadas	899.005	**48,72**
Actas que Faltan Asociar	**946.100**	**51,28**

3. CANTIDAD DE ACTAS ASOCIADAS Y PRODUCTIVIDAD ALCANZADA

3.1. Cantidad de Actas Asociadas desde 03 de octubre del 2008, hasta el 31 de Mayo de 2010.

Detalle	Total Actas Verificadas
Oct-08	3.244
Nov-08	4.975
Dic-08	6.242
Ene-09	3.537
Feb-09	11.600
Mar-09	14.784
Abr-09	18.368
May-09	13.679
Jun-09	23.108
Jul-09	25.239
Ago-09	28.050
Sep-09	27.976
Oct-09	37.107
Nov-09	32.401
Dic-09	37.430
Ene-10	36.388
Feb-10	44.992

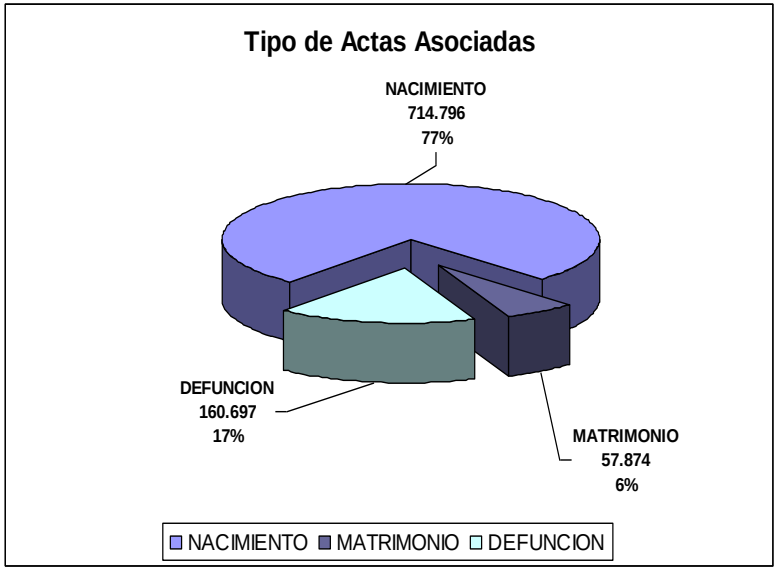
Mar-10	51.387
Abr-10	50.934
May-10	131.182
TOTAL	**602.623**

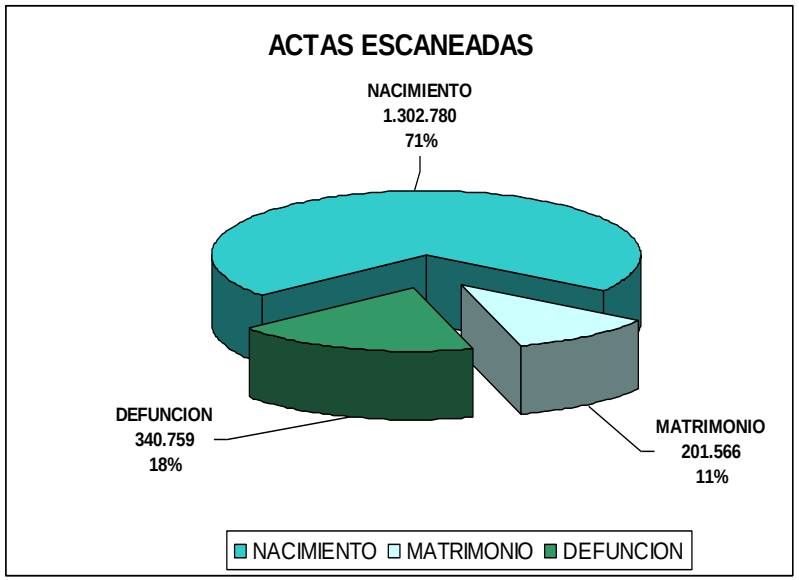
3.2. Cantidad de actas verificadas respecto al total de actas escaneadas y cortadas:

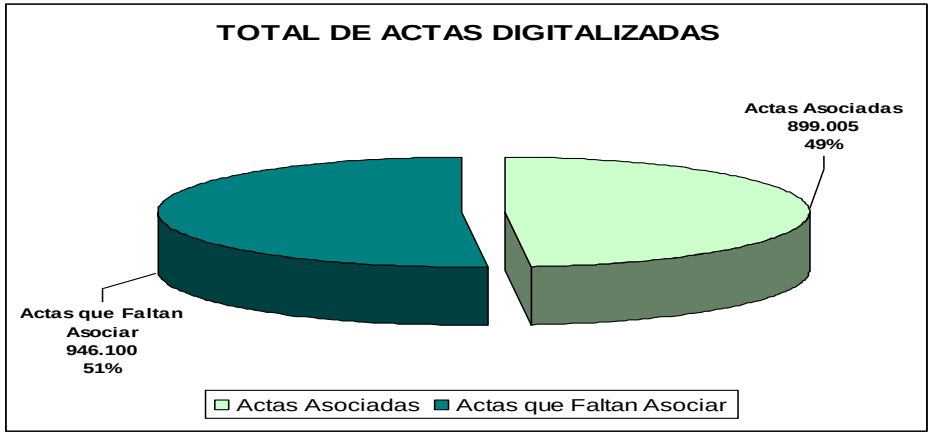
Detalles	Cantidad	Porcentaje
Cantidad de Actas Cargadas	1.845.105	**100**
Cantidad de Actas Verificadas	602.623	**32,66**
Cantidad de Actas que Faltan Verificar	**1.242.482**	**67,34**

4. OBJETIVOS ALCANZADOS

TIPO	ESCANEADO		ASOCIADOS	
	ACTAS	LIBROS	ACTAS	LIBROS
NACIMIENTO	1.302.780	2.411	714.796	1.213
MATRIMONIO	201.566	626	57.874	150
DEFUNCION	340.759	620	160.697	235
TOTAL	1.845.105	3.657	933.367	1.598


Tipo de Actas Asociadas
NACIMIENTO
714.796
77%
DEFUNCION
160.697
17%
MATRIMONIO
57.874
6%
NACIMIENTO
MATRIMONIO
DEFUNCION


ACTAS ESCANEADAS
NACIMIENTO
1.302.780
71%
DEFUNCION
340.759
18%
MATRIMONIO
201.566
11%
NACIMIENTO
MATRIMONIO
DEFUNCION


TOTAL DE ACTAS DIGITALIZADAS
Actas Asociadas
899.005
49%
Actas que Faltan Asociar
946.100
51%
Actas Asociadas
Actas que Faltan Asociar

CONCLUSION

En la investigación que encaramos, pudimos notar que el proceso modernizador de la sociedad permitió que a través de la firma digital el usuario-ciudadano pueda estar representado virtualmente utilizando diferentes herramientas tecnológicas.

A su vez, pudimos notar que estas herramientas constituyen puntos básicos en el reemplazo de lo que fue la forma de vincularnos oficialmente durante los últimos 4000 años; desde los papiros en Egipto, los papeles usados por los emperadores romanos, las cédulas mandadas por los reyes de España en la época de las colonias; en donde la mayoría de la historia humana vivió representada por este tipo de mecanismos en papel. Ahora bien, para poder hacerlo, advertimos que es necesario contar con un instrumento tecnológico que se adopte ante la constante evolución tecnológica, y sea capaz de ser flexible ante estos cambios, para lo cual es altamente necesario contar con un instrumento normativo que regule la utilización y administración de este tipo de herramientas.

Esta novedad implica un avance en el comercio electrónico, existiendo supermercados, aerolíneas, agentes bursátiles y bancos que ofrecen sus productos y servicios directamente por Internet. Pero el comercio electrónico no es el único beneficiario de la firma digital. Actualmente las empresas y los organismos públicos están atorados de grandes cantidades de documentos en soporte papel que ocupan un significativo y costoso espacio de archivo en sus oficinas y que dificultan su informatización, provocando un acceso lento y costoso a la información.

Si bien lo que hizo la LDF es dotar de igual tratamiento legal que la firma en papel, todavía queda por delante el desafío más importante, que es profundizar este desarrollo no sólo en el Poder Ejecutivo, sino también en el Poder Legislativo y en el Poder Judicial, porque la Justicia lenta no es justicia, y adoptar normas tecnológicas también va a permitir al poder judicial

tener mayor capacidad de respuesta a partir de la informatización y eliminar procedimientos dilatorios, que tanto entorpecen el funcionamiento de la misma.

Pensemos en lo que significaría para los ciudadanos argentinos que las causas tarden un 40% menos de tiempo en resolverse con este tipo de procedimientos, como así también la despapelización de nuestros tribunales, que brindaría más transparencia y seguridad.

Es decir que debemos ir avanzando, ampliar el uso de esta herramienta y no destinarla sólo a la administración pública, sino legislarla e implementarla en la justicia, el comercio, y todos los demás ámbitos en los que la sociedad se desenvuelve.

Para terminar, podríamos decir que el sistema de firma digital ha recorrido en la Argentina un camino particularmente dificultoso. La adopción de tecnologías informáticas requiere un proceso de adecuación de los distintos recursos, tanto humanos como materiales, para integrarlos de forma eficiente a nuestras prácticas administrativas en el Sector Público.

Pero para su correcto establecimiento se requerirá un desarrollo legislativo adecuado por parte de los gobiernos, además de una buena información al ciudadano y a la empresa. Sólo con el esfuerzo de todas las partes intervinientes se podrá llegar a la “aldea global” en la que todo el mundo pueda comunicarse y operar de forma segura y eficaz. Debemos tener la posibilidad de entrar y salir del Estado de manera electrónica, desde cualquier lugar del país. Tenemos que tener un Estado inteligente, eficiente y transparente, y eso se logra usando todas las herramientas que hoy la tecnología nos pone a nuestro alcance para que la relación Estado ciudadano no sea una entelequia y sea una realidad constante.

ÍNDICE BIBLIOGRÁFICO

a) General:

PALACIOS, Lino Enrique, "Manual del Derecho Procesal Civil"; 14º edición, (Buenos Aires, s.f.).

AGLIANO, Humberto, Compendio de Derecho Civil, (año 2002).

LARDENT, Alberto, Sistema de Información para la Gestión Empresaria: Planeamiento, Tecnología y Calidad, 1º Edición, (Buenos Aires, 2001).

LLAMBÍAS, Jorge Joaquín, Tratado de Derecho Civil Argentino, Parte General, séptima edición actualizada, Editorial Perrot, (Buenos Aires, 1878, t. II, N° 1584).

COUTURE, Eduardo J., Vocabulario jurídico (Depalma, Buenos Aires, 1976).

b) Especial:

GIANNANTONIO, Ettore, Valor jurídico del documento electrónico; Informática y Derecho. Aportes de la Doctrina Internacional. Tomo I, Ediciones Depalma, (Buenos Aires, 1987).

CARLINO, Bernardo P., Firma Digital y derecho Societario; Rubinzal-Culzoni Editores; (Buenos Aires, 2004).

c) Otras Publicaciones:

NIEVA CONEJOS, María Isabel; Ponencia: Firmas Digitales, ¿El comercio electrónico esta beneficiado con la reglamentación de la ley 25506?; cátedra de Derecho Comercial II; (Facultad de Ciencias económicas de la UNT; AÑO 2007).

DESCHKA, Fridolin, El documento electrónico, Revista Internacional del Notariado, N° 87, volumen 42, (Argentina, 1991).

Diccionario de la Lengua Española. Real Academia Española, Vigésima segunda edición, (Madrid, 2002).

Código Civil de la Republica Argentina, 8ª edición, (Buenos Aires, 2010).

d) Consultas en Internet:

http://www.pki.gov.ar/index.php?option=com_content&view=article&id=96&Itemid=107.htm

http://www.sgp.gov.ar/contenidos/paginas_de_banners/resoluciones/docs/SGP/07/Resoluciones_SGP_57-25-10-07.pdf

http://edant.clarin.com/diario/2009/03/09/um/m-01950688.htm

ÍNDICE

Págs.

Prólogo.....1

Introducción.....3

CAPÍTULO I

DOCUMENTO

1.- Introducción.....4
2.- Documento.....5
3.- Documento Electrónico.....6
4.- Documento electrónico como medio de prueba.....10

CAPÍTULO II

LA FIRMA

1.- Introducción.....13
2.- Concepto.....14
3.- Importancia y elementos.....15
4.- Características.....16
5.- Funciones.....17
6.- La firma y el documento electrónico.....18
7.- Autenticidad, inalterabilidad y seguridad del documento electrónico.21

CAPÍTULO III

LA FIRMA DIGITAL

1.- Introducción.....23
2.- Firma digital y firma electrónica.....24
3.- Firma manuscrita y firma digital.....27
4.- Comparación entre las firmas.....29
5.- Procedimiento de firma digital.....30
6.- Criptografía.....34
7.- Consecuencias de la firma digital.....43
8.- Ventajas y desventajas.....44
9.- Aplicaciones.....46

10.- Validez jurídica del documento electrónico. 47

CAPÍTULO IV

ESTRUCTURA DEL SISTEMA DE FIRMA DIGITAL

1.- Infraestructura de firma digital 53
2.- Infraestructura del sector público.....54

CAPÍTULO V

MARCO NORMATIVO

1.- Introducción.....74
2.- Marco Normativo sobre Firma Digital: Alcance y Estructura.....75
3.- Objetivos de la Ley 75
4.- El Decreto Reglamentario 2628/2002.....76
5.- Infraestructura de Firma Digital.....77
6.- Resumen de Legislación Vigente sobre Firma Digital.....79
7.- Otras normas específica sobre Firma Digital.....81
8.- Adhesión en las Provincias.....83
9.- Estado y Firma Digital: Normativa sobre Firma Digital para el Sector Público 83
10.- Normativa sobre aplicaciones en el Sector Público. 86
11.- Antecedentes legales internacionales de la firma digital.....88

CAPÍTULO VI

DESPAPELIZACION DEL SECTOR PÚBLICO

1.- Introducción.....89
2.- Deficiencias en el uso del papel como soporte de información 90
3.- Despapelización de la administración pública: Implicancias del proceso 91
4.- Herramientas tecnológicas necesarias.....93
5.- Cambio de paradigmas.....98
6.- Posibilidades a futuro que ofrece la firma digital 100
7.- Situación en la Provincia de Tucumán. 104

Apéndice 110

Conclusión.....117

Índice Bibliográfico.....119

Índice.....121