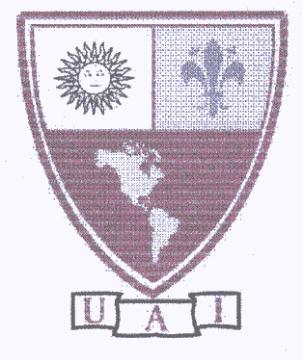


FIRMA DIGITAL

TOMÁS VERNET

Abogado

Universidad Abierta Interamericana

Sede Regional Rosario

Facultad de Derecho

Agosto 2003.

RESUMEN

La presente tesis comienza con una breve introducción sobre el derecho digital, pasando luego a explicar el fenómeno de la Internet, donde se explica el origen, su concepto, funcionamiento, y otros tipos de redes.

Luego se trata la ley de firma digital, que incluye sus antecedentes nacionales e internacionales, su objeto y la técnica legislativa utilizada. Pasa luego a explicar el tema de la criptografía, los diversos tipos de criptografía, el sistema adoptado por la ley argentina, se trata la función hash, y como se generan y almacenan las claves.

Sentado lo anterior se pasa a explicar la firma digital, donde se explica el concepto, sus características, particularidades y efecto, su comparación con la ológrafa y sus aplicaciones, la firma electrónica y el aspecto penal. Luego se analiza el documento digital, como documento en general, concepto requisitos, su valor jurídico y probatorio, sus aplicaciones y el aspecto penal.

Luego se trata el certificado digital, donde analizamos el concepto, sus requisitos, sus aplicaciones y los derechos y obligaciones del titular del certificado.

Por último se trata la infraestructura de la firma digital, donde luego de una introducción de la misma, se pasa a la autoridad certificante licenciada, a el ente administrador de la firma digital, a la autoridad de aplicación, a la comisión asesora y los sistemas de auditorias. Terminando con una opinión personal.

OBJETIVO GENERAL

Analizar la Ley Nº 25.506

de Firma Digital de Argentina.

OBJETIVOS ESPECIFICOS

1. Observar, en el contexto del avance tecnológico, la sanción de la Ley de Firma Digital en la Argentina y su técnica legislativa, teniendo en cuenta los antecedentes internacionales y los antecedentes nacionales.

2. Analizar la definición de la Firma Digital y sus características en el marco de la Ley Nº 25.506, y la ampliación del concepto tradicional de Firma.

3. Analizar el documento digital y el certificado digital, como así también la Infraestructura de la Firma Digital contemplada en la Ley de Firma Digital y en su Decreto Reglamentario Nº 2628/02.

FUNDAMENTACION

Me he planteado realizar la presente tesis, para hacer un estudio de la Ley de Firma Digital, sancionada el 14 de noviembre de 2001, promulgada por el Poder Ejecutivo el 11 de diciembre del año 2001 y publicada en el Boletín Oficial el 14 de diciembre de 2001; confrontándola con antecedentes existentes en la Argentina y antecedentes internacionales.

Esto se debe a que en la actualidad, si bien existen, escasos, trabajos doctrinarios sobre el tema, no lo tratan en forma completa. Por ello me propongo ensayar un trabajo exhaustivo sobre el tema, si bien los puntos más importantes, hoy por hoy, son entender que es una firma digital, su utilización, sus aplicaciones y lo mismo con el documento digital, por los efectos que produce la Ley 25.506 para con ellos en el ordenamiento jurídico.

Me propongo hacer un breve análisis del constante avance tecnológico que se ha y seguimos experimentado, que nos ha inmerso en una infinidad de desafíos no sólo en el campo del derecho, originado nuevas formas de comunicación y comercialización por medio de las redes, como internet, lo que encuentro imprescindible analizar ya que es en donde se desenvuelve la nueva era digital, y en definitiva, donde vive la Firma Digital.

En ésta tesis pretendo observar la técnica legislativa utilizada para la realización de la Ley de Firma Digital, y en definitiva del sistema criptográfico adoptado para el mecanismo de la firma digital, es cual es imprescindible para la misma.

Para lograr mis objetivos realizaré un análisis concreto del texto de la Ley, intentando permanentemente tener una visión explicativa de los distintos artículos, ya que han enriqueciendo y adaptando nuestro ordenamiento jurídico al marco tecnológico existentes y a las necesidades actuales, a la par de los países del primer mundo.

Creo imperioso reparar en él efecto de la Firma Digital, ampliando el concepto de Firma, y observar la validez jurídica y probatoria del documento digital y su valor como instrumento. Ya que esto es lo que remarca el valor de la Ley.

Una vez analizados los puntos fundamentales, como así también explicados todos los artículos de la Ley sobre el tema, pasaré a tratar el certificado digital, que es propio de la Firma Digital y hace posible las garantías de ella.

Por último examinaré la Infraestructura de la Firma Digital, detallando los entes que la componen, sus funciones y obligaciones, con el fin de hacer un análisis de los supuestos necesario para la implementación de la Firma Digital.

Todo esto me permitirá efectuar una conclusión acerca de la importancia de la sanción de la Ley y de los efectos que produce en nuestro derecho.

DESARROLLO DEL TEMA

INTRODUCCIÓN AL DERECHO DIGITAL.

Sabemos que la Tecno-era o Era Digital ha producido un drástico cambio de paradigma científico y social, con terribles impactos en el resideño de la producción cultural y la industria.

El avance tecnológico constante que se ha experimentado en el siglo XX ha creado, ciertamente, infinidad de desafíos no sólo en el campo del derecho.

La revolución tecnológica en general, el desarrollo de la informática, los constantes y extraordinarios avances de las telecomunicaciones, en particular, han determinado un profundo cambio en la forma de relacionarnos, nos hallamos transitando la era de la economía globalizada, de la economía de la "red".

La velocidad y avance que han tenido las comunicaciones a nivel mundial han originado nuevas formas de comercialización de productos, resultando en definitiva un acercamiento de los países del mundo y una conexidad económica impensada décadas atrás.

Nadie discute ya que la globalización de los mercados ha coincidido y se ha potenciado por la globalización de las redes telemáticas de comunicaciones interactivas.

Sin la informática las sociedades actuales colapsarían, generándose lo que se conoce como "computer dependency", a los efectos de entender el grado de poder de la informática, se puede hacer una comparación entre la civilización con escritura y la civilización sin ella o la civilización sin el papel.

El impacto de la informática en la sociedad, ha producido transformaciones en todos los ámbitos de la vida social, planteando, en consecuencia, nuevos problemas e interrogantes que requieren, desde el ámbito del derecho la elaboración de respuestas adecuadas.

En efecto, es función y objetivo de la moderna disciplina del Derecho Informático, observar el nuevo fenómeno tecnológico, detectar aquellos nuevos problemas e interrogantes y elaborar finalmente, soluciones jurídicas pertinentes ante los mismos.

Sin lugar a dudas se puede afirmar que Internet, en su máxima expresión, es funcional al proceso de globalización. Dentro de estos procesos, el comercio electrónico

y el marketing directo aparecen en escena como elementos relevantes y en continua mutación.

Se están presentando, y estamos asistiendo al mismo tiempo, a un cambio en las, técnicas contractuales para la venta de todo tipo de productos y a la evolución de las técnicas informativas y de promoción de esos mismos productos, tendiendo siempre a una personalización creciente.

Por medio de Internet se ha creado un nuevo desafío para juristas, gobernantes, jueces, empresarios, inversionistas, etc. Este nuevo reto implica la regulación legal necesaria para la protección y defensa tanto de los derechos individuales de las personas como de los derechos colectivos necesarios para la vida en comunidad.

El crecimiento vertiginoso que ha experimentado Internet desde su creación al presente, no sólo en el orden de usuarios sino también en la cantidad de operaciones comerciales efectuadas a través de ella, ha puesto en alerta a los gobernantes de las grandes economías del mundo en busca de soluciones en el campo legal general, en vista de las particularidades que envuelve esta vía de comercialización cibernética.

INTERNET.

Conocer el contexto y el funcionamiento en donde se desenvuelve la nueva era digital es vital e imprescindible para el tema que estamos tratando, por ello debemos conocer Internet.

ORIGEN.

Si bien Internet es ahora una red abierta a innumerable cantidad de compañías, esto sucedió recién en la última década del siglo XX, ya que "Internet comenzó en los años setenta como una red del Departamento de Defensa de los Estados Unidos de Norteamérica, llamada A.R.P.A., Advanced Research Proyect Agency". El objetivo principal fue desarrollar un programa de investigación militar que permitiera, luego de un contraataque nuclear norteamericano, que la red siguiera funcionando.

Fue así como en 1958 se organiza en los EE.UU. la agencia gubernamental de investigación, A.R.P.A, creada en respuesta a los desafíos tecnológicos y militares de Rusia de la cual surgirán una década mas tarde los fundamentos de la futura red global de computadores Internet.

A comienzos de la década del 60 A.R.P.A. emprendió la tarea de desarrollar un sistema militar de comunicaciones en red diseñado específicamente para interconectar computadores en forma descentralizada cuyo objetivo principal debía ser continuar operando aun en el caso de alguno o varios de sus nodos de comunicaciones fueran destruidos durante un ataque enemigo, la red de comunicación fue bautizada con el nombre de Arpanet.

En 1962 el Dr. J.C.R. Licklider uno de los responsables principales del proyecto influyo para lograr que esta tecnología de comunicaciones sirviese para interconectar las universidades dentro de los EE.UU.

La primera descripción documentada acerca de las interacciones sociales que podrían ser propiciadas a través del *networking* (trabajo en red) está contenida en una serie de memorándums escritos por J.C.R. Licklider, del Massachusetts Institute of Technology, en Agosto de 1962, en los cuales Licklider discute sobre su concepto de *Galactic Network* (Red Galáctica). El concibió una red interconectada globalmente a través de la que cada uno pudiera acceder desde cualquier lugar a datos y programas. En esencia, el concepto era muy parecido a la Internet actual.

En Julio de 1961 Leonard Kleinrock publicó desde el MIT el primer documento sobre la teoría de conmutación de paquetes, Kleinrock convenció a Lawrence G. Roberts de la factibilidad teórica de las comunicaciones vía paquetes en lugar de circuitos, lo cual resultó ser un gran avance en el camino hacia el trabajo informático en red. El otro paso fundamental fue hacer dialogar a los ordenadores entre sí. Para explorar este terreno, en 1965, Roberts conectó un ordenador TX2 en Massachusetts con un Q-32 en California a través de una línea telefónica conmutada de baja velocidad, creando así la primera (aunque reducida) red de ordenadores de área amplia jamás construida. El resultado del experimento fue la constatación de que los ordenadores de tiempo compartido podían trabajar juntos correctamente, ejecutando programas y recuperando datos a discreción en la máquina remota, pero que el sistema telefónico de conmutación de circuitos era totalmente inadecuado para esta labor. La convicción de Kleinrock acerca de la necesidad de la conmutación de paquetes quedó pues confirmada.

A causa del temprano desarrollo de la teoría de conmutación de paquetes de Kleinrock y su énfasis en el análisis, diseño y medición, su *Network Measurement Center* (Centro de Medidas de Red) en la UCLA fue seleccionado para ser el primer nodo de la red científica y académica que se conocerá en adelante como ARPANET. Todo ello ocurrió en Septiembre de 1969, cuando quedó conectado el primer ordenador

host. Un mes más tarde, cuando el SRI fue conectado a ARPANET, el primer mensaje de *host* a *host* fue enviado desde el laboratorio de Leinrock al SRI. Se añadieron dos nodos en la Universidad de California, Santa Bárbara, y en la Universidad de Utah. Así, a finales de 1969, cuatro ordenadores *host* fueron conectados conjuntamente a la ARPANET inicial y se hizo realidad una embrionaria Internet.

Se siguieron conectando ordenadores rápidamente a la ARPANET durante los años siguientes y el trabajo continuó para completar un protocolo *host* a *host* funcionalmente completo, así como software adicional de red. En Diciembre de 1970, el *Network Working Group* (NWG) liderado por S.Crocker acabó el protocolo *host* a *host* inicial para ARPANET, llamado *Network Control Protocol* (NCP, protocolo de control de red). Cuando en los nodos de ARPANET se completó la implementación del NCP durante el periodo 1971-72, los usuarios de la red pudieron finalmente comenzar a desarrollar aplicaciones

La agencia cambiará su denominación en 1972 y será conocida de allí en mas como DARPA (Defense Advanced Research Projects Agency) transfiriendo finalmente la red ARPANET a la Agencia de Comunicaciones de la Defensa para su uso como red operativa a mediados de 1975. Recién casi una década mas tarde se abrirán las posibilidades para su uso civil en lo que será el prólogo del nacimiento de Internet.

Hacia fines de la década de 1990 la agencia, a través del Departamento de Defensa y bajo una nueva política, comenzará a incursionar en el mercado comercial de tecnología avanzada en electrónica, ordenadores y comunicaciones como un competidor mas de negocios.

La ARPANET original evolucionó hacia Internet. Internet se basó en la idea de que habría múltiples redes independientes, de diseño casi arbitrario, empezando por ARPANET como la red pionera de conmutación de paquetes, pero que pronto incluiría redes de paquetes por satélite, redes de paquetes por radio y otros tipos de red. Internet como ahora la conocemos encierra una idea técnica clave, la de arquitectura abierta de trabajo en red.

INTERNET.

Internet es definido por la Internet Society como una red global de redes que posibilita a computadoras de todo tipo comunicarse en forma directa y transparente y compartir servicios a través de la mayor parte del mundo. Por ser la Internet un enorme activo, permitiendo capacidades para tantas personas y organizaciones; también

constituye un recurso global compartido de información, conocimiento, y medios de colaboración y cooperación entre incontables diferentes comunidades1.

Podemos decir que es un grupo de computadoras denominadas servidores (servers), conectadas entre sí, similar al sistema telefónico internacional, es decir, interligados por cables ópticos, líneas conmutadas y otras, dependiendo de la conexión y ubicación mundial. Estos servidores tienen la característica particular de almacenar infinidad de información separada por archivos o mejor conocidos como "páginas" (sites) desde una computadora personal, que al establecer contacto, se puede consultar.

Cada transmisión efectuada a través de la red es simplemente un intercambio de información, este intercambio de datos o información electrónica no difiere en gran medida con el servicio de correo que todos conocemos; cada uno tiene una dirección y para enviar o recibir información no se necesita más que la dirección (IP numbers/lnternet Domain Name) para encontrar o dirigirse al destino deseado; ya que internet está provista de infinidades de servers conectados, formándose distintas rutas y conforme la dirección de cada site la red se guía por el camino necesario para llegar a destino. Para conectarse a la red es indefectible, en primer término, tener acceso a una computadora personal y que ésta se encuentre provista de un elemento denominado módem. Paso seguido, para tener acceso a Internet es necesario contratar los servicios de un ISP (Internet Service Provider/ Proveedor de servicios de Internet), estas empresas se encuentran provistas de licencia para autorizar el uso de la red, funcionando de "puente" entre los usuarios y la red de redes; si bien ya es común el acceso en forma gratuita.

Es decir, si Internet es equivalente a una autopista de información (information superhighway); los ISP juegan el rol de calles locales de acceso a la red. Por ello, cuando un usuario contrata los servicios de un ISP, éste no se encuentra simplemente conectado a Internet, sino que pasa a ser parte de la red de redes.

FUNCIONAMIENTO DE LA RED.

El secreto de la red es un protocolo creado por militares estadounidenses, el TCP/IP. Esto es, un tipo de sistema codificador que permite a las computadoras describir datos electrónicamente.

El término describe dos partes separadas, el protocolo de control de transmisión *(transmission control protocol:* TCP) y el protocolo de Internet *(lnternet protocol:* IP).

Juntos forman el *esperanto* de la red. Cada computadora que accede a Internet entiende estos dos protocolos y los utiliza para enviar y recibir datos a lo largo de la red. El TCP/IP crea lo que se denomina *paquete-conector,* un tipo de red que intenta minimizar la posibilidad de perder cualquier dato que se envía por el cableado.

En principio, TCP fragmenta cada pieza de los datos enviados (como un mensaje de e-mail), agrupándolos en pequeños conjuntos llamados *paquetes,* los cuales, codificados electrónicamente, poseen direcciones Web De remitente y destinatario. El protocolo IP reconfigura el dato como se supone que va a ser recibido en el punto A desde el E, atravesando una serie de guías, asemejándose a una oficina de correo tradicional, en especial, a su sección de clasificación.

Cada guía examina el destino al cual se dirigen los paquetes que recibe y luego los pasa a otra, hasta que son recibidos en su destino final.

Si una ruta no funcionara, se reasignan otras; y una vez que esté verificado por TCP que los paquetes están intactos, éstos se montan para volver a formar el mensaje original.

TCP/IP es el más importante de la larga lista de protocolos de Internet. A veces, se lo emplea como un término global para describir otros adicionales, como protocolos de traslados de correos simples *(simple mail transfer protocol:* SMTP), protocolos de transferencia de archivos *(file transfer protocol:* FTP) y protocolos de transferencia telnet *(telnet transference protocol:* TTP) [2].

OTROS TIPOS DE REDES.

Intranets.

Las intranets son redes internas que no permiten su acceso y utilización a otras compañías u organizaciones que no sean las propietarias de las mismas. Estas redes utilizan la tecnología en la cual se basa la red Internet, es decir, el protocolo de comunicación TCP/IP. Las ventajas que poseen las intranets frente a la red Internet son la seguridad y confianza que otorga el uso privado de la red, ya que solamente puede ser utilizada por los usuarios autorizados.

Este tipo de redes intercompañía son utilizadas para comunicar a los diferentes usuarios de una misma organización, se encuentren estos dentro del mismo o en diferentes edificios, provincias, países.

Otro de los beneficios que otorga la intranet es que al utilizar el protocolo TCP/IP, los usuarios pueden comunicarse utilizando diferentes plataformas (PC, Machintosh, Linux, etc.).

Extranets.

Las extranets son redes intranet que permiten el acceso a usuarios externos a la organización. Generalmente son utilizados para que proveedores o clientes de la compañía accedan a través de una clave a determinada información de esa compañía o interactúen con ella a través de pedidos, consultas, órdenes de compra, etc. Las redes extranets están constituidas por la misma tecnología que utiliza Internet (protocolo TCP/IP). El acceso a éstas puede hacerse ya sea vía Internet o a través de redes privadas, siendo estas últimas más seguras y confiables en cuanto al resguardo de la información.

Algunas ventajas son: reducción de costos operativos y acceso a información en línea, entre otras.

EDI Networks.

Las redes EDI (42) han sido utilizadas para realizar transacciones electrónicas durante un largo tiempo. A través de ellas se envía y recibe documentación comercial, como por ejemplo órdenes de compras y facturas comerciales, entre otros. La tecnología utilizada en este tipo de redes es bastante onerosa, razón por la cual el advenimiento de Internet permitió que empresas medianas y pequeñas tengan lugar en la realización de transacciones electrónicas sin la necesidad de invertir en esta tecnología. Las EDI Networks utilizan redes privadas electrónicas denominadas value-added-networks (VAN's).

Usenet y Newsgroups. Comunidades Virtuales.

Existen cientos de usenets y newsgroups. Consisten en una forma de correspondencia que uno recibe individualmente sobre diferentes temas. En la actualidad estos "usenets y newsgroups" cubren una temática amplísima. Son utilizados frecuentemente para expandir información sobre una diversidad de productos, provocando efectos positivos o adversos, de acuerdo a los comentarios que se hagan de los mismos.

Otros tipos de comunidades son: chatroom online, message board[3].

EL AVANCE DE INTERNET.

Las redes abiertas como Internet revisten cada vez mayor importancia para la comunicación mundial. Esas redes permiten una comunicación interactiva entre interlocutores que no necesariamente han entablado previamente relación alguna. Además, ofrecen nuevas posibilidades empresariales, creando herramientas que mejoran la productividad y reducen los costos, así como nuevas formas de llegar al cliente. Las redes están siendo utilizadas por empresas que desean aprovechar los nuevos tipos de actividad y nuevas formas de trabajo, como el teletrabajo y los entornos virtuales compartidos. También las administraciones públicas las utilizan en su gestión interna y en su interacción con empresas y ciudadanos. El comercio electrónico brinda al país una excelente oportunidad para avanzar en su integración económica con las naciones del resto del mundo.

Para aprovechar todas estas posibilidades es necesario disponer de un entorno seguro en relación con la autenticación digital.

En este sentido, el derecho no puede permanecer estático: debe abocarse entre otras cosas, al estudio de las nuevas formas de contratación que nos impone la realidad virtual de nuestros días.

Internet ha determinado la modificación de principios jurídicos en el Derecho Comparado: ya sea tipificando nuevos delitos o buscando formas seguras para el desarrollo del comercio electrónico, baste como muestra, la legislación existente sobre Firma Digital.

CIBERESPACIO.

El ciberespacio fue definido en 1984 en la novela Neuromancer, de William Gibson: "... Un nuevo universo, un universo paralelo creado y sustentado por los computadores del mundo y líneas de comunicación... La tablilla se convierte en una página, la página se convierte en una pantalla, la pantalla se convierte en un mundo, un mundo virtual... Una geografía mental común, construida, a su vez, por el consenso y la revolución, el canon y el experimento... Sus corredores se forman donde quiera que corra la electricidad con inteligencia... El reino de completa información...".

En el auténtico ciberespacio, no sólo se representarían los datos de forma tridimensional, sino que el usuario podría interactuar con los objetos verbal o incluso físicamente.

Mientras que la realidad virtual supone engañar a los sentidos para que la persona crea que está en un entorno distinto del real, el auténtico ciberespacio supondría una integración completa de la persona y la máquina

Ahora la palabra forma parte del vocabulario futurista, se utiliza como sinónimo de Internet, también se lo entiende como ese espacio no físico donde se encuentran todos los datos e informaciones a las que accedemos a través de internet o las que nosotros mismos enviamos.

El ciberespacio se refleja en un sistema para organizar las ingentes cantidades de datos almacenados en los ordenadores o computadoras y para acceder a esos datos.

El ciberespacio presenta como característica fundamental un ensanchamiento artificial y arbitrario del mundo real como consecuencia de la masificación de los medios electrónicos, de los acumuladores de información y de las redes de intercomunicación de datos que permiten a individuos, gobiernos y empresas interactuar bajo formas, modelos sociales y características diferentes (quizás simplemente complementarias) al mundo real. Para algunos es un nuevo mundo, descubierto o creado por el hombre.

LA LEY DE FIRMA DIGITAL.

INTRODUCCIÓN.

Las redes abiertas como Internet revisten cada vez mayor importancia para la comunicación mundial. Para aprovechar todas estas posibilidades es necesario disponer de un entorno seguro en relación con la autenticación digital. En la práctica existen diversos métodos para firmar documentos digitalmente, que van desde algunos muy sencillos, por ejemplo, insertar la imagen escaneada de una firma manuscrita en un documento creado con un procesador de textos, lo que no permite otorgarle validez jurídica a la firma, a otros muy avanzados, por ejemplo, la firma digital que utiliza la criptografía de clave pública, que sí lo permiten. Para tener validez jurídica, las firmas digitales deben permitir verificar tanto la identidad del autor, como comprobar que dichos datos no han sufrido alteración desde que fueron firmados[4].

La firma digital se utiliza en algunos sectores de la administración pública y pronto se aplicará en todo los sectores. Pero esto es solo el primer paso para la implementación en la actividad privada.

Para favorecer la integración en el actual contexto de globalización es imprescindible que el marco legal y técnico que adopte el país para el desarrollo de la firma digital sea compatible con el que ya existe en otros países.

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

El fin que persigue la firma digital es el mismo que el de la firma ológrafa, es decir dar asentimiento y compromiso con el documento firmado.

El beneficio de la firma digital sería facilitar la autenticación a distancia entre partes que no necesariamente se conocen previamente, constituyendo el mecanismo esencial para proveer seguridad y desarrollar la confianza en las redes abiertas. Por ello constituye un elemento clave para el desarrollo del comercio electrónico en Internet.

El mercado global electrónico hace necesario que el marco legal y técnico adoptado por nuestro país para el desarrollo de la firma digital, sea compatible con el de otros países, es más, es necesario que todos los ordenamientos jurídicos del mundo sean compatibles fundamentalmente en este tema. La adopción de criterios legales diferentes a los aplicables en otros países en cuanto a los efectos legales de la firma digital, y

cualquier diferencia en los aspectos técnicos en virtud de los cuales las firmas digitales son consideradas seguras, resultaría perjudicial para el desarrollo futuro del comercio electrónico nacional y, por consiguiente, para el crecimiento económico del país y su incorporación a los mercados internacionales, cada vez más globalizados.

Esta homogeneidad normativa es para fomentar la comunicación y la actividad empresarial por redes abiertas con las naciones del Mercosur y del mundo, al facilitar el libre uso y prestación de servicios relacionados con la firma digital y el desarrollo de nuevas actividades económicas vinculadas con el comercio electrónico.

ANTECEDENTES INTERNACIONALES.

En el derecho comparado existen numerosos antecedentes internacionales sobre firma digital, que han servir como pilares para la legislación mundial, entre ellos encontramos:

- La Ley Modelo sobre Comercio Electrónico de la CNUDMI o UNCITRAL (Comisión de las Naciones Unidas para el Derecho Mercantil Internacional), que fue aprobada en Nueva York en 1996 por la Asamblea General de las Naciones Unidas, con la adición del art. 5 bis en el año 1998, con el fin de fomentar la armonización y unificación del derecho mercantil internacional.

- La Directiva de la Unión Europea sobre Comercio Electrónico realizada en 1997, junto con la Directiva de 1999 por la que se establece un marco comunitario para la Firma Electrónica, que tiene por finalidad facilitar el uso de la firma electrónica y contribuir a su reconocimiento jurídico y la Directiva del 2000 sobre Comercio Electrónico relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior.

- Las Disposiciones de la Organización Mundial de Comercio (OMC) y las recomendaciones de la Organización de Cooperación y desarrollo Económico (OCDE).

- La normativa de Firma Digital del Comité de Seguridad de la Información de la Sección de Ciencia y Tecnología de la American Bar

Association ("ABA", Asociación de Abogados de los EE.UU.), que redactó su normativa de Firma Digital en 1996, en la que participaron casi ochenta profesionales de las disciplinas del derecho, la informática y la criptografía de los sectores público y privado, en la que especifica un mecanismo de firma digital a base de la criptografía asimétrica, los certificados de clave pública y los certificadores de clave pública.

Además de los mencionados antecedentes, han servido de pilares diversas Leyes de Firma Digital, como:

- La Ley de Firma Digital del Estado de Utah, EE.UU., en 1995, ésta se destaca ya que fue el primer estado en legislar el uso comercial de la firma digital. Regula la utilización de la criptografía asimétrica y fue diseñada para ser compatible con varios estándares internacionales. Prevé la creación de certificadores de clave pública licenciados por el Departamento de Comercio de Estado. Además protege la propiedad exclusiva de la clave privada del suscriptor del certificado, por lo que su uso no autorizado queda sujeto a responsabilidades civiles y criminales.
- La Electronic Signatures in Global and National Commerce Act (E-Sign) de EE.UU de 1999.
- La Ley de Firma Digital Alemana que entró en vigencia en el 2001 con su reglamentación, estableciendo las condiciones para considerar segura una firma digital, regulando la acreditación voluntaria de proveedores de servicios de certificación, la elaboración de un catálogo de medidas de seguridad de la misma.
- La Ley Italiana de Firma Digital de 1998, estableciendo el reconocimiento legal de los documentos digitales, y de la firma digital.
- El Real Decreto de Firma Electrónica de España 14/1999, que regula el uso de la firma electrónica, el reconocimiento de su valor jurídico y la prestación de servicios de certificación.

Numerosos países del mundo ya han sancionado su legislación en materia de firma digital, y muchos de los que todavía no la han sancionado se encuentran discutiendo los proyectos de ley de firma digital, entre los que han aprobado su legislación están:

- Estados Unidos.
- Canadá.
- Australia.
- Irlanda.
- El Reino Unido.
- Alemania.
- Dinamarca.
- España.
- Francia.
- Italia.
- Portugal.
- Colombia.
- Perú.
- Méjico.
- Chile.
- Malasia.
- Japón.
- Hong Kong.
- Corea.
- Otros.

ANTECEDENTES NACIONALES.

En nuestro país existen numerosos antecedentes legislativos que han precedido a nuestra ley de firma digital, podemos ver normas referidas a internet, al correo electrónico, a nombres de dominio y a la firma digital, dichas normas han sido las siguientes:

Normas sobre internet, correo electrónico y nombres de dominio:

- Decreto 554/97. Declarase de Interés Nacional el acceso de los habitantes de la República Argentina a la red mundial Internet. Autoridad de Aplicación.

- Resolución 2132/97. Adoptase el procedimiento de Audiencia Pública, previsto en el Reglamento General de Audiencias Públicas y Documentos de Consulta, para la presentación de inquietudes sobre aspectos relacionados con Internet (Secretaría de Comunicaciones).
- Decreto 1279/97. Declarase comprendido en la garantía constitucional que ampara la libertad de expresión al servicio de Internet.
- Resolución 1616/98. Adoptase el procedimiento de Audiencia Pública previsto en el Artículo 15 del "Reglamento General de Audiencias Públicas y Documentos de Consultas" a fin de que los distintos interesados hagan conocer al Gobierno Nacional sus inquietudes sobre diferentes aspectos relacionados con Internet (Secretaría de Comunicaciones).
- Decreto 1018/98. Créase el Programa para el desarrollo de las comunicaciones telemáticas argentin@internet.todos.
- Resolución 2320/98. Proyecto Ciberciudad La Carlota (Secretaría de Comunicaciones).
- Resolución 2651/98. Creación del equipo "Autopistas de la Información" (Secretaría de Comunicaciones).
- Resolución 412/99 (Ministerio de Economía y Obras y Servicios Públicos).
- Decreto 1335/99. Una dirección de Correo Electrónico para cada Argentino.
- Resolución 4536/99. Designase al correo oficial de la República Argentina como Autoridad Oficial de Certificación de la Firma Digital de los poseedores de una dirección de correo electrónico asignada de conformidad con lo establecido por el Decreto N° 1335/99. Mecanismos y Procedimientos para que cada habitante disponga de una Casilla de Correo Electrónico (Secretaría de Comunicaciones).
- Resolución 2226/2000. Registración de nombres de dominio en Internet (Ministerio de Relaciones Exteriores y Culto).

Los antecedentes normativos referidos a la firma digital que dieron lugar a la sanción de la ley de firma digital, son:

- Ley Nº 24.624 (B.O. 29/12/1995). Su art. 30 autoriza el archivo y conservación en soporte electrónico u óptico indeleble de la documentación financiera, de personal y de control de la Administración Pública Nacional, dándole pleno valor al documento electrónico archivado y lo transforma en original, autorizando la destrucción del original en papel.
- Resolución MTSS N° 555/97. Ministerio de Trabajo y Seguridad Social. Normas y Procedimientos para la Incorporación de Documentos y Firma Digital. Define el documento digital, la firma digital, el certificador de clave pública, el certificado, la clave privada, la clave pública y establece que los documentos digitales se considerarán válidos y eficaces, surtiendo todos los efectos legales y probatorios cuando estén firmados digitalmente. (Ver: http://www.pki.gov.ar/PKIdocs/Informe.html).
- Resolución SFP Nº 45/97 (B.O. 24/03/1997). Secretaria de la Función Pública. Incorporación de Tecnología de Firma Digital a los Procesos de Información del Sector Público. La Secretaria de la Función Pública adhiere y hace suyos los conceptos vertidos por el Sub-Comité de Criptografía y Firma Digital del CUPI en el documento "Pautas Técnicas en la Materia de Normativa de Firma Digital" y autoriza el empleo de ésta tecnología para la promoción y difusión del documento y la firma digitales en el ámbito de la Administración.(Ver:http://www.pki.gov.ar/PKIdocs/Res4597.htmlhttp://www.sfp.gov.ar/res45.html).
- Resolución SAFJP Nº 293/97 (B.O.29/05/1997). Superintendencia de Administradoras de Fondos de Jubilación y Pensiones. Incorporación del Correo Electrónico con Firma Digital. Implementa en el ámbito de la Superintendencia de Administradoras de Fondos de Jubilaciones y Pensiones el sistema de Telecomunicaciones de la SAFJP con el fin de establecer un correo electrónico entre las Administradoras de Fondos de Jubilaciones y Pensiones y éste Organismo. Establece que los CD-ROMs remitidos por las Administradoras de Fondos de Jubilaciones y Pensiones, debidamente identificados por el Sistema, serán válidos y eficaces, surtiendo todos los efectos legales y probatorios, a partir de la fecha y hora en que queden disponibles en las bandejas de entrada y que la firma electrónica o clave de seguridad habilitante para acceder al

sistema poseerá el mismo valor legal que la firma manuscrita.(Ver:http://infoleg.mecon.ar/txtnorma/43569.htm)

- Decreto MJ Nº 427/98 (B.O.21/04/1998). Ministerio de Justicia. Autoriza la utilización de la firma digital en la instrumentación de los actos internos del Sector Público Nacional, que no produzcan efectos jurídicos individuales en forma directa. La firma digital tiene los mismos efectos de la firma manuscrita, siempre que se hayan cumplido los recaudos establecidos y dentro del ámbito de aplicación en el Sector Público Nacional, dentro del cual se comprende la administración centralizada y la descentralizada, los entes autárquicos, las empresas del Estado, las Sociedades del Estado, las Sociedades Anónimas con participación estatal mayoritaria, los bancos y entidades financieras oficiales y todo otro ente, cualquiera sea su denominación o naturaleza jurídica, en que el Estado Nacional o sus organismos descentralizados tengan participación suficiente para la formación de sus decisiones. La correspondencia entre una clave pública, elemento del par de claves que permite verificar una firma digital, y el agente titular de la misma, se acredita mediante un certificado de clave pública emitido por un certificador de clave pública. Se establecen los requisitos y condiciones para la vigencia y validez de los certificados de clave pública (emisión, aceptación, revocación, expiración y demás contingencias del procedimiento), así como las condiciones bajo las cuales deben operar los certificadores de clave pública licenciados integrantes de la citada Infraestructura de Firma Digital para el Sector Público Nacional. El Decreto fue redactado por el Sub-Comité de Firma Digital del CUPI ("Comité de Usuarios de Procesamiento de Imágenes"), convocado por el Banco Central de la República Argentina y del que parciparon representantes de distintos organismos estatales. (Ver: http://pki.gov.ar/PKIdocs/Dec427-98html).
- Resolución SFP Nº 194/98 (B.O. 04/12/1998). La Secretaria de la Función Pública dicta los estándares Aplicables a la Infraestructura de Firma Digital para el Sector Público Nacional del Decreto Nº 427/98. La Secretaria de la Función Pública dicta los estándares de homologación de algoritmos criptográficos para la Infraestructura de Clave Pública de la Adm. Pública

Nacional.(Ver:http://infoleg.mecon.ar/txtnorma/54714.htmhttp://ol.pki.gov.ar/standard/actual.html).

- El Proyecto de Unificación del Código Civil y Comercial de 1998, el cual contiene normas referidas a la forma y prueba de los actos jurídicos incluyendo al soporte y firma digitales (Ver arts. 260 a 315).
- Resolución SFP Nº 212/99 (B.O.06/01/1999). Secretaria de la Función Pública. Políticas de Certificación para el Licenciamiento de Autoridades Certificantes. La Secretaria de la Función Pública dicta los estándares de licenciamiento y operación de las autoridades certificantes de la Administración Pública Nacional (Ver:http://ol.pki.gov.ar/policy/actual.html http://infoleg.mecon.ar/txtnorma/55346.htm).
- Resolución AFIP Nº 474/1999 (LA 1999-8-1502), Administración Federal de Ingresos Públicos, Régimen de Declaraciones Juradas Impositivas y Previsionales por Internet.
- Decreto Nº 673/01 (B.O. 24/05/2001). Poder Ejecutivo Nacional. 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.
- Decreto Nº 677/2001 denominado "Régimen de transparencia de la Oferta Pública" por el que se reconoce a los documentos digitales, firmados digitalmente de acuerdo a las reglamentaciones establecidas por la Autoridad de aplicación, que se remitan a la Comisión Nacional de Valores efectos equivalentes al papel.
- Decreto JGM Nº 889/01 (B.O. 11/07/2001) (LA 2001-B-1563). Jefatura de Gabinete de Ministros. Aprueba la estructura organizativa de la Secretaría para la Modernización del Estado de la Jefatura de Gabinete de Ministros (creada por decreto 673/2001) 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.

- Ley Nº 25.237 (B.O. 10/01/2000) (LA 2000-D-4372). Presupuesto. Establece en el artículo 61 que la Sindicatura General de La Nación 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.
- Decreto 103/01. P.E.N. B.O. 29/01/2001. Aprueba el Plan Nacional de Modernización de la Administración Pública Nacional.
- Decreto 673/01. P.E.N. B.O. 24/05/2001. 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.
- Decreto 677/01. P.E.N. B.O. 28/05/2001. 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 1023/01. P.E.N. B.O. 16/08/2001. En su artículo 21 permite la realización de las contrataciones comprendidas en el Régimen en formato digital firmado digitalmente.

LEY ARGENTINA.

La ley Nº 25.506 de firma digital se sancionó el 14 de noviembre de 2001, promulgada por el Poder Ejecutivo el 11 de diciembre del año 2001, y publicada en el Boletín Oficial el 14 de diciembre de 2001.

La Ley además de regular la firma digital, define a la firma electrónica, también regula el Documento Digital, los Certificados digitales, el Certificador licenciado, el Titular de un certificado digital, establece la Organización institucional, la Autoridad de Aplicación, el Sistema de Auditoria, la Comisión Asesora para la Infraestructura de Firma Digital, las responsabilidades, las sanciones, y contiene al final de la misma disposiciones complementarias.

El proyecto de ley se encontraba en el Senado desde el 23 de agosto pasado, enviado por la Cámara de Diputados, que ya le había dado media sanción.

Según el dictamen del proyecto ahora convertido en ley, para la redacción de la norma se tuvo en cuenta la Ley Modelo aprobada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, UNCITRAL, en cuanto es "un modelo de referencia que tiene en miras fomentar la armonización y unificación progresivas del derecho mercantil, garantizando la seguridad jurídica y proveyendo una legislación que facilite el uso del comercio electrónico en los Estados con sistemas jurídicos diferentes, propiciando el reconocimiento jurídico de los documentos electrónicos, estableciendo estándares mínimos de requisitos de forma, dejando librado al acuerdo entre las partes las especificaciones técnicas a través de las cuales se cumplen los requisitos mínimos establecidos, y estableciendo definiciones referidas al proceso de comunicación de mensaje de datos".

Entre los proyectos de ley considerados por las Comisiones de Comunicaciones e Informática y de Legislación General, referentes a la regulación de la firma digital se encontraban los de los siguientes presentantes:

1. Poder Ejecutivo Nacional, julio 1999. Presentado en Diputados.
2. Fontdevila y Parentella, junio 2000. Presentado en Diputados.
3. Del Piero y Molinari Romero, junio 2000. Presentado en Senadores.
4. Corchuelo Blasco, julio 2000. Presentado en Diputados.
5. Puiggros, septiembre 2000. Presentado en Diputados.
6. Cardesa, noviembre 2000. Presentado en Diputados.
7. Atanasoff, noviembre 2000. Presentado en Diputados.

<u>Su importancia.</u>

La fundamental importancia de ésta Ley reside en haber modificado el ordenamiento jurídico argentino, y entre ellos el Código Civil, en el sentido que su protección incorpora o se extiende a nuevos elementos digitales, como la firma digital y el documento digital.

Además, no podemos dejar de destacar que es una herramienta fundamental para la inserción del país en la sociedad de la información y la economía digital. Las nuevas tecnologías de la información se presentan como una oportunidad para que los países menos desarrollados, como el nuestro, puedan achicar la brecha que los separa con los denominados países del primer mundo, formando parte desde un primer momento en este nuevo mundo digital, para no quedar al margen del mercado global digital.

La firma digital es un instrumento más que permite la adaptación a éste nuevo paradigma socio-económico-cultural, que posibilita la expansión del comercio dentro de este nuevo mercado digital globalizado, que rediseña las relaciones humanas y, a su vez, en el ámbito administrativo o gubernamental, optimiza la eficiencia a un bajo costo, con intervención y participación de los administrados, lo que importa dotar al sistema de una mayor transparencia y obtener la consecuente reducción del gasto público y restablecer la credibilidad en las instituciones democráticas, algo que debe garantizar todo Estado social de Derecho[5].

Su decreto reglamentario.

El decreto Nº 2628/02 que reglamenta la ley 25.506 de Firma Digital, fue publicado en el Boletín Oficial el 20/12/2002. La reglamentación contiene consideraciones generales, la Autoridad de Aplicación, la Comisión Asesora para la Infraestructura de Firma Digital. Ente Administrador de Firma Digital, el Sistema de Auditoria, Estándares Tecnológicos, la revocación de Certificados Digitales, los Certificadores Licenciados, las Autoridades de Registro y disposiciones para la Administración Pública Nacional.

La reglamentación de la Ley N° 25.506 permite establecer una Infraestructura de Firma Digital que ofrezca autenticación, y garantía de integridad para los documentos digitales o electrónicos y constituirá la base tecnológica que permita otorgarles validez jurídica.

OBJETO DE LA LEY.

El art. 1 de la Ley establece el objetivo de ella, por el cual "Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley". Esta norma le otorga pleno valor y eficacia jurídica a la firma electrónica, a la firma digital, y al documento digital; agregando o extendiendo el concepto de documento, al documento digital, y al de firma, a la firma electrónica y a la digital, en las condiciones que más adelante establece.

TÉCNICA LEGISLATIVA.

Una de la cuestiones más debatidas en cuanto a la política legislativa en el Derecho Comparado, como también en la Argentina, ha sido referida a sí la Ley de Firma digital debe ser una ley de principios generales o bien una disposición que imponga tecnologías específica, como la criptografía asincrónica6.

Las distintas técnicas legislativas para el tratamiento de los métodos tendientes a lograr la protección de la información que circula en red, dio lugar a la disyuntiva entre los que adhieren a un sistema amplio de técnica legislativa y quienes adhieren a un sistema restrictivo.

Quienes optan por un sistema legislativo restricto, establecen que la ley debe regular una técnica específica de firma digital, estableciendo un procedimiento tecnológico concreto, como por ejemplo la criptografía asincrónica (o asimétrica) en la Ley de Firma Digital del Estado de Utah de 1995.

Quienes optan por un sistema legislativo amplio, se enrolan en la teoría de la neutralidad tecnológica, donde la ley brinda un marco general regulatorio en torno a la seguridad informática. Sostienen que una ley previsora solo debe proporcionar lineamientos generales, sin adherir a un método específico de protección del comercio electrónico. Para esta posición cualquier método de firma digital será válido siempre y cuando provea a un sistema (que veremos más adelante en extenso) de:

- ✓ Autenticidad: consiste en la seguridad de que las personas que intervienen en el proceso de comunicación son las que dicen ser.
- ✓ Confidencialidad: se trata de la seguridad de que el mensaje no sea interceptado por un extraño.
- ✓ No repudio: se refiere a que una ves enviado el mensaje o documento, el emisor no pueda negar haber sido el autor de dicho envío.
- ✓ Integridad*:* se trata de la seguridad de los que los datos que contiene el documento no sean modificados o alterados por terceros.

Estos son los parámetros que debe definir una ley neutral, dejando a la Autoridad de Aplicación la elección del método más adecuado según la realidad histórica del momento[7]. Estos se fundamentan en la evolución tecnológica, la cual pronto nos mostrará cada vez métodos más seguros, más rápidos o simplemente iguales

lo que nos permitirá elegir entre distintos métodos, y que seguramente diferirán según el país o región o el derecho imperante en los mismos.

En los fundamentos del proyecto luego convertido en ley se dice que se "intenta legislar para el presente y para el futuro, evitando el condicionamiento a la tecnología que se utiliza hoy en día pues ello llevaría a tener que modificarla a quizás breve plazo", es decir que se pretendió y se incorporó, el principio de neutralidad tecnológica.

Sin embargo, el sistema de firma digital de la ley, aseguran algunos especialistas, está estructurado en forma tal que, si bien se deja en manos de la Autoridad de Aplicación la facultad de "establecer, previa recomendación de la Comisión Asesora para la Infraestructura de la Firma Digital, los estándares tecnológicos y operativos de la Infraestructura de Firma Digital", esta Infraestructura está pensada para adoptar el sistema de criptografía de clave asimétrica. De hecho, el anexo de la ley 25.506 define conceptos como los de clave criptográfica privada, clave criptográfica pública y criptosistema asimétrico.

Esto es así porque actualmente la criptografía es el único mecanismo que se puede implementar, para que se asegure un medio tan inseguro como son las redes abiertas, pero no por eso la ley adoptó un sistema restrictivo de regulación.

La Ley Argentina, que como dije anteriormente, sigue principalmente el modelo de la CNUDMI o UNCITRAL, y se inclina por un sistema legislación amplia, consagrando el principio de neutralidad tecnológica, como es tendencia mayoritaria en el derecho comparado, estableciendo en el art. 2 in fine de la ley que "Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes". Ya que se intenta legislar para el presente y para el futuro, evitando el condicionamiento a la tecnología que se utiliza hoy en día, pues ello llevaría a tener que modificarla quizás a breve plazo, por el avance tecnológico.

CRIPTOGRAFIA.

INTRODUCCION.

La criptografía es la ciencia que estudia el resguardo de la privacidad e integridad de la información, es una incumbencia de la matemática que persigue asegurar la confidencialidad de textos, como así también la integridad de los datos y la identidad de los participantes en un intercambio de información.

El término criptografía proviene del griego "kryptos" que significa esconder u ocultar y "gráphein" escritura, y es definido por el Diccionario de la Real Academia Española como "el arte de escribir con clave secreta o de un modo enigmático"[8].

La criptografía estudia el modo de transformar un mensaje (texto original) en un texto en cifra o encriptado(criptograma) mediante una operación de cifrado que hace imposible a un tercero tomar conocimiento del contenido del mensaje. Generalmente, utiliza un algoritmo matemático para cifrar datos con el fin de hacerlos incomprensibles para cualquiera que no posea su clave, o sea, la información secreta necesaria para descifrar los datos cifrados.

Encriptar un texto significa aplicarle un algoritmo que, en relación a una cierta variable (clave de encriptación), lo transforma en otro texto incomprensible e indescifrable por parte de quien no posee la clave. La función es reversible, por lo cual la aplicación del mismo algoritmo y de la misma clave al texto cifrado devuelve el texto original.

Básicamente es cifrar un texto, transformarlo en ininteligible para luego descifrarlo, volviéndolo nuevamente inteligible.

La encriptación ha sido inventada y utilizada originalmente para fines de seguridad en las trasmisiones de mensajes militares.

Ya los espartanos habían ideado un ingenioso instrumento de criptografía, Plutarco en Vidas Paralelas dice que los magistrados de Esparta enviaron a Lisandro una scítala con la orden de regresar a la patria.

La scítala consiste en esto: Los magistrados, cuando enviaban un jefe militar al exterior, le entregaban un bastón de madera, al que llamaban cítala, otro exactamente igual lo conservaban ellos. Cuando quieren comunicar alguna cosa de gran importancia y que ningún otro debe saber, cortan un rollo de papiro y lo envuelven alrededor de la scítala que tienen en posesión, cubriendo toda la superficie del bastón

sin dejar ningún espacio. Cumplida esta operación, escriben sobre el papiro el mensaje, una vez escrito, envían el papiro sin el bastón. El general cuando lo recibe, no puede leer el mensaje hasta tanto no envuelva el papiro en su bastón..

En este ejemplo ya podemos reconocer los elementos constitutivos de cualquier sistema criptográfico:

- El algoritmo;
- la clave (llave)

El algoritmo es el conjunto de operaciones que permite hacer incomprensible el mensaje descomponiéndolo en una secuencia de caracteres no inteligibles inmediatamente, en el ejemplo que acabamos de ver sería el papiro.

La clave es el elemento que, asociado a un algoritmo criptográfico, permite la encriptación y la descencriptación del texto cifrado, en el ejemplo sería el bastón.

Este ha sido el primer ejemplo de criptografía, esto es de escritura escondida, registrado en la literatura. Y cuatro siglos después de Lisandro, es Giulio Cesare que utiliza otro método distinto de criptografía.

Así Svetonio, en la Vita Del Divo Giulio, describe el método empleado por Julio César cuando quería intercambiar mensajes con los comandantes de su legión. Para estos casos usa escribir en cifra, y esta cifra consistía en una disposición aparentemente caótica de las letras, que hacía imposible reconstruir la palabra original. Y quien quería descubrir el mensaje y descifrarlo tenía que saber que debía sustituir cada letra por la tercera anterior en el alfabeto y así sucesivamente.

Método traslación:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
A	B	C	D	E	**F**	G	H	**I**	J	K	L	**M**	N	O	P	Q	**R**

CLAVE = 3

FIRMA = ILUPD

Entre otros métodos más modernos se encuentra la escritura cifrada, que consiste en suplantar letras por cifras; o el cambio de significado de palabras importantes por otras corrientes; la realizada con la cartulina con rejilla superpuesta al papel, la cual resulta imprescindible para descifrarla, puesto que el resto del papel se rellena con

palabras sin sentido; los códigos o diccionarios, en donde las palabras y expresiones se sustituyen por reducciones de palabras, etc.

El uso de la criptografía es, como podemos ver con estos ejemplos, casi tan antiguo como la escritura, que ha renacido en nuestros días con un inusitado vigor debido a su aplicación por medio de sistemas informáticos y el desarrollo de nuevos métodos y algoritmos de cifrado de la información asegurando así los pilares fundamentales sobre los que se basa la criptografía:

- Seguridad: certeza de que el texto del mensaje solo puede ser leído por el destinatario.
- Integridad: certeza del mensaje, asegura que no ha existido ninguna manipulación posterior de los datos.
- Autenticidad: certeza del remitente, acredita quien es su autor.
- No rechazo: no se puede negar la autoría de un mensaje enviado[9].

DIVERSOS TIPOS DE CRIPTOGRAFÍA.

Dentro de este sistema existen dos métodos de cifrado:

1._ La Clave Simétrica o Cifrado Simétrico: Es el sistema de cifrado más antiguo, en el cual se utiliza la misma clave en las operaciones de cifrado y descifrado. Es un sistema sencillo para redes pequeñas y decae en cuanto a seguridad frente a terceros, debido a que las partes comparten la clave única. Esto es por que si bien éste sistema es un medio idóneo de autenticación entre las partes, presenta el inconveniente del intercambio de claves entre ellas ya que si se realiza en redes abiertas, existe la posibilidad de vulneración o interceptación, por lo cual la desventaja de utilizar este sistema de criptografía implica que si un tercero accede a esa clave secreta podrá descifrar el mensaje.

Este criptosistema es denominado de clave abierta o privada. Un ejemplo de éste sistema es el “D.E.S.” (Data Encryption Standard) desarrollado por I.B.M., otros son TDES, IDEA, RC2, RC4 y SkipJack.

2._ La Clave Asimétrica o Cifrado Asimétrico: Creado por Whitfield Diffie y Martin Hellman en 1976 (que mejora al anterior). Es el sistema en el que se utiliza una pareja de claves, una para cifrar y la otra para descifrar, éstas dos claves se asignan a

una persona siendo una pública y otra privada. La clave privada queda en poder del titular, conocida únicamente por éste (o aún desconocida por éste, si se mantiene en una tarjeta inteligente a la que se accede mediante un número de identificación personal o un dispositivo de identificación biométrica); y la clave pública, que se relaciona matemáticamente con la clave privada, y que puede ser accesible para cualquiera, ya que se da a conocer. De ésta manera, el titular de la clave privada puede enviar mensajes encriptados con su clave privada, y estos serán desencriptados con su clave pública. Esto es posible porque la criptografía de clave pública funciona de forma tal que lo que se encripta con la clave privada se desencripta con la pública y viceversa.

Si se desea aun mayor seguridad puede recurrirse al siguiente esquema: el usuario encripta el documento con su clave privada, y luego con la clave pública del receptor del mensaje. Cada clave (pública y privada) puede desencriptar lo que encripta la otra, por lo que el encriptado hecho con la clave privada del redactor del mensaje se desencripta con su clave pública, que como vimos es conocida por todos. Al recibir el mensaje doblemente encriptado, el destinatario lo desencripta con la clave pública del remitente. Este desencriptado puede hacerlo cualquiera que tenga la clave pública de quien envía el mensaje. Pero quien lo recibe además lo desencripta con su propia clave privada, que solo el posee (pues el mensaje fue enriptado con su clave pública).

Este criptosistema se llama de clave pública. Por ejemplo el "R.S.A." (Ron Rivest, Ad Shamir y Leonard Adelman, nombre de sus creadores), aplica la descomposición factorial de los números primos. En el sistema RSA, se toman dos numero primos (es decir aquellos que pueden ser divididos solo por uno y por si mismos) y se obtiene un producto. Cuando multiplicamos dos números primos entre sí, obtenemos un número que sólo es divisible entre ellos dos (por ejemplo 35 sólo es divisible por 5 y 7). La búsqueda de los números primos se llama descomposición factorial. Si bien es fácil obtener el producto de dos números primos extensos, es muy difícil descomponer un producto porque el cálculo lleva mucho tiempo.

SISTEMA ADOPTADO PARA LA LEY.

Dentro de los mecanismos criptográficos se ha decidido unánimemente por la *criptografía asimétrica o de clave pública,* que es la más segura y la única que se puede

implementar de manera que cumpla con las características de la firma ológrafa hoy en día.

Como dije en el punto anterior, éste sistema consta de un par de claves, una para encriptar el mensaje y la otra para desencriptarlo, cada clave realiza una transformación única e inversa a la otra clave, solo una clave puede desencriptar lo que su par ha hecho. Una clave, la privada, permanece secreta en poder del usuario y otra pública que es conocida por todos. La clave privada es aquella que se utiliza para firmar digitalmente y la clave pública es utilizada para verificar una firma digital.

El sistema funciona de la siguiente manera:

Al mensaje o documento que se quiere enviar se le aplica una "Función Hash" o "Función de Digesto Seguro" (que veremos en el punto siguiente), sobre éste digesto de mensaje se aplica la clave privada, encriptandoló y obteniéndose así la firma digital.

Luego se envía al destinatario el documento y el resumen hash encriptado o documento firmado digitalmente. Así mismo transmite su clave pública para ser utilizada en el proceso de verificación.

El receptor aplica la función hash al documento y desencripta el resumen encriptado, con la clave publica del emisor.

FUNCIÓN HASH:

Generalmente en el intercambio de información lo que se cifra no es el mensaje original, sino un resumen o hash o digesto seguro del mismo.

Un mensaje resumido mediante la función hash y encriptado con una llave privada es lo que en la vida real se denomina *firma digital,* dado que los sistemas de clave pública son muy lentos en vez de firmar digitalmente el texto completo se realiza sobre el hash.

La función hash es una función matemática o algoritmo criptográfico que transforma un documento digital en una secuencia de bits de longitud fija, transforma al documento que contiene palabras y eventualmente números, en un resumen numérico llamado extracto o digesto de mensaje o resumen hash.

A partir de un mensaje en texto plano, se obtiene su resumen al aplicar una función hash determinada. Este resumen se firma con la clave privada del emisor y se

envía el receptor. Simultáneamente se envía el mensaje original al receptor. Éste descifra el resumen mediante la clave pública del emisor, y aplica la misma función hash que él al mensaje recibido para obtener un resumen. Compara el resumen recién obtenido y el enviado por el emisor, si son iguales el mensaje es el inicial.

El mecanismo es el siguiente:

- El emisor genera un resumen del mensaje que quiere enviar con una determinada función hash, y lo cifra con su clave privada.
- El emisor envía el resultado anterior, junto con el mensaje original (cifrado o no con su clave privada) al receptor.
- El receptor descifra con la clave pública del emisor el resumen (y el mensaje si procede) recibido junto con el mensaje original.
- El receptor genera un resumen con la misma función hash que empleó el emisor, y lo compara con el resumen recibido.
- Si ambos resúmenes son iguales se acepta la firma.

Esta forma de realizar firma digital se denomina RSA. Existen otras formas de realizar firmas digitales como la denominada EIGamal que no es utilizada.

Las características de la función hash son:

- Unidireccional: Conocido un resumen, es computacionalmente imposible encontrar el mensaje a partir de dicho resumen.
- Compresión: A partir de un mensaje de cualquier longitud, el resumen debe tener una longitud fija. Lo normal es que la longitud del resumen sea menor que la del mensaje original.
- Difusión: El resumen es una función compleja de todos los bits del mensaje.
- Colisión simple: Conocido el mensaje, será computacionalmente imposible encontrar otro mensaje tal que su resumen sea igual al resumen de otro mensaje. Se conoce como resistencia débil a las colisiones.
- Colisión fuerte: Será computacionalmente difícil encontrar un par de mensajes cuyos resúmenes sean iguales. Se conoce como resistencia fuerte a las colisiones.

Las funciones hash más conocidas y usadas son:

- MD2, abreviatura de Message Digest 2, diseñado para ordenadores con procesador de 8 bits. Todavía se usa, pero no es recomendable, debido a su lentitud de proceso.
- MD4, abreviatura de Message Digest 4, desarrollado por Ron Rivest, uno de los fundadores de RSA Data Security Inc. y padre del sistema asimétrico RSA. Aunque se considera un sistema inseguro, es importante porque ha servido de base para la creación de otras funciones hash. Un sistema de ataque desarrollado por Hans Dobbertin posibilita el crear mensajes aleatorios con los mismos valores de hash (colisiones), por lo que ya no se usa. De hecho, existe un algoritmo que encuentra una colisión en segundos.
- MD5, abreviatura de Message Digest 5, también obra de Ron Rivest, que se creó para dar seguridad a MD4, y que ha sido ampliamente usado en diversos campos, como autenticador de mensajes en el protocolo SSL y como firmador de mensajes en el programa de correo PGP, Si embargo, fue reventado en 1996 por el mismo investigador que lo hizo con MD4, el señor Dobbertin, que consiguió crear colisiones en el sistema MD5, aunque por medio de ataques parciales. Pero lo peor es que también consiguió realizar ataques que comprometían la no-colisión, por lo que se podían obtener mensajes con igual hash que otro determinado. Realiza resúmenes de 128 bits. A pesar de todo esto, MD5 se sigue usando bastante en la actualidad.
- SHA-1, Secure Hash Algorithm, desarrollado como parte integrante del Secure Hash Standar (SHS) y el Digital Signature Standar (DSS) por la Agencia de Seguridad Nacional Norteamericana, NSA. Sus creadores afirman que la base de este sistema es similar ala de MD4 de Rivest, y ha sido mejorado debido a ataques nunca desvelados. La versión actual se considera segura, con resumen de 160 bits y es muy utilizada algoritmo de firma, como en el programa PGP en sus nuevas claves DH/DSS (Diffie-Hellman/Digital Signature Standar). Destacar también que en la actualidad se están estudiando versiones de SHA con longitudes de clave de 256, 384 y 512 bits.
- RIPEMD-160, desarrollada por un grupo de investigadores europeos, entre los que se encuentra Hans Dobbertin (el reventador de MD4-MD5) y otros investigadores incluidos en el proyecto RIPE (RACE Integrity Primitives Evaluation). Su primera versión adolecía de las mismas debilidades que MD4, produciendo colisiones, pero las versiones mejoradas actuales son consideradas seguras. Maneja claves muy robustas, normalmente de 160 bits, aunque existen

versiones de 128 y se están planteando nuevas de 256 y 320 bits. Es muy rápido, no está patentado y su código fuente es abierto, de libre acceso.

GENERACIÓN DE CLAVES Y SU ALMACENAMIENTO.

Toda persona que quiera firmar digitalmente debe generar su propio par de claves. Las Claves son una combinación de letras y números, es decir, un conjunto de bits, que a su vez constituyen un conjunto de ceros y unos. La generación del par de claves se hace una sola vez. La vida útil de un par de claves se extiende en general por varios meses o años, según sus características particulares.

El proceso de creación del par de claves lo realiza un software especial, la clave privada puede quedar almacenada en distintos medios como:

- Diskette

Presenta características que lo hacen, por el momento, el medio más práctico y económico: se puede leer en todas las computadoras, es fácilmente transportable y permite almacenar un gran volumen de información. Sin embargo no es un medio confiable ya que su uso intensivo puede causar pérdida de información. En caso de utilizarse se recomienda realizar copias de resguardo de la clave privada del titular.

- Disco Rígido

Al igual que el diskette se encuentra en todos los equipos aunque es más confiable con respecto al mantenimiento de la información. Sin embargo cuenta con varias desventajas:

  - no es transportable, lo que implica que el usuario sólo puede utilizar su clave privada desde una sola estación de trabajo,
  - la mayoría de los equipos no cuentan actualmente con un Sistema Operativo que impida el acceso de usuarios no habilitados a los archivos donde se almacene la clave privada. Aunque esta clave se encuentra protegida por un sistema criptográfico que restringe su uso al titular de la misma, no puede evitarse su destrucción voluntaria o involuntariamente.

Es recomendable contar con una política de seguridad para los equipos, no sólo a nivel de red, si se desea utilizar este tipo de dispositivos.

Los discos rígidos removibles solucionan el problema de la seguridad, pero igualmente deben ser utilizados personalmente.

- Smart Cards

Los Smart Cards (Tarjetas Inteligentes) son los dispositivos mejor considerados para esta tarea. Cuentan con varias características que hacen apropiado su uso para almacenar las claves privadas: son fácilmente transportables y seguros.

Incluso es posible incorporar dentro de estos dispositivos los algoritmos necesarios para la generación del par de claves, la firma y la verificación de manera tal de proteger la clave privada de todo acceso externo.

El inconveniente actual es la poca disponibilidad de lectores instalados sobre el parque actual de computadoras personales. Dichos lectores pueden ser incorporados a las computadoras de manera externa o interna. Es posible el uso de un dispositivo que es incorporado dentro del lector de diskette.

Con respecto a la seguridad de estos dispositivos algunas tarjetas tienen características que deben evitarse:

  - Baja entropía utilizada para la generación de los números primos a ser utilizados para la generación del par de claves
  - La protección de la clave privada se realiza utilizando una clave de solo 4 dígitos, algo que es fácilmente detectable con un ataque de fuerza bruta. Se deben evitar este tipo de mecanismos para la protección de una clave privada.

- Tarjetas de memoria

Estas tarjetas permiten solamente almacenar información, sin ninguna capacidad criptográfica. Cuenta con las mismas limitaciones que los Smart Cards en lo que respecta a los lectores y al almacenamiento seguro de la información. Es recomendable, por lo tanto, el uso de Smart Cards en lugar de estos dispositivos.

- Módulos Criptográficos en hardware

Estos dispositivos permite almacenar la clave privada y realizar todos los cálculos criptográficos dentro del mismo. Su capacidad, tanto en seguridad como en velocidad de cálculo, es superior a la una implementación y ejecución por software, lo

que lo hacen apropiados para aplicaciones críticas, de máxima seguridad donde se requiera dicha capacidad. Sin embargo, no son apropiados para almacenar las claves privadas de los usuarios ya que no son transportables.

METODOS BIOMÉTRICOS.

Los métodos biométricos son aquellos métodos de identificación que se basan en medir las particularidades biológicas de una persona. Se establece la identidad de la persona si la medición biométrica del momento se corresponde con los registros biométricos previamente obtenidos de esa persona.

A título ejemplificativo, la información biométrica puede consistir en la estructura vascular de la retina ocular, la estructura visible del iris, la composición espectral de la voz, la imagen facial o la dinámica de posición, velocidad y presión de generación de una firma manuscrita.

La información biométrica es única pero no es secreta: cualquier persona puede grabar la voz de otro, u obtener las huellas digitales de otra persona de, por ejemplo, un vaso. Por ello los métodos biométricos pueden utilizarse para la identificación de una persona para autorizar su acceso a una instalación física o su ingreso a un sistema informático propietario (como ser un sistema para transferir fondos electrónicamente entre un banco y otro) pero por sí solos no son utilizables para firmar digitalmente pues no conllevan un secreto no compartido. Por ello los mecanismos de firma que los utilizan en forma exclusiva crean firmas digitales que podrían ser desconocidas por el firmante.

Sin embargo, los métodos biométricos pueden utilizarse en conjunto con la criptografía de clave pública para crear firmas digitales. Normalmente la clave privada del firmante se guarda en un archivo en disco o en una tarjeta inteligente con microchip ("smartcard"). La clave privada debe almacenarse pues es binaria y de considerable longitud, por lo cual no puede ser memorizada por su titular. Por ello y a fin de impedir su utilización por un tercero, la clave privada se protege encriptándola con criptografía simétrica en base a una clave nemotécnica de acceso suministrada por el titular de la clave privada y sólo conocida por él.

Es factible utilizar métodos biométricos para asistir en la protección de dicha clave privada, es decir para activar la clave privada para la creación de una firma por su titular.

Adicionalmente los métodos biométricos tienen el beneficio de que, al requerir la presencia física del titular de una clave privada para activarla, impiden que una persona divulgue su frase de acceso y por ello su clave privada a un tercero conocido y confiable (por ejemplo, a su secretaria) a fin que el tercero impersone al titular cuando éste está ausente, por ejemplo de vacaciones, para que firme en su lugar.

LA FIRMA DIGITAL.

INTRODUCCIÓN.

La firma se puede componer del nombre y apellido de la persona y eventualmente de su rúbrica, o bien puede consistir en otro "trazado gráfico" o en "iniciales" o en "grafías ilegibles". Lo que se requiere es la nota de habitualidad como elemento vinculante de esa grafía con su autor. Igualmente, se ha planteado el interrogante de si la firma tiene que ser siempre autógrafa u ológrafa, es decir, puesta de puño y letra por el firmante, respondiéndose que la firma autógrafa no es la única manera de firmar ya que hay otros mecanismos que no son la firma autógrafa pero que constituyen "trazados gráficos" que dan autoría y obligan, como es el caso de las claves, los códigos, los signos y, entre otros, los sellos.

A tales efectos podemos dividir a la firma en dos grupos:

- Firma ológrafa: Es aquella realizada de puño y letra por el firmante.
- Firma no ológrafa: Es aquella por cualquier otro medio que no sea de puño y letra del firmante, a las cuales las podemos subdividir en:
  - Firma no ológrafa no electrónica: Es aquella realizada por cualquier otro procedimiento que no sea por un medio electrónico, como el sello o la huella dactilar.
  - Firma no ológrafa electrónica: Es aquella realizada por medio de un procedimiento electrónico, como la firma digital y la firma electrónica.

La firma (ológrafa, electrónica o digital) debe cumplir con las siguientes características:

1. Identificación: Es porque la firma en sí misma identifica a quien la ha realiza .
2. Presunción de autoría o atribución: Esta surge de relacionar un determinado trazo representativo de una persona a los

documentos que la contengan, por ello, si un documento determinado posee una firma se presupone que el mismo ha emanado del firmante, iuris tantum.

3. Conformidad con el texto que la antecede: Al encontrarse la firma al final del texto hace presumir, también admitiendo prueba en contrario la conformidad del firmante con el texto anterior a la firma en sí, aunque en algunos casos por falta de espacio se pueda firmar en forma marginal, para reconocer un texto a foja completa.
4. Presunción de Integridad del texto que avala: Al presumirse la conformidad, se presume asimismo la integridad del texto que conforma, el mismo sin enmiendas ni raspaduras o añadidos, ya que la presunción legal alcanza al contenido completo del documento firmado y que se presume completo y conocido por el firmante, quien a través del trazo otorga su conformidad[10].

FIRMA DIGITAL.

El concepto de firma digital nació como respuesta al avance tecnológico que ha generado nuevas forma de comunicación y comercialización, entrando así al mercado globalizado.

La firma digital es una secuencia de caracteres alfanuméricos asociados a un mensaje que garantizar la integridad, la autenticidad y el no repudio del mensaje.

La ley la define en su art. 2, diciendo que "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.

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

La firma digital no es un password, como tampoco lo es la clave privada, si bien ésta es necesaria en el procedimiento de firmado digital, siendo el resultado de dicho proceso La Firma Digital.

En consecuencia la firma digital es un procedimiento, que consiste en aplicar a un documento digital, la clave privada del firmante (a través de la utilización de la criptografía asimétrica), la cual es de su exclusivo conocimiento y solo él tiene acceso, de modo que no puede negar su autoría (no repudio), permitiendo al receptor por medio del procedimiento de verificación, acreditarle la identidad o autoría al firmante (autenticación) y detectar cualquier alteración del documento digital con posterioridad a la firma (integridad).

A la vista, una firma digital se representa por una extensa e indescifrable cadena de caracteres (letras y números), cual es el resultado del procedimiento matemático aplicado al documento.

FIRMA Y VERIFICACIÓN:

Toda persona que quiera firmar digitalmente primero debe generar su propio par de claves. Luego al mensaje o documento que se quiere enviar se le aplica una "Función Hash" o "Función de Digesto Seguro", que es un algoritmo criptográfico que transforma al documento que contiene palabras y eventualmente números, en un resumen numérico llamado extracto o digesto de mensaje o resumen hash, Sobre éste digesto de mensaje se aplica la clave privada, encriptandoló y obteniéndose así la firma digital.

Luego se envía al destinatario o receptor el documento original plano o inicial y el resumen hash encriptado o documento firmado digitalmente. Así mismo transmite su clave pública para ser utilizada en el proceso de verificación.

El receptor, en el proceso de verificación, aplica la función hash al documento original plano o inicial y desencripta el resumen encriptado, con la clave publica del emisor. Si ambos resúmenes coinciden es válido y está seguro que el documento ha sido enviado por el emisor o titular de la clave privada, y si no coinciden está seguro de que no ha sido enviado por el emisor o que en el envío ha sido interceptado y modificado, por lo que el documento no es válido.

Cómo se hace para usar la firma digital:

Se usa un *software* (programa de computación) especial.

Una vez que se redacta el documento a enviar (archivo de texto: escrito a presentar al juzgado o resolución para notificar), se elige la opción adecuada (en

Outlook Express: Herramientas --> Firmar digitalmente) y simplemente se hace clic con el mouse.

¿Qué sucede cuando se hace clic con el mouse?

Dos cosas que el usuario no ve, pero que el *software* hace:

a) El documento (escrito a presentar al juzgado o resolución para notificar), que obviamente contiene palabras y eventualmente números, es procesado por medio de un algoritmo y convertido en un resumen numérico (función de *hash).* Es prácticamente imposible o computacionalmente no factible encontrar otro documento que, algoritmo de hash mediante, genere el mismo resumen numérico; se dice que un cálculo matemático es "computacionalmente no factible" cuando para ser llevado a cabo se requeriría un tiempo y recursos informáticos que superan ampliamente a los disponibles en la actualidad.

b) A ese resumen numérico obtenido por medio de la función de *hash,* se le aplica la clave privada del autor del documento.

El resultado de ese proceso es la firma digital.

La firma digital es el resultado de la transformación de un documento digital (archivo de texto), empleando una función de *hash* y la clave privada de su autor, de forma tal que el destinatario al que se le envíe el documento digital firmado -por un lado- y el documento digital inicial y la clave pública del firmante -por otro lado- pueda determinar con certeza:

a) si la transformación se llevó a cabo utilizando la clave privada que corresponde a la clave pública del firmante;

b) si el documento digital inicial ha sido modificado desde que se efectuó la transformación.

La firma digital no es algo que se agrega al documento, como la firma ológrafa que se inserta al pie del papel. La firma digital es el documento digital una vez procesado a través de la función de *hash* y una vez que se le ha aplicado luego la clave privada de su autor. Decir firma digital es decir documento digital cifrado mediante clave privada.

A continuación, el autor del documento (ya firmado digitalmente) debe enviarlo a su destinatario, para lo cual debe hacer un nuevo click con el mouse (en Outlook Express, sobre el ícono Enviar).

¿Qué es lo que se envía?

El documento + el resumen numérico del documento firmado digitalmente (también se envía el certificado digital).

¿Qué sucede cuando el destinatario recibe todo eso que se le envió?

Entra a funcionar su propio *software,* el cual:

a) genera un nuevo resumen numérico del documento recibido usando la misma función de *Hash;*

b) después descifra, con la clave pública del autor del documento (ya conocida por el destinatario del documento o contenida en el certificado de firma digital que también envía el autor del documento) el resumen numérico firmado digitalmente;

c) si el resumen numérico firmado digitalmente coincide con el resumen que se ha generado por el destinatario la firma digital es válida: el mensaje no ha sido alterado[11].

CARACTERÍSTICAS DE LA FIRMA DIGITAL.

El método de la firma digital garantiza la *integridad* del documento, ya que si el documento fuera interceptado y modificado en el camino, el resumen del documento sería distinto al resumen firmado.

Asimismo, garantiza la *autenticidad* y el *no repudio* del mensaje enviado, debido a que solo el dueño de la clave privada pudo firmar un documento que viene firmado por él, lo que garantiza que ha sido él y no otro el que ha enviado dicho documento. Si la firma es válida, el titular de la clave privada utilizada para firmar un documento no podría desconocerla. Pero podría negar la autoría del envío de un documento cifrado con su clave privada alegando que se la hayan sustraído y hayan firmado por él, pero entonces hay que tener en cuenta que él es la única responsable del buen uso de su llave privada, por lo que está obligado a comunicar inmediatamente a la autoridad correspondiente cualquier circunstancia que ponga en peligro la seguridad de la misma.

Esto es análogo a lo que ocurre con las tarjetas de débito o crédito, siendo siempre en último extremo responsable del uso indebido de las mismas el dueño de la tarjeta si no ha avisado a tiempo a su entidad financiera o banco de la perdida o sustracción.

De allí que resulte indispensable la existencia de un sistema de administración de claves que establezca reglas claras y concretas sobre el funcionamiento y utilización de las claves, de forma tal que se puedan atribuir válidamente efectos a determinadas situaciones preestablecidas.

Aparece aquí la figura de la "autoridad certificante" (que veremos más adelante), persona autorizada o licenciada, encargada de certificar a quien pertenece la clave publica y las condiciones de su vigencia, a través de la emisión de un "certificado digital".

La firma digital no garantiza la confidencialidad o privacidad de la información, debido a que el mensaje puede ser interceptado y leído por un tercero durante su transmisión. Una solución a esto es encriptar el mensaje con la clave pública del receptor. Es decir, después de firmado digitalmente un documento se podría encriptar dicha información con la clave pública del destinatario. Esto significa que los caracteres de la información firmada (documento digital o digesto de mensaje, firma digital y certificado de clave pública) se mezclan con los de la clave pública del destinatario, obteniéndose una combinación de caracteres ininteligibles. Sólo el destinatario, mediante la aplicación de su clave privada, que únicamente él conoce y que corresponde a la clave pública con la que se ha cifrado el mensaje, podría descifrar el mensaje.

PRESUNCIONES.

El art. 7 de la ley de firma digital establece la presunción de autoría, diciendo que "Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma".

La norma introduce el término "certificado digital" (el cual veremos más adelante) y regula una presunción iuris tantum, para cuando el procedimiento de verificación de la firma le otorgue autoría al titular del certificado digital.

El art. 8 establece una presunción de integridad, al decir que "Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital

es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma".

La ley establece una presunción iuris tantum, para cuando del procedimiento de verificación de una firma aplicado a un documento digital resulte que éste no ha sido modificado desde el momento de su firma, ya que si ambos resúmenes hash del documento digital coinciden, es verdadero, es válido y está seguro que el documento ha sido enviado por el emisor o titular de la clave privada, y si no coinciden es por que en el envío ha sido interceptado y modificado, por lo que el documento no es verdadero.

En el art 10 reza que "Cuando un documento digital sea enviado en forma automática por un dispositivo programado y lleve la firma digital del remitente se presumirá, salvo prueba en contrario, que el documento firmado proviene del remitente".

Esta presunción también iuris tantum, reafirma la presunción de autoría del art. 7.

REQUISITOS.

La ley establece los requisitos de validez de la firma digital en su art. 9, y dice que "Una firma digital es válida si cumple con los siguientes requisitos:

a) haber sido creada durante el periodo de vigencia del certificado digital válido del firmante;

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

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

No solo tiene que haber un certificado digital, sino que la firma digital tiene que haber sido estampada durante su período de vigencia pues en caso contrario no vale como tal. El inc. c) requiere, además, que dicho certificado digital haya sido emitido o reconocido por un certificador licenciado. Al terminar esta disposición se consigna que una autoridad de aplicación regulará todo lo referido a cuestiones tecnológicas. Esto nos está introduciendo en el tema de la infraestructura: no puede haber firma digital sin un certificado digital y éste sólo puede ser válido si ha

intervenido un "certificador licenciado", y los procedimientos sólo podrán ser los determinados por la "autoridad se aplicación". Todo ello es lo que se conoce como la infraestructura de firma digital[12].

EFECTOS.

Sin duda uno de los efectos más importantes de la ley es la equiparación de la firma ológrafa y la firma digital en cuanto a su valor jurídico, que si bien ya había sido otorgado por el decreto Nº 427/98 para los actos internos de la Administración Pública Nacional, el art. 3 de la ley de firma digital lo amplia al campo privado, y dice que "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 25.506 modifica los Códigos y leyes de fondo incorporando o ampliando al concepto tradicional de firma, la firma digital. Consagrando el principio de no discriminación, por lo que cuando una ley requiera la solemnidad de la firma, se puede cumplir con la realización de una firma manuscrita o una firma digital. Las únicas excepciones a la equiparación son las exclusiones establecidas en el art 4 que veremos a continuación.

EXCLUSIONES.

El art. 4 establece que "Las disposiciones de esta ley no son aplicables:

a) a las disposiciones por causa de muerte;

b) a los actos jurídicos del derecho de familia;

c) a los actos personalísimos en general;

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

Nuestra ley de firma digital se autoexcluye, en los 3 primeros incisos, en las cuestiones relativas a las disposiciones por causa de muerte, a los actos jurídicos del derecho de familia y a los actos personalísimos en general. En el derecho comparado no se ofrecen soluciones únicas y nuestra ley ha optado por respetar la formalidad jurídica

tradicional, la cual requiere la presencia de los interesados para la realización de ciertos actos.

El inciso d) de este artículo fue tomado del artículo 6 del Proyecto de Ley de Firma Digital del Poder Ejecutivo (1999). La redacción de dicho proyecto comenzó en 1997 y en ese entonces se prefirió limitar el ámbito de aplicación de las firmas digitales a los instrumentos privado. Al hacerse referencia a "formalidades incompatibles con la utilización de la firma digita" se tuvo en cuenta fundamentalmente a los actos que deben instrumentarse en escritura pública, bajo pena de nulidad, y aquellos actos en los que las partes optan por instrumentarlos por escritura pública aunque el CC no lo imponga (por ej. un boleto de compraventa de inmuebles, que puede ser otorgado por instrumento privado o por escritura pública, si las partes así lo resuelven). Las legislaciones han evolucionado en los últimos años, ésta evolución se advierte incluso en nuestro país. Así, por ejemplo, el Proyecto de Reforma del Código Civil confiere validez jurídica a la firma electrónica ("En los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho si se utiliza un método para identificarla; y ese método asegura razonablemente la autoría e inalterabilidad del instrumento"), sin discriminar según el tipo de documento respecto del cual la firma haya sido creada, y expresamente establece la posibilidad del instrumento público electrónico y la firma electrónica del oficial público. En cuanto a las escrituras públicas, remite a las reglamentaciones locales la formación y archivo del protocolo. Ello significa que estaría contemplando la posibilidad de un protocolo en un soporte distinto al papel y con firmas electrónicas de los otorgantes y escribano. La escritura pública es instrumento público, pero existen otros instrumentos públicos además de la escritura pública[13].

Por lo que todos los actos jurídicos lícitos pueden celebrarse válidamente por medio de documentos digitales, los que valdrán como instrumentos públicos o privados, siguiendo así, el criterio amplio propuesto por la CNUDMI y receptado por distintos ordenamientos internacionales, entre ellos el chileno.

FIRMA ELECTRÓNICA.

La ley define a la firma electrónica en su art. 5 estableciendo que “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 caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez".

De manera que, si bien tanto la firma digital como la firma electrónica gozan de valor jurídico según lo dispone el art 1, la diferencia entre una firma y otra es que a la firma electrónica le falta alguno de los requisitos legales de la firma digital establecidos en el art. 9. Siendo la firma electrónica el género y la firma digital una especie dentro del género firma electrónica.

Otra diferencia entre la firma digital y la firma electrónica se da en el tema de las presunciones, mientras que en la firma digital se presume por el art. 7 la autoría y por el 8 al integridad, en la firma electrónica no, correspondiendo a quien la invoca acreditar su validez. Esto no es aparte de lo dicho en el párrafo anterior, ya que es consecuencia de aquello que carezca de presunciones, y que por el hecho de carecer de por lo menos uno de los requisitos legales del art. 9, hace que no cumpla con las características o funciones que dotan de segura a una firma digital.

Parecería que la ley solo define la firma electrónica en el art.5 y la invoca en el art. 1 reconociendo su el empleo y dotándola de valor jurídico en las condiciones que establece la presente ley, dejándola luego al margen de la legislación, pero esto no es así, si no cuales serían las condiciones que establece la ley para la firma electrónica, en efecto, ésta firma, que no llega a ser digital, también cumple con la exigencia de firma, quedando también equiparada a la firma manuscrita, en las condiciones que marca el art. 3; si bien otros autores dicen que solo tendrá valor en los actos jurídicos en los que no se requieran formas solemnes.

FIRMA DIGITAL Y FIRMA OLOGRAFA.

La Firma ológrafa o manuscrita, es una expresión de voluntad en un medio o soporte papel. La Firma Digital manifiesta la misma intención y expresión de voluntad para el medio electrónico.

La tecnología propuesta de firma digital no es perfecta ni infalible. Los dispositivos en hardware y en software de creación y verificación de firmas digitales deben ser homologados previa auditoria de su funcionamiento para poder ser utilizados para crear firmas y verificar firmas digitales con plena eficacia jurídica, sin embargo, el requisito de homologación no debe constituirse en una barrera que impida implementar los rápidos avances en el ámbito internacional

Por otro lado, es importante destacar que la firma manuscrita tampoco es perfecta o infalible, puesto que es decididamente posible en ciertos casos alterar de forma indetectable el contenido de un documento en soporte papel o falsificar una firma manuscrita. Adicionalmente, debe considerarse que siempre existe un margen de error en la labor de los peritos caligráficos, con lo cual una firma apócrifa puede darse por auténtica y viceversa.

Es usual, por ejemplo, que importantes contratos de compra-venta entre empresas en soporte papel sean firmados por las partes solo en su última página, contando solamente con iniciales en las restantes, lo que a simple vista resulta riesgoso considerando que generalmente el precio establecido en el contrato tiende a no figurar en la última página, sino en alguna página anterior.

Adicionalmente, en Internet es de público acceso la información que indica que es técnicamente posible sintonizar un láser para que se corresponda con el color de una tinta, tal que al accionar el láser, la tinta literalmente se vaporiza y se levanta del papel sin dejar rastro detectable alguno.

Sin embargo, las aludidas imperfecciones de los mecanismos de firma manuscrita en documentos en soporte papel no impiden los actos jurídicos, ni gubernamentales ni comerciales que se basan en ella, ni que la firma manuscrita figure como requisito en las leyes y reglamentos de éste país o de otros, por lo que es de inferir que la alternativa propuesta de firma digital de documentos digitales tampoco precisa ser perfecta e infalible para ser de gran utilidad.

Lo que es importante notar es la necesidad de gradualismo y proporcionalidad en la especificación de los sistemas y parámetros de firma digital en relación con el tipo de acto en particular, teniendo en consideración las consecuencias jurídicas del acto y/o el valor económico involucrado. De la misma manera que además de requerir soporte papel y firma manuscrita la venta de un inmueble requiere la intervención de un escribano público y la utilización de un protocolo notarial, pero una compra de un electrodoméstico con tarjeta de crédito no, análogamente serán diferentes los requisitos para otorgar validez jurídica a los documentos digitales firmados digitalmente, dependiendo de la naturaleza del acto o de la transacción subyacente[14].

APLICACIONES Y BENEFICIOS DE LA FIRMA DIGITAL.

La Firma Digital, en concreto, sirve para la *Identificación Indubitable* de una persona que emite un mensaje, transacción o documento en medios electrónicos, con el importante incremento de la impersonalización que se produce día a día, imaginándonos que ciertas actividades se han realizado durante años por la simple emisión verbal y hoy requieren de un respaldo mayor, adicionándole la facilidad de ahorros importantes en el tiempo, costos y exactitud en la trasmisión.

Al facilitar la autenticación a distancia entre partes que no necesariamente se conocen previamente, las firmas digitales constituyen el mecanismo esencial para proveer seguridad y desarrollar la confianza en las redes abiertas. Por ello constituyen un elemento clave para el desarrollo del comercio electrónico en Internet, y proporciona un amplio abanico de servicios de seguridad, que superan con creces a los ofrecidos en un contexto físico por el DNI o pasaporte y las firmas manuscritas.

En el ámbito nacional el comercio electrónico ya se está manifestando, existiendo supermercados, aerolíneas, agentes bursátiles y bancos que ofrecen sus productos y servicios directamente por Internet permitiendo así la compra de alimentos y artículos del hogar, de pasajes aéreos, de títulos valores bursátiles y de transferencias de fondos entre cuentas bancarias y el pago de facturas de servicios.

Pero el comercio electrónico no es el único beneficiario de la firma digital, actualmente las empresas y los organismos públicos de nuestro país 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 resultando en un acceso a la información mas lento y costoso. Los requerimientos legales que exigían la utilización del papel con firma manuscrita impedían la implementación de los modernos sistemas informáticos mediante los cuales se puede acceder a documentos a distancia y a la información en forma inmediata, dando lugar por ejemplo a nuevas modalidades de desempeño laboral como ser el tele-trabajo (tele-commuting) o los entornos virtuales compartidos.

En el ámbito de la Administración Pública (relación administración - administrado), la firma digital tiene enormes aplicaciones, algunas de las cuales son, presencia de la Administración en la red, consulta de información personal desde Internet, realización de cualquier trámite por Internet (pago de tributos), acceso a aplicaciones informáticas de gestión por ciudadanos y empresas, comunicación entre

dependencias de distintas administraciones, integración de información al ciudadano desde distintas administraciones, democracia electrónica (plebiscitos, sufragio).

Y es aquí donde se produce el mayor beneficio de la utilización de la firma digital, tanto estas nuevas modalidades de trabajo como el incremento en la velocidad de circulación de la información que permite hace factible el documento digital permitirían que las organizaciones de nuestro país ofrezcan un mejor nivel de servicios a sus clientes y simultáneamente reduzcan sus costos, aumentando su productividad y su competitividad en lo que hoy son mercados cada vez mas globalizados y competitivos.

Es así que vistos los tiempos en que vivimos, es aplicable entre otras a :

• Firma y/o Cifrado de Correo Electrónico, tanto Interno como Externo.

• Firma y/o Cifrado de Documentos (Pericias, Dictámenes, Planos, Software, Políticas, Procedimientos, Normativas, Minutas, y otros).

• Identificación de Personas ante Sistemas Internos en redes locales y abiertas (Intranets), Sitios Web (sin necesidad de registrar datos). Determinación implícita del Perfil de Usuario.

· Identificación de Sistemas ante el Usuario.

• Auditoría de Transacciones EDI (Electronic Data Interchange)..

• Seguridad al operar Comercialmente (Compra-venta de Acciones, Transacciones Bancarias, Operaciones con Tarjeta de Crédito, y otras).

• Identificación de los componentes físicos de una red (Computadores, Ruteadores, Teléfonos Celulares, y otros).

Y tantas otras aplicaciones como las del documento digital firmado digitalmente (que mencionamos más adelante) como:

• Receta Médica Electrónica.

• Historia Clínica única.

• Declaraciones Juradas.

• Solicitudes de Prestación de Servicios.

• Proyectos.

• Diseños.

• Tarjetas de Crédito (sin utilizar el número y consecuentemente disminuir el fraude).

• Factura Electrónica.

• Cheque Electrónico.

• Contratos.

• Etc[15].

FIRMA DIGITAL Y PODER JUDICIAL.

El sistema de la firma digital ha sido reconocido por prestigiosas instituciones jurídicas como una importante alternativa para la desburocratización de la justicia y para la agilización de muchos trámites.

Las Provincias Argentinas aglutinadas en la JUFEJUS y el Ministerio de Justicia de la Nación ya han tratado el contenido de un protocolo técnico que permite establecer las bases de las comunicaciones electrónicas interjurisdiccionales.

Ha jugado un papel vital en este proceso la Subsecretaría de la Función Pública, desde esta oficina dependiente de la Jefatura del Gabinete de Ministros, se ha trabajado intensamente, primero desarrollando la tecnología de la Firma Digital, luego dando apoyo técnico y operativo a las áreas informáticas de los tribunales provinciales, además de capacitación en la materia.

El Consejo de la Magistratura suscribió un convenio con el fin de facilitar la comunicación a través de medios electrónicos entre los distintos poderes judiciales del país.

De esta forma, el plenario del cuerpo decidió suscribir el convenio de "Comunicación Electrónica Jurisdiccional", que se había rubricado el 6 de septiembre de 2003 en la sede del Ministerio de Justicia por la Procuración General de la Nación, la Defensoría General de la Nación y veinte representantes de las justicias provinciales, pero sin la participación del Poder Judicial nacional.

Las distintas jurisdicciones están respondiendo prestamente a la convocatoria, así las provincias de Santiago del Estero, Río Negro y Chubut ya han dictado acordadas y resoluciones creando áreas de implementación, registro y control de firmas digitales. Las provincias de Neuquen y Buenos Aires y el Consejo de la Magistratura de la Ciudad Autónoma, participan activamente en la elaboración de documentos que fijan los procedimientos a aplicar por las oficinas de registro.

A partir de noviembre de 2003 el Poder Judicial de la Provincia de Buenos Aires comenzará a utilizar la firma digital para aprovechar las nuevas posibilidades, para la agilización de trámites y optimización de recursos. Así lo resolvió la Suprema Corte de Justicia Bonaerense por medio del acuerdo nº 3098. Según el acuerdo nº 3098, esto se limitará a documentos digitales de uso interno comunicados por correo electrónico, cuya emisión o recepción se realice por medios oficiales habilitados, quedando excluida toda documentación relativa a trámites jurisdiccionales o que produzcan efectos jurídicos individuales en forma directa a personas o entes ajenos al Poder Judicial.

Asimismo, el Superior Tribunal de Justicia de la Provincia del Chubut ya ha implementado una autoridad certificante de firma digital (ACSTJCh) y ha creado el REFIDI (Registro de Firma Digital). Esto fue posible gracias al convenio que firmara el Alto Cuerpo Provincial con la Subsecretaría de la Función Pública dependiente de la Jefatura de Gabinete de Ministros a principios del año 2000. La cesión de tecnología y "know how" que se realizara mediante ese acuerdo ha hecho posible alcanzar este objetivo. En este marco el Poder Judicial la Provincia de Santa Cruz se encuentra interesado en utilizar dicha tecnología aprovechando la infraestructura de esta autoridad certificante en el marco de las actividades de intercambio y cooperación que realiza el Foro Patagónico de Superiores Tribunales de Justicia.

Aplicaciones prácticas de esta tecnología dentro de la Justicia:

La iniciativa llevada adelante por el Ministerio de Justicia de la Nación y por la JUFEJUS, tiene por objetivo concreto agilizar los trámites jurisdiccionales que implican a Tribunales de los distintos estados provinciales; así, las comunicaciones que prevé la ley 22172, encontrarán una herramienta apropiada.

De tal forma se complementarán el Correo Electrónico y la Firma Digital asimétrica para emitir a modo de oficio (art. 1 de la ley 22.172) en este caso electrónico, las comunicaciones entre los distintos tribunales. La signatura alcanzará al documento que se envía como a los documentos que se adjunten electrónicamente, es decir archivos de procesador de textos, planillas de cálculo u otros.

Es decir el protocolo técnico que se acordará, contempla un nuevo soporte para la misma expresión en materia de comunicaciones interjurisdiccionales.

A estos efectos la Subsecretaría de la Función Pública proporcionará los Certificados de Firma Digital acreditantes de los requisitos de validez del documento alcanzado por la signatura digital o como en el caso del Poder Judicial del Chubut los certificados serán generados por esa Autoridad Certificante del Superior Tribunal de Justicia produciéndose un reconocimiento cruzado, situación ésta que alcanzaría a otros poderes judiciales a medida que se constituyan en Autoridades Certificantes, si lo consideran necesario.

La aplicación de esta tecnología se extiende a otras actividades en el ámbito de la justicia con innumerables beneficios, por ejemplo para trámites administrativos internos (notas y oficios ante los organismos de la Administración del Poder Judicial) o para aquellos que se realizan ante registros dependientes del Poder Judicial, abaratando

costos para los Profesionales y para el propio Poder Judicial. A modo de ejemplo, la asociación del correo electrónico y la firma digital para realizar los procedimientos ante el Registro de Juicios Universales o de Alimentantes Morosos (cuando el registro depende de la justicia) o cualquier otro.

Estas comunicaciones tienen especial importancia sobre todo en lo que se refiere a la traba de medidas cautelares, ya que en muchos casos deben trabarse con suma celeridad para evitar que se tornen ilusorios los derechos de los peticionantes.

Notificaciones Judiciales.

Para la actividad jurídica y especialmente del Poder Judicial, el afianzamiento de esta tecnología aporta los medios materiales para que en ámbito del proceso, los principios de seguridad y celeridad se realicen en su expresión más moderna. Ya no será necesario renunciar a la seguridad para hacer más rápidos los procesos judiciales, ya estamos en condiciones de afirmar que ha desaparecido aquella ecuación proporcionalmente inversa, por la cual la seguridad hacía decrecer la celeridad y viceversa.

Otorgada la validez jurídica al procedimiento de Firma Digital, la aplicación inmediata a las notificaciones judiciales es tan posible, como lo es la implementación de los sistemas que permiten administrarla.

La tecnología de administración de correo electrónico complementada con sistemas que administren la tecnología de signatura a que referimos, no resultan de una complejidad tal que impida avanzar sobre el proyecto en el mediano plazo. En una primera etapa, se pueden realizar las notificaciones que tienen destino en domicilios constituidos, para lo cual se invitaría a los profesionales a adherir al sistema, manteniendo por supuesto el modelo actual para quienes no deseen hacerlo.

Pero no necesariamente allí finaliza la utilidad de esta herramienta, ya que se ampliará su utilidad a otras las transacciones que se registran en una causa, como por ejemplo: la notificación tácita consulta en mesa de entradas virtual.

La constitución de una “dirección de correo electrónico2 operará a modo de domicilio constituido con efectos jurídicos similares en este caso. En esta instancia sólo diremos que se trata de un domicilio “sui generis”, ya que es preciso avanzar sobre esta institución con mayor rigor científico, a efectos de determinar los elementos, similitudes y diferencias con el domicilio.

Con el tiempo la notificación mediante correo electrónico firmado digitalmente, podría hacer que desapareciera o se acotara también, la forma automática de notificación; ya que la celeridad, valor que fundamenta su existencia, se vería incrementada sin desmedro de la seguridad y por qué no, con mayor grado de la misma, manteniendo un absoluto respeto de la garantía del debido proceso.

Este medio de notificación sería el más rápido, seguro, eficiente y eficaz, en consecuencia podría provocar el desplazamiento de los demás a situaciones puntuales y específicas.

Los Altos Cuerpos de las distintas jurisdicciones tendrán a su cargo complementar la operatoria de los procesos de firma digital, mediante preceptos de tercer nivel (acordadas) en las que deberán establecerse además las normas mínimas de seguridad, las responsabilidades derivadas del uso, la autoridad de control y administración de este nuevo sistema y sus efectos.

Otras aplicaciones:

*Presentaciones judiciales: La habilitación de la Signatura Digital para otras actuaciones judiciales, abre otras posibilidades y expectativas. Así, se puede imaginar la presentación de escritos en mesas de entradas virtuales para ser incorporados a expedientes completamente informatizados, hasta se podría hacer en horas inhábiles.

*Mejor aprovechamiento los recursos humanos existentes en tareas de mayor complejidad, revalorizando y jerarquizando la función de los empleados que integran la Administración de Justicia.

*Se acortarán los tiempos de los procesos.

En lo inmediato debería comenzar la conformación de equipos de trabajo interjurisdiccionales que se dispongan a construir los estándares para la conformación de los Documentos Digitales Judiciales (DDJ). Se trata de los requisitos tecnológicos y procesales a los que deberán responder los mismos, cuando el medio elegido para su presentación sea el electrónico.

- Resolución SFP 45/97. Secretaría de la Función Pública. B.O. 24/03/1997. 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.
- Resolución SFP 194/98. Secretaría de la Función Pública. Establece los estándares sobre tecnología de Firma Digital para la Administración Pública Nacional.

- Decreto 427/98. M J. B.O. 21/04/98.

Administración Pública Nacional - Firma Digital – Regimen. Régimen al que se ajustará el empleo de la firma digital en la instrumentación de los actos internos, que no produzcan efectos jurídicos individuales en forma directa, que tendrá los mismos efectos de la firma ológrafa. Autoridad de aplicación.

Artículo 1º- Autorízase por el plazo de DOS (2) años, a contar del dictado de los manuales de procedimiento y de los estándares aludidos en el artículo 6º del presente Decreto, 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, en las condiciones definidas en la Infraestructura de Firma Digital para el Sector Público Nacional que como Anexo I integra el presente Decreto. En el régimen del presente Decreto la firma digital tendrá los mismos efectos de la firma ológrafa, siempre que se hayan cumplido los recaudos establecidos en el Anexo I y dentro del ámbito de aplicación definido en el artículo 3.

Nota: Por art. 1° de la Decisión Administrativa N° 102/2000 B.O. 25/01/2001, se prorroga por 2 años a partir del 31 de diciembre de 2000 el plazo establecido en el art. 1°.

- Ley 25.237. B.O. 10/01/2000. Presupuesto.

Artículo 61. - Establécese que la Sindicatura General de la Nación 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.

- Decreto 103/01.- B.O. 29/01/01. Aprobación del plan nacional de modernización de la administración publica nacional.

  Anexo A: anexo I. Plan nacional de modernización del Estado.

Gobierno electrónico: Democratización de la información e impacto de las nuevas tecnologías son conceptos de los que mucho se habla, pero poco es lo hecho para aprovechar los nuevos recursos técnicos para acercar el Estado al ciudadano. Si bien la mayoría de los organismos públicos ha introducido nuevas tecnologías de gestión, su alcance no fue generalizado de forma de aprovechar integralmente sus ventajas. Las tecnologías quedaron fuera de contexto y sólo sirvieron para solucionar problemas muy específicos de cada organismo. No se aprovecharon, diseminaron ni compartieron las experiencias. La introducción de tecnologías estuvo, en muchos casos, asociada a la disponibilidad financiera de cada organismo y no a una estrategia de fortalecer a las organizaciones más débiles o donde el impacto hubiera sido más efectivo. Existen organismos equipados con tecnología de última generación y otros que se mantienen en las viejas prácticas de gestión, sin posibilidad de revertir la situación. El Plan Nacional de Modernización del Estado propone utilizar los nuevos recursos informáticos a fin de facilitar la interacción del ciudadano con el Estado, optimizar las inversiones de los organismos en tecnología informática e impulsar una adecuada gestión estratégica de los recursos informáticos. - Líneas de trabajo y resultados esperados: Desarrollo de una red telemática que permita intercomunicación rápida y eficiente entre los organismos de la Administración Nacional. Consolidación de la infraestructura de Firma Digital (normativa, estándares tecnológicos, red de autoridades certificantes). Instrumentación progresiva a partir del 2001 de procedimientos administrativos digitalizados que eliminen progresivamente el uso de papel como portador de información. Diseño e instrumentación de un sistema único de seguimiento de expedientes. Uso generalizado del e-mail en la Administración Pública Nacional. Racionalización del desarrollo de portales en la Administración Pública Nacional.

- Decreto JGM 889/01. Jefatura de Gabinete de Ministros. B.O. 11/07/2001. 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.

1) Entender en la elaboración del marco regulatorio del régimen relativo a la validez legal del documento y firma digital, así como intervenir en aquellos aspectos vinculados con la incorporación de estos últimos a los circuitos de información del sector público y con su archivo en medios alternativos al papel.

- Resolución JGM 57/02. Jefatura de Gabinete de Ministros. B.O. 21/2/2002. Estructura organizativa. Aperturas inferiores del primer nivel operativo. Establece que la Oficina Nacional de Tecnologías de Información deberá intervenir en la elaboración del marco regulatorio del régimen relativo a la validez legal del documento y firma digital y en la incorporación de estos últimos a los circuitos de información del sector público y con su archivo en medios alternativos al papel.
- Decreto 2628/2002.

Que la reglamentación de la Ley N° 25.506 permitirá establecer una Infraestructura de Firma Digital que ofrezca autenticación, y garantía de integridad para los documentos digitales o electrónicos y constituir la base tecnológica que permita otorgarles validez jurídica.

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

ASPECTOS PENALES.

Siendo el Derecho Penal una rama de las ciencias jurídicas donde se halla prohibida la interpretación por analogía, en virtud de lo dispuesto por el art. 18 de la Constitución Nacional, en consecuencia, ciertas conductas penales relacionadas con la alteración de documentos o la falsedad de las firmas ológrafas pueden resultar atípicas

cuando se usa una firma digital. Es por eso que era necesaria una reforma al Código Penal, para contemplar situaciones como el uso de la firma digital perteneciente a otra persona; la creación de una firma digital atribuyéndola a un nombre falso, como medio comisivo de una posterior estafa; la alteración de un mensaje conociendo la clave privada del destinatario; entre otras.

El marco legislativo que le otorga validez jurídica a la firma digital, penaliza las falsificaciones que se puedan cometer utilizando esta tecnología. Para tipificar estos delitos la ley extiende el significado del concepto de firma a la firma digital. En tal sentido se expresa la ley en el art. 51, referido a la equiparación de los efectos del derecho penal, incorporando el siguiente texto como art. 78 (bis) del Código Penal: "Los términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos documento, instrumento privado y certificado comprenden el documento digital firmado digitalmente."

DOCUMENTO.

INTRODUCCIÓN.

El documento es, en sentido amplio, todo objeto capaz de reflejar un hecho presente o pasado.

Debe cumplir con tres requisitos básicos a saber: inalterabilidad (que no se pueda cambiar su esencia), perdurabilidad (que permanezca en el tiempo) y autoría (que asegure la identidad de las partes).

Todos los documentos son hechos idóneos para exteriorizar la voluntad de las personas, como lo expresa el art. 913 del Cód. Civil, y que según el art. 917 puede manifestarse verbalmente, o por escrito, o por otros signos inequívocos.

El Código Civil establece como principio general la libertad de las formas en su art. 974, cuando éste Código, o leyes especiales, o las partes en concurso, no designaren la forma para el acto jurídico. Entendiéndose por forma, según art. 973, a "el conjunto de prescripciones de la ley, respecto de las solemnidades que deben observarse al tiempo de la formación del acto jurídico: tales como la escritura del acto, la presencia de testigos, o por un oficial público, o con el concurso del juez del lugar"

Dentro del género documento, se encuentran los instrumentos tanto públicos (arts. 979) como particulares diferenciando éstos entre los firmados, que se llaman instrumentos privados (art. 1012), y los no firmados, que se llaman instrumentos particulares. Los instrumentos particulares pueden tener cualquier tipo de soporte, no siendo indispensable que la manifestación de voluntad se exprese por escrito (art. 917), a diferencia de los instrumentos públicos y privados que deben cumplir con las solemnidades exigidas por ley.

El documento puede cumplir distintas funciones ya sea como requisito esencial del acto jurídico o como elemento probatorio del mismo acreditando la existencia o eficacia de un acto jurídico, o entre otras, para oponerlo a terceros.

En todo documento se distinguen dos dimensiones básicas, el soporte y la grafía.

SOPORTE DE INFORMACIÓN.

El documento es una cosa corporal que enseña, nos muestra algo. Posee dos elementos intrínsecos al concepto: el material o corporal, formado a su vez por el hábeas, el papiro egipcio, el moderno papel o el soporte electrónico, y la grafía, escritura, lenguaje binario, u otro.

Todo documento requiere para su representación de un soporte. Entendemos por soporte todo elemento o substrato material sobre el que, o dentro del cual, se asienta o sostiene la información. Es donde se fija, almacena o archiva los actos o hechos.

La representación de un hecho mediante un objeto, para que tenga valor documental, debe expresarse por un medio permanente que permita su reproducción, que es la forma por excelencia de su representación.

El documento es una cosa, un objeto, con una significación determinada. Una de las partes del objeto documento es el soporte, que puede ser papel, madera, piedra, dibujos, planos, marcas, cuadros, que son clases de soportes no electrónicos y que se pueden agregar los soportes electrónicos como discos rígidos, discos compactos (CDs), disquetes, cintas magnéticas, etc. Estos soportes pueden considerarse equivalentes al soporte papel, en tanto medio capaz de contener o almacenar información, para su posterior reproducción con fines representativos[16].

LA GRAFÍA.

La ley no sólo incorpora o extiende el concepto de soporte, abarcando lo digital, sino que también incorpora o extiende el concepto de grafía, abarcando el lenguaje binario.

La grafía es la forma por la cual se manifiesta extremamente el pensamiento representativo de un hecho. Debe sin embargo distinguirse, dentro de la grafía, al medio de lenguaje. El medio sería el instrumento por el cual es posible trasladar los signos al soporte; el lenguaje, en cambio, estaría dado por el conjunto de signos, inteligibles y aptos para representar al pensamiento o declaración.

DOCUMENTO DIGITAL.

El documento digital es simplemente una secuencia informática de bits (unos y ceros) que puede representar cualquier tipo de información. Esta representación de la información en base a dígitos implica en el ámbito informático una representación binaria, es decir por medio de unos y ceros.

Todo tipo de información es apta para ser representada digitalmente: mediante el escaneo, la imagen de una fotografía o la imagen de un documento en soporte papel; mediante un procesador de palabras, la información escrita; mediante una plaqueta digitalizadora, la voz, la música y el video; mediante hojas de cálculo, la información numérica y financiera; y mediante bases de datos, la información estadística y diversos bancos de información.

Corresponde hablar de documento digital y no de documento electrónico, vocablo éste último que se utiliza erróneamente, a pesar de su popularidad. Porque el procesamiento informático consiste en procesar dígitos binarios, no electrones.

Aunque es cierto que, cuando el documento digital se encuentra momentáneamente almacenado en la memoria volátil de una PC (memoria "RAM"), los dígitos de ese documento consisten de magnitudes eléctricas, también es cierto que cuando se encuentra almacenada en el disco duro de la PC, consiste en campos magnéticos (o, con mayor precisión, en imanes moleculares), cuando se encuentra perdurablemente almacenado en un CD-ROM consiste en agujeros perforados en la capa de aluminio del CD y, finalmente, cuando es transmitido por una fibra óptica de telecomunicaciones, consiste en fotones.

Lo que también es cierto es que en todas estas modalidades diferentes de almacenamiento y transmisión, el documento no pierde su cualidad numérica, es decir digital. Por eso, los especialistas consideran que conviene denominarlo como tal[17].

Todo tipo de información representada digitalmente constituye un documento digital y es susceptible de ser firmada digitalmente.

Son ejemplos de documentos digitales un correo electrónico, un archivo, factura electrónica, etc.

Algunos autores distinguen el “documento electrónico” del “instrumento informático”. En este sentido, señalan que entre documento e instrumento existe una relación de género a especie. Mientras que documento es toda representación de pensamiento, en el instrumento. aquella representación se manifiesta mediante grafía escrita, contenida en soporte de papel. Así, si toda representación material destinada e

idónea para reproducir una cierta manifestación del pensamiento representativo de un hecho y apta para producir efectos jurídicos. es documento (género), y aquella que por escrito se vuelca en papel, es instrumento (especie), atendiendo al tipo de soporte (disco rígido, diskette), al documento guardado en el disco de la computadora (soporte magnético), no legible alojo humano, se lo denomina documento electrónico; y a ese mismo documento, una vez sacado escrito por la impresora en una hoja de papel (soporte material), legible alojo humano, lo llaman instrumento informático.

Ahora bien, el concepto de documento electrónico no se limita a aquel que, archivado en el soporte magnético de una computadora o en cualquier otro registro electrónico o magnético, es ilegible para el ojo humano, sino que comprende también las grabaciones, las emisiones de fax, etc. En el ejemplo de la computadora, el soporte es el disco rígido o el diskette donde está registrado el documento. La grafía está compuesta por el teclado, la CPU y el programa utilizado para ingresar la información, que son los medios que permiten la exteriorización del pensamiento, y el lenguaje estaría constituido por el "lenguaje de máquina" mediante el cual la declaración es grabada en el soporte magnético, de manera ilegible para el ojo humano[18].

DEFINICIÓN DE LA LEY.

El art. 6° de la ley 25.506 de Firma Digital establece que “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”.

Este art. deja en claro que el documento digital cumple con el requisito de la forma escrita, estableciendo que la grafía en lenguaje binario que se aplica al soporte electrónico, en este caso al documento digital, satisface de igual manera al requerimiento de escritura exigido por la ley o por acuerdo de partes. De esta manera, pone en igualdad jurídica al documento digital con lenguaje binario y al documento papel con escritura.

Además es definido por el decreto 427/98, como “ Representación digital de actos, hechos o datos jurídicamente relevantes”.

En materia de reformas, el proyecto de Código Civil de 1998 en su art. 263, establece que “la expresión escrita puede tener lugar por instrumentos particulares

firmados o no firmados, salvo los casos en que determinada forma de instrumento sea exclusivamente impuesta. Puede hacerse constar en cualquier soporte siempre que su contenido pueda ser representado como texto inteligible aunque para su lectura se requiera la intervención de medios técnicos".

REQUISITOS DEL DOCUMENTO DIGITAL.

El documento digital debe cumplir con los requisitos de todo documento, entre los cuales podemos mencionar, tres requisitos básicos: inalterabilidad, perdurabilidad y autoría.

1) Inalterabilidad: El documento digital se enfrenta al requisito de que su contenido no sea alterado o modificado, o bien detectar si lo ha sido, disminuyendo su seguridad y confiabilidad, y teniendo en cuenta que el soporte papel no es fácil de alterar pero no inalterable dando lugar al delito de falsificación, éste requisito se cumple con el procedimiento de verificación de la firma digital, a través de la función hash, que permite observar si un mensaje a sido o no alterado, y en caso de ser el resumen hash igual al mensaje original o inicial, la ley presume iuris tantum, que el documento digital no ha sido modificado desde el momento de su firma, según reza el art. 8 de la ley que dice que "Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma".

2) Perdurabilidad: El requisito de durabilidad del soporte digital se da mejor que el soporte papel, cumpliendo con la permanencia en el tiempo que debe de tener todo documento.

3) Autoría: a través de la firma digital del documento se asegura la identidad del operador, mediante el procedimiento de verificación de la firma. La ley establece en su art. 7 la presunción de autoría de dicha firma diciendo que "Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación".La cual se complementa con el art. 10 que establece que "Cuando un documento digital sea enviado en forma automática por un dispositivo programado y lleve la firma digital del remitente

se presumirá, salvo prueba en contrario, que el documento firmado proviene del remitente".

DOCUMENTO ORIGINAL.

Otro tema que reviste importancia, en orden a determinar el valor como medio de prueba del documento electrónico, es el relativo a originales y copias. Si tenemos, por un lado, el documento grabado en un disco rígido (documento electrónico), el mismo documento en un soporte volátil (monitor), ya ese documento lo sacamos escrito por la impresora (instrumento informático), tendremos tres documentos: uno sobre soporte magnético, otro sobre soporte fósforo y el tercero sobre papel. Así, surgen estos interrogantes: ¿cuál de los tres documentos es el original? , y los demás, ¿son copias?. Entendemos que cuando nos referimos a la declaración contenida en el soporte magnético, en la pantalla y en el papel salido de la impresora, estamos en presencia del mismo documento plasmado en diferentes soportes y todos revestirían, a los efectos del reconocimiento, el carácter de originales[19].

En tal sentido, la norma en su art. 11, refiriéndose al original dice que "Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación". Acogiendo así, lo expresado por la ley 24.624 en su art. 30 que sustituye el artículo 49 de la Ley N° 11.672, Complementaria permanente de presupuesto (t.o. 1995) por el siguiente: "La documentación financiera, la de personal y la de control de la Administración Pública Nacional, como también la administrativa y comercial que se incorpore a sus Archivos, podrán ser archivados y conservados en soporte electrónico u óptico indeleble, cualquiera sea el soporte primario en que estén redactados y construidos, utilizando medios de memorización de datos, cuya tecnología conlleve la modificación irreversible de su estado físico y garantice su estabilidad, perdurabilidad, inmutabilidad e inalterabilidad, asegurando la fidelidad, uniformidad e integridad de la información que constituye la base de la registración.

Los documentos redactados en primera generación en soporte electrónico u óptico indeleble. y los reproducidos en soporte electrónico u óptico indeleble a partir de

originales de primera generación en cualquier otro soporte, serán considerados originales y poseerán, como consecuencia de ello, pleno valor probatorio, en los términos del artículo 995 y concordantes del Código Civil.

Los originales redactados o producidos en primera generación en cualquier soporte una vez reproducidos, siguiendo el procedimiento previsto en este artículo, perderán su valor jurídico y podrán ser destruidos o dárseles el destino que la autoridad competente determine, procediéndose previamente a su anulación.

La documentación de propiedad de terceros podrá ser destruida luego de transcurrido el plazo que fije la reglamentación transcurrido el mismo sin que se haya reclamado su devolución o conservación, caducará todo derecho a objetar el procedimiento al cual fuera sometida y el destino posterior dado a la misma.

La eliminación de los documentos podrá ser practicada por cualquier procedimiento que asegure su destrucción total o parcial, con la intervención y supervisión de los funcionarios autorizados.

Facultase al Jefe de Gabinete de Ministros a reglamentar las disposiciones del presente artículo".

CONSERVACIÓN DE DOCUMENTOS.

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

El Decreto reglamentario Nº 2628/2002 establece es su artículo 4 las normas técnicas, facultando a la jefatura de gabinete de ministros, a determinar las normas y los procedimientos técnicos para la generación, comunicación, archivo y conservación del documento digital o electrónico, según lo previsto en los artículos 11 y 12 de la Ley N° 25.506. Y su artículo 5 reza "Conservación. El cumplimiento de la exigencia legal de conservar documentos, registros o datos, conforme a la legislación vigente a la materia, podrá quedar satisfecha con la conservación de los correspondientes, documentos digitales firmados digitalmente. Los documentos, registros o datos electrónicos, deberán

ser almacenados por los intervinientes o por terceros confiables aceptados por los intervinientes, durante los plazos establecidos en las normas específicas.

Se podrán obtener copias autenticadas a partir de los originales en formato digital firmado digitalmente. La certificación de autenticidad se hará de conformidad a los procedimientos legales, vigentes para el acto de que se trate, identificando el soporte que procede la copia".

El documento electrónico se ha ido transformando en la principal fuente de archivo de la cultura escrita, ya que por razones de espacio, los documentos escritos se van traduciendo en "bites" para su conservación, y es mucho más seguro y conservable que la forma escrita. Establecida la decisión de la conservación de los documentos, hay que tener en cuenta que se ha creado una base de datos que interesa a las partes, pero también a terceros, por ello debe establecerse que la guarda de datos tenga una forma fiable y sea accesible.

LEGISLACIÓN COMPARADA.

_La ley del Estado de Utah de 1995, establece que un documento electrónico es cualquier documento generado o archivado en un computador.

_La Ley Modelo de la CNUDMI (UNCITRAL) sobre las firmas electrónicas (2001) -art. 2, inc. c-, al igual que la Ley Modelo de la CNUDMI sobre comercio electrónico (1996) -art. 2, inc. a-, define al mensaje electrónico de datos como la "información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax".

_ Chile. "Ley sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma."

Artículo 2º.- Para los efectos de esta ley se entenderá por:

d) Documento electrónico: toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior;

_Italia. Decreto Nº 513/97.-

Artículo 1.- Definiciones.

A los fines del presente reglamento se interpreta:

-por *documento informático:* a la representación informática de los actos, hechos o datos jurídicamente relevantes;

Art. 2. Documento informático

El documento informático del formato que sea, el archivo en base a soporte informático y la transmisión con instrumentos telemáticos, son válidos y relevantes a todos los efectos de ley si se encuentran conforme con las disposiciones del presente reglamento.

_ Ecuador. "Proyecto de ley de comercio electrónico, firmas electrónicas y mensajes de datos".

Art. 2.- Glosario de Términos:

Mensajes de Datos: Toda aquella información generada por medios electrónicos, digitales o similares que puede ser almacenada o intercambiada por cualquier medio. Podrán ser mensajes de datos sin que esta enumeración limite su definición los siguientes: Documentos Electrónicos, Correo electrónico, páginas web, telegrama, telex, fax, facsímile e Intercambio electrónico de datos.

Documento Electrónico: Documento en formato electrónico con información electrónica o digital que se genera o almacena por cualquier medio.

EL DOCUMENTO DIGITAL, SU VALOR JURÍDICO Y PROBATORIO.

Como dije anteriormente, todo tipo de información representada digitalmente constituye un documento digital y es susceptible de ser firmada digitalmente. Es por ello que la firma digital otorgar validez jurídica o eficacia probatoria a toda declaración de voluntad o de conocimiento, con independencia de su extensión o de su medio de almacenamiento, sin limitación alguna.

Es importante destacar que la firma digital está ligada íntimamente al documento digital que la origina y que junto a ese documento y el certificado de clave pública correspondiente permiten en conjunto y de manera autosuficiente verificar la integridad del documento y la identidad del creador de la firma.

Los requisitos de inalterabilidad, autoría, no rechazo y confidencialidad mencionados anteriormente, son necesarios para la admisibilidad y eficacia probatoria de los documentos digitales.

El que un documento este escrito en lenguaje digital no hace que pierda su contenido, el carácter de mensaje, aún cuando sea de más difícil comprensión, como tampoco se pierde si está escrito en chino, japonés o castellano frente a quien no comprende está lenguas. Habitualmente se captará en pantalla, se reproducirá por impresora o por cualquier otro medio, pero tal nueva representación del mensaje no hace que pierda aquél su consideración de documento y así será en todos los casos en que se pretenda su uso como medio de prueba.

La prueba es la demostración de la verdad de un hecho a través de los medios que la ley establece y los dota con fuerza probatoria para acreditar la verdad del hecho. Dentro de los medios de prueba se halla la prueba documental, que consiste en acreditar la verdad del hecho utilizando documentos, concepto que hoy recepta a los documentos digitales. El documento como medio de prueba puede constar en escritos o en objetos de otra índole, siempre que exprese con claridad una idea o hecho.

La importancia de la ley 25.506 en éste tema, reside en que le otorga *valor jurídico y probatorio* al documento digital, es decir aquel no soportado sobre papel, ni escrito en grafía tradicional, ni firmado. En relación a esto es importante resaltar que la norma incorpora a nuestra legislación de fondo un moderno concepto de documento, que, sustentado en el contenido de numerosos proyectos de ley elaborados con anterioridad, otorga pleno valor jurídico al documento digital.

Ello se sustenta en la extensión o modernización del concepto de firma, ya que si el artículo 3° dice: "Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital...", y en la extensión también del concepto de documento ya que el artículo 6° dice: "...Un documento digital también satisface el requerimiento de escritura".

Hay que tener en cuenta que para la elaboración legislativa actual, en nuestro país se tuvo en cuenta básicamente la ley modelo de CNUDNI (UNCITRAL) sobre comercio electrónico, que en el art. 9 inc. 2, establece que "toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria..."

El problema que se planteaba antes de contar con la ley era que los documentos electrónicos no podían ser utilizados como prueba en un juicio, porque son muy fáciles

de falsificar y por ello era necesario contar con un medio que valide o dé fuerza jurídica a esos documentos, para ello se utiliza la firma digital.

Antes de la sanción, estos efectos solo podían basarse en un contrato de legitimación, mediante el cual las partes otorgan validez a las declaraciones que harán en el futuro en forma electrónica; o en la costumbre, que es fuente del derecho y en ausencia de una ley especial, pude ser considerada como legitimante si se prueba que el documento digital es utilizado normalmente y es una costumbre en el lugar; o en la conducta anterior de las partes que las obliga a comportarse del mismo modo.

EL DOCUMENTO DIGITAL COMO INSTRUMENTO.

Recordemos que dentro del género documento, se encuentran los instrumentos públicos y los instrumentos particulares firmados y no firmados, los primeros se llaman instrumentos privados, y los segundos se llaman instrumentos particulares que no necesariamente deben ser escritos, a diferencia de los instrumentos públicos y privados que son en forma escrita y deben cumplir con las solemnidades exigidas por ley.

Como instrumento particular.

El documento digital también puede ser firmado o no firmado digitalmente, en el supuesto de que no este firmado hay una declaración de voluntad documentada, pero no hay una vinculación directa con el autor, por el hecho de no haber firma. Tal es el caso de cuando introducimos nuestra tarjeta magnetizada en un cajero automático, donde ordenamos con nuestra clave de la extracción de dinero, que nos es debitado de nuestras cuentas; o depositamos dinero, que se nos acredita; o efectuamos transferencias entre distintos tipos de cuenta u ordenamos por debito se pague aun tercero, etc. y al final de la operatoria nos es entregado un comprobante. En este como en otros supuestos, la autoría debe ser probada por otros medios distintos de la firma, como ser testigos, pero no va a carecer de validez el documento, digital o no, por no estar firmado.

El proyecto de reforma del código civil de 1998 establece en su art. 264 que "son instrumentos particulares, si no están firmados, los impresos, los registros visuales o auditivos de cosas o hechos y, cualquiera que sea el medio empleado, los registros de la palabra y de información, y en general todo escrito no firmado". Y en el art. 296 establece que “El valor probatorio de los instrumentos particulares debe ser apreciado por el tribunal ponderando, entre otras pautas, los usos del tráfico, las relaciones

precedentes de las partes si las hubiere habido, y la razonable convicción que pueda alcanzarse sobre su autoría, legibilidad e inalterabilidad de acuerdo a los métodos utilizados para su creación y transmisión a terceros".

Como instrumento instrumento privado.

El documento digital firmado digitalmente es el que vincula directamente el documento con su autor a través de la firma y por lo tanto sirve para imputarle la autoría de la declaración. La firma es un requisito o condición esencial para este acto según el art. 1012.

Es un documento privado debido a que la firma digital esta equiparada a la firma ológrafa o manuscrita, y permite la individualización del autor de la misma, por ello goza del mismo valor que cualquier otro instrumento privado, los cuales reconocidos judicialmente tienen el mismo valor que los instrumentos públicos entre los que lo han suscripto y sus sucesores (art. 1026).

En cuanto al proyecto de reforma del Código Civil de 1998 en su art. 265, referido a los instrumentos privados establece que "Son instrumentos privados los instrumentos particulares firmados". En el art. 289 contempla que "El único requisito de validez de los instrumentos privados es la firma del o de los otorgantes". El art. 290, referido al reconocimiento de la firma dice que "Todo aquél contra quien se presente un instrumento cuya firma se le atribuye, debe manifestar si ésta le pertenece. Los herederos pueden limitarse a manifestar que ignoran si la firma es o no de su causante. La autenticidad de la firma puede ser probada por cualquier medio". El 294, fecha cierta, dice que "La eficacia probatoria de los instrumentos privados reconocidos se extiende a los terceros desde que adquieren fecha cierta. Adquieren fecha cierta el día en que acontece un hecho del que resulta como consecuencia ineludible que el documento ya estaba firmado o no pudo ser firmado después. La prueba puede producirse por cualquier medio, y debe ser apreciada rigurosamente por el tribunal".

Como instrumento público.

El instrumento público es aquel que se otorga con las formalidades que la ley establece, en presencia de un oficial público a quien la ley confiere facultad para autorizarlo.

El inciso d) del art. 4 que establece (como vimos en el punto de las exclusiones) que “Las disposiciones de esta ley no son aplicables a los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes”.

Vale repetir en este punto, que éste artículo fue tomado del artículo 6 del Proyecto de Ley de Firma Digital del Poder Ejecutivo (1999). La redacción de dicho proyecto comenzó en 1997 y en ese entonces se prefirió limitar el ámbito de aplicación de las firmas digitales a los instrumentos privado. Al hacerse referencia a "formalidades incompatibles con la utilización de la firma digita" se tuvo en cuenta fundamentalmente a los actos que deben instrumentarse en escritura pública, bajo pena de nulidad, y aquellos actos en los que las partes optan por instrumentarlos por escritura pública aunque el Código Civil no lo imponga (por ej. un boleto de compraventa de inmuebles, que puede ser otorgado por instrumento privado o por escritura pública, si las partes así lo resuelven). Las legislaciones han evolucionado en los últimos años, ésta evolución se advierte incluso en nuestro país.

Aludiendo al proyecto de reforma del código civil de 1998, en su art. 268 referido a los requisitos de validez del instrumento público, en su inc. e) propone “Que el instrumento conste en el soporte exigido por la ley o las reglamentaciones. Los instrumentos generados por medios electrónicos deben asegurar la autenticidad, integridad e inalterabilidad del contenido del instrumento y la identificación del oficial público”. Vemos que hace mención expresa del instrumento público digital y a los elementos que debe asegurar, función que cumple la firma digital. Y el art. 269 establece la validez como instrumento privado del instrumento público que no reúne los recaudos del artículo precedente.

En cuanto a las escrituras públicas, remite a las reglamentaciones locales la formación y archivo del protocolo. Ello significa que estaría contemplando la posibilidad de un protocolo en un soporte distinto al papel y con firmas electrónicas de los otorgantes y escribano. La escritura pública es instrumento público, pero existen otros instrumentos públicos además de la escritura pública[20].

Por lo que todos los actos jurídicos lícitos pueden celebrarse válidamente por medio de documentos digitales, los que valdrán como instrumentos públicos o privados, siguiendo así, el criterio amplio propuesto por la CNUDMI y receptado por distintos ordenamientos internacionales, entre ellos el chileno, el español y el italiano.

Considero que el documento digital emanado de autoridad o funcionario público en ejercicio de su cargo, más que se cumplimenten los requisitos exigidos por la ley,

revisten calidad de público, o sea que son instrumentos públicos; ya que no son actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital. Si bien es necesario un marco normativo, como consecuencia de una modificación de leyes existentes que las adecue a la realidad tecnológica existente, para estructurar y poner en funcionamiento una aplicabilidad más del documento digital firmado digitalmente.

EL DOCUMENTO DIGITAL EN LA ADMINISTRACIÓN PÚBLICA NACIONAL.

- Ley 24.624.–

Artículo 30.- Sustituyese el artículo 49 de la Ley N° 11.672, Complementaria permanente de presupuesto (t.o. 1995) por el siguiente: "La documentación financiera, la de personal y la de control de la Administración Pública Nacional, como también la administrativa y comercial que se incorpore a sus Archivos, podrán ser archivados y conservados en soporte electrónico u óptico indeleble, cualquiera sea el soporte primario en que estén redactados y construidos, utilizando medios de memorización de datos, cuya tecnología conlleve la modificación irreversible de su estado físico y garantice su estabilidad, perdurabilidad, inmutabilidad e inalterabilidad, asegurando la fidelidad, uniformidad e integridad de la información que constituye la base de la registración.

Los documentos redactados en primera generación en soporte electrónico u óptico indeleble. y los reproducidos en soporte electrónico u óptico indeleble a partir de originales de primera generación en cualquier otro soporte, serán considerados originales y poseerán, como consecuencia de ello, pleno valor probatorio, en los términos del artículo 995 y concordantes del Código Civil.

Los originales redactados o producidos en primera generación en cualquier soporte una vez reproducidos, siguiendo el procedimiento previsto en este artículo, perderán su valor jurídico y podrán ser destruidos o dárseles el destino que la autoridad competente determine, procediéndose previamente a su anulación.

La documentación de propiedad de terceros podrá ser destruida luego de transcurrido el plazo que fije la reglamentación transcurrido el mismo sin que se haya reclamado su devolución o conservación, caducará todo derecho a objetar el procedimiento al cual fuera sometida y el destino posterior dado a la misma.

La eliminación de los documentos podrá ser practicada por cualquier procedimiento que asegure su destrucción total o parcial, con la intervención y supervisión de los funcionarios autorizados.

Facultase al Jefe de Gabinete de Ministros a reglamentar las disposiciones del presente artículo".

- Ley 25.237.-

Artículo 61. - establécese que la Sindicatura General de la Nación 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.

- Decreto 677/01.

Artículo 45.- Firma digital. Los documentos firmados digitalmente que se remitan por vía electrónica a la Comisión Nacional de Valores de acuerdo a las reglamentaciones dictadas por dicha Comisión para su identificación, a todos los efectos legales y reglamentarios gozarán de idéntica validez y eficacia que los firmados en soporte papel.

- Decreto 889/01.-

1) Entender en la elaboración del marco regulatorio del régimen relativo a la validez legal del documento y firma digital, así como intervenir en aquellos aspectos vinculados con la incorporación de estos últimos a los circuitos de información del sector público y con su archivo en medios alternativos al papel.

- Decreto 1023/01. Régimen de contrataciones de la administración nacional.-

Artículo 21.- Contrataciones en formato digital. Las contrataciones comprendidas en este régimen podrán realizarse en formato digital firmado digitalmente, utilizando los procedimientos de selección y las modalidades que correspondan. También podrán realizarse en formato digital firmado digitalmente los contratos previstos en el artículo 5° del presente.

Las jurisdicciones y entidades comprendidas en el artículo 2° estarán obligadas a aceptar el envío de ofertas, la presentación de informes, documentos, comunicaciones, impugnaciones y recursos relativos a los procedimientos de contratación establecidos en

este régimen, en formato digital firmado digitalmente, conforme lo establezca la reglamentación.

Se considerarán válidas las notificaciones en formato digital firmado digitalmente, en los procedimientos regulados por el presente.

Deberá considerarse que los actos realizados en formato digital firmados digitalmente cumplen con los requisitos del artículo 8° de la Ley N° 19.549, su modificatoria y normas reglamentarias, en los términos establecidos en las disposiciones referentes al empleo de la firma digital en el Sector Público Nacional, las que se aplicarán, en el caso de las contrataciones incluidas en los artículos 4° y 5° de este régimen, aun a aquellos actos que produzcan efectos individuales en forma directa.

Los documentos digitales firmados digitalmente tendrán el mismo valor legal que los documentos en soporte papel con firma manuscrita, y serán considerados como medio de prueba de la información contenida en ellos.

Art. 22. — Regulación. La reglamentación establecerá la regulación integral de las contrataciones públicas electrónicas, en particular el régimen de publicidad y difusión, lo referente al proceso electrónico de gestión de las contrataciones, los procedimientos de pago por medios electrónicos, las notificaciones por vía electrónica, la automatización de los procedimientos, la digitalización de la documentación y el expediente digital.

- Decreto 658/2002. Obligaciones Tributarias. Modificase el Dec. 1397/79.-

Artículo 1.- Sustituyese el artículo 28 del Decreto Nº 1397/79 y sus modificaciones, por el siguiente: " Artículo 28. - Las declaraciones juradas deberán ser presentadas en soporte papel, y firmadas en su parte principal y anexos por el contribuyente, responsable o representante autorizado, o por medios electrónicos o magnéticos que aseguren razonablemente la autoría e inalterabilidad de las mismas y en las formas, requisitos y condiciones que a tal efecto establezca la Administración Federal de Ingresos Públicos entidad autárquica en el ámbito del Ministerio de Economia.

En todos los casos contendrán una fórmula por la cual el declarante afirme haberlas confeccionado sin omitir ni falsear dato alguno que deban contener y ser fiel expresión de la verdad."

Art. 2º - Agregase como último párrafo del artículo 48 del Decreto Nº 1397/79 y sus modificaciones, el siguiente:

"La Administración Federal de Ingresos Públicos podrá establecer procedimientos para la confección, transmisión y conservación de comprobantes, documentos, libros y registros por medios electrónicos y/o magnéticos que aseguren razonablemente su autoría e inalterabilidad, aun en los casos de documentos que requieran la firma de una persona."

- Decreto 2628/2002.-

Que la reglamentación de la Ley N° 25.506 permitirá establecer una Infraestructura de Firma Digital que ofrezca autenticación, y garantía de integridad para los documentos digitales o electrónicos y constituir la base tecnológica que permita otorgarles validez jurídica.

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

- Decreto 283/2003.-

Artículo 1º — Autorízase con carácter transitorio y hasta tanto se encuentre la Administración Pública Nacional en condiciones de emitir certificados digitales en los términos previstos en la Ley Nº 25.506 y en su Decreto Reglamentario Nº 2628/2002, a la Oficina Nacional de Tecnologías Informáticas dependiente de la Subsecretaria de la Gestión Pública de la Jefatura de Gabinete de Ministros 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.

- Resolución 176/2002. Jefatura de Gabinete de Ministros. Firma digital. Documentación digital – Tramitación.

Habilitase el sistema de tramitación electrónica para la recepción, emisión y archivo de documentación en formato digital firmada digitalmente, el que funcionara en

el departamento delegación de mesa de entradas y despacho de la Subsecretaria de la gestión pública de la Jefatura de Gabinete de Ministros.

ASPECTOS PENALES.

El marco legislativo que le otorga validez jurídica al documento digital firmado digitalmente, penaliza las falsificaciones que se puedan cometer utilizando esta tecnología. Para tipificar estos delitos la ley extiende el significado de los conceptos documento, instrumento privado, instrumento público, al documento digital. En tal sentido se expresa la ley en el art. 51, referido a la equiparación de los efectos del derecho penal, incorporando el siguiente texto como art. 78 (bis) del Código Penal: "Los términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos documento, instrumento privado y certificado comprenden el documento digital firmado digitalmente."

La inserción de este concepto amplio de documento en el sistema de falsedades del Código Penal permite cubrir tanto la falsedad ideológica como la falsedad material de documentos materiales.

QUÉ PERMITE EL DOCUMENTO DIGITAL FIRMADO.

- Realizar declaraciones juradas, por ejemplo por mail (ver decreto 658/2002)
- Firmar el boleto de compraventa, por ejemplo de una propiedad.
- Realizar trámites que hoy en día tardan días, por ejemplo, que al momento de hacerse una escritura el escribano pueda consultar en su computadora, usando su firma digital, si el inmueble está embargado, o es bien de familia, si alguien constituye una sociedad, recibe un número de CUIT, proceso que hoy tarda bastante, si se implementa la firma digital, obtenerlo en forma inmediata.
- Firmar un contrato.
- Cotizaciones de Bienes y Servicios (tanto el pedido como la cotización y condiciones del Proveedor).
- Resúmenes de Cuenta.

- Recibos de Pago.
- Adjudicaciones.
- Factura Electrónica.
- Cheque Electrónico.
- Invitaciones.
- Promociones.
- Remitos de Entrega.
- Ordenes de Compra.
- Solicitudes de Adhesión.
- Actas.
- Planos.
- Planificaciones.
- Circulares internas y/o externas.
- Reservas o Turnos para distintas prestaciones (Talleres, Médicos, Hoteles, Pasajes, etc.).
- Confirmaciones.
- Autorizaciones de Prestaciones Médicas.
- Receta Médica Electrónica.
- Historia Clínica única.
- Solicitudes de Prestación de Servicios.
- Proyectos.
- Diseños.
- Tarjetas de Crédito (sin utilizar el número y consecuentemente disminuir el fraude).
- Etc.

JURISPRUDENCIA.

1. CNCrim. y Correc., Sala VI, marzo 4-999, “Lanata, Jorge” (La Ley, 1999-C-458; con nota de Marcelo Alfredo Riquert en La Ley, 1999-E-70).

Aplicación de los artículos 153 a 155 del Código Penal. Equiparación del correo electrónico con el correo tradicional.

Corresponde equiparar -a los fines de la protección de los papeles privados y la correspondencia prevista en los arts. 153 al155 del Cód. Penal- al correo electrónico "e-mail" con el correo tradicional, dado que aquél posee características de protección de la privacidad más acentuadas que la inveterada vía postal, en tanto que para su funcionamiento se requiere un prestador del servicio, el nombre de usuario y un código de acceso que impide a terceros extraños la intromisión en los datos que a través del mismo puedan emitirse o archivarse.

2. "G., D. E. c/C. SA s/ diligencia preliminar" – Juzgado Nacional de 1ª Instancia en lo Comercial N° 18 - Sec. N° 36 - 23/10/2001, Buenos Aires.

Correo Electrónico. E-Mail. Naturaleza. Valor Probatorio. Protección Jurídica. Prueba Anticipada: Allanamiento de computadoras de la demandada para determinar la existencia de correos electrónicos por aquella remitidos o recibidos. Correspondencia entre comerciantes.

La Corte ha considerado a la inviolabilidad del domicilio y de la correspondencia en términos sustancialmente entrañables, calificándolos como un derecho "básico" o "fundamental" de la persona humana.

No se advierten motivos para que -aún sin existencia de legislación específica- el denominado "correo electrónico" escape a dicha protección, tanto más si así fue admitido jurisprudencialmente en el ámbito del derecho penal, donde la analogía está prohibida (CNCrim. y Correc., Sala VI, marzo 4-999, "Lanata, Jorge").

Sin perjuicio de lo expuesto, el caso en examen debe resolverse considerando que se trata en el caso de mensajes atinentes a una contratación mercantil.

La exhibición de la correspondencia entre comerciantes con motivo de una negociación debe asimilarse a la parcial de los libros de comercio, que es admitida por la legislación mercantil en caso de pleito pendiente, o como medida preliminar, pues reposa en el principio de la comunidad de los asientos.

Sin embargo, se ha dicho que ello no autoriza a efectuar esa exhibición en forma compulsiva, ya que la negativa trae aparejada la sanción prevista por el art. 56, es decir, el litigio será resuelto en función de los libros de su adversario.

Siendo así, la medida requerida aparece violatoria del principio de igualdad procesal que este Juez debe preservar (art. 34, inc. 5° c del Código Procesal).

CERTIFICADO DIGITAL.

INTRODUCCION.

Los certificados digitales, tienen una similitud con las licencias de conducir, las primeras permiten viajar por las carreteras, los certificados digitales permiten navegar por la red Internet, la principal característica es que da identidad al usuario y puede navegar con seguridad. De igual forma que la sola licencia de conducir o un pasaporte sirve para dar identidad a quien la porta en ciertos casos, el certificado digital da identidad a una clave pública y se comporta como una persona en el espacio cibernético.

El nacimiento del certificado digital fue a raíz de resolver el problema de administrar las claves públicas y que la identidad del dueño no pueda ser falsificada. La idea es que una tercera entidad intervenga en la administración de las claves públicas y asegure que las claves públicas tengan asociado un usuario claramente identificado. Esto fue inicialmente planteado por Kohnfelder del MIT en su tesis de licenciatura.

Las tres partes más importantes de un certificado digital son:

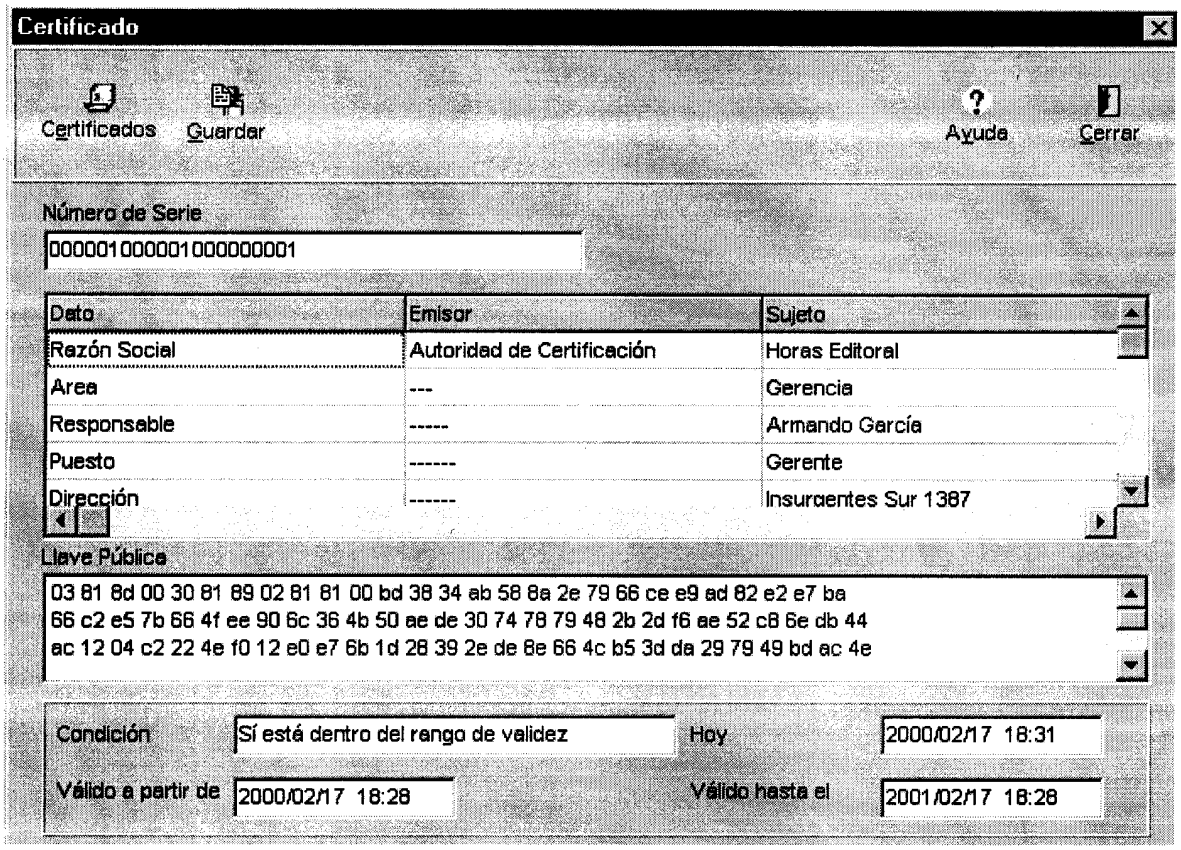
_Una clave pública

_La identidad del implicado: nombre y datos generales

_La firma privada de una tercera entidad llamada autoridad certificadora que todos reconocen como tal y que válida la asociación de la clave pública en cuestión con el tipo que dice ser.

En la actualidad casi todas las aplicaciones de comercio electrónico y transacciones seguras requieren un certificado digital, se ha propagado tanto su uso que se tiene ya un formato estándar de certificado digital, este es conocido como X509[21], en versiones 1, 2 y3, que está basado en la criptografía asimétrica y la firma digital. En X.509 se define un framework (una capa de abstracción) para suministrar servicios de autenticación a los usuarios del directorio X.500. La autenticación se realiza mediante el uso de certificados.

Un certificado digital se puede ver como la siguiente pantalla:



DEFINICIÓN.

La ley 25.506 en su Capitulo II "De los certificados digitales", comienza en el art. 13 con la definición del Certificado digital, estableciendo que "Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular".

El certificado digital también llamado certificado de clave pública, es un documento digital firmado digitalmente por un certificador que da fe, y relaciona los datos de verificación de firma con su titular. Los Certificados emitidos por una Autoridad de Certificación, brindan a sus usuarios garantía de Confidencialidad, Autenticación, Integridad y No-repudio en el uso de la información en medios electrónicos, ya que permiten la identificación indubitable de las personas, documentos, sitios de internet, correo electrónico y otros en el ámbito de los sistemas de información, como así también permite conocer si esta en su período de vigencia, o fue revocado. Permiten verificar que una clave pública específica pertenece, efectivamente, a un

individuo determinado. Los certificados ayudan a prevenir que alguien utilice una clave para hacerse pasar por otra persona.

El certificado digital, como dije, contiene diversos datos, entre ellos el nombre de un usuario y su clave pública, y es firmado por una Autoridad de Certificación (AC). Como el emisor y el receptor confiarán en esa AC, el usuario que tenga un certificado expedido por ella se autenticará ante el otro, en tanto que su clave pública está firmada por dicha autoridad.

En síntesis, la misión fundamental de los certificados es permitir la comprobación de que la clave pública de un usuario, cuyo conocimiento es imprescindible para autenticar que la firma electrónica, pertenece realmente a ese usuario, ya que así lo hace constar en el certificado una autoridad que da fe de ello. Representan además una forma conveniente de hacer llegar la clave pública a otros usuarios que deseen verificar sus firmas. Normalmente, cuando se envía un documento firmado digitalmente, éste siempre se acompaña del certificado del signatario, con el fin de que el destinatario pueda verificar la firma electrónica adjunta.

El decreto 2628/02 reglamentario de la firma digital establece en su art. Art. 3, de los certificados digitales emitidos por certificadores licenciados, que " Los certificados digitales contemplados, en el artículo 13 de la Ley N° 25.506 son aquellos cuya utilización permite disponer de una firma digital amparada por las presunciones de autoría e integridad establecidas en los artículos 7° y 8° de la ley citada.

Y en el art 2, el decreto habla de la validez de los certificados digitales emitidos por certificadores no licenciados, y dice que "Los certificados digitales emitidos por certificadores no licenciados serán válidos para producir los efectos jurídicos que la ley otorga a la firma electrónica".

REQUISITOS DE VALIDEZ.

El art. 14 dice que "Los certificados digitales para ser válidos deben:

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".

Para que un certificado digital sea válido, debe ser emitido por un certificador licenciado por la autoridad licenciante, y responder a los formatos estándares, reconocidos internacionalmente, los que van a ser fijados por la autoridad de aplicación, y establece los datos que como mínimo serán indispensables.

Entre los datos necesarios podemos mencionar:

- Nombre del titular del certificado.
- Tipo y número de documento del titular.
- Clave Pública del titular, identificando el algoritmo utilizado.
- Número de serie del certificado.
- Período de vigencia del certificado.
- La dirección de Internet de las condiciones de emisión y utilización del certificado.
- La dirección de Internet de la lista de certificados revocados que mantiene la Autoridad de Certificación (AC).
- La dirección de Internet del manual de Procedimientos, Políticas de Certificación y Términos y Condiciones para la obtención de Certificados.
- Nombre de la Autoridad de Certificación Licenciada (ACL) que emitió el certificado.
- Firma Digital de la Autoridad de Certificación Licenciada (ACL) que emitió el certificado, identificando los algoritmos de cifrado utilizados.
- La Autoridad de Certificación Licenciada, puede incluir información no verificada, debiendo indicar claramente tal circunstancia en las correspondientes condiciones de emisión y utilización del certificado.

Los certificados emitidos contienen los siguientes campos como mínimo:

Versión		Número de versión del formato X.509
Número de Serie (Serial Number)		Único número identificador del certificado generado por el emisor del mismo.
Firma (Signature)	ID del Algoritmo	Algoritmo usado para firmar el certificado
Emisor (Issuer)		Nombre del emisor del certificado (en formato X.500)
Validez (Validity)	No antes de (Not Before)	Fecha de inicio de validez
	No después de (Not After)	Fecha de finalización
Titular (Subject)		Nombre del titular del certificado (en formato X.500)
Información de la clave pública del Titular	ID del Algoritmo	Algoritmo de firma del titular
	Parámetros	Parámetros aplicables a la clave pública
	Clave Pública	Clave Pública del titular
Extensiones	(Opcional)	Extensiones agregadas a los certificados tal como lo indica el estándar.
Firma del Emisor	ID del Algoritmo	Algoritmo usado para esta firma
	Encriptado de resultado de la función de Hash sobre el certificado	

Por el contrario un certificado digital no va a ser válido cuando se utilice para una finalidad distinta para la cual fue emitido, o para una operación la cual supere el monto máximo autorizado para dicho certificado, o una vez revocado el certificado

digital. Así regula el desconocimiento de la validez de un certificado digital el art. 23, diciendo que "Un certificado digital no es válido si es utilizado:

a) para alguna finalidad diferente a los fines para los cuales fue extendido;

b) para operaciones que superen el valor máximo autorizado cuando corresponda;

c) una vez revocado".

VIGENCIA DE LOS CERTIFICADOS DIGITALES.

La ley regula el período de vigencia del certificado digital, diciendo en el art. 15 que "A los efectos de esta ley, el certificado digital es válido únicamente dentro del período de vigencia, que comienza en la fecha de inicio y finaliza en su fecha de vencimiento, debiendo ambas ser indicadas en el certificado digital, o con su revocación si fuere revocado.

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

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

Podemos observar en el gráfico del certificado digital que el mismo contiene la fecha de inicio, a partir de la cual el certificado es válido, y la fecha de finalización de la validez, es cuando el certificado vence y deja de ser válido. También se puede ver que contiene el estado del certificado, indicando su condición actual que puede ser que esté dentro del rango de validez, o por el contrario, que esté vencido o revocado.

REVOCACIÓN DE CERTIFICADOS.

La revocación de un certificado digital es la acción por la cual se lo deja sin efecto en forma permanente a partir de una fecha cierta, incluyéndolo en la lista de certificados revocados la cual se da a publicar por la Autoridad Certificante Licenciada. Cualquier firma digital realizada con la clave privada asociada a ese certificado con posterioridad a la fecha efectiva de revocación no tendrá validez.

El Decreto 2628/02 reglamentario de la firma digital establece en el art. 23, que "Se deberán revocar los certificados digitales emitidos en los siguientes casos:

a) A solicitud del titular del certificado digital.

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

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

d) Por condiciones especiales definidas en las Políticas de Certificación.

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

f) Por fallecimiento del titular.

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

h) Por declaración judicial de incapacidad del titular.

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

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

De ésta manera amplia las funciones del certificador licenciando en cuanto a la revocación de los certificados digitales establecida en el art. 19 inc. e, de la ley 25.506, agregando los últimos cuatro incisos del art. del decreto.

El inc. c del art. 25 de la ley, establece la obligación del titular del certificado de "Solicitar la revocación de su certificado al Certificador Licenciado ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma".

Una de las funciones del certificador licenciando establecidas en el art. 19 de la ley, es la del inc f, que dice que debe "Informar públicamente el estado de los certificados digitales por él emitidos. Los certificados digitales revocados deben ser incluidos en una lista de certificados revocados indicando fecha y hora de la revocación. La validez y autoría de dicha lista de certificados revocados deben ser garantizadas". A tal efecto se expresa el art. 21 de la ley estableciendo en el inc k, la obligación de "Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, *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".

CERTIFICADOS EXTRANJEROS.

En el art. 16 de la ley se establece que “Los certificados digitales emitidos por certificadores extranjeros podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley y sus normas reglamentarias cuando:

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

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

La norma deja en claro bajo que circunstancia el certificado digital emitido en el extranjero va a ser reconocido en la argentina, teniendo iguales consecuencias que el certificado digital emitido en el país. Para esto deben ser reconocidos o emitidos por un certificador licenciado en el país, en tal sentido lo repite en el art 26 al decir que “Los certificados digitales regulados por esta ley deben ser emitidos o reconocido, según lo establecido por el artículo 16, por un certificador licenciado”.

A los efectos del reconocimiento de los certificados extranjeros, el decreto reglamentario establece en el art. 28, que “De acuerdo a lo establecido en el artículo 6° de la presente reglamentación, facultase a la Jefatura de Gabinete de Ministros a elaborar y firmar acuerdos de reciprocidad con gobiernos de países extranjeros, a fin de otorgar validez, en sus respectivos territorios, a los certificados digitales emitidos por certificadores de ambos países, en tanto se verifique el cumplimiento de las condiciones establecidas por la Ley N° 25.506 y su reglamentación para los certificados emitidos por certificadores nacionales.

Los certificadores licenciados no podrán reconocer certificaciones emitidas por certificadores extranjeros correspondientes a personas con domicilio o residencia en la República Argentina. El Ente Administrador de Firma Digital establecerá las relaciones que los certificadores licenciados deberán guardar entre los certificados emitidos en la República Argentina y los certificados reconocidos de certificadores extranjeros”.

TITULAR DE UN CERTIFICADO DIGITAL.

El titular o suscriptor de un certificado digital, es la persona a cuyo nombre se emite un certificado y posee una clave privada que se corresponde con la clave pública contenida en el mismo. Los Titulares de un certificado de clave pública pueden ser personas físicas o jurídicas.

La ley en su capitulo IV, establece los derechos y obligaciones del titular del certificado digital, normas que se complementan con la ley de Defensa del Consumidor.

Art. 24.- Derechos del titular de un certificado digital. "El titular de un certificado digital tiene los siguientes derechos:

a) a ser informado por el certificador licenciado, con carácter previo a la emisión del certificado digital, y utilizando un medio de comunicación sobre las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de este sistema de licenciamiento y los procedimientos asociados. Esa información deberá darse por escrito en un lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;

b) a que el certificador licenciado emplee los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por él, y a ser informado sobre ello;

c) a ser informado, previamente a la emisión del certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago;

d) a que el certificador licenciado le informe sobre su domicilio en la República Argentina, y sobre los medios a los que pueda acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema, o presentar sus reclamos;

e) a que el certificador licenciado proporcione los servicios pactados, y a no recibir publicidad comercial de ningún tipo por intermedio del certificador licenciado".

Art. 25.- Obligaciones del titular del certificado digital. "Son obligaciones del titular de un certificado digital:

a) mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;

b) utilizar un dispositivo de creación de firma digital técnicamente confiable;

c) solicitar la revocación de su certificado al Certificador Licenciado ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;

d) informar sin demora al certificador licenciado el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación".

SOLICITUD Y EMISION DEL CERTIFICADO DIGITAL.

Una Autoridad Certificante Licenciada puede emitir distintos tipos de certificados. Estos pueden ser diferenciados por el grado de compromiso empleado en la verificación de cada uno de los datos que contienen, por los diferentes atributos, diferentes algoritmos y diferentes extensiones, para ser utilizados en distintos aplicaciones o funciones, y debe redactar y publicar un Manual de Procedimientos y una Política de Certificación para cada uno de los tipos de certificados que emita, detallando los pasos que deben ser seguidos para la emisión de un certificado y las responsabilidades, derechos y demás aspectos relativos a la emisión.

Para solicitar un certificado digital por parte de un suscriptor a la Autoridad de Certificación Licenciada, el suscriptor debe:

- Generar un par de claves:

Ya que la solicitud debe encontrarse firmada digitalmente, y debe incluirse la clave pública en la solicitud.

El par de claves debe ser generado por un algoritmo aceptable y con una longitud mínima que garantice que no existen riesgos de que sea vulnerable. Estas especificaciones se deben encontrar detalladas en la Política de Certificación del tipo de certificado a ser solicitado.

El par de claves puede ser generado por distintos medios, como se indica más adelante, pero en ningún caso la ACL debe conocer ni tomar contacto con la clave privada.

- Remitir la clave pública con sus datos personales a la ACL y cumplimentar los controles necesarios para verificar su identidad.

Es obligación de la ACL cumplimentar los pasos indicados en el Manual de Procedimientos. Una vez aprobada la solicitud, se debe generar un certificado, remitirlo a su titular (o informarle que debe pasar a retirarlo) y publicarlo en un repositorio de certificados emitidos.

- Retirar el certificado

Dependiendo de la aplicación y del formato de exportación del certificado, el titular del mismo incorporará dicho certificado en el medio de almacenamiento correspondiente.

Por ejemplo, para obtener un certificado de firma digital, uno puede conectarse con la Autoridad Certificante de la Subsecretaría de la Gestión Pública (http://ca.sgp.pki.ar) y hacer click en el link que dice Solicitar un Certificado para correo electrónico (donde se explica paso por paso el procedimiento para obtener un certificado de firma digital).

Una ves retirado el certificado, en caso de utilizar Internet Explorer como navegador y Microsoft Outlook Express como cliente de correo electrónico se debe habilitar el certificado para poder enviar correos firmados digitalmente. El primer paso es cerciorarse de haber instalado el certificado de la Autoridad Certificante que emitió mi certificado. Una vez cumplido este requisito se deben realizar los siguientes pasos:

- Abrir el Microsoft Outlook Express e ir al menú Herramientas (Tools) y elegir Cuentas (Accounts). En la pantalla que aparece a continuación se debe seleccionar la cuenta de correo que para la cual fue emitido el certificado, o sea la cuenta de correo de donde quiero enviar el mensaje firmado, y hacer click en el botón Propiedades (Properties).
- A continuación se debe hacer click en la opción Seguridad (Security) y luego cliquear en Seleccionar identificador digital (Use a digital ID...), se va a habilitar entonces el botón Identificador Digital (Digital ID...).
- Al presionar este botón se abrirá una ventana que permite seleccionar los certificados que se hayan tramitado y que sean válidos en ese momento.
- Efectuados los pasos anteriores, para firmar digitalmente un correo electrónico se deberá abrir un correo nuevo y redactarlo como se hace comúnmente. Antes de enviarlo se debe hacer un click en el menú de Herramientas (Tools) y luego en el ítem Firmar Digitalmente (Digitally Sign). Otra opción es hacer un click en el ícono con un sobre y una estampilla de color rojo con la leyenda Firmar (Sign) que se desplegará a la derecha de la barra de herramientas[22].

APLICACIONES DE LOS CERTIFICADOS.

Estos certificados permiten a sus titulares realizar una gran cantidad de acciones a través de Internet: acceder por medio de su navegador a sitios web restringidos, a los cuales les deberá presentar previamente el certificado, cuyos datos serán verificados y en función de los mismos se le permitirá o denegará el acceso; enviar y recibir correo electrónico cifrado y firmado; entrar en intranets corporativas, e incluso a los edificios o instalaciones de la empresa, donde se le pedirá que presente su certificado, posiblemente almacenado en una tarjeta inteligente; firmar software para su uso en Internet, como applets de Java o controles ActiveX de Microsoft, de manera que puedan realizar acciones en el navegador del usuario que de otro modo le serían negadas; firmar cualquier tipo de documento digital, para uso privado o público; obtener confidencialidad en procesos administrativos o consultas de información sensible en servidores de la Administración; realizar transacciones comerciales seguras con identificación de las partes, como en SSL, donde se autentica al servidor web, y especialmente en SET, donde se autentican tanto el comerciante como el cliente.

Algunas de las aplicaciones más habituales en las que se utilizan certificados digitales son:

- Para la autenticación de Servidores Web---> Certificados de Servidor Web.
- Para la autenticación de Clientes Web---> Certificados de Cliente Web.
- Para la protección de correos electrónicos ---> Certificado de correo electrónico.
- Para el sellado de tiempos ---> Certificado de tiempo.

INFRAESTRUCTURA DE LA FIRMA DIGITAL.

INTRODUCCION.

Teniendo y habiendo explicado la firma digital, el sistema criptográfico asimétrico, el documento digital y el certificado digital, ahora el problema es la administración de todos éstos. De ello se ocupa la infraestructura de firma digital, que no es otra cosa que una infraestructura de seguridad, lo que hace posible la implementación de todo este mecanismo para poder firmar digitalmente.

Una Infraestructura de Firma Digital es el conjunto de Autoridades de Certificación (AC) o Autoridades Certificantes Licenciadas (ACL), un Organismo Licenciante (OL) y un Organismo Auditante (OA).

La infraestructura permite contar, a partir de la existencia de Autoridades de Certificación, con órganos responsables del mantenimiento de los estándares tecnológicos nacionales e internacionales y de los acuerdos de partes que surjan del uso y disponibilidad de los servicios de certificación que otorguen confianza a sus usuarios.

Este conjunto de órganos se encuentra en un contexto electrónico, en el que no existe contacto directo entre las partes, para dar fe de la identidad del firmante como mecanismo que permite atestiguar la identidad y relacionar los datos de verificación de firma con el titular de la firma digital. Hace que resulte posible que los usuarios de un servicio puedan presentar un documento digital que ofrezca las mismas funcionalidades que los documentos físicos, pero sin perder ni un ápice de la seguridad y confianza de que estos últimos están dotados

La Infraestructura de Firma Digital de la Administración Pública Nacional (IFDAPN), comenzó en con el decreto 427 del 21/04/1998, que 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. Disponiendo en el art. 6, que la Secretaría de la Función Pública, dependiente de la Jefatura de Gabinete de Ministros, sea la Autoridad de Aplicación del presente decreto; en el art. 8 que la Secretaria de la Función Pública de la Jefatura de Gabinete de Ministros cumplirá las funciones de Organismo Licenciante; y en el art. 9 que la Contaduría General de la Nación, dependiente de la Subsecretaría de Presupuesto de la

Secretaría de Hacienda del Ministerio de Economía y Obras y Servicios Públicos, cumplirá las funciones de Organismo Auditante, luego la Ley 25.237 del 10/01/2000 que estableció en el artículo 61 que la Sindicatura General de La Nación 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; siendo los órganos administrativos Autoridades Certificantes Licenciadas.

Además, es posible implementar una infraestructura de seguridad para la gestión de estos certificados, como por ejemplo la PKI, basada en criptografía de clave pública.

INFRAESTRUCTURA DE CLAVE PUBLICA.

La Infraestructura de Clave Pública o PKI (Public Key Infrastructure), es aceptada internacionalmente, para la emisión masiva de Certificados que permiten la identificación indubitable de las personas, documentos, sitios de internet, correo electrónico y otros en el ámbito de los sistemas de información.

Una PKI es el conjunto de servicios de seguridad que posibilitan el uso y administración de:

- Certificados y criptografía de clave pública,
- en sistemas de computación distribuidos,
- incluyendo claves, certificados y políticas.

Con la estructura PKI se pretende asegurar:

- La Confidencialidad:

  Se define como la protección de la información frente a agentes no autorizados. Se proporciona mediante la generación de una clave secreta por parte del emisor que se utiliza para codificar los datos del receptor utilizando un algoritmo. Los algoritmos se utilizan para mejorar el rendimiento de la codificación.
- La Integridad de los datos:

  Pretende asegurar que los datos enviados no han sido modificados. Esto es posible mediante la generación de un resumen a partir del documento inicial con una función Hash. La aplicación de este Hash sobre el documento que se recibe, permite comparar los resúmenes generados, pudiendo detectar un cambio del documento enviado.
- La Autenticación de Entidades y de Mensajes:

La autenticación de Entidades se basa en el nivel de confianza del receptor en el emisor de la información. Hasta ahora la autenticación se ha llevado a cabo por medio de usuario y contraseña, ahora mediante la utilización de certificados digitales se proporciona una autenticación más robusta y sencilla.

Una arquitectura PKI general de una corporación consiste en los siguientes elementos:

- Servidor PKI: constituido por una Autoridad Certificadora (CA), un directorio, y opcionalmente una recuperación de claves.
- Clientes PKI: consiste en un servidor web, en un browser, e-mail o en aplicaciones que utilicen la clave pública.
- Certificados Digitales: se serán emitidos por el servidor y utilizados por los clientes[23].

LA INFRAESTRUCTURA EN LA LEY.

Más del 80% de la Ley se dedica a normar la infraestructura de la firma digital, regulando:

- Al Certificador Licenciado.
- La Autoridad de Aplicación.
- Los Sistema de Auditoria.
- La Comisión Asesora para la Infraestructura de Firma Digital.

El Decreto 2628/02 Reglamentario de la Ley N° 25.506, también se ocupa en su mayoría de ésta infraestructura, regulando:

- Los Certificadores Licenciados.
- La Autoridad de Aplicación.
- Los Sistema de Auditoria.
- La Comisión Asesora para la Infraestructura de Firma Digital.
- El Ente Administrador de Firma Digital.
- Las Autoridades de Registro.

DE INTERES.

En el país, el primer sector que ha empezado a utilizar este sistema son los importadores, quienes están firmando de manera digital la declaración de mercancías que envían electrónicamente a la Dirección General de la Renta de Aduanas, aprovechándose del sistema de Teledespacho.

El proyecto es ejecutado en la parte técnica por la Dirección Estratégica de Comercio Electrónico (Diesco), de la Cámara de Comercio, quien se encarga de "autenticar" que la persona que envió la información realmente es quien dice ser. Para dicha autenticación Diesco emite un "certificado digital. Esta norma de seguridad es importantísima cuando se trata de transacciones comerciales donde se autoriza el pago de cheques, facturas o cualquier otro convenio.

Otro sector es la Bolsa de Comercio de Rosario, que emitirá certificados de firma digital mediante los cuales los usuarios del servicio podrán realizar la instrumentación y registración de los contratos de compraventa, que actualmente se realizan en forma manual.

La entidad se incorporó a la VeriSign Trust Network, al llegar a un acuerdo con CertiSur S.A., afiliado principal de VeriSign para los países de la región. Mediante dicho acuerdo, la Bolsa de Comercio rosarina actuará como autoridad certificante y emitirá certificados para los corredores, vendedores y compradores que operen con el servicio de firma digital de contratos de compraventa de granos que próximamente será habilitado.

Un sistema como el que utilizará la Bolsa rosarina necesita de una Infraestructura de Firma Digital, donde tendremos un Ente Licenciante, (en este caso es Certisur S.A.), que es el órgano encargado de otorgar las licencias a los certificadores de clave pública y de supervisar su actividad. A su vez, la Bolsa de Comercio actuará como Autoridad Certificante, y su función consiste en otorgar los certificados. Por último, los titulares de los certificados de clave publica serán los usuarios del sistema (vendedores, compradores y corredores que actúan en la Bolsa).

AUTORIDAD CERTIFICANTE LICENCIADA.

NOCION.

También llamada Autoridad Certificadora (AC) o como lo llama la ley Certificador Licenciado (CL).

El Certificador Licenciado es un ente u organismo que, de acuerdo con unas políticas y algoritmos, da fe de la identidad del titular de la firma digital, de la autenticidad del usuario, certifica -por ejemplo- claves públicas de usuarios o servidores. Un usuario enviará a otro su certificado (firmada por el CL) y éste comprobará su autenticidad, y lo mismo en sentido contrario.

En pocas palabras, es órgano responsable de la emisión de los Certificados luego de la verificación, por los métodos que considere en sus Políticas de Certificación, proveedora de la tecnología criptográfica para la emisión de las claves y la encargada de publicar las Claves Públicas en los denominados Directorios de Clave Pública.

Para todo ello, la Autoridad de Certificación debe detentar medidas de seguridad que infundan la confianza requerida para el éxito de su gestión, proveedor de innovaciones tecnológicas acordes a su gestión y altos niveles de Calidad en lo que hace a la atención y disponibilidad.

Toda persona que desee firmar digitalmente deberá obtener un Certificado Digital mediante un Certificador Licenciado. Los Certificadores Licenciados son empresas u organismos públicos que estén autorizados por el Ente u Organismo Licenciante para emitir certificados digitales y prestar otros servicios relacionados con la firma digital.

La Ley lo define en el art 17 diciendo que “Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados y presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el Ente Licenciante.

La actividad de los certificadores licenciados no pertenecientes al Sector Público se prestará en régimen de competencia. El arancel de los servicios prestados por los Certificadores Licenciados será establecido libremente por éstos”.

Desde ya hay que tener presente que en diversos países de Latinoamérica, entre ellos en al argentina, están operando desde el extranjero y mediante Internet empresas transnacionales que certifican digitalmente, como www.verising.com, y

también lo ralizan www.certisur.com.ar, y www.camerfirma.com, entre otras, situación que debiera ser revisada con cuidado.

LICENCIA.

Vimos que es necesario que el Certificador Licenciado (CL) cuente con una licencia, y según indica el art. 20 "Para obtener una licencia el certificador debe cumplir con los requisitos establecidos por la ley y tramitar la solicitud respectiva ante el Ente Licenciante, el que otorgará la licencia previo dictamen legal y técnico que acredite la aptitud para cumplir con sus funciones y obligaciones. Estas licencias son intransferibles".

El decreto reglamentario 2628/02 en el art. 24, establece que "Para obtener una licencia, los proveedores de servicios de certificación deberán particularizar las actividades para las cuales requieren la licencia y acreditar por los medios que este determine ante el Ente Administrador de Firma Digital:

a) Documentación que demuestre:

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

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

3.- En el caso de organización pública, la autorización de su máxima autoridad para iniciar el proceso de licenciamiento y la correspondiente aprobación de la Jefatura de Gabinete de Ministros, de acuerdo con lo dispuesto en el artículo 41 de la presente reglamentación.

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

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

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

El otorgamiento de la licencia no significa que el Ente Licenciante garantice su actividad, así se pronuncia el decreto reglamentario en el art. 25, que deja en claro que "El otorgamiento de la licencia no implica que el Ente Administrador de la Infraestructura de Firma Digital, la Jefatura de Gabinete de Ministros, las entidades

auditantes o cualquier organismo del Estado garantice la provisión de los servicios de certificación o los productos provistos por el Certificador Licenciado".

La duración de las licencias esta regulado en el art 26 del decreto, el cual reza que "Las licencias tendrán un plazo de duración de CINCO (5) años y podrán ser renovadas.

Los certificadores licenciados deberán efectuar anualmente una declaración jurada en la cual conste el cumplimiento de las normas establecidas en la Ley N° 25.506, en el presente decreto y en las normas complementarias.

Los certificadores licenciados serán sometidos a auditorias anuales".

Así mismo, el decreto regula las causales de caducidad de la licencia en su art. 27, estableciendo que "El Ente Administrador podrá disponer de oficio, y en forma preventiva la caducidad de la licencia en los siguientes casos:

a) Falta de presentación de la declaración jurada anual.

b) Falsedad de los datos contenidos en la declaración jurada anual.

c) Dictamen desfavorable de auditoría basado en causales graves.

d) Informe de la inspección dispuesta por el Ente Administrador desfavorable basado, en causales graves.

e) Cuando el certificador licenciado no permita la realización de auditorías o inspecciones dispuestas por el Ente Administrador".

CERTIFICADOS DE PROFESION.

La Ley en el art. 18 regula los certificados por profesión, diciendo que "Las entidades que controlan la matricula, 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. A ese efecto deberán cumplir los requisitos para ser certificador licenciado".

Un ejemplo de esto es la autoridad certificante del notariado argentino, la cual lleva adelante el Consejo Federal del Notariado Argentino Argentino (www.cfna.org.ar, que agrupa a los Colegios de Escribanos provinciales), a través del acuerdo que alcanzó con la empresa CertiSur SA.

FUNCIONES.

La Ley determina las funciones del Certificador, estableciendo en el art. 19 que "El certificador licenciado tiene las siguientes funciones:

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

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

c) identificar inequívocamente los certificados digitales emitidos;

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

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

1. a solicitud del titular del certificado digital

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

3. si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguro;

4. por condiciones especiales definidas en su política de certificación.

5. por resolución judicial o de la Autoridad de Aplicación.

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

OBLIGACIONES.

Las obligaciones del Certificador nos las dice el art 21 de la Ley, normando que "Son obligaciones del certificador licenciado:

a) informar a quien solicita un certificado con carácter previo a su emisión y utilizando un medio de comunicación las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de un sistema de

licenciamiento y los procedimientos, forma que garantiza su posible responsabilidad patrimonial y los efectos de la revocación de su propio certificado digital y de la licencia que le otorga el Ente Licenciante. Esa información deberá estar libremente accesible en lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;

b) abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de firma digital de los titulares de certificados digitales por él emitidos;

c) mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación;

d) operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la Autoridad de Aplicación;

e) notificar al solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable y de las obligaciones que asume por el solo hecho de ser titular de un certificado digital;

f) recabar únicamente aquellos datos personales del titular del certificado digital que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional;

g) mantener la confidencialidad de toda información que no figure en el certificado digital;

h) poner a disposición del solicitante de un certificado digital toda la información relativa a su tramitación;

i) mantener la documentación respaldatoria de los certificados digitales emitidos, por diez (10) años a partir de su fecha de vencimiento o revocación;

j) incorporar en su política de certificación los efectos de la revocación de su propio certificado digital y/o de la licencia que le otorgara la Autoridad de Aplicación;

k) publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, 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;

l) publicar en el Boletín Oficial aquellos datos que la Autoridad de Aplicación determine;

m) registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas;

n) informar en las políticas de certificación si los certificados digitales por él emitidos requieren la verificación de la identidad del titular;

o) verificar, de acuerdo con lo dispuesto en su manual de procedimientos, toda otra información que deba ser objeto de verificación, la que debe figurar en las políticas de certificación y en los certificados digitales;

p) solicitar inmediatamente al Ente Licenciante la revocación de su certificado, o informarle la revocación del mismo, cuando existieren indicios de que los datos de creación de firma digital que utiliza hubiesen sido comprometidos o cuando el uso de los procedimientos de aplicación de los datos de verificación de firma digital en él contenida haya dejado de ser seguro;

q) informar inmediatamente al Ente Licenciante sobre cualquier cambio en los datos relativos a su licencia;

r) 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;

s) emplear personal idóneo que tenga los conocimientos específicos, la experiencia necesaria para proveer los servicios ofrecidos y en particular, competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma digital y experiencia adecuada en los procedimientos de seguridad pertinentes;

t) someter a aprobación del Ente Licenciante el manual de procedimientos, el plan de seguridad y el de cese de actividades, así como el detalle de los componentes técnicos a utilizar;

u) constituir domicilio legal en la República Argentina;

v) disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la presente ley y su reglamentación;

w) cumplir con toda otra obligación emergente de su calidad de titular de la licencia adjudicada por el Ente Licenciante".

El decreto reglamentario agrega en el art. 34, que "Además de lo previsto en el artículo 21 de la Ley N° 25.506, los certificadores licenciados deberán:

a) Comprobar por sí o por medio de una Autoridad de Registro que actúe en nombre y por cuenta suya, la identidad y cualquier otro dato de los solicitantes considerado relevante para los procedimientos de verificación de identidad previos a la emisión del certificado digital, según la Política de Certificación bajo la cual se solicita.

b) Mantener a disposición permanente del público las Políticas de Certificación y el Manual de Procedimientos correspondiente.

c) Cumplir cabalmente con las políticas de certificación acordadas con el titular y con su Manual de Procedimientos.

d) Garantizar la prestación establecida según los niveles definidos en el acuerdo de servicios pactados con sus usuarios, relativo a los servicios para los cuales solicitó el licenciamiento.

e) Informar al solicitante de un certificado digital, en un lenguaje claro y accesible, en idioma nacional, respecto de las características del certificado solicitado, las limitaciones a la responsabilidad, si las hubiere, los precios de los servicios de certificación, uso, administración y otros asociados, incluyendo cargos adicionales y formas de pago, los niveles de servicio al proveer, las obligaciones que el suscriptor asume como usuario del servicio de certificación, su domicilio en la República Argentina y los medios a los que el suscriptor puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema o presentar sus reclamos.

f) Disponer de un servicio de atención a titulares y terceros, que permita evacuar las consultas y la pronta solicitud de revocación de certificados.

g) Garantizar el acceso permanente, eficiente y gratuito de los titulares y terceros al repositorio de certificados revocados.

h) Mantener actualizados los repositorios de certificados revocados por el período establecido por el Ente Administrador.

i) Abstenerse de generar, exigir, tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada del suscriptor.

j) Informar al Ente Administrador de modo inmediato la ocurrencia de cualquier evento que comprometa la correcta prestación del servicio.

k) Respetar el derecho del titular del certificado digital a no recibir publicidad de ningún tipo por su intermedio, salvo consentimiento expreso de éste.

l) Publicar en el Boletín Oficial durante un (1) día, el certificado de clave pública correspondiente a la política para la cual obtuvo licenciamiento;

m) Cumplir las normas y recaudos establecidos para la protección de datos personales.

n) En los casos de revocación de certificados contemplados en el apartado 3 del inciso e) del artículo 19 de la Ley N° 25.506, deberá sustituir en forma gratuita aquel certificado digital que ha dejado de ser seguro por otro que sí cumpla con estos requisitos.

El Ente Administrador deberá establecer el proceso de reemplazo de certificados en estos casos. En los casos en los que un certificado digital haya dejado de ser seguro

por razones atribuibles a su titular, el certificador licenciado no estará obligado a sustituir el certificado digital.

o) Enviar periódicamente al Ente Administrador, informes de estado de operaciones con carácter de declaración jurada.

p) Contar con personal idóneo y confiable, con antecedentes profesionales acordes a la función desempeñada.

q) Responder a los pedidos de informes por parte de un tercero respecto de la validez y alcance de un certificado digital emitido por él".

POLITICA DE CERTIFICACION.

El decreto en su art. 29, dice que "La Jefatura de Gabinete de Ministros definirá el contenido, mínimo de las políticas de certificación de acuerdo con los estándares nacionales e internacionales vigentes, las que deberán contener al menos la siguiente información:

a) Identificación del certificador licenciado.

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

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

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

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

RESPONSABILIDAD.

La Ley de firma digital establece la responsabilidad del Certificador Licenciado en el capitulo IX, el art. 37, que se refiere a convenio de partes, dice que "La relación entre el certificador licenciado que emita un certificado digital y el titular de ese certificado se rige por el contrato que celebren entre ellos, sin perjuicio de las previsiones de la presente ley y demás legislación vigente".

En el art. 38, regula la responsabilidad ante terceros, y dice que "El Certificador que emita un Certificado Digital, o lo reconozca en los términos del art. 16 de la

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

El art. 39 regula las limitaciones de responsabilidad, estableciendo que "Los Certificadores Licenciados no son responsables en los siguientes casos:

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

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

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

El decreto 2628/02 en el art. 31 repite la regla del art. 25 del mismo decreto, que dice que el otorgamiento de la licencia no significa que el Ente Licenciante garantice su actividad, art. 31 dice que "En ningún caso, la responsabilidad que pueda emanar de una certificación efectuada por un certificador licenciado, público o privado, comprometerá la responsabilidad pecuniaria del Estado en su calidad de Ente Administrador de la Infraestructura de Firma Digital".

El art. 30 del decreto regula la obligación del Certificador de contar con un seguro, que va a variar según las responsabilidades asumidas por él y debe contar con los requisitos allí exigidos. "El certificador licenciado debe contar con seguros vigentes acordes con las responsabilidades asumidas, que cumplan con los siguientes requisitos.

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

b) Establecer la obligación de la entidad aseguradora de informar previamente al Ente Administrador de la Infraestructura de Firma Digital la terminación del contrato o las modificaciones que reduzcan el alcance o monto de la cobertura.

Los certificadores licenciados pertenecientes a entidades y jurisdicciones del sector público quedarán exentos de la obligación de constituir el seguro previsto en el presente artículo".

RECURSOS DE LOS CERTIFICADORES LICENCIADOS.

El decreto en el art. 32, dice que " Para el desarrollo adecuado de las actividades de certificación, el certificador deberá acreditar que cuenta con un equipo de profesionales, infraestructura física tecnológica y recursos financieros, como así también procedimientos y sistemas de seguridad que permitan:

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

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

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

d) Expedir certificados que cumplan con:

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

2.- Los estándares tecnológicos aprobados por la Jefatura de Gabinete de Ministros.

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

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

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

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

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

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

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

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

SERVICIOS DE TERCEROS.

En el art. 33 del decreto se establece que "En los casos en que el certificador licenciado requiera o utilice los servicios de infraestructura tecnológicos prestados por un tercero, deberá prever dentro de su Plan de Contingencia los procedimientos a seguir en caso de interrupción de estos servicios, de modo tal que permita continuar prestando sus servicios de certificación sin ningún perjuicio para los suscriptores.

Los contratos entre el certificador licenciado y los proveedores de servicios o infraestructura deberán garantizar la ejecución de los procedimientos contemplados en el Plan de Cese de actividades aprobado por el Ente Licenciante. El certificador licenciado o en proceso de licenciamiento deberá facilitar al Ente Licenciante toda aquella información obrante en los contratos vinculada a la prestación de servicios de certificación y a la implementación del Plan de Cese de actividades y el Plan de Contingencia.

La contratación de servicios o infraestructura no exime al prestador de la presentación de los informes de auditoría, los cuales deberán incluir los sistemas y seguridades del prestador contratado".

SANCIONES

La Ley 25.506 en el capitulo X establece las sanciones para los Certificadores Licenciados. El art. 40 regula el procedimiento, diciendo que "La instrucción sumarial y la aplicación de sanciones por violación a disposiciones de la presente ley será realizada por el Ente Licenciante. Es aplicable la Ley de Procedimientos Administrativos Nº 19.549 y sus normas reglamentarias".

En el art. 41 se establecen las sanciones ante "El incumplimiento de las obligaciones establecidas en la presente ley para los certificadores licenciados dará lugar a la aplicación de las siguientes sanciones:

a) apercibimiento;

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

c) caducidad de la licencia.

Su gradación según reincidencia y/u oportunidad será establecida por la reglamentación.

El pago de la sanción que aplique el Ente Licenciante no relevará al certificador licenciado de eventuales reclamos por daños y perjuicios causados a terceros y/o bienes de propiedad de éstos como consecuencia de la ejecución del contrato que celebren y/o por el incumplimiento de las obligaciones asumidas conforme al mismo y/o la prestación del servicio".

La sanción de apercibimiento la regula el art. 42, y "Podrá aplicarse sanción de apercibimiento en los siguientes casos:

a) emisión de certificados sin contar con la totalidad de los datos requeridos, cuando su omisión no invalidare el certificado;

b) no facilitar los datos requeridos por el Ente Licenciante en ejercicio de sus funciones;

c) cualquier otra infracción a la presente ley que no tenga una sanción mayor".

La de multa el art, 43, que dice que "Podrá aplicarse sanción de multa en los siguientes casos:

a) incumplimiento de las obligaciones previstas en el artículo 21;

b) si la emisión de certificados se realizare sin cumplimentar las políticas de certificación comprometida y causaren perjuicios a los usuarios, signatarios o terceros, o se afectare gravemente la seguridad de los servicios de certificación;

c) omisión de llevar el registro de los certificados expedidos;

d) omisión de revocar en forma o tiempo oportuno un certificado cuando así correspondiere;

e) cualquier impedimento u obstrucción a la realización de inspecciones o auditorías por parte de la Autoridad de Aplicación y del Ente Licenciante;

f) incumplimiento a las normas dictadas por la Autoridad de Aplicación;

g) Reincidencia en la comisión de infracciones que dieran lugar a la sanción de apercibimiento".

El art. 44 regula la caducidad de la licencia, y dice que "Podrá aplicarse la sanción de caducidad de la licencia en caso de:

a) no tomar los debidos recaudos de seguridad en los servicios de certificación;

b) expedición de certificados falsos;

c) transferencia no autorizada o fraude en la titularidad de la licencia;

d) reincidencia en la comisión de infracciones que dieran lugar a la sanción de multa;

e) quiebra del titular.

La sanción de caducidad inhabilita a la titular sancionada y a los integrantes de órganos directivos por el término de 10 años para ser titular de licencias".

En cuanto a los recursos para las sanciones, el art. 45 regula que "Las sanciones aplicadas podrán ser recurridas ante los tribunales federales con competencia en lo Contencioso Administrativo correspondientes al domicilio de la entidad, una vez agotada la vía administrativa pertinente.

La interposición de los recursos previstos en este capítulo tendrá efecto devolutivo.

La jurisdicción la establece el art. 46, que dice que "En los conflictos entre particulares y certificadores licenciados es competente la Justicia en lo Civil y Comercial Federal. En los conflictos en que sea parte un organismo público certificador licenciado, es competente la Justicia en lo Contencioso Administrativo Federal".

CESE DEL CERTIFICADOR LICENCIADO.

La Ley en el art. 22 regula el cese del certificador, y dice que "El certificador licenciado cesa en tal calidad:

a) por decisión unilateral comunicada al Ente Licenciante;

b) por cancelación de su personería jurídica;

c) por cancelación de su licencia dispuesta por el Ente Licenciante.

La Autoridad de Aplicación determinará los procedimientos de revocación aplicables en estos casos".

AUTORIDADES DE REGISTRO.

Además, la Autoridad de Certificación, se puede valer de Autoridades de Registro (AR, o RA registration authorities) que son las encargadas de realizar las verificaciones de personas y solicitar la emisión del correspondiente Certificado, bajo los procedimientos que determine la Autoridad de Certificación de la cual depende. Por

ejemplo, una corporación se erige como una autoridad de registro, cuando solicita los certificados para sus propios empleados, siendo suficiente aval su solicitud. El certificado de esa persona lo habilitará a firmar como miembro de la organización, y será la misma organización la que solicitará su revocación cuando esa persona no pertenezca mas a la empresa.

El decreto reglamentario en el art. 35 establece que "Los Certificadores Licenciados podrán delegar en Autoridades de Registro las funciones de validación de identidad y otros datos de los suscriptores de certificados y de registro de las presentaciones y trámites que les sean formuladas, bajo la responsabilidad del Certificador Licenciado, cumpliendo las normas y procedimientos establecidos por la presente reglamentación.

Una autoridad de Registro es una entidad responsable de las siguientes funciones:

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

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

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

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

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

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

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

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

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

Y en el art. 36 regula la responsabilidad del certificador licenciado respecto de la Autoridad de Registro, diciendo que "Una Autoridad de Registro puede constituirse como una única unidad o con varias unidades dependientes jerárquicamente entre sí,

pudiendo, delegar su operatoria en otras autoridades de registro, siempre que medie la aprobación del Certificador Licenciado. El Certificador, Licenciado es responsable con los alcances establecidos en la Ley N° 25.506, aún en el caso de que delegue parte de su operatoria en Autoridades de Registro, sin perjuicio del derecho del certificador de reclamar a la Autoridad de Registro las indemnizaciones por los daños y perjuicios que aquél sufriera como consecuencia de los actos y/u omisiones de ésta".

También pueden valerse de Autoridades de fechado digital (AFD oTSA time stamping authorities), que vinculan un instante de tiempo a un documento electrónico avalando con su firma la existencia del documento en el instante referenciado (resolverían el problema de la exactitud temporal de los documentos electrónicos).Estas autoridades (AR y AFD) pueden materializarse como entes individuales, o como una colección de servicios que presta una entidad multipropósito.

ENTE ADMINISTRADOR DE LA FIRMA DIGITAL.

INTRODUCCION.

El Ente Administrador de la Firma Digital es el Ente Licanciante (EL), el cual depende de la Jefatura de Gabinete de Ministros y es un órgano técnico y administrativo encargado de otorgar las licencias a los certificadores y de supervisar su actividad.

Este Ente u Organismo Licenciante (OL), autoriza a los Certificadores a emitir certificados digitales y a prestar otros servicios relacionados con la firma digital. La autorización consiste en la licencia que éste ente otorga a los Certificadores prevista en el art. 20 de la ley y en el 24 del decreto reglamentario, Licenciando así a los Certificadores.

El art. 11 del decreto reglamentario creo "...el Ente Administrador de Firma Digital dependiente de la Jefatura de Gabinete de Ministros, como órgano técnico, administrativo encargado de otorgar las licencias a los certificadores y de supervisar su actividad, según las exigencias instituidas por el presente decreto y las normas reglamentarias, modificatorias o de aplicación que se dicten en el futuro y de dictar las normas tendientes a asegurar el régimen de libre competencia, equilibrio de participación en el mercado de los prestadores y protección de los usuarios".

En cuanto a sus autoridades el art. 12 del decreto estableció que "El Ente Administrador de Firma Digital será conducido por un Directorio integrado por tres (3) miembros, designados por el Jefe de Gabinete de Ministros, previo concurso. Hasta tanto, sea realizado el concurso el Jefe de Gabinete de Ministros designará a los integrantes del Directorio, uno de los cuales ocupará el cargo de Presidente del Ente. El gerenciamiento del Ente estará a cargo del Coordinador Ejecutivo designado por el Jefe de Gabinete de Ministros".

Con respecto a la organización del Ente Administrador, se estableció en el art. 15 que "Dentro del plazo de sesenta (60) días corridos de la fecha de constitución del Directorio, el Ente Administrador de Firma Digital elevará para su consideración al Jefe de Gabinete de Ministros la propuesta de su estructura organizativa y de su reglamento de funcionamiento".

FUNCIONES.

Las Funciones del Ente Administrador están reguladas en el art. 13 del decreto y establece que "Son funciones del Ente Administrador:

a) Otorgar las licencias habilitantes para acreditar a los certificadores en las condiciones que fijen el presente decreto y las normas reglamentarias, modificatorias o de aplicación que se dicten en el futuro.

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

c) Denegar las solicitudes de licencia a los prestadores de servicios de certificación que no cumplan con los requisitos establecidos, para su licenciamiento.

d) Revocar las licencias otorgadas a los Certificadores licenciados que dejen de cumplir con los requisitos establecidos para su licenciamiento.

e) Aprobar las políticas de certificación, el manual de procedimiento, el plan de seguridad, de cese de actividades y el plan de contingencia, presentado por los certificadores solicitantes de la licencia o licenciados.

f) Solicitar los informes de auditoría en los casos que correspondiere.

g) Realizar inspecciones a los certificadores licenciados por sí o por terceros.

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

i) Disponer la instrucción sumarial, la aplicación de sanciones e inhabilitar en forma temporal o permanente a todo certificador o licenciado que no respetare o incumpliere los requerimientos y disposiciones de la Ley N° 25.506, el presente decreto y las normas complementarias.

j) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, números telefónicos, direcciones de internet y certificados digitales de los certificadores licenciados.

k) Publicar en internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, los números telefónicos, direcciones de internet y certificados digitales de los certificadores cuyas licencias han sido revocadas.

I) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, el domicilio,

números telefónicos, direcciones de internet y certificados digitales del Ente Administrador.

m) Administrar los recursos generados de acuerdo con lo dispuesto por el artículo 16 de la presente reglamentación, provenientes de las distintas fuentes de financiamiento.

n) Fijar el concepto y los importes de todo tipo de aranceles y multas previstos en la Ley N° 25.506 y en el artículo 16 de la presente reglamentación.

o) Solicitar la ampliación o aclaración sobre la documentación presentada por el certificador.

p) Dictar las normas tendientes a asegurar el régimen de libre competencia, equilibrio de participación en el mercado de los prestadores y protección de los usuarios".

OBLIGACIONES.

Las obligaciones del Ente Administrador las establece el art. 14, diciendo que "El Ente Administrador tiene idénticas obligaciones que los titulares, de certificados y que los Certificadores Licenciados, en su caso, y además debe:

a) Permitir el acceso público permanente a la nómina actualizada de certificadores licenciados con los datos correspondientes.

b) Supervisar la ejecución del plan de cese de actividades de los Certificadores licenciados que discontinúan sus funciones;

c) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas.

d) Supervisar la ejecución de planes de contingencia de los certificadores licenciados.

e) Efectuar las tareas de control del cumplimiento de las recomendaciones formuladas por el Ente Administrador para determinar si se han tomado las acciones correctivas correspondientes.

f) Recibir, evaluar y resolver los reclamos de los usuarios de certificados digitales relativos a la prestación del servicio por parte de certificadores licenciados".

RECURSOS Y FINANCIAMENTO.

El decreto en el art. 16 define como estarán compuestos los recursos del Ente Administrador, diciendo que "El Ente Administrador podrá arancelar los servicios que preste para cubrir total o parcialmente sus costos. Los recursos propios del Ente Administrador se integrarán con:

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

1.- Servicios de certificación digital,

2.- Servicios de certificación digital de fecha y hora,

3.- Servicios de almacenamiento seguro de documentos electrónicos,

4.- Servicios prestados por autoridades de registro,

5. - Servicios prestados por terceras partes confiables,

6. - Servicios de certificación de documentos electrónicos firmados digitalmente

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

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

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

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

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

f) El producido de multas.

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

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

Luego regula en el art. 17 el financiamiento del Ente Administrador, para lo cual establece que se instruya "...a la Jefatura de Gabinete de Ministros para que proceda a incluir en su presupuesto los fondos necesarios para que el Ente Administrador pueda cumplir adecuadamente sus funciones.

Transitoriamente, desde la entrada en vigencia de la presente reglamentación y hasta que se incluyan las partidas necesarias en el Presupuesto Nacional los costos de

financiamiento del Ente Administrador serán afrontados con el crédito presupuestario correspondiente a la Jefatura de Gabinete de Ministros".

AUTORIDAD DE APLICACION.

INTRODUCCION.

La Ley de Firma Digital en el art. 29 establece cual es la Autoridad de Aplicación, y dice que "La Autoridad de Aplicación de la presente ley será la Jefatura de Gabinete de Ministros".

El decreto 2628/02 reglamentario de la firma digital establece las normas técnicas en el art. 4, diciendo "Facúltase a la Jefatura de Gabinete de Ministros, a determinar las normas y los procedimientos técnicos para la generación, comunicación, archivo y conservación del documento digital o electrónico, según lo previsto en los artículos 11 y 12 de la Ley N° 25.506".

Y en el art. siguiente (art. 5) regula dicha conservación, para lo que establece que "El cumplimiento de la exigencia legal de conservar documentos, registros o datos, conforme a la legislación vigente a la materia, podrá quedar satisfecha con la conservación de los correspondientes, documentos digitales firmados digitalmente. Los documentos, registros o datos electrónicos, deberán ser almacenados por los intervinientes o por terceros confiables aceptados por los intervinientes, durante los plazos establecidos en las normas específicas.

Se podrán obtener copias autenticadas a partir de los originales en formato digital firmado digitalmente. La certificación de autenticidad se hará de conformidad a los procedimientos legales, vigentes para el acto de que se trate, identificando el soporte que procede la copia".

En cuanto a la regulación, se expresa el art. 6 por el cual se faculta "...a la Jefatura de Gabinete de Ministros a establecer:

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

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

c) Las condiciones mínimas de emisión de certificadosdigitales.

d) Los casos en los cuales deben revocarse los certificados digitales.

e) Los datos considerados públicos contenidos en los certificados digitales.

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

g) La información que los certificadores licenciados deberán publicar por internet.

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

i) Los procedimientos mínimos de revocación de certificados digitales cualquiera que sea la fuente de emisión, y los procedimientos mínimos de conservación de la documentación de respaldo de la operatoria de los certificadores licenciados, en el caso que éstos cesen su actividad.

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

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

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

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

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

o) Los procedimientos aplicables para el reconocimiento de certificados extranjeros.

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

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

r) Los niveles de licenciamiento.

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

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

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

En el art. 32 de la Ley se establece el arancelamiento y establece que"La Autoridad de Aplicación podrá cobrar un arancel de licenciamiento para cubrir su costo operativo y de las auditorias realizadas por sí o por terceros contratados a tal efecto".

FUNCIONES.

Las funciones de la Autoridad de Aplicación las menciona el art. 30, el cual dice que "La Autoridad de Aplicación tiene las siguientes funciones:

a) dictar las normas reglamentarias y de aplicación de la presente;

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

c) determinar los efectos de la revocación de los certificados de los certificadores licenciados o del Ente Licenciante;

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

e) determinar las pautas de auditoria, incluyendo los dictámenes tipo que deba emitirse como conclusión de las revisiones;

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

g) determinar los niveles de licenciamiento.

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

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

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

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

OBLIGACIONES.

Las obligaciones de éste Ente las establece el art. 31,que dice que "En su calidad de titular de certificado digital, la Autoridad de Aplicación tiene las mismas obligaciones que los titulares de certificados y que los Certificadores Licenciados. En especial y en particular debe:

a) abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos utilizados para generar la firma digital de los Certificadores Licenciados;

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

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

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

e) supervisar la ejecución del plan de cese de actividades de los Certificadores Licenciados que discontinúan sus funciones".

COMISION ASESORA.

La Comisión Asesora para la Infraestructura de la Firma Digital es creada por la Ley de Firma Digital en su art. 28, que dice "Créase en el ámbito jurisdiccional de la Autoridad de Aplicación, la Comisión Asesora para la Infraestructura de Firma Digital".

El art. 7 del decreto reglamentario dice que "En el ámbito de la Jefatura de Gabinete de Ministros funcionará la Comisión Asesora para la Infraestructura de Firma Digital, que se constituirá de acuerdo a lo dispuesto por el artículo 35 de la Ley N° 25.506".

La integración y funcionamiento de la Comisión esta regulada en el art. 35 de la Ley, el que establece que "La Comisión Asesora para la Infraestructura de Firma Digital estará integrada multidisciplinariamente por un máximo de 7 (siete) profesionales de carreras afines a la actividad de reconocida trayectoria y experiencia, provenientes de Organismos del Estado Nacional, Universidades Nacionales y Provinciales, Cámaras, Colegios u otros entes representativos de Profesionales.

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

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

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

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

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

b) Antecedentes académicos y/o profesionales o laborales en la materia".

El Art. 9 del decreto dice que "El ejercicio de las funciones como miembro de la Comisión Asesora para la Infraestructura de Firma Digital será ad honorem".

Y el art. 10 del mismo decreto regula que "La Comisión Asesora para la Infraestructura de Firma Digital establecerá los mecanismos que permitan mantener un intercambio de información fluido con organismos públicos, Cámaras, usuarios y asociaciones de consumidores sobre los temas que se está tratando a los efectos de recibir aportes y opiniones. Para cumplir con este cometido podrá implementar consultas públicas presenciales, por escrito o mediante foros virtuales, abiertos e indiscriminados, o cualquier otro medio que la Comisión considere conveniente o necesario.

La Ley establece las funciones de la Comisión en el art. 36, el que dice que "La Comisión debe emitir recomendaciones por iniciativa propia o a solicitud de la Autoridad de Aplicación, sobre los siguientes aspectos:

a) estándares tecnológicos;

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

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

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

e) otros que le sean requeridos por la Autoridad de Aplicación".

SISTEMA DE AUDITORIA.

La Ley 25.506 regula el Sistema de Auditoría en el art. 27, donde establece que "La Autoridad de Aplicación, con el concurso de la Comisión Asesora para la Infraestructura de Firma Digital, diseñará un sistema de auditoría para evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, como así también el cumplimiento con las especificaciones del manual de procedimientos y los planes de seguridad y de contingencia aprobados por el Ente Licenciante".

En cuanto a los sujetos a auditar, el art. 33 dice que "El Ente Licenciante y los Certificadores Licenciados, deben ser auditados periódicamente, de acuerdo al sistema de auditoria que diseñe y apruebe la Autoridad de Aplicación.

La Autoridad de Aplicación podrá implementar el sistema de auditoria por sí o por terceros habilitados a tal efecto. Las auditorias deben como mínimo evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, como así también el cumplimiento con las especificaciones del manual de procedimientos y los planes de seguridad y de contingencia aprobados por el Ente Licenciante".

Con respeto a las auditorías por terceros, el art. 34 establece que "Podrán ser terceros habilitados para efectuar las auditorias las Universidades y organismos científicos y/o tecnológicos nacionales o provinciales, los Colegios y Consejos profesionales, que acrediten experiencia profesional acorde en la materia".

El art. 18 del decreto reglamentario establece que "La Jefatura de Gabinete de Ministros convocará a concurso público para la precalificación de entidades de auditoría entre las universidades y organismos científicos y/o tecnológicos nacionales o provinciales, los Colegios y Consejos profesionales, que acrediten experiencia profesional acorde en la materia, interesadas en prestar el servicio de auditoría de entidades prestadoras de servicios de certificación digital. A tal fin, elaborará un Pliego Estándar de Precalificación de Entidades de Auditoría, y determinará la periodicidad de la convocatoria".

El Informe de auditoría lo regula el art. 19 del decreto, que dice que "El informe de auditoría evaluará los sistemas utilizados por el certificador de acuerdo con los requerimientos de la Ley N° 25.506, el presente decreto y las normas complementarias".

El art. 20 del mismo decreto dice que "Para garantizar la objetividad e imparcialidad de la actividad de auditoría no podrán desempeñarse en la prestación de

servicios de auditoría aquellas entidades o personas vinculadas con prestadores de servicios de certificación, lo que será establecido en el Pliego Estándar de Precalificación de Entidades de Auditoría previsto en el artículo 18 del presente decreto".

Por último, el art. 21 del decreto se refiere al deber de confidencialidad, diciendo que "Las entidades auditantes y las personas que efectúen las auditorías deben mantener la confidencialidad sobre la información considerada amparada bajo normas de confidencialidad por el Certificado Licenciado".

CONCLUSION.

Nadie puede discutir el avance tecnológico constante que se ha experimentado y que día a día seguimos experimentando, esto que se ha dado a llamar "la revolución tecnológica" nos produjo un profundo cambio en la forma de relacionarnos.

La computadora, como un día lo hizo el televisor, se ha vuelto un elemento básico y necesario en la vida de toda persona y de toda familia, para pasar a serlo de toda empresa y de todo Estado; y si no, como podríamos imaginarnos sin una computadora; sin la informática.

Nos hallamos en una economía globalizada que se potenciado por este fenómeno tecnológico, siendo Internet su máxima expresión, donde se ven nuevas formas de información, de comunicación y de comercialización.

Todos estos cambios en la vida social, acarrean nuevos problemas e interrogantes que requieren, desde el ámbito del derecho la elaboración de respuestas adecuadas.

En efecto, es función y objetivo de la moderna disciplina del Derecho Informático, observar el fenómeno tecnológico, detectar aquellos nuevos problemas e interrogantes y elaborar finalmente, soluciones jurídicas.

Siendo una de esas soluciones la Firma Digital, la cual es una herramienta fundamental para la inserción del país en el mercado globalizado, que ha receptado al mercado digital, y no permitir que la brecha que nos separa con los países más desarrollados se amplíe, formando parte desde un primer momento de este nuevo mundo digital.

En este mercado internacional cada ves más global, es necesario que los países adopten un marco legal compatible o similar, para facilitar su uso y desarrollo.

Legislativamente hemos empezado bien, siguiendo el modelo de la UNCITRAL, adoptamos el principio de la "neutralidad tecnológica" para la Ley de Firma Digital, utilizando una técnica legislativa amplia, de principios generales, donde la ley brinda un marco general regulatorio en torno a la seguridad informática, como es tendencia mayoritaria en el derecho comparado. Ya que se intenta legislar para el presente y para el futuro, evitando el condicionamiento a la tecnología que se utiliza hoy en día, pues ello llevaría a tener que modificarla quizás a breve plazo. Si bien, se utiliza la criptografía asimétrica, ya que es la más segura y la única que se puede implementar de manera que cumpla con las características de la firma ológrafa.

El sistema criptográfico asimétrico utilizado para firmar digitalmente por la ley se podría emplear, en el futuro, en forma conjunta con los métodos biométricos como puede ser la estructura vascular de la retina ocular, la estructura visible del iris, la composición espectral de la voz, la imagen facial o la dinámica de posición, velocidad y presión de generación de una firma manuscrita, etc., dotando a la firma digital de más seguridad y evitando concientizar a las personas de mantener secreta la clave privada e impedir su utilización por un tercero. Existen en el mercado dispositivos que integran la biometría como acceso a los certificados almacenados en su interior. Los tres tipos de dispositivos biométricos que se pueden encontrar según su técnica de comparación de huellas son:

- System-on-Card: el sensor biométrico, el procesador y el algoritmo están implementados en la tarjeta. La extracción, la comparación y el almacenamiento de los datos biométricos se realizan en la tarjeta.
- Match-on-Card: el sensor biométrico y el procesador se encuentran integrados en el lector de la tarjeta. La extracción se realiza en el lector, mientras que la comparación y el almacenamiento de los datos biométricos se realizan en la tarjeta.
- Template-on-Card: el sensor biométrico y el procesador se encuentran integrado en el lector de la tarjeta. El algoritmo se divide entre el lector y la tarjeta. La extracción y la comparación se realiza en el lector mientras que el almacenamiento de los datos se realiza en la tarjeta.

La fundamental importancia de ésta Ley reside en haber modificado el ordenamiento jurídico argentino, entre ellos al Código Civil, incorporando o extendiendo su protección, a nuevos elementos digitales, como la firma digital y el documento digital, consagrando el principio de “no discriminación”, otorgándole pleno valor y eficacia jurídica a la firma digital, a la firma electrónica y al documento digital.

La firma digital que es el resultado del procedimiento matemático aplicado al documento, es igual a la firma ológrafa en cuanto a su valor jurídico y formas de utilización. Al igual que el documento digital, que es una secuencia informática de bits (unos y ceros) que puede representar cualquier tipo de información, es igual al documento escrito en cuanto a su valor jurídico y probatorio, y formas de utilización, si bien hay que agregarle todas las aplicaciones, tanto a la firma digital como al documento digital, que devienen como consecuencia del uso de un medio electrónico, y su rapidez y la mayor seguridad que brinda.

Por que se bien la tecnología utilizada para la firma digital no es perfecta ni infalible, es importante destacar que la firma manuscrita tampoco es perfecta o infalible, puesto que es posible alterar de forma indetectable el contenido de un documento en soporte papel o falsificar una firma manuscrita y además existe un margen de error en la labor de los peritos caligráficos. Y es por ello y por todo el procedimiento utilizado para firmar digitalmente y las garantías que ella brinda, que la firma digital sin ser perfecta ni infalible, es más segura que la firma ológrafa.

La firma digital sirve para identificar al titular de ella, constituyendo un mecanismo esencial para proveer seguridad y desarrollar la confianza en las redes abiertas. Por ello constituyen un elemento clave para el desarrollo del comercio electrónico en redes, y proporciona un amplio abanico de servicios de seguridad, que superan ampliamente a los ofrecidos en un contexto físico por el DNI o pasaporte y las firmas manuscritas.

Pero el comercio electrónico no es el único beneficiario, actualmente las empresas y los organismos públicos de nuestro país 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 resultando en un acceso a la información mas lento y costoso. Los requerimientos legales que exigían la utilización del papel con firma manuscrita impedían la implementación de los modernos sistemas informáticos mediante los cuales se puede acceder a documentos a distancia y a la información en forma inmediata.

En el ámbito de la Administración Pública, la firma digital tiene enormes aplicaciones, algunas de las cuales son: presencia de la administración en la red, consulta de información personal desde Internet, realización de cualquier trámite por internet, acceso a aplicaciones informáticas de gestión por ciudadanos y empresas, comunicación entre dependencias de distintas administraciones, integración de información al ciudadano desde distintas administraciones, democracia electrónica realizando el sufragio por red, DNI- digital como ya lo tienen Finlandia y Austria, etc.

El mayor beneficio de la utilización de la firma digital, se produce tanto en las nuevas modalidades de trabajo como en el incremento en la velocidad de circulación de la información que permite hacer factible el documento digital, lo que permite que las organizaciones y empresas de nuestro país ofrezcan un mejor nivel de servicios a sus clientes y simultáneamente reduzcan sus costos, aumentando su productividad y su competitividad en lo que hoy son mercados cada vez más globalizados y competitivos.

La firma digital se utiliza en algunos sectores de la administración pública y pronto se aplicará en todo los sectores. Pero esto es solo el primer paso para la implementación en la actividad privada, para lo cual aún faltan cumplir ciertos requerimientos técnicos, falta lo que la ley denomina certificador licenciado, que es una cuestión administrativa, y que para su correcto establecimiento se además de una buena información al ciudadano y a la empresa. Sin embargo, la ley habilita a firmar digitalmente, siempre y cuando las partes involucradas estén de acuerdo, para lo cual firman un convenio, lo que es ampliamente utilizado por empresas privadas, principalmente con los proveedores.

Pronto veremos en nuestros Tribunales, juicios en donde se cumplimenten con todos los requisitos legales así como con todas sus etapas procesales por medios electrónicos, tanto las que dependen de la instancia de las partes como los actos a cargo del Tribunal. Como sucedió en el mes de julio de 2003 en los Tribunales de Colombia, donde el actor presentó el escrito y sus anexos, admitiendo el juez la acción y por consiguiente, corriendo traslado a los demandados, quienes contestaron y aportaron sus pruebas en tiempo y forma, siendo finalmente dictado y notificado el fallo, todo por medios electrónicos. En todo el expediente no existe un solo papel, ni las partes tuvieron que comparecer ante las autoridades jurisdiccionales.

Pronto veremos como nuestra profesión se informatiza, seremos pioneros en vernos cyber-abogados.

CITAS.

[1] La versión completa de la Internet Society está disponible en: http://www.isoc.org.

[2] Pardini A. A., Derecho de Internet. Ed. La Rocca, Bs. As., 2002, pág. 50.

[3] Nuñez A. S., Internet y el comercio electrónico. Ed. La Ley, Bs. As., 2001, pág. 30 y 31.

[4] Comisión Redactora del Anteproyecto de Ley de Firma Digital. El Informe de la Comisión Redactora está disponible en: http://www.pki.gov.ar/PKIdocs/Informe.html.

[5] Carrión H. D., Análisis comparativo de la legislación y proyectos a nivel mundial sobre firmas y certificados digitales. Disponible desde: URL: http://www.delitosinformaticos.com/firmaelectronica/analisis.shtml.

[6] Lorenzetti R. L., Revista de Derecho comparado, Comercio Electrónico, La Ley Argentina de Firma Digital. Ed. Rubinzal-Culzoni, Bs. As., 2002, pág. 106 y 107.

[7] Álvarez F., Bournissent M. J. y Sánchez S., La Firma Digital en el Proyecto de Código Civil Argentino. En: II Congreso de noveles abogados del Litoral, Libro de Ponencias, 2000, noviembre 17-18, Santa Fe, pág. 90.

[8] Real Academia Española. Diccionario de la Lengua Española, 19 ed., T. II, Ed. Espasa, Madrid, 1970, pág. 381.

[9] Pascale M., Firma Digital. En: VIII Congreso Iberoamericano de Derecho e Informática, CD de Memorias, 2000, noviembre 21-25 , México, DF.

[10] Campoli GA, Argentina: Firma Ológrafa y Firma No Ológrafa. Disponible desde: URL: http://www.alfa-redi.org.

[11] Sosa T. E., Nociones sobre Firma Digital, DJ/Conocimiento y actualización del Derecho, DJ 2001-2, pág. 725.

[12] Linch H. M., Comentario a la ley 25.506 de firma y documento digital. Antecedentes Parlamentarios, 2002-A, pág 855 y 856.

[13] Devoto M., Comercio Electrónico y Firma Digital. Ia. ed., Ed. La Ley, Buenos Aires, 2001, pág. 232.

[14] Arce A. J., La Firma Digital, Aspectos Jurídicos. Disponible desde: URL: http://alfa-redi.org.

[15] Cortes D. E., Certificado y firma digital: Nuevas tecnologías de comunicación e información. Disponible desde: URL: http://www.certificadodigital.com.ar.

[16] Quiroga E. M., La eficacia probatoria de los medios informáticos en el consentimiento contractual. Jurisprudencia Argentina, JA-2001-IV, pág. 1152.

[17] Documento y Firma Digital: Para entrar en tema**,** Nota de fondo. Diario Judicial del 19-05-00. Disponible desde: URL: http://www.diariojudicial.com.

[18] Colerio J., Pautas para una Teoría del Valor probatorio del Documento Electrónico, Jurismática n. 4, Ed. Abeledo-Perrot, Bs. As., 1993, pág. 13, 18 y 19.

[19] Colerio J., Ob. Cit., pág. 20 y 21.

[20] Devoto M., Ob. Cit., pág. 232.

[21] Jesús Angel J., Criptografía para principiantes. Disponible en: URL: www.htmlweb.net.

[22] Secretaria de la Función Pública. La Infraestructura de la Firma Digital está disponible en: http://www.pki.gov.ar.

[23] La versión completa de las Aplicaciones de Internet: La necesidad de sistemas seguros, está disponible en http://www.cetenasa.es.

BIBLIOGRAFIA.

- Pardini A. A., Derecho de Internet. Ed. La Rocca, Bs. As., 2002.
- Nuñez A. S., Internet y el comercio electrónico. Ed. La Ley, Bs. As., 2001.
- Lorenzetti R. L., Revista de Derecho comparado, Comercio Electrónico, La Ley Argentina de Firma Digital. Ed. Rubinzal-Culzoni, Bs. As., 2002.
- Lorenzetti R. L., Comercio Electrónico. Ed. Abeledo-Perrot, Bs. As., 2001.
- Colerio J., Pautas para una Teoría del Valor probatorio del Documento Electrónico, Jurismática n. 4, Ed. Abeledo-Perrot, Bs. As., 1993.
- Sarra A.V., Comercio electrónico y derecho. Ed. Astrea, Bs. As., 2000.
- Altmark D. R., Informática y derecho, Tomo 7. Ed. Depalma, Bs. As., 2001.
- Giannantonio E., El valor jurídico del documento electrónico. Ed Depalma, Bs. As., 1987.
- Beltramone G. y Zabale E., El Derecho en la era digital. Derecho Informático de fin de siglo. Ed. Juris, Rosario, 1997.
- Zarich F., Derecho Informático, Tomo 1. Ed. Juris, Rosario, 2000.
- Lambertucci P. y La Peruta M. V., Comercio electrónico. Derecho Informático, Tomo 2. Ed. Juris, Rosario, 2001.
- Zarich F., Derecho Informático, Tomo 3. Ed. Juris, Rosario, 2000.
- Devoto M., Comercio Electrónico y Firma Digital. Ia. ed., Ed. La Ley, Buenos Aires, 2001.
- Devoto M., Claves para el éxito de una infraestructura de firma digital. La Ley, 2000-A.
- Linch H. M., Comentario a la ley 25.506 de firma y documento digital. Antecedentes Parlamentarios, 2002-A.

- Linch H. M. Y Devoto M., Banca, comercio, moneda electrónica y la firma digital. La Ley, 1997-B.
- Sosa T. E., Nociones sobre Firma Digital, DJ/Conocimiento y actualización del Derecho, DJ 2001-2.
- Quiroga E. M., La eficacia probatoria de los medios informáticos en el consentimiento contractual. Jurisprudencia Argentina, JA-2001-IV.
- Quiroga E. M., Nuevas Tecnologías aplicadas al procedimiento judicial. Jurisprudencia Argentina, JA-2002-III.
- Gaibrois L. M., Criptografía, informática y derecho. Jurisprudencia Argentina, JA-1999-II.
- Altmark D. R., Documento electrónico. Jurisprudencia Argentina, JA-1999-II.
- Álvarez F., Bournissent M. J. y Sánchez S., La Firma Digital en el Proyecto de Código Civil Argentino. II Congreso de noveles abogados del Litoral, Libro de Ponencias, 2000, noviembre 17-18, Santa Fe.
- Pascale M., Firma Digital. VIII Congreso Iberoamericano de Derecho e Informática, CD de Memorias, 2000, noviembre 21-25, México, DF.
- Palazzi P., Firma digital y comercio electrónico en internet. VI Congreso Iberoamericano de Derecho e Informática, 1998, mayo, Montevideo, Uruguay.
- Jesús Angel J., Criptografía para principiantes. Disponible en: URL: www.htmlweb.net.
- Carrión H. D., Análisis comparativo de la legislación y proyectos a nivel mundial sobre firmas y certificados digitales. Disponible desde: URL: http://www.delitosinformaticos.com/firmaelectronica/analisis.shtml.
- Campoli GA, Argentina: Firma Ológrafa y Firma No Ológrafa. Disponible desde: URL: http://www.alfa-redi.org.

- Falivene A., Ley de firma digital Argentina. Disponible desde: URL: http://www.alfa-redi.org.
- Arce A. J., La Firma Digital, Aspectos Jurídicos. Disponible desde: URL: http://alfa-redi.org.
- Cortes D. E., Certificado y firma digital: Nuevas tecnologías de comunicación e información. Disponible desde: URL: http://www.certificadodigital.com.ar.
- Comisión Redactora del Anteproyecto de Ley de Firma Digital. El Informe de la Comisión Redactora está disponible en: http://www.pki.gov.ar/ PKIdocs/Informe.html.
- Secretaria de la Función Pública. La Infraestructura de la Firma Digital está disponible en: http://www.pki.gov.ar.
- Real Academia Española. Diccionario de la Lengua Española, 19 ed., T. II, Ed. Espasa, Madrid, 1970.
- Documento y Firma Digital: Para entrar en tema. Diario Judicial del 19-05-00. Disponible desde: URL: http://www.diariojudicial.com.
- Aplicaciones de Internet: La necesidad de sistemas seguros, disponible en: http://www.cetenasa.es.
- Internet Society, disponible en: http://www.isoc.org.

SUPRIMIR DESDE ACA.

[1] Ver http://www.isoc.org

[2] Pardini, Aníbal A., "Derecho de Internet", ed. La Rocca, Bs. As., 2002, pág. 50.

[3] deefefefefefeefefe
[4] Ver http://www.pki.gov.ar/PKIdocs/Informe.html

[5] Ver: http://www.delitosinformaticos.com/firmaelectronica/analisis.shtml.

[6] Lorenzetti, Ricardo Luis, Revista de Derecho comparado, Comercio Electrónico, La Ley Argentina de Firma Digital, Ed. Rubinzal-Culzoni, Bs. As., 2002, pág. 106 y 107.

[7] II Congreso de noveles abogados del Litoral, Libro de Ponencias, La Firma Digital en el Proyecto de Código Civil Argentino, ponentes: Fabián Álvarez, Maria José Bournissent y Sabrina Sánchez, Pág. 90.

[8] Diccionario de la Lengua Española, 19 ed., T. II, pág. 381, Madrid, 1970.

[9] Memorias del VIII Congreso Iberoamericano de Derecho e Informática, México, 21 a 25 de Noviembre de 2000, Ponencia "Firma Digital", de Maricarmen Pascale.

[10] Campoli, Gabriel A., "Argentina: Firma Ológrafa y Firma No Ológrafa", Ver: www.alfa-redi.org.

[11] DJ/Conocimiento y actualización del Derecho, DJ 2001-2, Pág. 725, Nociones sobre Firma Digital, por Toribio E. Sosa

[12] Linch, Horacio M., "Comentario a la ley 25.506 de firma y documento digital", Antecedentes Parlamentarios, 2002-A, pág 855 y 856.

[13] Devoto, Mauricio, "Comercio Electrónico y Firma Digital", ed. LALEY, Buenos Aires, Ia. ed., 2001, pág. 232.

[14] Ver: http://pki.gov.ar.

[15] Ver: www.certificado digital.com.ar.

[16] [16] Jurisprudencia Argentina, JA-2001-IV, pág. 1152, La eficacia probatoria de los medios informáticos en el consentimiento contractual, por Eduardo Molina Quiroga.

[17] [17] Documento y Firma Digital: Para entrar en tema**.** Nota de fondo. Diario Judicial del 19/05/00.

[18] [18] Colerio J., "Pautas para una Teoría del Valor probatorio del Documento Electrónico", "Jurismática" n. 4, Ed. Abeledo-Perrot, Bs. As., 1993, pág. 13, 18 y 19.

[1919] Colerio, J., ob. Cit., pág. 20 y 21.

[2020] Devoto, Mauricio, "Comercio Electrónico y Firma Digital", ed. LALEY, Buenos Aires, Ia. ed., 2001, pág. 232.

[2121] Ver: www.htmlweb.net.

[22] [22] Ver: www.pki.gov.ar.

[23] [23] Ver: http://www.cetenasa.es.