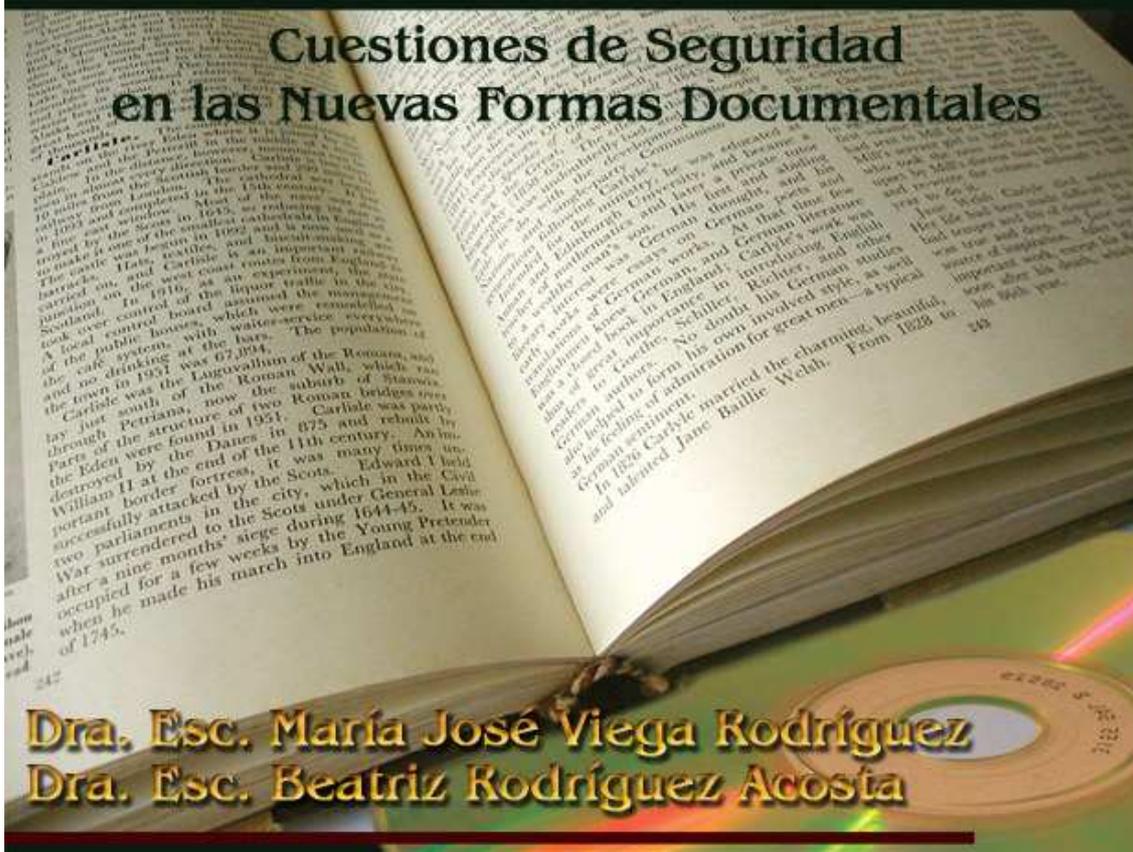


Documento Electrónico Firma Digital

Cuestiones de Seguridad en las Nuevas Formas Documentales



Dra. Esc. María José Viega Rodríguez
Dra. Esc. Beatriz Rodríguez Acosta

DOCUMENTO ELECTRONICO Y FIRMA DIGITAL

**Cuestiones de Seguridad en las Nuevas Formas
Documentales**

Dra. Esc. María José Viega Rodríguez

Dra. Esc. Beatriz Rodríguez Acosta

PROLOGO

Las Doctoras María José Viega y Beatriz Rodríguez me han pedido que prologue su obra titulada “Documento electrónico y firma digital”, la que lleva como subtítulo “Cuestiones de seguridad en las nuevas formas documentales”.

Asumo esta responsabilidad con verdadera satisfacción, que deriva no sólo del afecto a ambas sino también de la constatación de la madurez científica que exhibe su trabajo.

I

En cuanto a las autoras, me importa destacar en primer término que ambas han sabido encontrar el tiempo para estudiar y escribir, sin desmedro del cumplimiento de la tarea docente (con todo lo que ella implica), de su labor profesional (que me consta que es intensa), y de la atención de sus respectivas familias (habida cuenta de la responsabilidad que todos tenemos de cuidar ese ámbito que es “el lugar de la persona”¹, donde cada uno nace, crece, se desarrolla y vibra).

La Doctora María José Viega es una “veterana” en las lides del Derecho y las Nuevas Tecnologías de la Información. Habiéndose vinculado a la Cátedra de Informática Jurídica hace ya varios años, es una de las fundadoras del Instituto de Derecho Informático, ha completado con brillo su aspirantía docente y es actualmente Profesora Adjunta a cargo del curso de Derecho Telemático.

¹Adolfo GELSI BIDART - “La familia y el Derecho”m en A.A.V.V. - “El Derecho y la Familia” (F.C.U., Montevideo, 1998), pág. 248.

La Doctora Beatriz Rodríguez es una de las más flamantes incorporaciones al Instituto de Derecho Informático, aunque ha tenido siempre contacto con nuestra disciplina, antes desde su desempeño funcional en el Servicio Central de Informática de la Universidad de la República y ahora también como Directora de Información y Documentación Jurídica de la Suprema Corte de Justicia, cargo que ganó por concurso.

Las dos autoras, además de Abogadas, son Escribanas, extremo que merece destacarse en relación a la obra que han creado. En efecto, frente a visiones apocalípticas respecto al futuro de la profesión notarial ante las nuevas tecnologías de la documentación y la firma -los dos temas centrales que abordan- María José Viega y Beatriz Rodríguez hacen una afirmación contundente de la “vigencia de la profesión”², en línea con la Declaración de la Asamblea de Notariados Miembros de la Unión Internacional del Notariado Latino³ cuando proclamó que “la nueva tecnología no representa más que un cambio de instrumento de comunicación” frente al cual “es de la máxima importancia que las normas -técnicas y jurídicas- que reglan el nuevo sistema brinden las máximas garantías de seguridad... Seguramente habrá otros que ofrecerán en el mercado sus servicios Trusted Third Parties (bancos, cámaras de comercio, service providers en Internet, empresarios) análogamente a lo que ocurre hoy en día en el mundo del papel que nos es familiar; ninguno, de todos modos, podrá garantizar un tal nivel de imparcialidad y, sobre todo, que tal posición de equilibrio sea unánimemente reconocida. Esta exclusividad notaria -independientemente del instrumento técnico utilizado- merece siempre ser reconocida”.

II

La obra que tengo el gusto de prologar está escrita en forma ágil y descriptiva, explicando de modo sencillo aspectos complejos de las nuevas tecnologías aplicables a la documentación y autenticación.

²Fernando GOMA LANZON - “El desarrollo de la función notarial en el ámbito del comercio electrónico: explicaciones, reflexiones y comentarios”, en A.A.V.V. - “Notariado y Contratación Electrónica” (Colegios Notariales de España, Madrid, 2000), pág. 227 y sigtes.

³Declaración dada en Buenos Aires el 2 de octubre de 1998.

Documentos Electrónicos Firma Digital

La misma consta de 8 capítulos y un apéndice normativo, en el que se incluyen las principales normas vigentes en nuestro ordenamiento positivo.

Tras la Introducción (capítulo I), se analizan comparativamente el documento tradicional (capítulo II) y el documento electrónico (capítulo III), pasándose revista al Derecho comparado (capítulo IV) y al Derecho uruguayo en la materia (Capítulo V).

Del mismo modo, se estudian luego la firma ológrafa frente a las firmas electrónica y digital (capítulo VI), dedicando especial atención a las Autoridades de Certificación (capítulo VII) y al Notariado en la actual encrucijada tecnológica (capítulo VIII).

El apéndice normativo ofrece la ventaja de reunir un conjunto de disposiciones dispersas y cuyas recopilaciones anteriores son parciales⁴ o han quedado desbordadas por el tiempo en que fueron realizadas⁵.

A modo de síntesis, frente al desafío de lo que antes de ahora he calificado como “despapelización”⁶ administrativa y de los negocios, siento que puedo repetir las conclusiones que expuse en mi ponencia a las XVIII Jornadas Iberoamericanas y XI Jornadas Uruguayas de Derecho Procesal, realizadas en Montevideo en el año 2002. Allí afirmé lo siguiente⁷:

a) el Derecho uruguayo reconoce ampliamente la admisibilidad y valor probatorio del documento electrónico, entendido como el formado por el computador o por medio del computador, sea que esté soportado en medio magnético y no sea legible por el hombre (documento electrónico en sentido

⁴Así: sección Derecho Positivo de los anuarios “Derecho Informático”, tomos I a V (recogiendo la normativa dictada entre el 1º de enero de 2000 y el 31 de diciembre de 2004).

⁵Así: Aída NOBLIA y Beatriz RODRIGUEZ - “Recopilación de Normas aplicables al Derecho Informático y a la Informática Jurídica” (A.E.U., Montevideo, 2001); y Carlos E. DELPIAZZO - “Derecho Informático Uruguayo” (Idea, Montevideo, 1995).

⁶Carlos E. DELPIAZZO - “Informatización del procedimiento administrativo común”, en VI Congreso Iberoamericano de Derecho e Informática (Montevideo, 1998), pág. 776 y sigtes.; “Regulación del procedimiento administrativo electrónico”, en Procedimiento Administrativo Electrónico (O.N.S.C., Montevideo, 1998), pág. 151 y sigtes.; y “El procedimiento administrativo electrónico y el acto administrativo automático”, en Recopilación de conferencias y exposiciones (UTE, Montevideo, 1999), pág. 46 y sigtes.

⁷Carlos E. DELPIAZZO - “El documento y la firma ante las N.T.I. en Uruguay”, en XVIII Jornadas Iberoamericanas de Derecho Procesal y XI Jornadas Uruguayas de Derecho Procesal (F.C.U., Montevideo, 2002), pág. 725 y sigtes.

estricto) o que sea producido por el computador y perceptible por el hombre (documento electrónico en sentido amplio o documento informático);

b) nuestro Derecho también recibe con amplitud la firma electrónica -y, más específicamente, la firma digital (obtenida mediante criptografía)- entendida como el conjunto de signos, códigos, claves u otros elementos similares utilizados por una persona con el propósito de cumplir todas o algunas de las funciones de la firma ológrafa; y

c) es elogiable la postura de nuestro legislador de no embarcarse en regulaciones excesivas y casuísticas que afectan negativamente la capacidad de los particulares de adoptar las N.T.I. más adecuadas a sus actividades, impidiendo la innovación en las prácticas comerciales y obstaculizando el desarrollo de los negocios jurídicos a través de ese nuevo medio que es Internet.

Es que, como ya lo he postulado en más de una oportunidad, tanto el documento electrónico⁸ como la firma digital⁹ -los dos objeto principales de esta obra- son realidades ya instaladas en nuestro medio y que no es posible soslayar en el tráfico jurídico.

III

⁸Carlos E. DELPIAZZO - "El documento electrónico frente a la integración", en VI Congreso Iberoamericano de Derecho e Informática (Montevideo, 1998), pág. 333 y sigtes.; "Automatización de la actividad administrativa en el marco de la reforma del Estado", en Anuario de Derecho Administrativo (Montevideo, 1998), tomo VI, pág. 17 y sigtes.; "Nuevo horizonte para la automatización administrativa en Uruguay. A propósito de la aprobación del Decreto N° 65/998 sobre procedimiento administrativo electrónico", en Rev. Derecho de la Alta Tecnología (Buenos Aires, 1998), Año X, N° 116, pág. 24 y sigtes.; y "Marco legal de la automatización de la actividad administrativa", en Rev. Iberoamericana de Derecho Informático (Mérida, 1998), N° 19-22, pág. 718 y sigtes.

⁹Carlos E. DELPIAZZO - "Adecuación del Derecho a la necesidad de la firma electrónica", en Informática y Derecho (Depalma, Buenos Aires, 2001), volumen 7, pág. 113 y sigtes.; "La autenticación de las operaciones comerciales en Internet", en anuario "Derecho Informático" (F.C.U., Montevideo, 2001), tomo I, pág. 253 y sigtes.; "Validez y eficacia de la firma electrónica", en Tribuna del Abogado (Montevideo, 2000), N° 117, págs. 16 y 17; y "De la firma manuscrita a la firma electrónica: un caso de impacto de la Tecnología sobre el Derecho", en Rev. de Antiguos Alumnos del I.E.E.M. (Montevideo, 2001), Año IV, N° 1, pág. 76 y sigtes.; y "De la caligrafía a la criptografía", en Anales de las 30 Jornadas Argentinas de Informática e Investigación Operativa (Buenos Aires, 2001), pág. 209 y sigtes.

*Documentos Electrónicos
Firma Digital*

Para terminar, puedo afirmar que estamos ante una obra importante, no sólo por los temas que trata sino por su utilidad.

Al felicitar a las autoras, se impone destacar otra virtud de la obra: su servicialidad para estudiantes, abogados, escribanos y todos quienes deseen conocer, en perspectiva jurídica, los desafíos y posibilidades que plantean el documento electrónico y la firma digital, sin desmedro de la seguridad.

Dr. Carlos E. Delpiazzo

Director del Instituto de Derecho Informático

Mayo de 2005

CAPITULO I

INTRODUCCIÓN

El Profesor Losano ha dicho que la historia del Derecho "está condicionada por las tres revoluciones de la escritura, de la imprenta y de la ordenación electrónica de datos. En las tres revoluciones el Derecho es afectado a través del Lenguaje. En la primera se pasa de la expresión oral a la escrita; en la segunda, de la escritura manual a la impresa y en la tercera de la escritura tipológica, impresa o mecánica al lenguaje tratado electrónicamente"¹⁰.

"El fenómeno de la desmaterialización responde a la necesidad de cambio y adaptación que va a implicar para el desarrollo de la telemática a un concepto filosófico –antes que jurídico-. En efecto, es físicamente palpable por nuestros sentidos una gradual y ineludible desmaterialización de la realidad. Se observa con nostalgia, o satisfacción para algunos, el derrumbe de lo físico (el alto grado de la ausencia de lo material, la poca permanencia y duración de los objetos y la pérdida de su individualidad) y de lo ético o valorativo lo cual hace recordar la frase del pensador decimonónico: "todo lo sólido se desvanece en el aire". El fenómeno evolutivo de la desmaterialización al decir de ILLESCAS ORTIZ resulta equiparable a una alteración contractual de similar importancia a la que se produjo con la sustitución de la tabla o tablilla de piedra o barro por el papiro y la del pergamino por el papel"¹¹.

El fenómeno de la desmaterialización, desincorporación o espiritualización se manifiesta fundamentalmente en la despersonalización de las relaciones comerciales, en los medios de pago electrónico, en la

¹⁰ CARRASCOSA LOPEZ Valentín. "Valor Probatorio del Documento electrónico". Revista Informática y Derecho. Volumen 8. UNED Centro Regional de Extremadura, 1995. Página 133.

¹¹ HERNÁNDEZ AGUILAR Alvaro. "Comercio y contratación electrónica". IX Congreso Iberoamericano de Derecho e Informática. Costa Rica, 2002.

transferencia electrónica de fondos, en el documento electrónico, en la desmaterialización de los títulos valores, en el auge del comercio electrónico o desnudez del papel, lo que ha llevado a que se hable de la crisis de la sociedad del papel y se proponga un nuevo modelo social o cultural donde el papel será reemplazado por medios informáticos con soportes digitales y transferencia electrónica¹².

1. Efectos de la Tecnología en la Sociedad

Todos conocemos los efectos positivos de la tecnología en nuestras vidas, pero se habla muy poco de los riesgos. Por este motivo creemos necesario realizar un análisis, previo al enfoque puntual del documento y la firma electrónica, de las consecuencias o alcances que las tecnologías puedan tener en el futuro.

Las tecnologías han sido asimiladas en muchos casos con la cibernética y se ha dicho que las nuevas tecnologías de la información son portadoras de una humanidad unida, aunque al mismo tiempo de una humanidad reducida a la uniformidad.

Existen dos conceptos que han cambiado rotundamente en los últimos años con el desarrollo de las telecomunicaciones, que son el Tiempo y el Espacio. Asimismo encontramos otros que han cobrado relevancia, como es el caso del Acceso.

1.1 El Tiempo

Las nociones de tiempo y espacio cambian fundamentalmente con Internet. Cuando alguien dice "ahora", es ahora en todas partes, y por lo tanto la actividad que anuncio realizar en este momento en el ciberespacio es instantánea en el mundo real.

¹² HERNÁNDEZ AGUILAR Alvaro. "Comercio y contratación electrónica". IX Congreso Iberoamericano de Derecho e Informática. Costa Rica, 2002.

"La puesta en práctica del tiempo real para las nuevas tecnologías es, se quiera o no, la puesta en práctica de un tiempo sin relación con el tiempo histórico, es decir, un tiempo mundial. El tiempo real es un tiempo mundial. Hasta ahora toda la historia ha tenido lugar en un tiempo local: el tiempo local de Francia, el de América, el de Italia, el de París, o el de cualquier lugar. Y las capacidades de interacción y de interactividad instantáneas desembocan en la posibilidad de la puesta en práctica de un tiempo único, de un tiempo que, en ese sentido, nos remite al tiempo universal de la astronomía¹³."

Históricamente, la velocidad con que sucedían los acontecimientos han ido variando, o mejor dicho acelerándose. Así es que en la Edad Media la comunicación se realizaba mediante las palomas mensajeras. En la sociedad colonial se conoce el poder marítimo de Inglaterra y de Francia. La sociedad de la posguerra reconoce el poderío aéreo con la capacidad de los aviones supersónicos que sobrepasan la barrera del sonido. La sociedad actual no puede ser comprendida sin la velocidad de la luz.

También en relación con el tiempo, se habla de una historia hecha presente, debido a la instantaneidad de las noticias. Hemos visto la guerra por televisión, en el momento mismo en que ocurrían las batallas, lo que nos demuestra el alcance que tienen las transmisiones y el enorme poder de los medios de comunicación. El hombre se encuentra frente al tiempo en tres dimensiones: pasado, presente y futuro, asistiendo actualmente a una prolongación del presente.

En medio de este proceso de aceleración, de inmediatez, de instantaneidad, será el documento, en sus antiguas y nuevas formas, quien continúe cumpliendo su función de representación de los hechos, permitiéndonos su almacenamiento y recuperación.

¹³ VIRILIO, Paul. "Cibermundo, la política de lo peor". Entrevista con Philippe Petit. Traducido por Monica Poole. Segunda Edición. Cátedra, Madrid, 1999. Página 15.

1.2 El Espacio

En el ciberespacio debemos tener en cuenta que la internacionalidad está siempre presente, debido a la inexistencia de fronteras físicas. Esto ocasiona como principal problema la determinación de la ley aplicable y la jurisdicción competente frente a un hecho que realizo desde mi computadora de Montevideo, conectado a un servidor que está en Japón y estoy negociando con un español que se encuentra en una terminal en París.

Tengamos presente que en estos contratos telemáticos, la oferta, la aceptación son documentos electrónicos, que circulan a través de las redes telemáticas, formándose el consentimiento a través de este medio, e incluso pudiendo ejecutarse el contrato, el pago del bien y servicio o entrega de un bien virtual en esta misma modalidad.

Otro punto relativo al espacio, es el hecho de que los accidentes sucedían en un lugar determinado, un barco se hunde en un sitio específico, un tren descarrilaba en otro, pero un accidente en el ciberespacio, no es particular, sino general. Por ejemplo el crack bursátil es uno de los primeros ejemplos de estos accidentes inmateriales.

Desde el punto de vista documental, la unidad de acto que estudiaremos más adelante, ya no existe en virtud que cada parte suscribe electrónica o digitalmente un contrato en el ciberespacio, sin poder determinar su lugar de ubicación.

1.3 El Acceso

El ciberespacio produce como consecuencia la desmaterialización de los documentos, de los bienes, del dinero, pasándose a una economía de servicios. Esta desmaterialización tiene como consecuencia que ya no sea importante la posesión materializada de los bienes, sino el acceso a los mismos, el poder disponer de ellos en el momento y lugar en que los necesitemos.

Esto trae aparejado cuestiones de diferente índole, las cuales son analizadas por Jeremy Rifkin, quien se refiere a las relaciones entre las personas, donde se ha cambiado la casa por la seguridad de los condominios, se ha desplazado la actividad social de la plaza pública por los centros comerciales, teniendo un acceso restringido y vigilado en los condominios y reservándose el mismo en los shopping. El problema de los conectados y desconectados, comienza a ser una realidad, surgiendo una nueva forma de diferenciación basada en el conocimiento y en la forma de ver el mundo¹⁴.

Asistimos, entonces a la llamada era del acceso, en la cual podemos considerarnos privilegiados, porque tenemos acceso a estas nuevas herramientas. Pero es necesario realizar un cambio de mentalidad, darnos cuenta que somos ciudadanos del mundo, que estamos físicamente en un territorio, pero podemos estudiar o trabajar donde deseamos, que podemos abrir una empresa en un país que no es donde residimos y contratar empleados en otro, que geográficamente puede estar aún más lejano, buscando la mano de obra más barata o más calificada y que tenemos un experto en la materia que necesitamos en la distancia temporal en que demora un mail en ir y regresar.

¹⁴ RIFKIN, Jeremy. "La era del acceso. La revolución de la nueva economía". Editorial Paidós SAICF. Buenos Aires, 2000.

2. La respuesta del Derecho al Fenómeno Tecnológico

Existe actualmente una relación entre las computadoras, las redes, la información, las telecomunicaciones, su automatización, su tratamiento lógico, llevándonos a que se origine como respuesta del Derecho a la problemática de las Tecnologías de la Información y Telecomunicación nuevas ramas como son: la Informática Jurídica, el Derecho Informático y por último el Derecho Telemático.

La Informática es la ciencia que estudia el diseño y utilización de equipos, sistemas y procedimiento para obtener información. Esta, al ser aplicada al Derecho y buscar un tratamiento lógico y automático de la información legal, se convierte en una ciencia que forma parte de la Informática en general, adoptando el nombre de Informática Jurídica. Con esto vemos que la Informática tiene un rasgo multidisciplinario.

La primera aplicación de la Informática al Derecho es la que el Dr. Mario Losano denominó "informática en sentido estricto". Esta denominación abarca el almacenamiento, la clasificación y la recuperación de datos sobre leyes, jurisprudencia y doctrina.

La Informática Jurídica puede clasificarse en: Documental, de Gestión y Decisional o de ayuda a la decisión.

Desde los años ochenta la informática ha incursionado en el ámbito de las diferentes ramas del Derecho, por lo que se da la aparición de un Derecho especial al que llamamos Derecho Informático. El cual puede ser definido como el conjunto de leyes, normas, y principios aplicables a los hechos y actos derivados de la Informática.

En el Derecho Informático la Informática es *objeto* del Derecho, mientras que en la Informática Jurídica la Informática es *instrumento* de éste.

Documentos Electrónicos Firma Digital

El Derecho Informático como rama del Derecho es un área del orden jurídico integrado por las normas y principios que refieren a la actividad informática, y como ciencia es la disciplina que realiza el análisis de esa área del orden jurídico.

Según el Dr. Carlos Delpiazzo: "hoy ya es posible afirmar que el Derecho Informático es el hermano mayor dentro de la familia de disciplinas jurídicas vinculadas a la alta tecnología, de las cuales hacen parte el Derecho Biotecnológico y el Derecho Telemático, que ya puede considerarse un desgajamiento del tronco originario del Derecho Informático"¹⁵.

Podemos decir que el Derecho Telemático no sólo contiene aspectos que implican una automatización de la información (Informática) sino que se refiere también a las telecomunicaciones, o sea la transmisión, emisión y recepción de información (datos, sonido, imagen, etc.) a distancia. Surgiendo este concepto de telecomunicaciones a principios del siglo XX.

Podemos definir al Derecho Telemático como el derecho que regula las comunicaciones a distancia, a través de cualquier medio, capaz de reproducir el diálogo existente entre dos o más sujetos, situados en puntos diferentes del planeta, automatizando la información.

En el tema que nos ocupa estudiaremos normas tanto de Derecho Informático como Telemático, al analizar el régimen jurídico del documento y la firma electrónica y sus implicancias.

¹⁵ DELPIAZZO Carlos E. Curso on line: "Derecho del Ciberespacio". Módulo 1 Del Derecho informático clásico al nuevo Derecho telemático.

CAPITULO II

DOCUMENTO TRADICIONAL

1. Concepto

Es de suponer que desde que la humanidad tuvo conciencia de sí misma, habrá percibido, además de sus necesidades de comunicación, el hecho del transcurso del tiempo y la dilución en él de los demás acontecimientos. A su vez, de entre éstos, seguramente captó en seguida que tenía que rescatar alguno de su fugacidad y darles permanencia, informando a otros de su ocurrencia. Así debe haber nacido la tradición oral. Más la necesidad de comunicación y de conservación de los hechos, no se detendría allí y empezaría a traducirse en imágenes, en símbolos y después en letras. Dentro de este proceso, se gestó la noción de documento, como otra forma de representación de los hechos¹⁶.

Etimológicamente la palabra documento proviene del griego “dek”, correspondiente al verbo latino “doceo y ere” que significa enseñar, de donde proviene el vocablo “documentum” que quiere decir: enseñanza, lección.

Según el Diccionario de la Real Academia de la Lengua Española la palabra Documento tiene varias acepciones como:

1. *Instrucción que se da sobre cualquier materia.*
2. *Carta, diploma, relación o cualquier otro escrito que ilustra acerca de cualquier hecho principalmente de carácter histórico.*
3. *Escrito en que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo.*

¹⁶ SIRI, Julia. “El Notariado en la Era de la Tecnología”. Fundación de Cultura Universitaria. Montevideo, febrero 2001. Página 37.

Documentos Electrónicos Firma Digital

El sentido actual está documentado en castellano por primera vez en 1786 y se llegó a él probablemente a través de la expresión “lo que sirve para enseñar”, pasando luego a “escrito que contiene información” (para enseñar) y finalmente “escrito que contiene información fehaciente”¹⁷.

Según Eduardo Couture el documento es un objeto normalmente escrito, en cuyo texto se consigna o representa alguna cosa apta para esclarecer un hecho o se deja constancia de una manifestación de voluntades que produce efectos jurídicos¹⁸.

Para definir que se entiende por documento, podemos analizarlo desde un punto de vista estructural y funcional¹⁹.

Desde un punto de vista estructural, el documento es una cosa corporal que nos muestra algo, está constituido por un elemento material y un elemento intelectual.

Desde un punto de vista funcional, dice Carnelutti que es “una cosa que sirve para representar a otra”²⁰. Se hace énfasis entonces en el aspecto probatorio del documento.

¹⁷ RODRIGUEZ, Beatriz. “Documento electrónico”. Unidad 15 del Curso On Line “Introducción al Derecho de las Tecnologías de la Información y Comunicación”. <http://www.viegasociados.com/>

¹⁸ COUTURE, Eduardo J.. “Vocabulario Jurídico”. Ediciones Depalma, Buenos Aires, 1983.

¹⁹ VIEGA María José. Trabajo presentado en el Curso “Especialización en Gobierno y Administración Digital”. Organizado por Milenium 21(Rivera, 25 de julio de 2003) y en el 13º Ciclo de Encuentros Técnicos Regionales. Asociación de Escribanos del Uruguay (Rivera, 26 de julio de 2003).

²⁰ CARNELUTTI, Francesco, “Sistema de derecho procesal civil”. Buenos Aires (1944), tomo II, pág. 414.

Documentos Electrónicos Firma Digital

Otra posición, sustentada por Siegel, y aceptada por Núñez Lagos, define al documento como “una exteriorización del pensamiento, perceptible por la vista”, y así, éste último consigna como requisito de la grafía, entre otros, la visibilidad, esto es que el documentum sea apreciable por la vista. El disco fonográfico y la escritura Braille quedan excluidos. Si bien se trata de medios de comunicación, lo cierto es que en ellos es muy difícil el reconocimiento de su autor y agrega un concepto, sobre el cual desde ya, queremos llamar la atención, y relativo a que aún no se ha encontrado un equivalente funcional de la firma²¹.

Según Alicia Casas “los documentos son tales independientemente de la forma que tienen o del medio en el que fueron creados, recibidos, mantenidos y usados por una institución (pública o privada) o por un individuo en el cumplimiento de obligaciones legales o en la transacción de asuntos de los cuales forman parte o sobre los cuales dan pruebas”²².

Otro aspecto a tener en cuenta es que algunos autores distinguen entre documento e instrumento, mientras que otros lo utilizan como sinónimos.

La Escribana Julia Siri entiende que el concepto de documento es más amplio y por lo tanto abarcativo de sus especies, caracterizándose por el aspecto representativo o de forma, que, puede devenir, asimismo, aunque esta no fuera la finalidad perseguida originariamente en la instancia de su creación, puesto que en la medida que muestra, también demuestra llegado el caso. La noción de instrumento, aunque específica, es más rica, ya que además de incluir el aspecto representativo o de forma común a todos los documentos, es intencionalmente probatoria²³.

²¹ GAETE GONZALEZ Eugenio Alberto. “Instrumento público electrónico”. Editorial Bosch. España, abril de 2000. Página 71.

²² CASAS, Alicia y otros. “Gestión de documentos del sector público desde una perspectiva archivística” Tomo 1. Editado por Universidad de la República. Montevideo, 2003. Página 20.

²³ SIRI, Julia. “El Notariado en la Era de la Tecnología”. Ob. Cit., página 38.

2. Evolución Histórica

Fueron los asiobabilónicos, 2.900 años A. C., los primeros en utilizar el documento como medio de escritura, consistente dicho soporte en tablillas de arcilla cuneiforme. Tal es así que desde esa época, con las variantes de las civilizaciones modernas, se ha equiparado el documento con la escritura. Son los arameos los que traen de oriente a Asiria el pergamino y el papiro, a partir del siglo VIII A.C. De esta manera, las tablillas de barro van cediendo al paso de los escritos de pergamino y papiro, hasta llegar a desaparecer por completo dos siglos después del dominio macedónico²⁴.

Ya los egipcios distinguían dos clases de documentos: privados y públicos. Los documentos privados eran los que se solicitaban ante una autoridad pública para un asunto de carácter civil y los públicos, aquellos documentos otorgados por un funcionario especial, con facultades de policía y Juez.

Con la llegada del Derecho Romano y Germano, el documento tiene una importancia accesoria en los inicios del primero y principal en el segundo. Los romanos consideraban que las relaciones jurídicas nacían de la libre voluntad de las partes. La mayor parte de los negocios se efectúan en forma oral, siendo la escritura sólo una forma secundaria de contratación, y un modo de poder probar la relación jurídica existente. En cambio, el Derecho germánico anterior al imperio alemán, era predominantemente consuetudinario, no escrito. Con la influencia del periodo franco, surgen abundantes fuentes del derecho escrito; el negocio jurídico que incorpora no queda simplemente probado en el documento, sino que se celebra en él²⁵.

Fue a partir del siglo XV que se produjo una transformación con la invención de la imprenta, la que a su vez, fue posibilitada por una serie de revoluciones técnicas, primero en Asia y luego en Europa –a través del

²⁴ OCROSPOMA PELLA, Luis Enrique. "Concepto jurídico penal de documento". <http://www.derecho.com/boletin/articulos/articulo0083.htm>

²⁵ OCROSPOMA PELLA, Luis Enrique. "Concepto jurídico penal de documento". <http://www.derecho.com/boletin/articulos/articulo0083.htm>

traspaso de tecnologías de un continente a otro-, la que se vio facilitada a través de los Califatos árabes. En efecto, en China, ya a partir del siglo II D.C. se utilizaba papel derivado de la seda, el que llegará a Europa en el siglo XIII a través de los musulmanes. Asimismo las técnicas utilizadas para grabar en madera y en metales blandos, como el cobre, los avances en la metalurgia, y en las tintas utilizadas y particularmente la imprenta van a constituir la segunda gran invención luego de la escritura²⁶.

En el año 105 D.C., el señor T'sai Lun, que era un empleado del emperador chino Ho Ti, fabricó por primera vez un papel, desde una pasta vegetal a base de fibras de caña de bambú, morera y otras plantas, dando origen al papel que conocemos hoy. T'sai Lun emprendió esta tarea siguiendo órdenes expresas del emperador, quien le ordenó buscar nuevos materiales para escribir sobre ellos. Durante 500 años la técnica de la elaboración del papel perteneció sólo a los chinos, quienes la guardaron celosamente durante ese largo período²⁷.

Como consecuencia del advenimiento de la imprenta comenzó a difundirse a través de todo el continente europeo el documento, esencialmente el libro, posibilitando que el conocimiento llegara a toda la sociedad. Podemos observar que en este momento se identifica el documento con el soporte que lo contiene: el papel.

3. Clases de Documentos

En los documentos podemos encontrar dos valores fundamentales: el valor histórico, que dará lugar al documento histórico y el valor jurídico, al documento jurídico. Respecto a los documentos podemos encontrar diferentes clases.

²⁶ GAETE GONZALEZ Eugenio Alberto. "Instrumento público electrónico". Ob. Cit., página 76.

²⁷ http://www.papelnet.cl/papel/historia_papel.htm Página visitada el 15 de setiembre de 2004.

3.1 Según los aspectos que reúnen: externos e internos

- a) Externos: los cuales se dividen a su vez de acuerdo a:
- a. La clase: es el medio o procedimiento empleado para transmitir información. De acuerdo a este criterio podrán ser documentos textuales, gráficos, fotográficos, sonoros, audiovisuales e informáticos.
 - b. El soporte: es la configuración física del documento. Ejemplos de ellos son el soporte papel, fotográfico, magnético y óptico.
 - c. El formato: es la forma de presentación de los documentos, entiéndase por ello, su tamaño y las dimensiones del mismo. Por ejemplo documentos textuales en formato expediente o en legajos o documentos electrónicos en disquetes o CD.
 - d. La cantidad: es el número de unidades de instalación y el espacio que ocupan en metros lineales. Este es un elemento muy importante, en virtud a la cantidad de documentos que deben archivar y el espacio físico designado para ello.
 - e. La forma: de acuerdo a ella nos encontramos con documentos:
 - i. Borradores: son los documentos previos a la creación del documento definitivo. Es posible que a un documento original le correspondan varios borradores.
 - ii. Originales: “son aquellos que reúnen los requisitos que los habilitan para cumplir el objetivo para el que fueron creados, son auténticos, se corresponden al autor, fecha y lugar que expresan. Pueden ser únicos, que era

lo más común antiguamente, y múltiples cuando se producen varios ejemplares de igual valor²⁸.

iii. Copias: la finalidad es reproducir documentos originales para su circulación, las que adquieren relevancia cuando el original se ha extraviado. Para distinguir la copia del original debemos ver quien emitió el mismo.

f. El tipo: proviene de la actividad que el documento expresa, por tanto hay tantos tipos como actividades. Ejemplos: leyes, informes, oficios, acuerdos, cartas, etc.

b) Internos: los caracteres internos están dados por los elementos que definen el contenido del documento, por ejemplo: la entidad productora, el origen funcional, la fecha y lugar de creación y el contenido.

3.2 Según los valores del documento: primarios, secundarios y terciarios

a) Primarios: son aquellos documentos cuyos valores van unidos a la finalidad o idea fundamental para la cual fueron creados y capaces de servirle de testimonio. Dentro de estos valores podemos distinguir: el administrativo, jurídico-legal, fiscal o contable.

b) Secundario: con el transcurso del tiempo el documento va perdiendo su valor primario y acumulando un conjunto de valores de carácter secundario, como por ejemplo un valor histórico.

c) Terciarios: son aquellos documentos que registran algún conocimiento o información que resulta del procesamiento de la información secundaria.

²⁸ CASAS, Alicia y otros. "Gestión de documentos del sector público desde una perspectiva archivística" Tomo 1. Ob. Cit., página 27.

3.3 Según las edades y valores del documento: primera edad, edad intermedia y edad permanente

La teoría de las tres edades del documento fue enunciada por Carlos Wyffels en 1972, según la cual el documento pasa por distintas etapas, que da lugar a las diferentes edades.

a) Primera edad: cuando el documento posee un valor primario.

b) Edad intermedia: cuando el documento, ya archivado, tiene una función informativa.

c) Edad permanente: cuando el documento está dotado de un valor secundario, encontrándose en archivos históricos y poseyendo un interés cultural.

3.4 Según el emisor: públicos y privados

Tenemos que tener presente en este punto la discriminación realizada respecto a los términos documento e instrumento.

Nuestro Código Civil define en el artículo 1574 a los instrumentos públicos como *“todos aquellos que, revestidos de un carácter oficial, han sido redactados o extendidos por funcionarios competentes, según las formas requeridas y dentro del límite de sus atribuciones. Todo instrumento público es un título auténtico y como tal hace plena fe, mientras no se demuestre lo contrario mediante tacha de falsedad.*

Otorgado ante Escribano e incorporado en un protocolo o registro público, se llama escritura pública.

Se tiene también por escritura pública la otorgada ante funcionario autorizado al efecto por las leyes y con los requisitos que ellas prescriban”.

Los instrumentos privados están regulados en el Título IV Capítulo I Sección II artículos 1581 y siguientes del Código Civil. Pero no son definidos por el legislador, quedando conceptualizados por exclusión.

Alicia Casas los define como aquellos documentos creados, recibidos y mantenidos por organismos, instituciones, organizaciones, familias o individuos no gubernamentales y pueden estar relacionados con asuntos privados o públicos²⁹.

También se los ha definido como aquellos que dejan constancia de un hecho sin solemnidad alguna –hay libertad formal-, en cuyo otorgamiento no interviene un funcionario en calidad de tal, y que no llevan en sí ningún sello de autenticidad³⁰.

4. Caracteres

Podemos decir que un documento tiene las siguientes características:

- a) Ocupa un lugar en el espacio, es decir es una cosa material, visible y palpable, cuyos componentes son el soporte y la grafía.
- b) Se ubica en un tiempo específico.
- c) La doctrina y la legislación coinciden en que el documento es elaborado por el ser humano, es una obra de su creación. Al igual que el derecho positivo, forma parte del mundo de lo construido y no de lo dado³¹.
- d) De la característica anterior se desprende la importancia de la autoría, o sea la relación entre el autor y lo querido y expresado por éste.
- e) Tiene un valor probatorio, propio del documento jurídico, el cual es anterior al litigio en el se utiliza como medio de prueba.

²⁹ CASAS, Alicia y otros. "Gestión de documentos del sector público desde una perspectiva archivística" Tomo 1. Ob. Cit., página 28.

³⁰ JIJENA LEIVA Renato y otros. "El Derecho y la Sociedad de la información: la Importancia de Internet en el Mundo Actual". TEC de Monterrey. México, 2003. Página 269.

³¹ SIRI, Julia. "El Notariado en la Era de la Tecnología". Ob. Cit., página 39.

f) Tiene una finalidad representativa.

Al establecer estas características podemos pensar en dos teorías que son³²:

- a) La del escrito: para los que siguen esta teoría el documento siempre será un escrito, y por lo tanto es permanente y durable.
- b) La de la representación: según estos autores el documento no sólo es un escrito sino todo objeto representativo o que pueda informar sobre un hecho o sobre otro objeto. Así éste no está restringido a la naturaleza de su soporte, ni a la forma escrita, por lo que en esta hipótesis podríamos referirnos al documento electrónico o informático como una especie dentro del género documento.

Según Alicia Casas el soporte de los documentos es muy variado, ha ido cambiando con el paso del tiempo, como ha habido cambio en la manera que la información se fija en el soporte. Actualmente, en un archivo se puede encontrar desde textos manuscritos hasta discos ópticos, pasando por mapas cartográficos y cintas de video. Las características físicas señaladas, como el soporte, el procedimiento de fijación de la información, corresponden a la materialidad de los documentos, a los llamados caracteres externos de los mismos. Asimismo en los diferentes soportes también se asienta información que tiene que ver con el autor del documento, el creador, con el destinatario, o, con el contenido del mensaje, características éstas que identifican y definen los caracteres internos de los documentos³³.

El Derecho, ha tomado las pruebas a partir de esta materialidad (instrumentos, informes periciales) o bien, a partir de la expresión hablada (deposiciones, sean personales, como la confesión, o de terceros, como los testigos). Pero naturalmente las expresiones habladas no son perdurables, y para que lo sean deberán transformarse en escritas (transcripción al papel de lo

³² RODRIGUEZ, Beatriz. "Documento electrónico". Unidad 15 del Curso On Line "Introducción al Derecho de las Tecnologías de la Información y Comunicación". www.viegasociados.com

³³ CASAS, Alicia y otros. "Gestión de documentos del sector público desde una perspectiva archivística" Tomo 1. Ob. Cit, página 26.

Documentos Electrónicos Firma Digital

dicho, lo cual luego será firmado), de lo contrario, se corre el riesgo de que se pierda en el tiempo (sea por olvido, sea por fallecimiento de quien depone)³⁴.

La escritura sobre papel, tiene varias cualidades que la han tornado irremplazable: durabilidad, inalterabilidad, legibilidad y debidamente individualizada y firmada posee, además confiabilidad³⁵.

En el próximo capítulo analizaremos la verdad o falsedad de la afirmación anterior, poniendo énfasis en las características mencionadas.

³⁴ GAETE GONZALEZ Eugenio Alberto. "Instrumento público electrónico. Ob. cit., página 35.

³⁵ GUIBOURG Ricardo y otros. "Manual de Informática Jurídica. Editorial Astrea. Buenos Aires, 1996. Páginas 235 y siguientes.

CAPITULO III

DOCUMENTO ELECTRONICO

1. Concepto

Mencionábamos en el capítulo anterior, que según el Dr. Guibourg la escritura sobre papel, tiene varias cualidades que la han tornado irremplazable: durabilidad, inalterabilidad, legibilidad y debidamente individualizada y firmada posee, además confiabilidad³⁶.

Estudiaremos el documento electrónico a la luz de estos caracteres, analizando si el mismo presenta estas características y cuáles son sus fortalezas y debilidades desde el punto de vista jurídico.

Un aspecto relevante es tener presente las teorías que consideran al documento como un escrito o como una representación.

La función de la informática y las nuevas técnicas de comunicación, así como la transferencia electrónica de datos, que permite intercambiar mensajes electrónicos en lugar de documentos escritos, son elementos del actual contexto digital que revalúan la concepción tradicional del documento y dan paso a los documentos electrónicos. El mensaje electrónico de datos es la esencia de los documentos electrónicos³⁷.

Giannantonio distingue el documento electrónico³⁸:

³⁶ GUIBOURG Ricardo y otros. "Manual de Informática Jurídica. Editorial Astrea. Buenos Aires, 1996. Páginas 235 y siguientes.

³⁷ GRUPO DE ESTUDIOS en Internet, Comercio electrónico & Telecomunicaciones e Informática. Universidad de los Andes. "Internet, Comercio Electrónico & Telecomunicaciones". Editorial Legis, Colombia, 2002. Página 18.

³⁸ VIEGA, María José. "La influencia de la informática en la actividad probatoria y su regulación en Uruguay". Ponencia presentada al VII Congreso Iberoamericano de Derecho e Informática. Lima, abril de 2000.

Documentos Electrónicos Firma Digital

En sentido estricto: el que queda almacenado en la memoria del computador y no puede llegar a conocimiento del hombre sino mediante el empleo de tecnología informática.

En sentido amplio: el que es procesado por el computador por medio de periféricos de salida y se torna así susceptible de conocimiento por el hombre.

El punto crucial es el origen del documento: si ha sido generado por el hombre y se almacena o reproduce por intermedio del ordenador o si se admite que el propio computador genere el contenido del documento a partir de alguna combinación de la información disponible con ciertas instrucciones que operan en sus sistemas.

Entonces, el documento electrónico es aquel que se formó mediante el uso de un computador, así como aquel formado por el computador. ¿Cómo es esto? Bien, cuando decimos que es aquel formado por el computador queremos decir que el computador no sólo materializa una voluntad externa sino que determina el contenido de esa voluntad, o sea que decide en el caso concreto conforme a una serie de datos y parámetros y a una programación adecuada. En cambio cuando decimos que es aquel que se formó mediante el computador, éste último no forma sino que manifiesta una voluntad ya manifestada en otra forma u oportunidad³⁹.

Si analizamos la noción tradicional de documento referida al instrumento en el que queda plasmado un hecho que se exterioriza mediante signos materiales y permanentes del lenguaje, vemos como el documento electrónico cumple con los requisitos del documento en soporte papel, de que contiene un mensaje (texto alfanumérico o diseño gráfico) en lenguaje convencional (el de los bits) sobre soporte (cinta o disco) destinado a durar en el tiempo.

En cuanto a su contenido y forma el documento electrónico, reviste al igual que el documento en papel, un corpus, una grafía y un elemento

³⁹ RODRIGUEZ Beatriz. "Documento electrónico". Ponencia presentada en las V Jornadas Académicas del Instituto de Derecho Informático. Salto, 27 y 28 de mayo de 2004.

Documentos Electrónicos Firma Digital

intelectual o contenido, sólo que ellos se revelan diferentes en un caso y en otro. Desde el punto de vista amplio el documento electrónico es un objeto físico cuya finalidad es conservar y transmitir información a través de mensajes en un lenguaje natural, realizado con intermediación de funciones electrónicas. Desde un punto de vista estricto, éste se transforma en documento informático, en cuanto solamente la información puede ser recibida por el ser humano con la intervención de una máquina de traducción a un lenguaje entendible o natural, debido a que está elaborado en forma digital, a través de un sistema alfanumérico o similar, y depositado en la memoria central del computador⁴⁰.

Sin embargo, los diferentes autores se encuentran divididos en sus opiniones referente al documento escrito y al documento electrónico. Algunos entienden que los registros informáticos no constituyen un documento escrito basándose en las diferencias entre uno y otro. También existen aquellos que les encuentran muchas similitudes y opinan que el documento electrónico es otra forma de escribir, se habla de una nueva forma de alfabetización. Sin lugar a dudas ambos tienen razón, existen diferencias, pero también existen aspectos en que ambos se parecen⁴¹.

Comencemos hablando de las **diferencias** entre ambos, de las cuales podemos decir que:

a) Un documento escrito no puede concebirse sin el soporte material que es el papel. Sin embargo esto no siempre fue así. Existen a lo largo de la historia muchísimos tipos de documentos que nos demuestran la existencia de un hecho y que no necesariamente fueron realizados en soporte papel. Por otra parte, el papel, tan importante en nuestra época no lo ha sido en el pasado, y no vemos razones de peso por lo que deba serlo en el futuro. Y aquí no podemos obviar el problema de la seguridad, que, para quienes escribían en las cavernas, sobre la piedra, el papel no les resultaría seguro en absoluto,

⁴⁰ RODRIGUEZ Beatriz. Curso en línea Introducción al Derecho de la Tecnologías de la información y la Comunicación. Módulo 15. <http://www.viegasociados.com>

⁴¹ VIEGA María José. Trabajo presentado en el Curso “Especialización en Gobierno y Administración Digital”. Organizado por Milenium 21(Rivera, 25 de julio de 2003) y en el 13º Ciclo de Encuentros Técnicos Regionales. Asociación de Escribanos del Uruguay (Rivera, 26 de julio de 2003).

al igual que como hoy, muchos dudan de la seguridad de los soportes informáticos⁴².

Al respecto nos dice Bill Gates: “Durante más de 500 años, todo el volumen del conocimiento y de la información humanos se ha almacenado en forma de documentos de papel. (...) el papel estará siempre con nosotros, pero su importancia como medio de buscar, preservar y distribuir información está disminuyendo ya”⁴³.

El documento electrónico se diferencia básicamente de aquel *per cartam*, desde el punto de vista estructural. Se transforma su corporalidad, sus elementos materiales cambian, de tal manera, que su soporte será un sistema de conformación electrónica, expresado a través de un lenguaje binario. Tocante a su aspecto funcional, continuará siendo el mismo, *una cosa que docuit*, que enseña, designa algo⁴⁴.

“Hoy no resulta más suficiente, para indicar el apoyo destinado a acoger el documento informático, hablar de soporte magnético, porque en el ínterin la técnica ha alcanzado progresos tales como para llegar a permitir la escritura de documentos informáticos, aún en soportes metálicos con garantías de conservabilidad infinitamente superiores para poder confiar todo lo que hoy está garantizado por la impresión en papel, por lo que se podría hoy desenterrar, para los citados CD Rom, la antigua expresión aere peremnius (más perdurable que el bronce)”⁴⁵.

b) El registro informático puede ser fácilmente modificado, mientras que el documento escrito puede resultar más difícil de modificar sin dejar huellas en él. Creemos que el gran avance de la técnica, no sólo en materia informática, desmiente esta afirmación. Las fotocopiadoras láser color, por ejemplo,

⁴² VIEGA, María José. “La influencia de la informática en la actividad probatoria y su regulación en Uruguay”. Ponencia presentada al VII Congreso Iberoamericano de Derecho e Informático. Lima, abril de 2000.

⁴³ GATES, Bill. “Camino al futuro”, Ed. Mac Graw-Hill, España, 1996, Segunda Edición.

⁴⁴ GAETE GONZALEZ Eugenio Alberto. “Instrumento público electrónico. Ob. cit., página 177.

⁴⁵ MICCOLI Mario. “Primeras reflexiones acerca del reglamento italiano del comercio electrónico”. Versión de la Disertación efectuada el 11 de setiembre de 1997 en San Juan de Puerto Rico en la IX Jornada Notarial de Norteamérica, Centroamérica y el Caribe. Página 8.

permiten realizar copias de una calidad tal que nos resultaría muy difícil distinguir el original de la copia a simple vista.

c) La firma. La firma ológrafa no es la única forma de identificar a una persona, ésta también es falsificable y sólo un perito calígrafo nos dirá que grado de originalidad tiene. Respecto al documento electrónico se ha buscado el equivalente funcional a la firma.

Este principio del equivalente funcional se basa en un análisis de los objetivos y funciones del requisito tradicional con miras a determinar la manera de satisfacer sus objetivos y funciones en el contexto tecnológico. Así por ejemplo, a partir del conocimiento de las funciones y el rol jurídico que cumple el papel como medio físico, se diseñó una solución técnico-jurídica en un medio electrónico que cumpla las mismas funciones y además le imprima al documento electrónico las bondades propias de la tecnología (rapidez, ahorro de tiempo, etc.)⁴⁶.

d) En el documento informático desaparece la diferencia entre la copia y el original. Esta es quizá una de las apreciaciones más valederas, porque no es posible distinguir entre un documento informático original y su copia. Habría que prever una forma de distinguir a ambos, quizás con una determinada secuencia de código, o establecer a nivel contractual en caso de que los documentos se transmitan en forma telemática, cual es el documento original, si el que posee el que lo envía o el que lo recibe.

Con relación a las **similitudes** y entendiendo que el documento electrónico es una nueva forma documental, podemos decir que:

a) Constituye una forma nueva de documento en consideración a que desde los albores de la humanidad éste se ha caracterizado por tener una realidad, que comenzó revelándose a través de materiales consistentes, como las tablillas de arcilla mesopotámica, los papiros egipcios, las tablillas de

⁴⁶ Grupo de estudios en Internet, Comercio electrónico & Telecomunicaciones e Informática. Universidad de los Andes. "Internet, Comercio Electrónico & Telecomunicaciones". Ob. Cit., página 13.

madera chinas o egipcias, para pasar luego al pergamino, a la seda y finalmente al papel de pulpa, como se lo conoce en la actualidad⁴⁷.

b) Se considera en nuestra época a la informática como un nuevo lenguaje, hablamos de que en este siglo que se ha iniciado, quienes no conozcan el manejo informático serán considerados analfabetos, ya que podemos considerar el lenguaje binario como un alfabeto. El nivel de educación en esta área crece a pasos agigantados.

c) El lenguaje binario es criticado porque no puede ser leído directamente. La música también se escribe en forma diferente, y es leída sólo por aquellos que saben solfeo, sin embargo las partituras musicales no han planteado problemas. Tengamos presente que la ley no establece con qué signos debe manifestarse la escritura⁴⁸.

d) El carácter de indestructibilidad del soporte no constituye una exigencia legal, también el papel se destruye, por el fuego o la humedad. Con respecto a la posibilidad de modificación del documento informático frente a lo irreversible que puede ser el documento escrito, quizás podría ser cierto cuando pensamos en los Protocolos de los escribanos realizados en tinta negra de buena calidad, pero no lo será si pensamos en un documento enviado por fax, que al ser recibido en un papel estándar de transferencia térmica tiende a ser borrado. Y la realidad nos demuestra que hoy, a nivel mundial, un alto porcentaje de contratos se realizan por fax, a través de redes privadas, por correo electrónico o a través de Internet⁴⁹.

En la medida en que el contenido del documento sea relevante para el Derecho, es necesario que permanezca, esto es, que los datos queden fijados

⁴⁷ GAETE GONZALEZ Eugenio Alberto "Instrumento Público electrónico. Editorial Bosch. España, abril, 2000. Página 181.

⁴⁸ VIEGA, María José. "La influencia de la informática en la actividad probatoria y su regulación en Uruguay". Ponencia presentada al VII Congreso Iberoamericano de Derecho e Informático. Lima, abril de 2000.

⁴⁹ VIEGA, María José. "El documento electrónico y la firma digital". Trabajo final del Posgrado en Contratación electrónica. Universidad de Buenos Aires, 2001.

y la representación persista inalterable en todo el tiempo que sea menester para que se cumplan los fines jurídicamente perseguidos en cada caso⁵⁰.

Por tanto el soporte informático debe permitir conservar la información por el tiempo que sea necesario.

e) Interactividad de los textos informáticos. La posibilidad de añadir comentarios y nuevos datos a un documento, lo distingue del documento en papel. Esto ha dado origen al hipertexto, lo que da dinamismo al documento, el mismo deja de ser lineal, perdiendo importancia el principio y el final de éste.

2. Evolución Histórica

Así como en el capítulo anterior nos referimos a la evolución del papel como soporte del documento realizaremos, ahora, algunas precisiones acerca de la evolución histórica de las computadoras.

El objeto de referirnos a los elementos técnicos es debido a que el documento electrónico va a ser generado por estos medios y va a circular a través de las redes telemáticas, por lo que debemos comprender su funcionamiento y características principales.

Desde fines de la década del cuarenta surgen las computadoras llamadas de primera generación, siendo la primera absolutamente electrónica, la creada por Mauchly y Presper Eckert, llamada ENIAC (Electronic Numerical Integrator and Computer).

Hoy en día las computadoras son elementos familiares en todo el mundo, cada vez son más personales, apareciendo en la década del ochenta los PC (Personal Computer).

Las computadoras funcionan creando una imitación electrónica y un modelo de trabajo de números y operaciones.

⁵⁰ SIRI, Julia. "El Notariado en la Era de la Tecnología". Fundación de Cultura Universitaria. Montevideo, febrero 2001. Página 53.

Así es que ésta requiere para su funcionamiento de⁵¹:

- de si misma para ejecutar las órdenes recibidas,
- de otros aparatos accesorios conectados a ella para habilitar la recepción de datos como por ejemplo teclado, lápiz óptico,
- de accesorios aptos para reproducir la información obtenida luego de procesadas las instrucciones, por ejemplo impresoras,
- de un sistema operativo que contenga las instrucciones primarias para que pueda comunicarse con los aparatos conectados a ella y decirles como cumplir las órdenes que recibe,
- de un lenguaje especial que sea comprensible por ella, donde las instrucciones están dadas en ese lenguaje para que ésta pueda interpretarlas y ejecutarlas,
- un sistema de almacenamiento permanente para registrar instrucciones y datos, para ingresarlos una vez y poder utilizarlos nuevamente sin necesidad de otra instrucción nueva,
- de programas, o sea de conjuntos de instrucciones elaboradas estructuralmente, desarrolladas por el hombre, en lenguaje comprensible para la computadora.

Antes que nada debemos saber que existen diferentes clases de computadoras, como ser:

- a) **digital**: está apta para efectuar operaciones con datos representados en forma de números, basándose en el sistema de numeración binaria que veremos más adelante.
- b) **analógicos**: ellas realizan funciones aritméticas con los números y estos a su vez, se representan por alguna cantidad física.

⁵¹ GUIBOURG Ricardo y otros. "Manual de Informática Jurídica. Editorial Astrea. Buenos Aires, 1996. Páginas 235 y siguientes.

c) **híbridos:** es cualquier sistema de ordenador mixto en que se combinan dispositivos de los otros dos, o sea analógicos y digitales.

Las computadoras no pueden funcionar adecuadamente si no tienen instrucciones primarias orientadas a indicarle a la unidad central de proceso cómo tiene que procesar esas instrucciones y tampoco pueden hacer ninguna labor si no cuentan con los datos específicos que le indiquen lo que tienen que hacer, para eso es que necesitan los sistemas operativos y los programas.

Programa es el conjunto de instrucciones estructuralmente dispuesto, de modo que al ser leído y ejecutado por la computadora produzcan una tarea específica.

Existen programas cuya finalidad es contribuir al funcionamiento de la computadora y pueden ser llamados software de base y conforman junto con el hardware el medio indispensable para que un sistema de computación pueda operar.

Todos aquellos programas destinados directamente a desarrollar tareas específicas vinculadas al manejo de información y a procesos de gestión se denominan software de aplicación.

Tenemos dentro de los programas aquellos que son desarrollados a medida para utilizarlos en labores más sofisticadas y los conocemos como software vertical o a medida.

Se diferencian los segundos de los primeros en cuanto a su objetivo, ya que éste no es servir al computador sino por el contrario servirse de éste.

El documento electrónico, como mencionamos anteriormente, circula por redes telemáticas. Una red en sentido genérico es una estructura para la transmisión de mensajes, por ejemplo: la red telefónica.

A nivel informático y en el nivel más elemental, una red consiste en dos equipos conectados entre sí mediante un cable de tal forma que pueden compartir datos. Todas las redes, sin importar lo sofisticadas que sean, parten

de este sencillo sistema. Aunque la idea de dos equipos conectados mediante un cable no parece extraordinaria, visto en el tiempo ha sido el mayor logro en el mundo de las comunicaciones.

El concepto que hoy por hoy tenemos de la red tuvo su nacimiento en enero de 1969, fecha en que el Departamento de Defensa de Estados Unidos adjudicó el proyecto de conectar calculadores electrónicos mediante líneas telefónicas.

Este proyecto, aunque generaba muchas dudas, terminó con la conexión de cuatro computadoras de diferentes universidades norteamericanas, dando origen a la primera Red de comunicación por paquetes, que se llamó ARPANET. Cuando hablamos de ARPANET nos estamos refiriendo a los orígenes de la Internet actual.

Hasta ese momento la tecnología era de conmutación de circuitos, por la cual un computador sólo podía conectarse a otro a través de una línea dedicada.

A través de la conmutación de paquetes cualquier mensaje intercambiado entre computadoras es subdividido en diversos paquetes, cada uno de los cuales es enviado a través de líneas de conexión diferentes, que al llegar al destinatario se unen para conformar el mensaje enviado.

En estas redes, la información se envía a través de los cables en paquetes, de una computadora a la otra. Se ha dado el ejemplo de considerar esos paquetes como los “sobres postales” que enviamos por correo, los cuales contienen la dirección a la cual van destinados. También a estos paquetes de datos se les coloca la dirección de su destino en la red y se envían a través de la conexión Internet, en la cual cada computadora examina la dirección del mismo para averiguar si está o no destinado a ella. Esta labor la realiza el router, el cual detecta los paquetes que le pertenecen y los “ruteará” (enviará) a las computadoras incluidas en la red interna. Siguiendo el ejemplo, de la misma manera que la oficina de correos zonal, separa la correspondencia de su zona para enviarla a los destinatarios locales. Este es el viaje que realiza un documento electrónico.

Documentos Electrónicos Firma Digital

La velocidad con que el paquete llegue a destino dependerá del camino que recorra y del tráfico existente en la red. Cuando la información a transferir es mayor al tamaño de un paquete (576 bytes) será dividida en una serie de éstos, que pueden tomar caminos distintos.

Habiendo hecho referencia a la evolución de los medios técnicos nos referiremos a la evolución que sufre un documento electrónico en su proceso de creación y digitalización.

El proceso de generación o creación de un documento digital consta de tres etapas:

1. La digitalización: es la etapa en la cual no se produce ningún cambio en el documento que se ingresa al computador. Simplemente es una digitalización de la información, por ejemplo texto, sonido, imágenes, etc. En esta etapa lo que tenemos son bytes independientes.

2. La etapa de formateo previo. En esta etapa, además de la mera digitalización, se produce cierto procesamiento de la información, que generará datos agregados no implícitos en la misma, como por ejemplo reconocimiento de texto en imágenes o reconocimiento de voz en sonido.

3. Procesamiento concreto o edición. Es en este momento cuando se culmina con la creación y digitalización del documento electrónico, ya que además de lo sucedido en las etapas anteriores se le debe dar un formato. Existen formatos estándares para cada aplicación, por ejemplo jpg, bmp, gif para imágenes, mov, avi para video, doc, txt, rtf, htm para texto, entre otros. Existe cierta información que es adosada a cada documento por el propio sistema, como por ejemplo: quien lo modificó, el título del documento, la fecha de la modificación, dependiendo del sistema utilizado.

De acuerdo a este proceso, podemos decir que el documento electrónico es la digitalización de una representación física o la captura de información (por ejemplo una idea), más un conjunto de elementos que lo describen.

3. Clases de Documentos Electrónicos

Normalmente la tendencia es hablar de documentos electrónicos en forma generalizada. Pero es importante distinguir diferentes clases de éstos, así es que distintos autores conceptualizan los documentos electrónicos de acuerdo a diferentes criterios.

3.1 Según el soporte: Documentos Electrónicos, Magnéticos, Digitales o Informáticos

Los documentos soportados en medios magnéticos no responden al concepto tradicional o restringido de documento manuscrito en soporte papel, sino al amplio. Por exclusión entendemos que constituye un documento no electrónico aquel que es elaborado por las formas tradicionales, sean estas manuales, mecanográficas, micrograbadas, microcopiadas o fotográficas. Al hablarse de documentos electrónicos se alude a casos en que el lenguaje magnético constituye la acreditación, materialización o documentación de una voluntad quizás ya expresada en las formas tradicionales y en que la actividad de un computador o de una red sólo comprueban o consignan electrónica, digital o magnéticamente un hecho, una relación jurídica o una regulación de intereses preexistentes⁵².

El documento informático, por su parte, no puede ser fácilmente asimilado a las mismas características del electrónico, en cuanto este último no queda indudablemente incluido en las disposiciones que tipifican al instrumento per cartam; como se ha dicho, interpretativamente es posible considerar el documento electrónico asimilado al tradicional sobre todo porque es factible de expresarse a través de un lenguaje natural; pero no ocurre así con el informático, en cuanto éste usa un lenguaje binario que para ser comprensible requiere de una traducción a una lengua o idioma natural. Su función no es su traslado al papel, ya que –como hemos visto- se desnaturaliza debido a que

⁵² JIJENA LEIVA Renato y otros. "El Derecho y la Sociedad de la información: la Importancia de Internet en el Mundo Actual". TEC de Monterrey. México, 2003. Página 270.

pierde su dinamismo e interactividad⁵³.

3.2 Según la forma en que son transmitidos: Electrónico, Telemático, Vía Telefax o Facsímile

Según Miccoli documento electrónico es una definición muy genérica y falta de precisión, porque cualquier documento escrito con una máquina electrónica puede ser catalogado así. Cuando hablamos de comercio electrónico y de documento electrónico, lo que en realidad queremos decir es un documento telemático, o sea, un documento que se envía de un computador a otro sin papel, en forma electrónica⁵⁴.

Podemos distinguir, entonces, a raíz de la conceptualización anterior, la existencia de documentos electrónicos y de documentos telemáticos.

Los documentos enviados o transmitidos a distancia vía telefax o facsímile, ¿puede decirse que se trata de un documento soportado magnéticamente? Ocurre que aunque los fax son transmitidos vía líneas telefónicas siempre constan en un soporte papel, salvo cuando temporal y transitoriamente son magnéticamente almacenados en la memoria del fax receptor para su ulterior impresión en papel. Creemos que legalmente se debe establecer, con algunas precisiones, que la fotocopia o documento nuevo que resulta de la transmisión a distancia vía líneas telefónicas y que emana del fax receptor tenga legalmente el mismo valor que el original “enviado, pasado, leído o barrido” por el fax trasmisor⁵⁵.

En este caso estamos frente a un documento telemático, ya que es transmitido a distancia, pero el mismo es visualizado en soporte papel y no a

⁵³ GAETE GONZALEZ Eugenio Alberto "Instrumento Público electrónico. Ob. Cit., página 172.

⁵⁴ MICCOLI Mario. "El notario en la contratación electrónica". Versión taquigráfica de la Disertación realizada en la Asociación de Escribanos del Uruguay el 24 de setiembre de 1998. Página 2.

⁵⁵ JIJENA LEIVA Renato y otros. "El Derecho y la Sociedad de la información: la Importancia de Internet en el Mundo Actual". Ob. Cit., página 273.

través de un dispositivo informático.

3.3 Según el emisor: Públicos y Privados

Entendemos por documentos electrónicos privados aquellos que carecen de firma digital.

Mientras que en la mayoría de las legislaciones se les otorga a los documentos electrónicos firmados digitalmente la calidad de públicos, en la medida que se tienen por auténticos y hacen plena fe.

En España, por ejemplo, el artículo 115 de la ley 24/2001, añade un nuevo artículo (17 bis) a la Ley de 28 de mayo de 1862, que establece que los instrumentos públicos (a que se refiere el artículo 17) no perderán dicho carácter por el sólo hecho de estar redactados en soporte electrónico con la firma electrónica avanzada.

4. Caracteres

Las características del documento electrónico son⁵⁶:

- a) Es generado o emitido a través de un computador.
- b) Sólo puede hacerse público mediante tecnología informática.
- c) Es inmaterial.
- d) Para que tenga valor deberá estar sujeto a medidas técnicas de seguridad.

Analizando las características del documento en general, podemos decir que:

⁵⁶ VIEGA, María José. Trabajo presentado en el Curso "Especialización en Gobierno y Administración Digital". Organizado por Milenium 21(Rivera, 25 de julio de 2003) y en el 13º Ciclo de Encuentros Técnicos Regionales. Asociación de Escribanos del Uruguay (Rivera, 26 de julio de 2003).

Documentos Electrónicos Firma Digital

a) Es una cosa material. La corporalidad se refiere a la materialidad del documento. Soporte: cd, disquetes, disco duro, cintas, construidos en diferentes materiales: ópticos, magnéticos, metálicos, etc.

La grafía será –como veremos más adelante- caracteres binarios insertados mediante impulsos electrónicos.

El documento electrónico tiene momentos de desmaterialización, a diferencia del documento en soporte papel que siempre es material.

b) Se ubica en un tiempo específico.

c) Es elaborado por el ser humano. A pesar de que este tipo documental pueda ser creado por el computador en forma automática, la presencia humana no puede descartarse, ya que el software que lo ha creado, ha sido diseñado por el hombre.

d) Autoría. Es importa en este punto tener presente quién es el sujeto al cual se le imputa la creación del documento electrónico.

e) Tiene un valor probatorio, el cual como veremos al estudiar el derecho positivo, no se diferencia del documento tradicional.

f) Por último, la finalidad representativa está dada por su carácter de documento.

Habiendo analizado el documento electrónico desde un punto de vista conceptual y teórico, estudiaremos a continuación como el derecho lo ha incorporado a su legislación en los diferentes países.

CAPITULO IV

DERECHO COMPARADO

EL análisis de la evolución normativa en los diferentes Estados en relación al documento y la firma electrónica, tiene como objetivo primordial tener un panorama de las diferentes soluciones a las cuales se ha ido arribando, y comparar las mismas con las soluciones del derecho positivo de cada uno de nuestros países.

1. Estados Unidos

1.1 Estado de UTAH⁵⁷

La firma digital ha sido objeto de regulación en varios países, siendo la Ley de Firma Digital del Estado de UTAH (EEUU) la primera en aprobarse, entrando en vigencia el 1 de mayo de 1995 y teniendo una modificación en abril de 1996.

Está dividida en cinco partes:

Parte 1 – “Título, Interpretación y Definiciones”, en la cual se enumeran los propósitos:

- 1) Facilitar el comercio por medio de mensajes electrónicos confiables;
- 2) Minimizar la incidencia de falsificaciones de firmas digitales y fraudes en el comercio electrónico;

⁵⁷ VIEGA, María José. “Firma electrónica: antecedentes, proyecto de ley y repercusiones en Uruguay”. Exposición del III Congreso Internacional de Derecho e Informática. Quito, 2001.

Documentos Electrónicos Firma Digital

- 3) Para hacer legalmente efectiva la importación general de los estándares pertinentes, tales como el X.509 de la International Telecommunication Union
- 4) Establecer, en coordinación con múltiples Estados, reglas uniformes relacionadas con la autenticación y confiabilidad de los mensajes electrónicos.

Contiene también definiciones: “autoridad de certificación con licencia, “aceptar un certificado”, “sistema de criptografía asimétrica”, “firma digital” y “falsificación de firma digital”.

Parte 2 - Trata sobre la concesión de licencias y la regulación de Autoridades Certificantes.

Parte 3 - Se ocupa de los deberes de la Autoridad Certificante y del contenido de los certificados.

Parte 4 – Regula los efectos de la firma digital disponiendo en primer término que donde una regla legal requiere una firma o prevé ciertas consecuencias en su ausencia, esta regla será satisfecha por una firma digital si está verificada a una clave pública contenida en un certificado válidamente extendido por una Autoridad Certificante, o si esa firma ha sido estampada por el firmante con la intención de firmar el mensaje. Además requiere que el destinatario no conozca que el firmante haya infringido su deber como suscriptor o no haya conservado de acuerdo a derecho la clave privada usada para firmar.

Parte 5 – Se ocupa de los servicios estatales en la organización de los “repositorios” o archivos de claves públicas y los requisitos que deben reunir.

1.2 Ley Federal

En Estados Unidos fue promulgada la Electronic Signatures in Global and National Commerce Act el 30 de junio de 2000 entrando en vigencia el 1 de octubre de 2000.

Establece una regla de validez para todos los actos y transacciones celebrados por medios electrónicos, lo que significa que ninguna ley, reglamento o norma podrá negar valor legal a un acto o contrato por el sólo hecho que su firma esté en forma electrónica.

Incluye, además un capítulo sobre derechos básicos que deben tener los consumidores que van a realizar transacciones por medios electrónicos.

2. Italia

Fue el primer país de Europa en dictar reglamentación sobre firma digital y lo hizo con el “Regolamento contenente modalità di applicazione dell’ articolo 15, comma 2, della legge 15 marzo 1997, N° 59, in formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici”.⁵⁸

Este reglamento da diversos conceptos en su artículo 1º, como por ejemplo: firma digital, par de claves asimétricas, clave privada y certificado. En el artículo 2º se establece la validez y eficacia del documento electrónico.

Asimismo éste no regula a las Autoridades Certificantes, las define como sujetos públicos o privados que certifican y guardan las claves públicas de firma por 10 o más años.

Posteriormente se dictó el Decreto del Presidente del Consejo de Ministros, con fecha 8 de febrero de 1999, referente al documento electrónico.

⁵⁸ DELPIAZZO, Carlos E. “Relevancia jurídica de la encriptación y la firma electrónica en el comercio actual”. Memorias del VIII congreso Iberoamericano de Derecho e Informática México, noviembre 2000. Pág. 133.

Dicho decreto cuenta con la regulación de la formación, transmisión, conservación, duplicación, reproducción y valoración de los documentos informáticos establecidos en el artículo 3, numeral 1, del Decreto del Presidente de la República del 10 de noviembre de 1997, N°. 513

3. Alemania

La Ley de Firma Electrónica entró en vigor por primera vez el 1 de agosto de 1997 y el 1 de noviembre del mismo año se aprobó el Reglamento de Firma Electrónica con disposiciones complementarias.

Alemania se convirtió así en uno de los primeros países de Europa y del mundo con una reglamentación de este tipo. Como consecuencia del posterior debate, sobre todo a escala europea, y de la aprobación de la Directiva Europea sobre Firma Electrónica, la Ley y el Reglamento de Firma Electrónica fueron enmendados teniendo en consideración las primeras experiencias en la práctica y las indicaciones de la Directiva. La versión actualmente vigente de la Ley de Firma Electrónica entró en vigor el 22 de mayo de 2001 como “Ley sobre Condiciones Marco para Firmas Electrónicas” y el nuevo Reglamento de Firma Electrónica, el 16 de noviembre de 2001⁵⁹.

Respecto a las entidades de certificación, están permitidas las que no cumplan con las disposiciones mencionadas, pero no gozan de ningún privilegio en el proceso.

En el Derecho alemán, los actos jurídicos formales constituyen una excepción. Si se desea celebrar un negocio jurídico formal por medios electrónicos, esto es posible en el ámbito de la forma electrónica. El Código Civil alemán regula la forma electrónica según el modelo de la forma escrita. La forma electrónica requiere que el texto de la declaración esté provisto de una firma electrónica cualificada según la Ley de Firma Electrónica. La forma

⁵⁹ ERBER-FALLER Singrun, Notaria Hallhof 6. Ponencia de la Delegación Alemana en el Tema II “El notario y la contratación electrónica” en el XXIV Congreso Internacional del Notariado Latino. México, 2004. Página 12.

escrita puede sustituir a la forma electrónica en cualquier caso. La forma electrónica puede sustituir a la forma escrita por regla general pero no en los casos excepcionales determinados explícitamente por el legislador⁶⁰.

4. Directiva de la Unión Europea

El 24 de mayo de 1999, se dictó la Directiva Europea sobre un Sistema Común para Firmas Electrónicas. Señala que la firma electrónica adjuntada a un documento electrónico, tiene exactamente el mismo valor legal que la firma manuscrita adjuntada a un documento escrito en soporte papel. Por ello la admite como medio de prueba y reconoce su valor probatorio.

Además, establece un sistema voluntario de acreditación de los prestadores de servicios de certificación, basado en condiciones objetivas, transparentes, proporcionadas y no discriminatorias y cuyo objetivo es proveer un grado de confianza y seguridad superior.

5. Portugal

Decreto Ley N° 290-D/99 del 2 de agosto de 1999 regula la validez, eficacia y valor probatorio de los documentos electrónicos y de la firma digital, sin perjuicio de otras formas de firma electrónica que posean exigencias de seguridad como las de la firma digital.

La Resolución del Consejo de Ministros No. 115/98, de fecha 1 de setiembre de 1998, determinó la definición del régimen jurídico aplicable a los documentos electrónicos y firma digital, como los dos objetivos a alcanzar en el ámbito de la Iniciativa Nacional para el Comercio Electrónico, necesario para la plena afirmación del comercio electrónico.

⁶⁰ ERBER-FALLER Singrun, Notaria Hallhof 6. Ob. Cit., página 54.

6. España

El Real Decreto-ley N° 14/1999 del 17 de setiembre de 1999 distinguía entre: firma electrónica y firma electrónica avanzada, permitiendo en este último caso la identificación del signatario y que ha sido creada por medios que este mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.

Con fecha 19 de diciembre de 2003 se aprobó la Ley N° 59/2003 de Firma Electrónica, modificativa del Real Decreto-Ley mencionado anteriormente.

Siendo los puntos más relevantes de la nueva norma los siguientes:

- a) Es la denominación como firma electrónica reconocida de la firma electrónica que se equipara funcionalmente a la firma manuscrita.
- b) La eliminación del registro de prestadores de servicios de certificación.
- c) Modifica el concepto de certificación de prestadores de servicios de certificación para otorgarle mayor grado de libertad y dar un mayor protagonismo a la participación del sector privado en los sistemas de certificación y eliminando las presunciones legales asociadas a la misma, adaptándose de manera más precisa a lo establecido en la directiva.
- d) Clarifica la obligación de constitución de una garantía económica por parte de los prestadores de servicios de certificación que emitan certificados reconocidos.
- e) La ley refuerza las capacidades de inspección y control del Ministerio de Ciencia y Tecnología.

Documentos Electrónicos Firma Digital

- f) Se limita a fijar el marco normativo básico del nuevo DNI electrónico poniendo de manifiesto sus dos notas más características —acredita la identidad de su titular en cualquier procedimiento administrativo y permite la firma electrónica de documentos— remitiéndose a la normativa específica en cuanto a las particularidades de su régimen jurídico.
- g) Establecimiento en la ley del régimen aplicable a la actuación de personas jurídicas como firmantes, a efectos de integrar a estas entidades en el tráfico telemático.
- h) Se añade un régimen especial para la expedición de certificados electrónicos a entidades sin personalidad jurídica.
- i) Permite que los prestadores de servicios de certificación podrán, con el objetivo de mejorar la confianza en sus servicios, establecer mecanismos de coordinación con los datos que preceptivamente deban obrar en los Registros públicos, en particular, mediante conexiones telemáticas, a los efectos de verificar los datos que figuran en los certificados en el momento de la expedición de éstos.

7. Perú

El Decreto Legislativo N° 681 del 14 de octubre de 1991 y la Ley N° 26.612 del 21 de mayo de 1996 son normas que van a cimentar las bases de la contratación electrónica.

Las Leyes N° 27269 del 26 de mayo del 2000 y la N° 27291 del 23 de junio del mismo año regulan de manera directa la seguridad en la Contratación Electrónica.

La primera de ellas” Ley de Firmas y Certificados Digitales” tiene por objeto regular la utilización de la firma electrónica dándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que

Documentos Electrónicos Firma Digital

conlleve manifestación de voluntad, establece el concepto de firma y certificados digitales y garantiza en forma universal la autenticidad, integridad, confidencialidad y el no repudio de las transacciones electrónicas.⁶¹

Esta Ley a su vez sufrió modificaciones, siendo una de ellas la establecida en la Ley N° 27310, que modifica su artículo 11. Su nueva redacción le da una equivalencia recíproca a los Certificados de Firmas Digitales emitidos por Entidades Extranjeras, otorgándoles la misma validez y eficacia jurídica reconocidas a los nacionales, siempre y cuando tales certificados sean reconocidos por la autoridad administrativa competente.

En el año 2002 se aprueba el Decreto Reglamentario de la Ley de Firmas y Certificados Digitales de Perú N° 19/2002, que va a permitir poner en marcha y difundir el uso de las firmas electrónicas, así como las firmas y certificados digitales.

A su vez por este Decreto se designa al Instituto Nacional de Defensa de la Competencia y la Protección de la Propiedad Intelectual (INDECOPI) como la autoridad administrativa competente, conforme a lo establecido en el Artículo 15 de la Ley N° 27269, que se encargará del Registro de Entidades de Certificación y Entidades de Registro o Verificación.

Como habíamos mencionado anteriormente, el 23 de junio de 2000 se promulgó la Ley N° 27291 que modifica el Código Civil peruano, permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica.

Se modifican los artículos 141 y 1374 del Código Civil en lo que se refiere a la manifestación de voluntad y al conocimiento y contratación entre ausentes respectivamente.

Según el artículo 141 se incluye los medios electrónicos u otros análogos como forma de manifestación de voluntad expresa y en los casos en que la ley establezca que la manifestación de voluntad deba hacerse a través de alguna

⁶¹ HORNA, Pierre M. "Análisis legislativo de la Firma digital". Memorias del VIII congreso Iberoamericano de Derecho e Informática. México, noviembre 2000. Página 7.

formalidad expresa o requiera de firma, ésta podrá ser generada o comunicada a través de medios electrónicos, ópticos o cualquier otro análogo.

Tratándose de instrumentos públicos, la autoridad competente deberá dejar constancia del medio empleado y conservar una versión íntegra para su ulterior consulta.

A su vez el artículo 1374 refiere a que cuando el consentimiento se realiza a través de medios electrónicos, ópticos u otro análogo, se presumirá la recepción de la declaración contractual, cuando el remitente reciba el acuse de recibo.

8. Argentina

La resolución 45/97 de la Secretaría de la Función Pública, incorpora la tecnología de la firma digital a los procesos de información del sector público, adoptando las conclusiones el 30 de setiembre de 1996 del Subcomité de Criptografía y Firma Digital del Comité de Usuarios de Procesamientos e Imágenes (CUPI) autorizando la tecnología sugerida en el ámbito de la Administración Pública “para la promoción y difusión del documento y firma digitales en los términos y con los alcances allí definidos”, según el artículo 2°.⁶²

A través del Decreto 427/1998 publicado en el Boletín Oficial del 21 de abril de 1998, el Poder Ejecutivo dispuso promover el uso de la firma digital en toda la Administración Pública Nacional, estableciendo que el documento electrónico cumple con la condición de no repudio, lo que posibilita la prueba inequívoca de que una persona firmó efectivamente un documento digital, y que tal documento no sufrió alteración alguna desde el momento de la firma.

La Ley N°25.506 de firma digital sancionada por el Parlamento Argentino el 14 de noviembre del 2001 y promulgada de hecho el 11 de diciembre al no

⁶² CARLINO, Bernardo P. “Firma digital y Derecho Societario Electrónico”. Rubinzal – Culzoni Editores. Argentina, 1998. Pág. 30.

haber sido observada por el Poder Ejecutivo. La ley fue publicada en el Boletín Oficial el 12 de diciembre del dicho año.

Dicha Ley consta de 11 capítulos. En el capítulo primero referente a Condiciones Generales 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 (artículo 1º).

En el capítulo II regula los certificados digitales y en el III define al certificador licenciado, sus funciones y obligaciones. En el capítulo IV se establecen los derechos y obligaciones del titular de un certificado digital. En los capítulos V y VI se consagra la organización institucional y la autoridad de aplicación respectivamente. Los capítulos siguientes regulan el sistema de auditoría, la comisión asesora para la infraestructura de la firma digital, responsabilidades y sanciones.

El Decreto Reglamentario 2628/2002 consta de 46 artículos y otro Glosario de términos técnicos. Reconoce validez de certificados digitales emitidos por certificadores no licenciados. Faculta a la Jefatura de Gabinete de Ministros a determinar normas y procedimientos técnicos (Autoridad de Aplicación). Regula la integración y cometidos de la Comisión Asesora para la Infraestructura de Firma Digital. Crea el Ente Administrador de Firma Digital, el que por decreto posterior se disolvió, pasando su competencia a la Oficina Nacional de Tecnologías de la Subsecretaría de la Gestión Pública (decreto 1028/2003). Regula el Sistema de Auditoría y la revocación de certificados digitales. Estatuye requisitos y obligaciones para los certificadores licenciados. Prevé una posible delegación de los certificadores licenciados en las llamadas "autoridades de registro". Establece disposiciones varias para la Administración Pública.⁶³

Por Decreto 1028/03, de fecha 6 de noviembre de 2003 se asigna a la Oficina Nacional de las Tecnologías de la información, entre otras funciones:

⁶³ BAUZA, Marcelo. "La certificación digital en el MERCOSUR". Boletín Electrónico N° 12. <http://www.viegasociados.com/>

Documentos Electrónicos Firma Digital

a) actuar como Autoridad Certificante de los Organismos del Sector Público Nacional,

b) intervenir en el otorgamiento de licencias habilitantes para acreditar a los certificadores de Firma Digital y fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los certificadores licenciados

c) proponer el rechazo de las solicitudes y la revocación de las licencias de Firma Digital otorgadas a los prestadores de servicios de certificación que no cumplan con los requisitos establecidos en la normativa

d) intervenir en la aprobación de las políticas de certificación, el manual de procedimiento, el plan de seguridad, el cese de actividades y el plan de contingencia, presentado por los certificadores de Firma Digital solicitantes de la licencia o licenciados

e) solicitar los informes de auditoria y realizar inspecciones a los certificadores licenciados de Firma Digital

f) elevar propuestas de homologación de los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos, por la normativa vigente

g) elevar un registro que contenga los domicilios, números telefónicos, direcciones de Internet y certificados digitales de los certificadores de Firma Digital licenciados y de aquellos cuyas licencias hayan sido revocadas, y difundir los mencionados datos en forma permanente e ininterrumpida, a través de Internet

h) elaborar y proponer 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 el marco del régimen de Firma Digital

i) supervisar la ejecución del plan de cese de actividades de los Certificadores licenciados de Firma Digital que discontinúan sus funciones; y la ejecución de planes de contingencia de los mismos

j) recibir, evaluar y elevar propuestas de resolución de los reclamos de los usuarios de certificados digitales relativos a la prestación del servicio por parte de certificadores licenciados.

9. Chile

En junio de 1999 se dictó el Decreto Supremo N° 81, re gulador del uso de firmas digitales y documentos electrónicos al interior de la Administración del Estado. Este Decreto obedece a uno de los compromisos adoptados por una Comisión Presidencial de Nuevas Tecnologías que sesionó durante 1998, en orden a dotar a los órganos estatales del marco legal que permita el uso de la informática y de las telecomunicaciones en reemplazo de sus procedimientos manuales, específicamente relacionado con el uso de firmas y documentos digitales o electrónicos, pero solo al interior de la Administración del Estado y no de las relaciones con los administrados.⁶⁴

A partir del 12 de abril de 2002 entró en vigencia la Ley N° 19799 sobre documentos electrónicos, firma electrónica y los servicios de certificación de firma electrónica de Chile.

En ella se regulan los documentos electrónicos y sus efectos legales, la utilización en ellos de la firma electrónica, la prestación de servicios de certificación de estas firmas y el procedimiento de acreditación al que podrán sujetarse los prestadores de dicho servicio de certificación, con el objeto de garantizar la seguridad en su uso (artículo 1).

No sólo se regula la firma electrónica en la actividad privada sino también en la administración pública.

⁶⁴ JIJENA LEIVA, Renato. "Firma digital y Proveedores de Servicios de Certificación". Memorias del VII congreso Iberoamericano de Derecho e Informática. Perú, abril 2000. Pág. 268.

10. Brasil

Por el Decreto N° 3587 de 5 de setiembre del 2000, se establecen normas sobre infraestructura de claves públicas del Poder Ejecutivo Federal, así como la determinación de reglas y normas que determinará la Autoridad de Gerencia de Políticas y prevé se establezcan procesos de auditoría y fiscalización para garantizar el cumplimiento de las reglas de ICP-Gob.

Con posterioridad se dictaron dos normas relevantes la Medida Provisoria N° 2.200 de 24 de Agosto de 2001 y el Decreto 3996-2001 de 31 de octubre de 2001. Este último deroga el Decreto N° 3587

11. Paraguay

“Paraguay no cuenta al presente con un estatuto normativo específico en materia de entidades certificadoras, no obstante lo cual se señala como supletorio en cierta medida, y para ámbitos administrativos, algunas disposiciones de la Ley N° 2.051/2003 de 21-01-2003 sobre Contrataciones Públicas (Informaciones obtenidas merced a la gentileza de la colega paraguaya Dra. Natalia Enciso, especialista en Derecho y TICs.). Los arts. 66, 67 y 91 de la referida ley regulan el envío de ofertas por vía electrónica remitiéndose en buena medida a las disposiciones que establezca la Unidad Central Normativa y Técnica (UCNT), que tendrá a su cargo el sistema de certificación de los llamados “medios de identificación electrónica” que utilicen los oferentes, todo ello dentro del marco del Sistema de Información de Contrataciones Públicas (SICP). Por su parte el art.102 del Decreto Reglamentario N° 21.909 de 11-08-2003 alude a una cierta reglamentación especial a dictarse en la materia.⁶⁵ “

⁶⁵ BAUZA, Marcelo. “La certificación digital en el MERCOSUR”. Boletín Electrónico N° 12. www.viegasociados.com

12. Ecuador

En Ecuador a partir del año 2002, más precisamente el 17 de abril, se aprobó la Ley N°. 67 sobre Comercio Electrónico, Firmas y Mensajes de Datos.

Al igual que los demás Estados, en esta Ley observamos el principio de equivalencia funcional, ya que le confiere en su artículo 2, a los documentos electrónicos que se perfeccionen a través de la red, el mismo valor jurídico que los documentos o contratos tradicionales.

Introdujo y modificó infracciones, delitos y penas dentro de su Código Penal, actualizándolo a la nueva realidad que imponen los avances tecnológicos, tipificando figuras tales como los siguientes: delito de fraude informático, de daño informático, de falsificación electrónica, de intromisión indebida a los sistemas de información o telemáticos.

Se reconoce y regula en forma muy pormenorizada la existencia y funcionamiento de entidades certificadoras, las que quedan legalmente facultadas para generar firmas electrónicas, siguiendo la guía de la ley modelo de la CNUDMI, estableciendo varios requisitos que deberán cumplir todos aquellos que quieran ser considerados proveedores de servicios de certificación⁶⁶.

13. Venezuela

Venezuela ha regulado el documento electrónico y la firma electrónica por medio del Decreto Ley N° 1024, de fecha 10 de febrero de 2001, llamado Ley sobre Mensajes de Datos y Firmas Electrónicas.

Vemos reflejados en esta Ley los principios básicos de equivalencia funcional, autonomía de la voluntad y neutralidad informática.

⁶⁶ SANTOMAURO Alejandro. Trabajo realizado en el Curso Documento y Firma Electrónica On line. www.viegasociados.com. Montevideo, 2004.

En su artículo 4 la Ley equipara a los mensajes de datos en cuanto a su eficacia probatoria a los documentos escritos. Asimismo establece que cuando se requiera, por medio de ésta, que la información sea presentada o conservada en su forma original, dicho requisito quedará satisfecho con relación a un mensaje de datos si se ha conservado su integridad y cuando la información contenida en dicho mensaje de datos esté disponible.

De acuerdo al artículo 5, los mensajes de datos tienen los mismos efectos que los documentos electrónicos desde los siguientes puntos de vista: como materia probatoria con igual eficacia; cuando la ley exija el cumplimiento de solemnidades o formalidades; y cuando están sometidos a las disposiciones constitucionales y legales que garantizan los derechos a la privacidad de las comunicaciones y de acceso a la información de las personas.

La Ley venezolana atribuye a la firma electrónica la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa y siempre que en forma concurrente permita vincular al signatario con el mensaje de datos y atribuir autoría a éste. La firma electrónica podrá formar parte integrante del mensaje de datos o estar inequívocamente asociada a éste. Para que la firma electrónica tenga la validez y eficacia de la autógrafa deberá llenar los extremos señalados en el artículo 16.

Esta es de carácter supletorio y solo se aplicará en caso que las partes no hayan determinado un régimen de aplicación preferente, según lo establecido en el artículo 34⁶⁷.

14. México⁶⁸

La mas reciente norma legal relacionada directamente con la firma electrónica en México, es la expedida por el Secretario de Economía, publicada

⁶⁷ SUAREZ SAN EMETERIO Miguel. Trabajo realizado en el Curso Documento y Firma Electrónica On line. www.viegasociados.com Montevideo, 2004.

⁶⁸ ESPINOZA, José. "Legislación en materia de Documento Electrónico y Firma Digital en México". Trabajo realizado en el Curso Documento y Firma Electrónica On line. www.viegasociados.com Montevideo, 2004.

en el Diario Oficial con fecha 10 de agosto de 2004 referida a las Reglas Generales a que deben sujetarse los Prestadores de Servicio de Certificación, y en la misma se describe en forma detallada en 76 páginas y 11 artículos los requisitos y forma de cumplir el Reglamento del Código de Comercio en Materia de Prestadores de Servicio de Certificación aprobado con fecha 14 de julio de 2004.

En México la legislación se orienta a la Firma Electrónica y no a la Firma Digital, optando por la Firma Electrónica Avanzada; y con amplio criterio promueve el uso de cualquier tecnología o programa de cómputo acorde con los principios de neutralidad tecnológica y compatibilidad internacional.

Se estableció equivalencia funcional entre la firma electrónica y la firma autógrafa siempre y cuando la primera sea atribuible a persona obligada y accesible. En el Código Federal de Procedimientos Civiles se aceptó como prueba la información contenida en medios informáticos la misma que debía mantenerse íntegra, inalterable y ser accesible para su ulterior consulta.

Entendiéndose la integridad, respecto a la fiabilidad del método para generarla, comunicarla, recibirla y archivarla y como garantía que el contenido no fue modificado.

La atribución es la forma que garantiza que las partes son lo que dicen ser, y puede ser Simple cuando los datos asociados al mensaje son conocidos por las partes y Avanzada conceptuada como firma electrónica que requiere la intervención de Prestadores de Servicios de Certificación.

15. Cuadro Comparativo entre los Países del MERCOSUR⁶⁹

15.1 Documento Electrónico

⁶⁹ RODRÍGUEZ ACOSTA Beatriz. "Cuadro Comparativo entre los países del MERCOSUR respecto al documento electrónico y la firma digital". Congreso Notarial del MERCOSUR, Montevideo 2004.

*Documentos Electrónicos
Firma Digital*

CONCEPTO	ARGENTINA	BRASIL	PARAGUAY	URUGUAY
Normativa	Ley 19799	Medida Provisoria 2200-2, Código Civil de 2002 y Código de Proceso Civil de 1973		Admisibilidad: art. 146.2 del Código General del Proceso (CGP); Valoración de la Prueba: art. 140, 153, 170 del CGP;
Ambito de aplicación		Todos los documentos electrónicos de que trata la Medida Provisoria (art.10 MP 2200-2)		Ley 16002, art. 129: documentos emergentes de transmisión a distancia, entre dependencias oficiales; Ley 16736, art. 697: los documentos transmitidos por medios informáticos y telemáticos (elimina entre dependencias oficiales, lo que apareja la totalidad de la solución legal)
Eficacia del documento electrónico		Se presumen verdaderos con la utilización del proceso de certificación de la firma		Ambas leyes establecen que constituirá de por sí, documentación auténtica y hará plena fe a todos sus efectos

*Documentos Electrónicos
Firma Digital*

Sanciones			<p>Ley 16002 art. 130: voluntariamente transfiere a distancia, entre dependencias oficiales, un texto del que resulte un documento infiel incurre en los delitos de los arts. 236 a 239 del Código Penal (Falsificación de documentos);</p> <p>Ley 16736, art. 697: no habla de dependencias oficiales, sería todos los documentos; el que transmite, adultere o destruya un documento almacenado en soporte magnético o su respaldo incurre en los delitos mencionados anteriormente.</p>
------------------	--	--	--

*Documentos Electrónicos
Firma Digital*

Almacenamiento del documento electrónico			Dec. 83/01 se determina los medios técnicos de almacenamiento, reproducción y transmisión telemática de los documentos electrónicos a mediano y largo plazo.
---	--	--	--

15.2 Documento Electrónico en los Países Adheridos al MERCOSUR

CONCEPTO	BOLIVIA	CHILE
Normativa		Dec. 81/99
Ambito de aplicación		Regula la utilización del documento electrónico en los órganos de la Administración Pública.
Excepción del ámbito de aplicación		Contraloría General de la República, Banco Central y Municipalidades, (pueden acogerla voluntariamente comunicando al Ministerio Secretaría General de la Presidencia por escrito)
Definición de documento electrónico		Toda representación informática que da testimonio de un hecho
Eficacia del documento electrónico		Los mismos que el documento en soporte papel
Notificaciones y publicaciones a particulares		Estos deberán ser traspasados a soporte papel, que será certificado por el ministro de fe

*Documentos Electrónicos
Firma Digital*

Copias de documento electrónico	Las que fueron producidas anteriormente en papel o en otro medio electrónico se entenderán copias autorizadas, siempre que sean el ministro de fe del servicio correspondiente acredite su correspondencia con éste, mediante certificado firmado digitalmente, lo mismo a la inversa pero certificado firmado con firma ológrafa
--	---

15.3 Firma Electrónica y Digital en los países del MERCOSUR

CONCEPTO	ARGENTINA	BRASIL	PARAGUAY	URUGUAY
Normativa	Ley 19799	Dec. 3587/00, Ley 8935/95 art. 41 a 42		Ley 16713, art.84, Ley 16736, art.695, Dec. 65/98, art. 18 y 19, Dec. 312/98, Ley 17243, art. 25, Dec. 382/03
Clases de firma	Firma electrónica, firma electrónica avanzada			Firma electrónica y firma digital
Validez y eficacia de la firma electrónica y/o digital				Ley 16736 art. 695, Ley 17243, art. 25 inc. 1, Dec. 382/03 art. 3. en todos se establece que tendrán la misma validez y eficacia que la firma autógrafa

*Documentos Electrónicos
Firma Digital*

<p>Ambito de aplicación de la firma</p>	<p>No se aplica a las escrituras públicas, ni aquellos actos o contratos en que la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico, o requieran la concurrencia personal del funcionario que debe intervenir en ellos</p>			<p>Actualmente no existe normativa aplicable al ámbito notarial, si a la administración pública y a la actividad privada.</p>
<p>Infraestructura de clave pública (PKI – ICP)</p>	<p>No hay ninguna entidad certificadora de firma avanzada funcionando. Han presentado sus antecedentes a la subsecretaría de Economía tres hasta la fecha del Comité Notarial del 20/6/03 en Buenos Aires, las que están en proceso de revisión</p>	<p>Del Poder Ejecutivo Federal así como la determinación de reglas y normas que determinará la Autoridad de Gerencia de Políticas y prevé se establezcan procesos de auditoria y fiscalización para garantizar el cumplimiento de las reglas de ICP-Gob.</p>		<p>Ley 17243, art.25 inc.2, y el Dec. 382/03, establecen los requisitos para la Autoridad de Certificación, la no sujeción a autorización previa y su realización en régimen de libre competencia</p>

*Documentos Electrónicos
Firma Digital*

entidades certificadoras		El Colegio Notarial de Brasil firmó convenio con la Certificadora Notarial S.A.	Existen cuatro entidades de certificación: Asociación de Escribanos del Uruguay, Administración Nacional de Correos, Abitab, Cámara Nacional de Comercio
Equivalencia de los certificados digitales nacionales y extranjeros			Dec. 382/03 art. 9, se reconoce la equivalencia entre los certificados nacionales y extranjeros siempre que existan similares exigencias y reciprocidad

CAPITULO V

DERECHO URUGUAYO

1. Introducción

Luego de ver el tratamiento del documento electrónico y la firma digital en el derecho comparado, vamos a realizar un análisis del derecho uruguayo. Aquí debemos estudiarlo desde dos aspectos: el de la admisibilidad como medios probatorios de los documentos electrónicos y el de su valoración judicial.

Admisibilidad: ya desde el artículo 26 de la hoy derogada Ley de Abreviación de los Juicios N° 13.355 se los puede admitir como prueba al decir “podrán utilizarse otros medios probatorios no prohibidos por la ley”, solución que se reitera en el actual Código General del Proceso (CGP) en el artículo 146.2 como veremos más adelante.

Valoración: aquí nuestro ordenamiento jurídico ha optado por un sistema mixto de prueba legal para determinados medios probatorios, como los instrumentos públicos y privados y la confesión judicial que hace plena prueba y la apreciación judicial conforme a las reglas de la sana crítica para las restantes probanzas.

A continuación realizaremos un análisis del derecho positivo uruguayo referente al documento electrónico y firma digital en orden cronológico.

2. Código General del Proceso de fecha 18 de octubre de 1988

Artículo 77. “La notificación se practicará ... o por el medio idóneo que habilite la Suprema Corte de Justicia”.

Documentos Electrónicos Firma Digital

Tenemos la posibilidad de que la Suprema Corte reglamente por Acordada el uso de medios electrónicos para realizar las notificaciones dentro del proceso judicial.

Artículo 140. Dispone que “las pruebas se apreciarán tomando en cuenta cada una de las producidas y en su conjunto, racionalmente, de acuerdo con las reglas de la sana crítica, salvo texto legal que expresamente disponga una regla de apreciación diversa”.

Artículo 146.2. A su vez este artículo agrega que: *“También podrán utilizarse otros medios probatorios no prohibidos por la regla de derecho, aplicando analógicamente las normas que disciplinan a los expresamente previstos por la ley”.*

Si bien no menciona expresamente los medios electrónicos, deja una puerta abierta a su utilización.

Artículo 170.2 *“Los demás documentos privados emanados de las partes, se tendrán por auténticos, salvo que se desconozca su firma, si están suscritos o la autoría, si no lo están, ...”.*

Con relación a estos tres artículos el Dr. Bauzá⁷⁰ comenta: “El caso en que todos los artículos vinculados a la “prueba por documentos” (privados), la Comisión Legislativa que estudiaba el proyecto de ley introdujo ciertos cambios llamativos en la redacción de los textos respectivos, trocando ciertas expresiones limitativas como la de “suscritos” (o “manuscritos”) por la más amplia de “emanados”.”

Con estos artículos se destierra la idea restrictiva de documento, como aquel escrito y firmado por su autor. El “documento electrónico” podrá ser admitido en virtud a estas normas. Las Escribanas Siri y Wonsiak⁷¹ llegan a la siguiente conclusión: “Los documentos electrónicos que se sustentan en otro tipo de soporte, por la imposibilidad de cumplir con las “formas requeridas” –las

⁷⁰ BAUZA REILLY, Marcelo. “Aperturas del Derecho de la Prueba en Uruguay en materia de nuevas tecnologías de la información”.

⁷¹ SIRI Julia y WONSIK María “El documento electrónico”. Revista de la Facultad de Derecho y Ciencias Sociales, Montevideo, 1988.

que fueron pensadas para el documento papel-, en el estado actual de nuestra legislación no pueden ser documentos públicos, pero sí pueden llegar a alcanzar el valor de documento privado reconocido, si se dan las circunstancias para ello.”

3. Ley N° 15921 de fecha 17 de diciembre 1987

Esta ley fue reglamentada por el Decreto N° 454/988 de 8 de julio de 1988 y el presente artículo fue modificado por el artículo 65 de la Ley N° 17.292 de 25 de enero de 2001.

Artículo 2º.- Las zonas francas son áreas del territorio nacional de propiedad pública o privada, cercadas y aisladas eficientemente, las que serán determinadas por el Poder Ejecutivo previo asesoramiento de la Comisión Honoraria Asesora de Zonas Francas, con el fin de que se desarrollen en ellas con las exenciones tributarias y demás beneficios que se detallan en esta ley, toda clase de actividades industriales, comerciales o de servicios y entre ellas:

A) Comercialización, depósito, almacenamiento, acondicionamiento, selección, clasificación, fraccionamiento, armado, desarmado, manipulación o mezcla de mercancías o materias primas de procedencia extranjera o nacional.

B) Instalación y funcionamiento de establecimientos fabriles.

C) Prestación de servicios financieros, de informática, reparaciones y mantenimiento, profesionales y otros que se requieran para el mejor funcionamiento de las actividades instaladas y la venta de dichos servicios a terceros países.

D) Otras que a juicio del Poder Ejecutivo resultaren beneficiosas para la economía nacional o para la integración económica y social de los Estados.

El Poder Ejecutivo adoptará las medidas necesarias a los efectos de que estas actividades no perjudiquen la capacidad exportadora de las industrias ya instaladas en zonas no franca.

4. Ley Nº 16.002 de fecha 25 de noviembre de 1988

Artículo 129. *“La documentación emergente de la transmisión a distancia, por medios electrónicos, entre dependencias oficiales, constituirá, de por sí, documentación auténtica y hará plena fe a todos sus efectos en cuanto a la existencia del original transmitido”.*

Artículo 130. *“El que voluntariamente transmitiere a distancia entre dependencias oficiales un texto del que resulte un documento infiel, incurrirá en los delitos previstos por los artículos 236 a 239 del Código Penal, según corresponda”.*

Estos artículos regulan la autenticidad y prueba de los documentos transmitidos a distancia por medios electrónicos entre dependencias oficiales. Los delitos a que alude son los que penalizan la falsificación documentaria. El artículo 130 puede considerarse el primer delito informático regulado en el derecho positivo uruguayo.

5. Ley Nº 16.060 de fecha 5 de enero de 1990

Luego la nueva Ley de Sociedades Comerciales Nº 16060 introduce otras reformas al admitir ampliamente el uso de los medios técnicos disponibles, en sus artículos 11, 91 y 418, esto a su vez fue regulado por el Decreto 104/91. A través de estas normas se habilita el uso del documento electrónico en materia de libros y contabilidad de las sociedades, con el mismo valor probatorio de las formas tradicionales de documentación sobre papel.

Artículo 11. *“En el Registro Público de Comercio, realizada su inscripción, se formarán un legajo para cada sociedad, con las copias del contrato social, sus modificaciones y demás documentos que disponga la ley o su reglamentación. Su consulta será pública.”*

La Reglamentación podrá autorizar el empleo de todos los medios técnicos disponibles para el cumplimiento de lo dispuesto en el inciso anterior”.

Si bien resulta muy interesante la amplitud de este artículo, al referirse a “medios técnicos” fue suspendida la vigencia por la Ley 16.170, que en su artículo 383 establece *“Suspéndese la aplicación del artículo 11 de la Ley 16.060, de 4 de setiembre de 1989, hasta que el Poder Ejecutivo proceda a su reglamentación, la cual deberá dictarse cuando a su juicio se disponga de los medios técnicos apropiados, para la formación del legajo o de información equivalente”*.

Artículo 91. *“La reglamentación establecerá las normas contables adecuadas a las que habrán de ajustarse los estados contables de las sociedades comerciales.*

Asimismo podrá autorizar para estas sociedades, el empleo de todos los medios técnicos disponibles en reemplazo o complemento para estas sociedades de los libros obligatorios impuesto a los comerciantes”.

Artículo 418. *“Sin perjuicio de lo dispuesto por el artículo 11 el órgano estatal de control formará su propio legajo de cada sociedad anónima con la copia del contrato social, sus modificaciones, los documentos que deban incorporarse al legajo del Registro Público de Comercio, los referidos en el artículo 414 y aquellos que disponga la reglamentación.*

La reglamentación podrá autorizar el empleo de todos los medios técnicos disponibles para el cumplimiento de lo dispuesto en el inciso anterior.”

6. Decreto N° 500/991 de fecha 27 de setiembre de 1991

Artículo 14. *“Es de interés público, para mejor cumplimiento de los servicios, el intercambio permanente y directo de datos e información entre todas las unidades y reparticiones de la Administración Pública, sea cual fuere su naturaleza jurídica o posición institucional, a través de cualquier medio hábil de comunicación, sin más limitación que lo dispuesto en el artículo 80.*

A efectos de implementar sistemas de libre flujo de información se propenderá a la interconexión de los equipos de procesamiento electrónico de información u otros similares.

Asimismo podrá la Administración brindar el servicio de acceso electrónico a sus bases de datos a las personas físicas o jurídicas, estatales, paraestatales o privadas que así lo solicitaren”.

Este decreto es de suma importancia, ya que está enmarcado en el ámbito de la Reforma del Estado, en lo concerniente al proceso de desburocratización del mismo. Tengamos presente las palabras de Bill Gates⁷²: “La administración, quizá más que ninguna otra organización saldrá ganando con la eficiencia y la mejora del servicio que derivan de los procesos digitales. Los países desarrollados van a mostrar el camino de cómo se crean procesos sin papel para reducir la burocracia. Sin embargo la mayoría de las administraciones andan muy rezagadas, en comparación con las empresas, por lo que se refiere al empleo de los instrumentos de la era digital.”

Artículo 19 inciso final. *“Asimismo las dependencias de la Administración Central podrán admitir la presentación de los particulares por fax u otros medios similares de transmisión a distancia, en los casos que determinen”.*

Artículo 32. *“La documentación emergente de la transmisión a distancia, por medios electrónicos, entre dependencias oficiales, constituirá, de por sí, documentación automática y hará plena fe a todos sus efectos en cuanto a la existencia del original transmitido.*

⁷² GATES, Bill. “Los negocios en la era digital”. Editorial Sudamérica. 1999. Página 403.

Documentos Electrónicos Firma Digital

El que voluntariamente transmitiere a distancia entre dependencias oficiales un texto del que resulte un documento infiel, incurrirá en los delitos previstos por los artículos 236 a 239 del Código Penal, según corresponda (Ley 16.002 artículos 129 y 130)”.

Este artículo es relevante en la medida que equipara este tipo de documentos al documento público, ya que establece que el mismo hará plena fe.

Artículo 33. *“En aplicación a lo dispuesto por el artículo 14, la Administración propiciará el uso de soportes de información electrónicos, magnéticos, audiovisuales, etc., siempre que faciliten la gestión pública”.*

Artículo 70 inciso 1º. *“Los hechos relevantes para la decisión de un procedimiento podrán acreditarse por cualquier medio de prueba no prohibido por la ley”.*

Cualquier medio de prueba, dice este artículo, o sea que podemos utilizar tecnología actual o futura, y dependerá de nuestra imaginación el alcance que podamos darle. Sin duda, este artículo rige en el ámbito del procedimiento administrativo, pero no debemos olvidar que en el Código General del Proceso existe una norma similar que establece que podrán utilizarse otros medios probatorios no prohibidos por la regla de derecho.

Artículo 90. *“Autorízase la copia fotográfica y microfilmada de los expedientes y demás documentos archivados en todas las dependencias del Estado y demás Organismos Públicos, y la destrucción de los documentos originales cuando ello sea indispensable, de conformidad con las normas reglamentarias vigentes o a dictarse.*

Dichas copias tendrán igual validez que los antecedentes originales a todos los efectos legales, siempre que fueren debidamente autenticadas por las Direcciones de las respectivas Oficinas (Ley 14.106, de 14 de marzo de 1973, artículo 688)”.

Evidentemente lo que se busca aquí es ganar espacio físico y mejorar la búsqueda de información. Pero la crítica que podemos hacerle a este artículo, es que se trata de una norma cerrada, ya que la misma enumera en forma taxativa los medios técnicos que pueden utilizarse, eliminando la posibilidad de aplicar nuevas tecnologías.

Artículo 91 inciso final. *“También podrá practicarse la notificación a domicilio por telegrama colacionado certificado con aviso de entrega, por carta certificada con aviso de retorno, télex, fax o cualquier otro medio idóneo que proporcione certeza en cuanto a la efectiva realización de la diligencia y a su fecha, así como en cuanto a la persona a la que se ha practicado”.*

Si bien establece que se puede notificar por cualquier otro medio idóneo, pone como condición fundamental la existencia de certeza en la actuación.

Artículo 154 inciso 1º. *“Cualquiera sea la forma documental utilizada para la interposición de los recursos (escrito en papel simple, formulario o impreso, telegrama colacionado certificado con aviso de entrega, télex, fax, o cualquier otro medio idóneo), siempre deberá constar claramente el nombre y domicilio del recurrente y su voluntad de recurrir traducida en la manifestación de cuales son los recursos que se interponen y la designación del acto administrativo que impugna”.*

Artículo 157. *“En caso de que los recursos se hayan interpuesto mediante telegrama colacionado certificado con aviso de entrega, télex, fax, u otro procedimiento similar, por razones de conservación de la documentación y seguridad jurídica, la Administración procederá de inmediato a su reproducción a través de los medios pertinentes y formará el correspondiente expediente. El jefe o encargado de la unidad de administración documental extenderá la correspondiente certificación de la reproducción realizada.*

En los casos señalados precedentemente, el recurrente o su representante dispondrá de un plazo de diez días hábiles a contar del siguiente a la recepción del correspondiente documento por la Administración, para comparecer en la oficina a efectos de ratificar por escrito su voluntad de

recurrir, de cumplir con la exigencia legal de la firma letrada, para la agregación del mandato respectivo en caso de representación y, en general, para cumplir con todo otro requisito que para el caso sea exigible. Si no lo hiciera dentro del plazo señalado, sin justa causa, la Administración tendrá el recurso por no presentado”.

El avance que establece el artículo 154 se ve disminuido por la exigencia planteada por el artículo 157 al deber comparecer a ratificar, como forma de dar seguridad al acto jurídico.

Artículo 158 inciso final. *“En los demás procedimientos referidos en el artículo anterior, se tendrá por fecha y hora de recepción, la que luzca el reporte emitido por el equipo utilizado o, en su defecto, la que estampa el funcionario receptor”.*

Sin embargo, aquí se confía en la fecha y hora que emita el equipo utilizado. Cuando se redactó este artículo se pensaba en el fax como medio de comunicación.

Artículo 195. *“Los hechos relevantes para la decisión del procedimiento disciplinario podrán acreditarse por cualquier medio lícito de prueba (fotografías, fotocopias, croquis, cintas magnetofónicas, así como por todo otro medio hábil que provea la técnica)”.*

Este es un caso de artículo abierto, en el cual el software podría estar comprendido.

7. Ley N° 16.226 de fecha 29 de octubre de 1991

En 1991 la Ley N° 16.226 en su artículo 384 permitió al Tribunal de lo Contencioso Administrativo (TCA) practicar sus notificaciones procesales por “medios electrónicos o de similares características”. Esto habilita la conexión directa “on line” con ese tribunal, tanto para las notificaciones como para el seguimiento del trámite.

Artículo 383. “El tribunal de lo Contencioso Administrativo podrá, en forma directa o por concesión de terceros, brindar el servicio de acceso electrónico digital a sus bases de datos de jurisprudencia y gestión, por medio de la red telefónica pública, a las personas físicas o jurídicas, estatales, paraestatales o privadas que así lo solicitaren. El Tribunal de lo Contencioso Administrativo fijará los precios de los servicios, que no podrán superar los precios del mercado”.

Artículo 384. “Las comunicaciones procesales a las partes podrán efectuarse también por medios electrónicos o de similares características. Los documentos emergentes de la transmisión, constituirán documentación auténtica que hará plena fé a todos sus efectos, siendo de aplicación lo dispuesto por el artículo 130 de la Ley Nº 16.002 del 25 de noviembre de 1988.

El Tribunal de lo Contencioso Administrativo determinará y reglamentará la forma en que se practicarán las mismas”.

8. Ley Nº 16.713 de fecha 3 de setiembre de 1995

La Ley Nº 16.713 de 3 de setiembre de 1995, de Seguridad Social, en el capítulo referente al Banco de Previsión Social, artículo 84, establece: “En los cheques emitidos por el Banco de Previsión Social, destinados al pago de jubilaciones, pensiones y otros beneficios, podrá sustituirse la firma autógrafa por signos o contraseñas impuestos o impresos mecánica o electrónicamente”.

9. Ley Nº 16.736 de fecha 5 de enero de 1996

Artículo 694. “Las administraciones públicas impulsarán el empleo y aplicación de medios informáticos y telemáticos para el desarrollo de sus actividades y el ejercicio de sus competencias, garantizando a los administradores el pleno acceso a las informaciones de su interés”.

Consagra “el derecho de acceso” por parte del administrado sobre informaciones de su interés y se lo ha considerado también como el germen del llamado “derecho de rectificación”. El Dr. Delpiazzo⁷³ sostiene con razón que ya está consagrado en el artículo 14 del Pacto de San José de Costa Rica, el cual fue ratificado por ley en nuestro país y que dice: “*toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio... y que se dirijan al público en general tiene derecho a efectuar su rectificación o respuesta*”.

Artículo 695. “*Los trámites y actuaciones que conforman el procedimiento administrativo así como los actos administrativos podrán realizarse por medios informáticos.*”

Su validez jurídica y valor probatorio serán idénticos a los de las actuaciones administrativas que se tramiten por medios convencionales.

La firma autógrafa podrá ser sustituida por contraseñas o signos informáticos adecuados”.

Equipara los medios informáticos a los convencionales, reconoce su validez jurídica y les otorga el mismo valor probatorio. El inciso final de este artículo está consagrando la firma electrónica.

Artículo 696. “*La notificación personal de los trámites y actos administrativos podrá realizarse válidamente por correo electrónico u otros medios informáticos o telemáticos, los cuales tendrán plena validez a todos los efectos siempre que proporcionen seguridad en cuanto a la efectiva realización de la diligencia y a su fecha*”.

Hablar de notificaciones por correo electrónico es sin duda un gran avance, en cuanto a la rapidez con que se pueden realizar las actuaciones. Sin embargo, el legislador nunca pierde de vista la seguridad que debe darse a estos procedimientos.

⁷³ DELPIAZZO Carlos E. “Derecho Informático Uruguayo”. Montevideo 1995. Página 60.

Documentos Electrónicos Firma Digital

Artículo 697. *“La documentación emergente de la transmisión por medios informáticos o telemáticos constituirá de por sí documentación auténtica y hará plena fe, a todos sus efectos, en cuanto a la existencia del origen transmitido”.*

Vemos que esta norma amplía el artículo 129 de la ley 16.002 en dos aspectos: sustituye el término “medios electrónicos” por “medios informáticos y telemáticos” y elimina la frase “entre dependencias oficiales”, lo que hace a la norma aplicable a nivel general.

El inciso segundo establece: *“El que voluntariamente transmitiere un texto del que resulte un documento infiel, adultere o destruya un documento almacenado en soporte magnético, o su respaldo, incurrirá en los delitos previstos por los artículos 236 a 239 del Código Penal, según corresponda”.*

Comparando con el artículo 130 de la ley 16.002 podemos observar que en primer lugar hay una ampliación de los comportamientos reprimibles, en segundo lugar se elimina la expresión “entre dependencias oficiales” y se tiene en cuenta para quien adultere o destruya el “documento almacenado en soporte magnético o su respaldo”.

10. Decreto Nº 65/998 de fecha 10 de marzo de 1998

El Decreto 65/998 de fecha 10 de marzo de 1998, cumplió con lo prescripto por el artículo 698 de la Ley 16.736 y reglamentó el procedimiento administrativo electrónico.

En su artículo 1 inciso final establece: *“Cuando la substanciación de las actuaciones administrativas se realice por medios informáticos, las firmas autógrafas que la misma requiera podrán ser sustituidas por contraseñas o signos informáticos adecuados”.*

Y en el inciso segundo establece *“...constituirán instrumentos públicos y como tales se tendrán como auténticos y harán plena fe ...”*

Documentos Electrónicos Firma Digital

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

Artículo 3 inciso 1º. *“El expediente electrónico tendrá la misma validez jurídica y probatoria que el expediente tradicional”.*

Artículo 18 define la firma electrónica como *“el resultado de obtener por medio de mecanismos o dispositivos un patrón que se asocie biunívocamente a un individuo y a su voluntad de firmar.”*

Artículo 19 establece que la firma digital es: *“un patrón creado mediante criptografía, debiendo utilizarse sistemas criptográficos “de clave pública” o “asimétricos”, o los que determine la evolución de la tecnología”.*

Artículo 25. Reproduce el inciso 2 del artículo 697 de la Ley 16.736, que había modificado el artículo 130 de la Ley 16.002.

Artículo 26. Reproduce el artículo 130 de la ley 16.002, lo cual carece de sentido.

11. Decreto Nº 312/998 de fecha 3 de noviembre de 1998

Se establece el uso de la firma electrónica para el Documento Único Aduanero y la Declaración de Valor de Aduanas cuando se realicen por medios electrónicos (artículo 6).

El artículo 7 establece: *“La intervención del Despachante de Aduana en la operación aduanera y las responsabilidades derivadas de ella que no le sean directamente imputables, quedarán respaldadas por la firma del importador, exportador o remitente en la Declaración Jurada de Responsabilidad, la que presentará junto a la declaración aduanera, en tanto no se haga uso de la firma electrónica”.*

En el artículo 17 se establece que la contraseña enviada por el Organismo tendrá la misma validez jurídica y probatoria que las firmas autógrafas que sus funcionarios realizan sobre las declaraciones presentadas en papel.

12. Ley N° 17.243 de fecha 29 de junio de 2000

Por Ley N° 17.243 de 29 de junio de 2000 se ha regulado la firma electrónica bajo el título Sistema Informático del Estado.

Artículo 25 establece : *“Autorízase en todo caso la firma electrónica y la firma digital, las que tendrán idéntica validez y eficacia a la firma autógrafa, siempre que estén debidamente autenticadas por claves u otros procedimientos seguros, de acuerdo a la tecnología informática”* (inciso 1º). Y agrega en el inciso 2º que: *“La prestación de servicios de certificación no estará sujeta a autorización previa y se realizará en régimen de libre competencia, sin que ello implique sustituir o modificar las normas que regulan las funciones que corresponde realizar a las personas facultadas para dar fe pública o intervenir en documentos públicos”*.

Este artículo ha desatado grandes polémicas y ha dividido las opiniones de prestigiosos juristas en dos posturas diferentes:

a) Por un lado el Dr. Carlos E. Delpiazzo⁷⁴ extiende el alcance de la firma digital, con la referencia “en todo caso”, más allá de las fronteras de la Administración Pública. Esto surge según su opinión de la claridad de la norma y de la historia fidedigna de su sanción.

Teniendo presente la discusión parlamentaria, el Senador Ruben Correa Freitas ha manifestado que:

⁷⁴ DELPIAZZO, Carlos E. “La autenticación de las operaciones comerciales en Internet”. Primeras Jornadas Académicas del Instituto de Derecho Informático. Montevideo, 2000.

Documentos Electrónicos Firma Digital

- 1) la modificación se introdujo en el texto del articulado en el momento del pasaje del Proyecto por el Senado,
- 2) debe ampliarse la validez de la firma electrónica fuera del ámbito de la Administración Pública y
- 3) que la firma digital sea válida en cualquier acto jurídico, tanto en los documentos privados como en los públicos.

b) La Escribana Julia Siri entiende que no debe extenderse el alcance de este artículo fuera del ámbito de la Administración Pública en base a los siguientes argumentos:

- 1) El artículo 25 está inserto en la Sección 3 de la Ley de Urgencia, titulada “Sistema Informático del Estado”, por lo cual debe interpretarse en dicho contexto.
- 2) El artículo 24 establece la obligatoriedad del expediente electrónico para la Administración Pública.
- 3) La ley 16.736 posibilitaba el empleo de la firma digital por funcionarios del Estado (con la excepción del Presidente y los Ministros que debía seguir siendo ológrafa). La expresión “en todo caso” quizá está incluyendo a estos funcionarios.
- 4) El artículo 26 prevé que estos artículos puedan ser aplicados a los Gobiernos Departamentales.
- 5) Ninguna autoridad ajena al Notariado, puede ofrecer el mayor valor que la intervención notarial proporciona.

13. Ley Nº 17.292 de fecha 25 de enero de 2001

El artículo 65 de la Ley Nº 17.292 de 25 de enero de 2001 modifica el artículo 2 de la Ley Nº 15.921 de 17 de diciembre de 1987 referente a Zonas Francas y establece que *“los usuarios de zonas francas podrán brindar los*

siguientes servicios telefónicos o informáticos desde zonas francas hacia el territorio nacional no franco, respetando los monopolios, exclusividades estatales y/o concesiones públicas” y en el literal e) refiere a la “emisión de certificados de firma electrónica”.

14. Decreto Nº 83/2001 de fecha 8 de marzo de 2001

Por este decreto se determina los medios técnicos de almacenamiento, reproducción y transmisión telemática de los documentos electrónicos a mediano y largo plazo.

Artículo 1. Establece una lista de la cual podrán seleccionarse los medios de almacenamiento de documentos electrónicos a mediano y largo plazo:

* Discos de Video Digital sólo de lectura (conocidos por sus siglas en inglés DVD-R "digital Video Disc Recordable")

* Discos Magneto Ópticos de escritura única y lectura múltiple (conocidos por sus siglas en inglés MO-WORM "Magneto Optical Disc Write Once Read Many")

* Discos compactos de escritura única y lectura múltiple (conocido por sus siglas en inglés CD-R "Compact Disc Recordable").”

Artículo 2. Debe tenerse en cuenta que los medios de soporte de la tecnología a emplearse, deberán contar con certificación de calidad ISO y deberán tener una vida útil mínima de 20 años. Además, determina que el control de calidad de dichos medios será responsabilidad de los Centros de Cómputos de cada organismo del Estado.

Artículo 3. Los registros de documentos electrónicos que se realicen a través de la utilización de alguno de los medios indicados en el artículo 1º, deberán efectuarse en un mínimo de dos copias.

Documentos Electrónicos Firma Digital

Deberá utilizarse siempre la misma copia para el uso periódico, permaneciendo las restantes como archivo muerto. El archivo muerto deberá ubicarse en un lugar físico diferente al de la copia de uso periódico, asegurando sus condiciones de preservación.

Artículo 6. *“El proceso de copiado de los documentos a los medios citados, deberá contar con una etapa previa de control de calidad, en la que se registrará la fecha y la hora del control, así como el nombre, apellido, documento de identidad y la firma digital o contraseña del funcionario responsable de dicho cometido”.*

Artículo 7. *“A efectos del almacenamiento de documentos electrónicos a corto plazo, podrá utilizarse cualquier dispositivo de uso corriente en los equipos informáticos disponibles en cada organismo del Estado, debiendo contar los mismos con el correspondiente respaldo de acuerdo con las medidas de seguridad oportunamente adoptadas por los distintos Centros de Cómputos. El almacenamiento de dichos respaldos deberá realizarse de forma que asegure su protección e inalterabilidad y en lugares físicos alejados de los centros de procesamiento de la información”.*

15. Decreto N° 382/2003 de fecha 17 de setiembre de 2003

El presente decreto reglamenta el uso de la firma digital y el reconocimiento de su eficacia jurídica.

En el artículo 2 se establecen una serie de definiciones, de las cuales vamos a mencionar las siguientes:

a) Firma Digital es el resultado de aplicar a un documento un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, de manera tal que dicha verificación permita, simultáneamente, identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

b) Prestador de servicios de certificación es una tercera parte que expide certificados digitales, pudiendo prestar además, otros servicios relacionados con la firma digital.

El artículo 3 establece: “La firma digital tendrá idéntica validez y eficacia a la firma autógrafa, siempre que esté debidamente autenticada por claves u otros procedimientos seguros de acuerdo a la tecnología informática que:

1. garanticen que la firma digital se corresponde con el certificado digital emitido por un prestador de servicios de certificación de firma digital, que lo asocia con la identificación del signatario;

2. aseguren que la firma digital se corresponde con el documento respectivo y que el mismo no fue alterado ni pueda ser repudiado; y

3. garanticen que la firma digital ha sido creada usando medios que el signatario mantiene bajo su exclusivo control y durante la vigencia del certificado digital.

16. Decreto Nº 392/003 de fecha 26 de setiembre de 2003

El artículo 10 (Capítulo III – De las empresas industrializadoras y empresas exportadoras de arroz y derivados) establece:

“Las empresas exportadoras (industrializadoras o no), previo a cada embarque, deberán depositar el monto de la retención del 5% correspondiente a cada operación de exportación en la cuenta que a tales efectos se abrirá en el BROU, con el nombre MGAP/FFRAA, anexando la siguiente información: el volumen exportado, el precio declarado por los productos comprendidos en dicho documento, y el agente financiero a través del que se percibirá el producido de cada negociación de venta cursada.

Al recibo de cada pago realizado por las empresas o productores exportadores, el BROU expedirá un certificado en dos vías (una dirigida a la Dirección Nacional de Aduanas y otra a la Comisión de Contralor del FFRAA



creada por el Art. 8º de la ley N° 17.663, de 11 de julio de 2003), en el que se detallará la exportación a la que corresponde la retención y el importe efectivamente depositado. El BROU podrá sustituir, una o ambas vías de este certificado, por el documento electrónico que se considere adecuado.

La Dirección Nacional de Aduanas no aprobará ni numerará el Documento Unico de Exportación (DUA) correspondiente a exportaciones comprendidas en el Art. 2º de este decreto, ni permitirá que se cursen de ningún modo exportaciones de arroz alcanzadas por el Art. 2º de la ley N° 17.663, de 11 de Julio de 2003, sin constatar, previamente, que el exportador haya abonado la retención correspondiente en la cuenta del MGAP/FFRAA, cuya apertura se ha dispuesto en el BROU.

En caso de anulación o cumplimiento parcial de una exportación, una vez recibida la información oficial de la Dirección Nacional de Aduanas, el BROU podrá aceptar que las retenciones pagadas en exceso sean consideradas como pagos de nuevas exportaciones del productor o empresa exportadora.”

17. Decreto N° 396/003 de fecha 30 de setiembre de 2003

A partir del Decreto 258/92 de fecha 9 de junio de 1992, se puede llevar la historia clínica en forma electrónica.

Este decreto fue modificado por el 396/003, a través del cual se han adoptado una serie de normas mínimas que contemplen equilibradamente los derechos fundamentales de cada persona y el interés colectivo comprometido en la preservación de la higiene pública.

En el artículo 1 se define la historia clínica electrónica como el conjunto de datos clínicos, sociales y financieros referidos a la salud de una persona, procesados a través de medios informáticos o telemáticos.

Documentos Electrónicos Firma Digital

A pesar que Uruguay no ha legislado una ley específica en materia de documento electrónico y firma digital, ya desde el año 1988 el tema ha sido regulado a través de las diferentes normas que acabamos de analizar.

CAPITULO VI

FIRMA ELECTRÓNICA Y DIGITAL

1. Introducción

Según Reynaldo de la Fuente “El mito de los computadores ha enmascarado al verdadero héroe de estos tiempos que es la información”⁷⁵.

Esta es una apreciación de relevancia en la medida que el análisis de la vulnerabilidades tecnológicas y las diferentes medidas que apuntan a lograr su seguridad, nos interesa desde el punto de vista de la protección de la información, de la integridad de la misma, ya sea a la hora de transmitir documentos electrónicos, de celebrar contratos o de ejecutar los mismos⁷⁶.

La **seguridad informática** tiene como objetivo la protección del dato, que el mismo mantenga las siguientes cualidades⁷⁷:

a) La integridad: implica que el contenido, ya sea que se encuentre en un computador o que circule a través de una red, permanezca inalterado. En caso de sufrir modificaciones que sea por persona autorizada y que exista en el sistema la constancia de esta modificación, que hará viable su control al realizarse auditorías.

b) La disponibilidad: u operatividad de la información es su capacidad de estar disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el

⁷⁵ DE LA FUENTE Reynaldo. “Aportes a la Seguridad y Privacidad en Informática y Comunicación de Datos”. Polo Ltda. 2da. Edición Actualizada. Montevideo, 1995.

⁷⁶ VIEGA María José. “Seguridad Informática”. Boletín de Derecho y Tecnologías N° 8 Mayo 2004. www.viegasociados.com/moodle/mod/forum/view.php?id=91

⁷⁷ VIEGA María José “La firma Digital y la Autoridad Certificante en Uruguay”. Ponencia presentada al VI Congreso Iberoamericano de Derecho e Informática. Lima, Abril de 2000.

hardware o el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria⁷⁸.

c) La confidencialidad o privacidad: implica el conocimiento de la misma exclusivamente por las personas autorizadas. Esto se logra a través de control de acceso, sistemas criptográficos y métodos apropiados de conducción de las personas, los documentos y los medios de almacenamiento de datos.

Por otra parte, al hablar de **seguridad jurídica** nos encontramos con la existencia de diversas acepciones entre las que establecen⁷⁹:

- a) la seguridad jurídica es base y condición para que el derecho cumpla sus fines de justicia, a través de normas que regulan los derechos y obligaciones de los integrantes de una comunidad⁸⁰.
- b) La seguridad jurídica constituye el valor fundamental a cuya satisfacción tiende tanto el Notariado de tipo latino como las normas registrales⁸¹.

Para que el documento informático pueda ser asimilado y valorado en calidad de instrumento probatorio debe reunir al menos cuatro requisitos básicos: fehaciencia, individualización de las partes del documento y de la autoridad certificadora, que comprende además su datación, seguridad documental a través de un sistema de cifrado del documento y firmas digitales del mismo⁸².

⁷⁸ A.S.S. BORGHELLO, Cristian Fabián. Director de Tesis: Ing. GOTTLIEB Bernardo. Asesor científico: MINGO Graciela. "Tesis Licenciatura en Sistemas: Seguridad Informática sus implicancias e implementación". Universidad Tecnológica Nacional. Setiembre, 2001. www.cfbsoft.com.ar

⁷⁹ RODRÍGUEZ, Beatriz. La función notarial y la seguridad jurídica en los negocios electrónicos. IV Jornadas Académicas Internacionales del Instituto de Derecho Informático. Montevideo, 21 y 22 de Agosto de 2003.

⁸⁰ LOUREIRO Norma, RANZETTI Ana María, "Garantías de los Derechos Reales mediante el sistema de registro y seguro de título. Revista de la Facultad de Derecho. Enero – Julio/2001 N° 19.

⁸¹ MIRANDA Marcelo, "Estudio comparativo de la Transmisión y Constitución de Derechos Reales en E.E.U.U. frente a Sistemas que componen la intervención del Notariado". 1974.

⁸² GAETE GONZALEZ Eugenio Alberto. "Instrumento público electrónico. Ob. cit., página 177.

2. Firma Ológrafa

En Roma, los documentos no eran firmados. Existía una ceremonia llamada *manufirmatio*, por la cual, luego de la lectura del documento por su autor o el *notarius*, era desplegado sobre una mesa y se pasaba la mano por el pergamino en signo de aceptación. Solamente después de cumplir esta ceremonia se estampa el nombre del autor⁸³.

En el sistema jurídico visigótico existía la confirmación del documento por los testigos que lo tocaban (*chartam tangere*), signaban o suscribían (*firmatio*, *roboratio*, *stipulatio*). La firma del que da el documento o librador es corriente, pero no imprescindible. Los documentos privados son, en ocasiones confirmados por documentos reales. Desde la época euriciana las leyes visigodas prestaban atención a las formalidades documentales, regulando detalladamente las suscripciones, signos y comprobación de escritura. La “suscriptio”, representaba la indicación del nombre del signante y la fecha, y el “signum”, un rasgo que la sustituye si no sabe o no puede escribir. La suscriptio daba pleno valor probatorio al documento y el signum debía ser completado con el juramento de la veracidad por parte de uno de los testigos. Si falta la firma y el signo del autor del documento, este es inoperante y debe completarse con el juramento de los testigos sobre la veracidad del contenido⁸⁴.

En la Edad Media se implantaba el sello real, el cual pasó posteriormente a las clases nobles y privilegiadas.

Según el Dr. Eduardo Couture en su “Vocabulario Jurídico”, firma es: “ el trazado gráfico, conteniendo habitualmente el nombre, apellido y rúbrica de una persona, con el cual se suscriben los documentos para darle autoría y obligarse con lo que en ellos se dice”⁸⁵.

⁸³ CARRASCOSA LOPEZ Valentín. “Valor Probatorio del Documento electrónico”. Revista Informática y Derecho. Volumen 8. UNED Centro Regional de Extremadura, 1995. Página 140.

⁸⁴ LOPEZ Fernando Ernesto. “De la caligrafía a la criptografía”. Ponencia presentada al IX Congreso Iberoamericano de Derecho e Informática. Costa Rica, 2002.

⁸⁵ COUTURE, Eduardo J.. “Vocabulario Jurídico”. Ediciones Depalma, Buenos Aires, 1983.

Documentos Electrónicos Firma Digital

Pablo Palazzi⁸⁶ define la firma como “*el trazo particular por el cual el sujeto consigna habitualmente su nombre y apellido, o sólo su apellido, a fin de hacer constar las manifestaciones de su voluntad*”.

El Reglamento Notarial (Acordada 7533 de la Suprema Corte de Justicia del Uruguay de fecha 22 de octubre de 2004) en su artículo 162 prevé que: “Leída y otorgada la escritura, será firmada a continuación por los otorgantes y demás sujetos auxiliares intervinientes y autorizada por el Escribano, quien deberá firmar en último lugar” y el artículo 163 inciso 1º establece que: “Los otorgantes y demás sujetos auxiliares, firmarán sólo con iniciales, o con el apellido o apellidos que usen, o con grafías ilegibles, si es que así lo hacen habitualmente”.

Como vemos tanto en el derecho positivo como en la doctrina la firma puede ser de diferentes formas, pero siempre un dibujo que va a representar como habitualmente esa persona firma. Por lo que podemos ver que su característica principal es la de habitualidad; esa habitualidad hace que podamos vincular al autor de la firma con la firma⁸⁷.

Muchas veces nos preguntamos si la firma tiene que ser siempre autógrafa u ológrafa (puesta de puño y letra del 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, en algunos casos, los sellos. Se concluye que la firma no es un elemento esencial del documento sino que atañe a su eficacia y valor probatorio⁸⁸.

El artículo 166 del mencionado Reglamento Notarial establece la posibilidad de utilizar la huella dactilar, como rasgo biométrico identificatorio

⁸⁶ PALAZZI, Pablo Andrés. “Firma digital y comercio electrónico en Internet”. VI Congreso Iberoamericano de Derecho e Informática. Libro de Ponencias. Montevideo – Uruguay, 1998.

⁸⁷ RODRÍGUEZ Beatriz. Curso on line “Introducción al Derecho de las Tecnologías de la Información y la Comunicación”. www.viegasociados.com

⁸⁸ SIRI Julia y WONSIK María. “ El documento electrónico”, en Rev. De la Facultad de Derecho y C.S. Año XXIX y en la Rev. de la AEU, Tomo 74.

para aquellas personas que no saben o no pueden firmar, o no firman con caracteres latinos.

Dice Palazzi⁸⁹ que: *“Si se encuentra un medio que reemplace a la firma ológrafa en ambientes digitales, éste nuevo medio deberá cumplir con las funciones tradicionales de la firma. Estas son: (i) indicativa: informa acerca de la identidad de un autor; (ii) declarativa: se refiere al acuerdo respecto al contenido del acto; (iii) probatoria: permite vincular al autor con el signatario”*.

3. Firma Electrónica

De lo que venimos de ver podemos decir que “firma electrónica” en sentido amplio es “cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones de la firma manuscrita”⁹⁰.

Así es que el artículo 7 de la Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI o UNCITRAL) establece que: “Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos: a) si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; b) si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje incluido, cualquier acuerdo pertinente”. Consagrándose aquí el criterio de la “equivalencia funcional”.

La firma electrónica a su vez puede tener diferentes técnicas para firmar un documento, así tenemos las siguientes:

a) Código secreto o de ingreso: es la necesidad de una combinación determinada de números o letras, que son sólo conocidas por el dueño del

⁸⁹ PALAZZI, Pablo. “Firma digital y comercio electrónico en Internet”. Ob. Cit.

⁹⁰ MARTINEZ NADAL Apol-lonia. “Comercio electrónico, firma digital y autoridades de certificación”. Civitas, Madrid 1998.

documento, o lo que todos usamos, por ejemplo en los cajeros automáticos, es el famoso PIN o Personal Identification Number;

- b) Métodos basados en la Biometría: se realiza el acceso al documento mediante mecanismos de identificación física o biológica del usuario o dueño del documento.

3.1 La Biometría

La Biometría es la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos. La biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas. La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona por lo que es (manos, ojos, huellas digitales y voz)⁹¹.

Con relación a las diferentes técnicas utilizadas para firmar electrónicamente un documento, podemos distinguir⁹²:

- a) Una técnica disponible es el uso de una tableta sensible y un lápiz magnético conectados a un PC donde se registra la presión, velocidad y coordenadas donde el operador apoya el lápiz. Esos datos se combinan matemáticamente para formar la "firma electrónica" de la persona. Posteriormente, se puede comparar esa firma almacenada con otra para verificar si pertenecen a la misma persona⁹³.

- b) Emisión de calor: se mide la emisión de calor de un cuerpo (termograma) realizando un mapa de valores sobre la forma de cada persona.

⁹¹ BORGHELLO Cristian Fabian. "Seguridad Informática. Sus implicancias e implementación". Tesis Licenciatura en Sistemas. Universidad Tecnológica Nacional. Setiembre de 2001. Capítulo 2, página 11. www.cfsoft.com.ar

⁹² VIEGA María José. "Firma Digital". XIII Ciclo de Encuentros Técnicos Regionales". Rivera, 26 de julio de 2003. Edita Asociación de Escribanos del Uruguay.

⁹³ BALAY, Guillermo. "Enfoque informático del Decreto N° 65/998". Procedimiento administrativo electrónico. Presidencia de la República. Oficina Nacional del Servicio Civil. 1998.

c) Otra técnica de firma electrónica disponible en el mercado podría ser el registro de la huella digital y de ciertos factores biológicos de la piel que identifican unívocamente a la persona. El dispositivo consiste en un tablero donde la persona coloca su dedo. Allí se digitalizan la huella y los parámetros biológicos del dedo de la persona, de tal forma que es imposible reproducirlos salvo que se obligue a la persona a colocar su dedo en el dispositivo⁹⁴.

d) Verificación de la voz: la dicción de una (o más) frase es grabada y en el acceso se compara la voz (entonación, agudeza, etc.). Este sistema es muy sensible a factores externos como el ruido, el estado de ánimo y enfermedades de la persona, envejecimiento, etc⁹⁵.

e) Verificación de patrones oculares: estos modelos pueden ser basados en patrones del iris o de la retina y hasta el momento son los considerados más efectivos (en 200 millones de personas la probabilidad de coincidencia es casi 0). Su principal desventaja reside en la resistencia por parte de las personas a que les analicen los ojos, por revelarse en los mismos enfermedades que en ocasiones se prefiere mantener en secreto.

3.2 Sistemas de Cifrado

La ocultación o disimulación de mensajes no es un tema novedoso, ni su surgimiento se debe al desarrollo del documento electrónico. Históricamente, han existido distintas formas de cifrado, entre las que podemos destacar los cifrados por sustitución y por transposición.

a) Cifrado por sustitución

Cada letra o grupo de letras se reemplaza por otra letra o grupo de letras.

Ejemplo: cifrado de César se basa en la rotación del alfabeto N caracteres, que originariamente eran tres.

⁹⁴ BALAY, Guillermo. "Enfoque informático del Decreto N°65/998". Ob. Cit.

⁹⁵ BORGHELLO Cristian Fabian. "Seguridad Informática. Sus implicancias e implementación". Ob. Cit., Capítulo 2, página 12. www.cfbsoft.com.ar

Documentos Electrónicos Firma Digital

Texto en claro a b c d e f g z

Texto cifrado d e f g h i j k c

En el caso de sustitución monoalfabética cada letra se corresponde con otra arbitraria del alfabeto, existiendo entonces 26 claves diferentes. Se descifra fácilmente usando la frecuencia relativa de las letras.

c) Cifrado por transposición

Reordena las letras pero sin cambiarlas. Por ejemplo la transposición columnar, en la cual la clave es la palabra o frase que no contiene letras repetidas, enumerándose las columnas en el orden alfabético de las letras de la clave.

Es fácil descifrarlo conociendo la clave y ordenando las columnas.

Un ejemplo de cifrado por transposición es el siguiente⁹⁶:

```
H I P O T E C A
4 5 7 6 8 3 2 1
p o r f a v o r
t r a n s f i e
r a d e m i c u
e n t a d o s m
i l l o n e s d
e d o l a r e s
```

Texto cifrado: reumdsocissevfoierptreioranldfneaolradloasm dna

⁹⁶ DI PASCUA Diego. "Introducción a la Criptografía". Presentación a cargo del Ingeniero en el Servicio Central de Informática de la Universidad de la República.

4. Firma Digital

En el perfeccionamiento del cifrado de mensajes, llegamos a lo que se conoce como criptografía. La criptografía es la ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones.

La criptografía es una rama de las Matemáticas -y en la actualidad de la Informática y la Telemática- que hace uso de métodos y técnicas matemáticas con el objeto principal de cifrar un mensaje o archivo por medio de un algoritmo, usando una o más claves. Esto da lugar a los criptosistemas que permiten asegurar cuatro aspectos fundamentales de la seguridad informática: confidencialidad, integridad, disponibilidad y no repudio de emisor y receptor⁹⁷.

Esta consiste en un sistema de codificación de un texto con claves de carácter confidencial y procesos matemáticos complejos, de manera que para el tercero resulte incomprensible el documento si desconoce la clave decodificadora, que permite ver el documento en su forma original. De ahí es que surgen dos tipos de criptografía:

- a) de clave secreta o simétrica: las partes en los dos procesos de cifrado y descifrado comparten una clave común previamente acordada. Debe ser conocida solamente por ambas partes para evitar que un tercero ajeno a la operación pueda descifrar el mensaje transmitido. Esta tiene como desventaja que si se realiza en redes abiertas (Internet) puede ser interceptada por un tercero y además no sirve si el tercero que deba participar no tiene la clave.
- b) de clave pública o asimétrica: este sistema fue creado en 1976 en Estados Unidos y consiste en que ambas partes deben tener un par de claves que no son iguales sino que son asociadas, o sea, una clave privada en poder del titular, conocida sólo por él, y una clave pública, que se relaciona

⁹⁷ RAMÍO AGUIRRE Jorge. "Curso de Seguridad Informática". Universidad Politécnica de Madrid.

matemáticamente con la clave privada, y que puede estar tranquilo que sólo el destinatario va a poder descifrar su mensaje.

La accesibilidad a las claves pueden satisfacerse mediante la distribución manual (disquetes, CD) pero es un sistema no seguro.

La firma digital entonces, es “aquella que se crea usando un sistema de criptografía asimétrica o de clave pública”⁹⁸.

Como consecuencia del auge de las firmas digitales, ha sido necesaria la creación de una infraestructura de las claves, surgiendo así la Infraestructura de Clave Pública (ICP), más conocida por su nombre en inglés, como PKI (public key infrastructure). Por lo tanto, decimos que ésta es el conjunto de componentes y políticas necesarias para crear, gestionar y revocar certificados digitales que pueden ser utilizados para autenticar cualquier aplicación, persona, proceso u organización de una red de empresa, extranet o Internet⁹⁹.

La idea de una infraestructura de clave pública es simple, consta de varios componentes y elementos.

1. Los llamados componentes de una Infraestructura de Clave Pública, pueden ser:
 - a) Autoridad Certificante Raíz
 - b) Autoridades de Registro
 - c) Archivo
2. Los elementos de la PKI son:
 - a) Sistema de autenticación
 - b) Políticas de Certificación
 - c) Personal capacitado

⁹⁸ MARTINEZ NADAL Apol-Ionia. “Comercio electrónico, firma digital y autoridades de certificación”. Ob. Cit.

⁹⁹ RODRÍGUEZ Beatriz. “Autoridades de certificación”. XIII Ciclo de Encuentros Técnicos Regionales”. Rivera, 26 de julio de 2003. Edita Asociación de Escribanos del Uruguay.

Estos puntos se desarrollan en el próximo capítulo.

La criptografía continúa desarrollándose y actualmente se habla de que un cubo de cristal podría ser la llave criptográfica perfecta. Este cubo tendría el tamaño de un sello de correos y podría ser la llave criptográfica más segura para las operaciones económicas. Cada cubo contiene miles de pequeñas gotas de plástico que se leen con un láser especial. Cada gota de plástico tiene una forma y orientación única. Cuando el láser pasa a través de ellas, dibuja y proyecta una forma determinada en una superficie, que entonces se traduce en una llave criptográfica de 2400 bits de longitud. Si se altera la posición de las gotas la llave cambia completamente y deja de ser útil¹⁰⁰.

La encriptación de doble clave, debido a los avances en el aumento de potencia de procesamiento de los ordenadores, se convierte día a día en un sistema menos seguro. Científicos del MIT han demostrado este nuevo tipo de llave criptográfica, usando un objeto físico en lugar de una función matemática, confiando en que dicho objeto sea virtualmente imposible de duplicar. Sus desarrolladores confían en que dentro de poco podrán disminuir el tamaño de estos cubos e incluirlos como medida de seguridad dentro de las tarjetas de crédito.

En 1997 en Bonn (Alemania) se realizó una reunión de los países de la Unión Europea, elaborándose la Declaración gubernamental de Bonn sobre redes de información mundial, en la que se valoró positivamente la opción de cifrar la información transmitida vía redes usando sistemas criptográficos de acuerdo con las leyes vigentes, considerándose a la criptografía “de carácter fuerte”, aludiendo con esta expresión a claves compuestas por números de cifrados amplios, como un requisito imprescindible para el desarrollo de la Sociedad de la Información y el Comercio Electrónico¹⁰¹.

¹⁰⁰ <http://enlaceweb.net/mailman/listinfo.cgi/interlink>

¹⁰¹ JIJENA LEIVA Renato y otros. “El Derecho y la Sociedad de la información: la Importancia de Internet en el Mundo Actual”. TEC de Monterrey. México, 2003. Página 195. www.echo.lu/bonn/conference.html

CAPITULO VII

AUTORIDADES DE CERTIFICACION

1. Introducción

La Firma Digital y la fiabilidad de las transacciones on line, más allá del acceso a la información, los servicios al usuario final y la integración de Internet en los procesos de negocios de una compañía, necesitan más que nunca de un grado de confianza en el medio.

Sólo cuando ese grado de confianza se alcanza y se mantiene, podrá disminuirse ese gran inhibidor de desarrollo digital que es la sensación de inseguridad. El enorme desarrollo de las transacciones en la red de redes implica necesariamente abordar el tema de la seguridad, tanto desde el punto de vista técnico como jurídico.

La seguridad en Internet consiste básicamente en implementar los mecanismos necesarios para que se realice una operación a través de un medio electrónico, se asegure la integridad del contenido y se autentifique al remitente y al receptor, como hemos visto en los temas anteriores.

Para dar esa seguridad se necesita la existencia de una infraestructura que sea simple, pero que aporte a todos aquellos que la utilizan esa tranquilidad de saber quién es ese tercero que se presenta ante ellos.

La Infraestructura de Clave Pública (ICP), más conocida por su nombre en inglés, como PKI (public key infrastructure) es: “el conjunto de componentes y políticas necesarias para crear, gestionar y revocar certificados digitales que pueden ser utilizados para autenticar cualquier aplicación, persona, proceso u organización de una red de empresa, extranet o Internet”¹⁰².

¹⁰² RODRÍGUEZ Beatriz. XIII Ciclo de Encuentros Técnicos Regionales. Rivera, Julio 2003. Asociación de Escribanos del Uruguay. Páginas 26 y 27.

La idea de una infraestructura de clave pública es simple, consta de varios componentes y elementos que estudiaremos a continuación.

2. Componentes de una Infraestructura de Clave Pública

Los llamados componentes de una Infraestructura de Clave Pública, como mencionamos en el capítulo anterior, son¹⁰³:

- a) Autoridad Certificante Raíz
- b) Autoridades de Registro
- c) Archivo

2.1 Autoridad Certificante Raíz (AC) o Certificate Authority (CA)

Esta es el pilar básico del edificio de la PKI. Es una colección de hardware de computación, software, y personas que los manejan, quienes operan el sistema. La Autoridad Certificante (CA o AC) es conocida por dos atributos: su nombre y su clave pública.

Según se ha destacado por Apol-lonia MARINEZ NADAL, "tercera parte de confianza ("Trusted Third Party" o TTP) es cualquier entidad de confianza de las partes intervinientes en una transacción para proporcionar servicios de seguridad; aquella específica tercera parte de confianza que desempeña de forma fundamental la función de emisión de certificados se conoce, entre otras expresiones, como autoridad de certificación, entidad de certificación, proveedor o prestador de servicios de certificación o simplemente certificador. Como un juego de claves usado para crear una firma digital no tiene una asociación intrínseca con nadie, la solución es que una o más terceras partes, de confianza para las dos primeras partes, certifiquen la persona realmente

¹⁰³ HOUSLEY Russ y POLK Tim. "Planning for PKI. Best Practices Guide for Deploying Public Key Infrastructure". John Wiley & Sons, Inc. USA, 2001. Página 43.

asociada con un par de claves. La criptografía necesita pues, de una tercera parte de confianza: una entidad de certificación que debe realizar tal asociación vinculando una persona debidamente identificada con un par de claves determinado... Por ello, para asociar un par de claves con un potencial firmante, una entidad de certificación emite un certificado, un registro o documento electrónico que liga una clave pública con el sujeto del certificado, y confirma que el potencial firmante identificado en el certificado tiene la correspondiente clave privada"¹⁰⁴.

En la AC se llevan a cabo cuatro funciones básicas de la Infraestructura de Clave Pública¹⁰⁵:

- 1) Emisión de certificados (los crea y los firma).
- 2) Información sobre la vigencia de los certificados y emisión de las listas de revocación.
- 3) Publicación de los certificados no vigentes y de las listas de revocación, para que el usuario obtenga la información necesaria para implementar su sistema de seguridad.
- 4) Mantiene un archivo con la información actualizada sobre la validez o revocación de los certificados que ella emitió.

2.1.1 Emisión de Certificados

La primera función que realiza una ICP o PKI es establecer un sistema de autenticación. Esto significa que los usuarios puedan ser identificados antes de recibir los derechos de transmisión en la red, y eso se realiza certificando la identidad de las personas mediante los llamados certificados digitales.

¹⁰⁴ DELPIAZZO, Carlos. "Lecciones de Derecho Telemático". Fundación de Cultura Universitaria. Montevideo, abril 2004. Página 85.

¹⁰⁵ RODRÍGUEZ Beatriz. Curso on line "Introducción al Derecho de las Tecnologías de la Información y Comunicación". www.viegasociados.com

Documentos Electrónicos Firma Digital

Estos certificados son archivos electrónicos que tienen un tamaño determinado, y contienen los datos de identificación del emisor, la clave pública del emisor del mensaje y la firma privada del propio Prestador de Servicios de Certificación o AC.

Actualmente por el Decreto 382/003 en el artículo 2 literal c, se define lo que es un certificado digital, como aquel documento digital firmado digitalmente por un Prestador de servicios de certificación, que vincula la identidad del titular del mismo con una clave pública y su correspondiente clave privada.

Una AC puede emitir certificados a los particulares, personas físicas o jurídicas, a otra AC o a ambos. Cuando una AC emite un certificado, está acreditando que la persona o la organización poseedora de la clave privada, que se corresponde con una determinada clave pública, es la misma que contiene el certificado.

Si incluye información adicional en el certificado, la AC está aseverando que la información correspondiente a esa persona u organización es correcta. Esa información adicional es por ejemplo su correo electrónico, en que lugar se lo puede contactar, o también puede ser información sobre la clase de aplicaciones que puede llevarse a cabo con la clave pública, o hasta qué monto puede el usuario actuar con ese certificado. Cuando el sujeto del certificado es otra AC, la emisión certifica que ese certificado emitido por otra AC es viable, o sea es de confianza.

Dijimos anteriormente que los atributos de la AC era la clave pública y el nombre, generalmente es una información pública y la firma es la base de confianza del certificado. Por ejemplo: si un tercero, ajeno a la relación entre el emisor y el solicitante, obtiene la clave privada de la AC, los usuarios confiarán en los certificados que genere el tercero como si fuera la AC que los generara. Esta es la primera y principal responsabilidad de una Autoridad de Certificación, proteger su clave privada de la revelación.

Para proteger la clave privada, la Autoridad Certificante debe proteger ésta cuando está en uso y cuando está archivada. Para cumplir con este

Documentos Electrónicos Firma Digital

requerimiento la AC debe recurrir a la criptografía. La criptografía genera claves, protege las claves privadas e implementa los algoritmos criptográficos.

La clave privada de la AC está en riesgo cuando queda guardada en la memoria de una máquina de un tercero o en un sistema inválido de criptografía.

El contenido de los certificados debe ser correcto para el uso. La información que contiene el mismo, como por ejemplo la clave pública, los contactos, deben corresponder al sujeto identificado en dicho certificado.

La segunda responsabilidad de un Prestador de Servicios de Certificación es verificar la información en el certificado antes de ser emitido, como por ejemplo comprobando la identidad del usuario y su información personal, esto es diferente a amparar la clave privada de la AC.

La AC puede verificar alguno de los contenidos de los certificados basados en mecanismos técnicos, por ejemplo la Autoridad de Certificación puede usar el mecanismo de la firma digital para garantizar que el usuario que actualmente tiene la clave privada se corresponde con la clave pública en el certificado. Este proceso de verificación se llama frecuentemente, “prueba de posesión”, esta prueba puede ser archivada para examinar mejor los datos externos.

La tercera responsabilidad del la AC es garantizar que todos los certificados y las listas de revocación de los certificados emitidos confirman sus características.

Con respecto a los certificados otorgados por las AC tenemos de varios tipos:

- a) **De usuarios.** Existen dos tipos diferentes, siendo el más simple de ellos aquel que certifica solamente la dirección de correo electrónico del propietario, el cual tiene además un nivel bajo con respecto a la seguridad, pudiendo ser gestionados por cualquier persona, mediante correo electrónico o por Internet a través de una página web. En segundo lugar

tenemos certificados que poseen alta seguridad, los cuales deben ser solicitados por el interesado en la AC.

- b) **Certificados Empresa:** son emitidos para personas que van a representar a una Empresa, se verifica la identidad de la persona y de la empresa y documentación que habilite a actuar en representación de la misma¹⁰⁶.
- c) **De servidores:** “Estos certificados permiten la habilitación del protocolo SSL (https://) para el acceso seguro a la información publicada, dando garantías a los clientes de estar accediendo al servidor correcto. En este caso se verifica con la autoridad responsable correspondiente que el nombre de dominio solicitado corresponda a la empresa solicitante y se verifica la identidad del servidor¹⁰⁷.”

2.1.2 Mantenimiento de la información y emisión de listas de revocación de certificados (CRL)

Así como en los certificados, el contenido de las listas de revocación debe ser correcto para su uso. La información contenida en los CRL (lista de revocación) debe ser completa y correcta, por ejemplo: la fecha en que fueron revocados, la razón por la que fue revocado, etc.

Los errores de omisión podrían causar que el usuario aceptara un certificado no válido, o una revocación incorrecta. La cuarta responsabilidad de la AC es el mantenimiento fiel de la lista de certificados y que ésta sea confiable.

2.1.3 Publicación de los certificados no vigentes y de las listas de revocación

¹⁰⁶ VIEGA, María José. “La firma digital y la autoridad certificante en Uruguay”. Ponencia presentada al VII Congreso Iberoamericano de Derecho e Informática. Perú, abril 2000.

¹⁰⁷ Página de la Administración Nacional de Correo publicada en Internet: www.correo.com.uy Página visitada marzo 2000.

La publicación de certificados no vigentes y las listas de revocación son generadas por las AC y deben ser válidas para los usuarios. Si estos no pueden obtener esta información, la Autoridad de Certificación no cumpliría con el servicio de seguridad, función ésta de importancia relevante.

La quinta responsabilidad de una AC es dar publicidad de los certificados vigentes y de los revocados.

2.1.4 Mantenimiento de Archivos

La AC necesita el mantenimiento de la información de la identidad del firmante de un documento viejo basado en un certificado expirado. El archivo debe identificar la persona actual u organización actual identificado en el mismo, estableciendo que ellos lo solicitaron y mostrando que era válido al momento de firmarse dicho documento.

La sexta responsabilidad de la AC es el mantenimiento de suficiente información archivada para establecer la validez del certificado después de haber expirado.

Por lo que tenemos entonces, que la AC tiene como principales responsabilidades:

- a) proteger su clave privada de la revelación
- b) verificar la información en el certificado antes de ser emitido
- c) asegurar que los certificados y las listas son acordes a los perfiles de los usuarios
- d) mantener la lista de certificados actualizada para que sea confiable
- e) distribuir los certificados y las listas de revocación

- f) mantener suficiente información archivada para establecer la validez del certificado después de haber expirado

2.2 Autoridad de Registro (AR) o Registration Authority (RA)

Cuando hablamos del edificio de la PKI mencionamos que el segundo nivel lo ocupaban las Autoridades de Registro, cuando estaban separadas de las Autoridades de Certificación.

La Autoridad de Registro es designada para verificar el contenido de los certificados de la AC. Los mismos contienen información presentada por la entidad solicitante del certificado, semejante a una licencia de conducir. Ellos deben reflejar también la información dada por terceros. Por ejemplo: el límite de crédito asignado a la tarjeta, refleja información obtenida de la oficina de la tarjeta de crédito, y un certificado reflejaría datos desde la AC, un certificado de Juan podría indicar que él tiene una firma digital autorizada para pequeños contratos. La AR generalmente provee a la AC.

Como la AC, la AR es una colección de hardware, software y las personas que la operan. A diferencia de una AC una persona individualmente puede operar una AR. Cada AC mantiene una lista de las AR que existen, son AR determinadas por la confianza.

Cada AR es reconocida por una AC por su nombre y por la clave pública al igual que la AC, para verificar la firma de un AR en un mensaje, la AC puede estar segura que una AR es tal por su información. Y puede confiar. Asimismo es importante que la AR provea adecuada protección a su clave privada. Para eso utilizan criptografía en su hardware y software. A su vez como habíamos mencionado antes se pueden confundir ambas autoridades en una sola, ser a su vez AC y AR¹⁰⁸.

¹⁰⁸ HOUSLEY Russ y POLK Tim. "Planning for PKI. Best Practices Guide for Deploying Public Key Infrastructure". Ob. Cit., página 48.

2.3 Archivo

El archivo es parte integrante de la AC ya que en él se incluyen todas las funciones de archivo, mantenimiento y publicación de la información.

En el archivo se debe mantener actualizada y publicada las listas de revocación.

3. Los elementos de la PKI

Los elementos de la Infraestructura de Clave Pública son los siguientes:

- a) Sistema de autenticación
- b) Políticas de Certificación
- c) Personal capacitado

3.1 Sistema de autenticación

El sistema de autenticación es el primer elemento de la infraestructura de clave pública. Este consiste en un proceso por el cual los usuarios puedan ser identificados antes de recibir los derechos de red.

Si bien los registros basados en palabras secretas o contraseñas son un método muy extendido, son mucho más seguros los certificados digitales, debido a que contienen información específica sobre el usuario que permite su identificación.

Quien va a verificar la autenticidad de los certificados es la autoridad de certificación, como entidad que firma y publica ese certificado.

La autoridad de registro es la responsable de verificar la identidad de los poseedores de certificados. Este es un proceso diferente de la certificación en si, y puede suceder antes o después de que la autoridad de certificación genere un certificado¹⁰⁹.

3.2 Políticas de Certificación

El segundo elemento de la PKI, luego del sistema de autenticación que hemos visto anteriormente, son las políticas de certificación; estas son las que establecen las reglas de su uso y los servicios de certificados. Estas reglas deben prever todo tipo de situaciones como por ejemplo qué sucede cuando un usuario sin querer comparte su clave privada con otra persona.

Estas normas son de mucha importancia dentro de una PKI y se ha hecho una declaración de políticas de certificación que se usan como modelo, adaptándolas a cada Estado con el asesoramiento jurídico y del personal capacitado en las tecnologías de la información.

Ellas proporcionan una explicación detallada de cómo la AC ha de gestionar los certificados que edita y otros servicios anexos como la gestión de las claves.

Muchas veces estas políticas de certificación actúan como un contrato entre la AC y los usuarios, describiendo las obligaciones y limitaciones legales, estableciendo los principios también para futuras auditorías o verificaciones.

3.3 Personal Capacitado

¹⁰⁹ <http://www.idg.es> . Página visitada el 22 de mayo de 2003.

El tercer elemento que integra la infraestructura de clave pública es el personal capacitado para crear, administrar y gestionar una PKI.

Es obvio que dentro de ese personal capacitado necesitaremos una persona que sea la encargada de la seguridad, así como de establecer y administrar las políticas de seguridad, siendo necesario también que comprenda muy bien todo lo que se refiere a las cuestiones que están en juego.

Se va a necesitar un administrador que actúe como autoridad de registro, aunque es posible establecer una autoridad de registro automatizada para tratar las peticiones de los usuarios realizadas a través de sus navegadores web.

4. Obtención de un Certificado Digital

El sistema de certificados de clave pública supone la participación de los siguientes sujetos¹¹⁰:

- a) la entidad de certificación;
- b) el titular del certificado; y
- c) el usuario o persona que confía en el certificado.

El Dr. Delpiazzo define a los sujetos antes mencionados de la siguiente forma:

El proveedor del servicios de certificación, es una institución dedicada a proveer servicios de certificación mediante la emisión de certificados firmados digitalmente por dicha autoridad, usando una clave privada de firma.

En cuanto al titular del certificado, también llamado sujeto o suscriptor, es la persona incluida en el certificado, que tiene legítimamente la clave privada correspondiente a la clave pública que contiene el certificado.

¹¹⁰ DELPIAZZO, Carlos. "Lecciones de Derecho Telemático". Ob. Cit., página 86.

Documentos Electrónicos Firma Digital

El usuario del certificado es la persona que obtiene la clave pública del suscriptor a través del certificado y que actúa basándose en él y en la clave pública que contiene.

Hemos visto hasta ahora la infraestructura de clave pública, sus obligaciones, los sujetos que interactúan, analizando a continuación qué debemos hacer para obtener un certificado digital y cómo usarlo.

La firma digital se genera mediante la utilización de un par de claves de cifrado (pública y privada), que se utilizan para cifrar y descifrar el mensaje que enviamos.

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

El proceso de obtención de un certificado es el siguiente:

Cualquier persona puede dirigirse, personalmente, a una AC que cuente con los dispositivos necesarios para generar el par de claves y solicitar la creación de éstas, o enviar una petición a la Autoridad de Registro designada, que verifica su identidad y encarga a la AC la expedición del certificado.

Este certificado es un documento digital que generalmente, se almacena y administra en un directorio central, por ejemplo: si Juan está en su computador en su casa el certificado se almacena en su sistema; en otros casos se transmite automáticamente cuando es necesaria su utilización, sin interrumpir el trabajo del usuario.

Asimismo la autoridad verifica la autenticidad del certificado cuando lo necesita un tercero, hecho que se realiza de forma transparente, ya que en su realización debe utilizarse un máximo nivel de seguridad.

Los certificados se editan con una fecha de expiración, casi siempre un año, algunas veces deben ser revocados inmediatamente, como por ejemplo cuando un empleado abandona la empresa o cuando se conoce la clave privada del usuario. Para ello la autoridad mantiene actualizada la lista de revocación de certificados, de la cual ya habíamos hablado anteriormente, la cual puede ser consultada por los usuarios mediante correo electrónico o por la web, para asegurarse la validez del certificado.

La autoridad de registro es responsable de verificar la identidad de quien posee el certificado. Este es un proceso diferente de la certificación en sí, y puede ser antes o después de que se genere el certificado por la AC.

5. Actualidad

En Uruguay existen en éste momento cuatro Autoridades Certificantes que se basan en lo establecido por la Ley N° 17243 de 29 de junio del año 2000, más conocida como la Segunda Ley de Urgencias, artículo 25 inciso 2, las cuales funcionan en régimen de libre competencia.

Estas son: El Correo (es la actual prestadora de estos servicios a nivel público y consta con la aprobación de la Comisión Nacional de Informática (CONADI), Abitab, la Cámara Nacional de Comercio, y la Asociación de Escribanos del Uruguay.

Estas cuatro empresas expiden certificados digitales como los mencionados anteriormente: para usuarios personas físicas y jurídicas, para servidores y páginas web.

Respecto a El Correo a través de la “Recomendación de la Comisión Nacional de Informática de fecha 25 de setiembre de 1998”: se autoriza a la Administración Nacional de Correos a prestar servicios de Autoridad de Certificación en todo el país¹¹¹.

¹¹¹ VIEGA, María José. “La firma digital y la autoridad certificante en Uruguay”. Ponencia presentada al VII Congreso Iberoamericano de Derecho e Informática. Perú, abril 2000.

Documentos Electrónicos Firma Digital

La Administración Nacional de Correos establece que¹¹²: “La importancia de una Autoridad de Certificación en el contexto de las comunicaciones globales está dada no solamente por su confidencialidad y respeto nacional, sino también por su reconocimiento internacional. A este respecto corresponde destacar que la Administración Nacional de Correos integra la Unión Postal Universal (UPU) y la Unión Postal para las Américas, España y Portugal (UPAEP), organismos internacionales que tienden al incremento mundial de las comunicaciones postales. Los correos más importantes del mundo se han posicionado ya como Autoridad de Certificación Nacional en sus respectivos países, lo que constituye una verdadera Red Internacional con sólido respaldo y trayectoria.”

En lo que refiere al derecho positivo uruguayo, la norma anterior y el Decreto Nº 382/003, del Poder Ejecutivo de fecha 17 de setiembre de 2003, que reglamenta el uso de la firma digital, son las únicas normas que se refieren a las autoridades certificadoras, o prestadores de servicios.

¹¹² Página de la Administración Nacional de Correo publicada en Internet: www.correo.com.uy
Página visitada marzo de 2000.

CAPITULO VIII

EL NOTARIADO FRENTE A LAS NUEVAS TECNOLOGIAS

1. Introducción

Cuando pensamos en los notarios frente a las nuevas tecnologías, encontramos una gran cantidad de posibilidades de cambios, algunos fácilmente realizables, otros que implican un adecuación del derecho vigente y una reestructura en los procesos¹¹³.

Históricamente, la función del Notario está signada por la seguridad jurídica que proporciona a la sociedad. Y como es lógico la principal preocupación que nos despierta la tecnología es la seguridad. Esta seguridad podemos enfocarla desde un punto de vista informático o telemático y desde un punto de vista jurídico, como vimos anteriormente. La pregunta entonces es, si ante estos nuevos medios, el Escribano puede continuar cumpliendo su función, si esa función mantiene su vigencia o si por el contrario es necesario una nueva forma de otorgar seguridad a los negocios jurídicos.

Pero este planteo acerca de la seguridad no es consecuencia de las nuevas tecnologías de la información, de la telemática o de Internet, ésta es una problemática histórica.

Una anécdota que nos ilustra esta afirmación data del año 1914, en que la Alta Corte de Justicia dictó la Acordada N° 403, el 6 de noviembre de ese año, preocupados por la utilización de la máquina de escribir en los Protocolos Notariales, prohibiendo su uso para las matrices de las escrituras públicas y permitiendo la utilización de la misma únicamente para expedir las primeras copias¹¹⁴.

¹¹³ VIEGA, María José. "El Notariado ante las Nuevas Tecnologías". Trabajo presentado ante el Comité Notarial del MERCOSUR, Buenos Aires, Junio de 2003.

¹¹⁴ Libro de Acuerdos de la Suprema Corte de Justicia N° 1. Fs. 309 a 311.

Los argumentos utilizados por la Corte en ese momento fueron los siguientes¹¹⁵:

1º. Se adolecía de falta de uniformidad en las tintas y de la posibilidad de detectar inalterabilidad en las escrituras, que era posible en las escrituras a mano (Decreto 31/12/1858). Y esto era verdad, ya que la tinta azul-negro “de buena calidad” que se utilizaba en esa época comenzaba siendo de un tinte azul, pero cambiaba su color a negro con el transcurso del tiempo, de forma tal que era fácilmente detectable la realización de interlineados, por ejemplo.

Pero posteriormente surgió toda una técnica pericial a los efectos de detectar con que máquina se había escrito un determinado documento.

2º. Que contravenía lo dispuesto por la ley 28/06/1958 artículo 1, que establecía que los Protocolos deben formarse en cuadernillos enteros de 5 pliegos cada uno (la primera foja ligada con la 10º). La máquina requiere hojas sueltas o que se conserven en pliegos separados, lo que resulta fácil de perder y de cometer error en los pliegos.

3º. Que el artículo 34 de la Ley de Timbres y Papel Sellado autorizaba el uso de la máquina de escribir, pero sólo se refería a las copias de las escrituras públicas.

Como podemos apreciar, en el fondo son las mismas dudas de otras épocas, disfrazadas por las nuevas y “sofisticadas” herramientas, las que hoy se nos plantean.

Aunque parezcan pequeños los cambios que se han realizado en el Notariado, ya existen en relación a las tecnologías. Desde la incorporación de fotografías al Registro de Protocolizaciones, o ser depositarios de grabaciones y/o videos a través de actas notariales, también la técnica a sufrido cambios relativo a la utilización de la máquina de escribir (pliegos móviles) y también a

¹¹⁵ VIEGA, María José. “El Notariado en tiempos de Internet”. Derecho Informático. Tomo IV (Correspondiente al año 2003). Fundación de Cultura Universitaria. Montevideo, mayo 2004. Página 147.

raíz de la utilización de la computadora (comenzando cada escritura en una hoja nueva, quedando sin efecto el pasaje de foja).

2. La Función Notarial

Vamos a partir del análisis de la función notarial, para poder establecer si la función cumplida tradicionalmente en soporte papel, puede ser trasladada al mundo virtual y en que condiciones.

El artículo 1 del Decreto ley 1421 que el: *“Escribano Público es la persona habilitada por autoridad competente para redactar, extender y autorizar bajo su fe y firma, todos los actos y contratos que deben celebrarse con su intervención entre los particulares o entre éstos y toda clase de personas jurídicas”*.

El Escribano Bardallo ha definido la función del notario como la función pública, de ejercicio privado, que tiene por objeto dar forma jurídica y autenticidad a los negocios y demás actos jurídicos con fines de permanencia, validez y eficacia¹¹⁶.

Veamos entonces, como es y como podrá ser el quehacer del Escribano apoyado en estas nuevas herramientas tecnológicas. El contenido de la función notarial supone¹¹⁷:

- El autoexamen del Escribano en cuanto a su competencia y a la ausencia de limitaciones legales o deontológicas para su actuación en el caso planteado;
- Asesorar a los interesados para que, con pleno conocimiento de la situación, puedan decidir libremente;
- Analizar el caso y verificar su legalidad;

¹¹⁶ BARDALLO Julio Conf. “El Escribano, autor de la Forma Auténtica”, en Cuaderno de la Facultad de Derecho y Ciencias Sociales N°10.

¹¹⁷ SIRI, Julia. “El Notariado en la Era de la Tecnología”. Fundación de Cultura Universitaria. Montevideo, febrero 2001. Página 28.

- Confirmar la capacidad de los contrayentes;
- Estudiar la legitimación –en cuanto al nexo del sujeto con el objeto de la transacción y en cuanto a las representaciones invocadas- es decir, la aptitud de la persona para incidir en la situación jurídica de que se trate;
- Conformar la voluntad de los eventuales otorgantes, mediando imparcialmente en la negociación;
- Controlar los aspectos fiscales concernientes;
- Documentar públicamente la voluntad expresada;
- Velar por la ausencia de vicios del consentimiento y el cumplimiento estricto de las formalidades requeridas, incluidas las formas de publicidad necesarias o convenientes

2.1 La Fe Pública

El concepto de fe pública, según Couture, se asocia a la función notarial de manera más directa que a cualquier otra actividad humana. El escribano “da fe” de cuanto ha percibido y el Derecho “hace fe” de todo lo que él asegura haber percibido¹¹⁸.

La fe notarial es una especie dentro del género de la fe pública, con características especiales referente a la persona que ejerce dicha función, ya que es un profesional jurídico privado y que la ejerce en el campo extrajudicial, o más bien, no contencioso¹¹⁹.

Como señala el Escribano Pérez Montero la diferencia entre la fe notarial y otras, es que en éstas, el poder fedante lo tiene el órgano y no el funcionario

¹¹⁸ COUTURE, Eduardo J. “Introducción al Estudio del Derecho Notarial. Publicaciones Oficiales del Facultad de Derecho y Ciencias Sociales de Montevideo. Montevideo, 1954.

¹¹⁹ PEREZ MONTERO, Hugo. “Eficacia judicial y extrajudicial del documento notarial”. X Jornada Notarial Iberoamericana. Valencia, octubre de 2002. Página 13.

que certifica, por tanto, la responsabilidad recae sobre el Estado u órgano público al que pertenece el funcionario involucrado en el documento autorizado. En cambio, la fe notarial es personal y directa y la tiene el notario por mandato de la ley. La responsabilidad es personal, directa e ilimitada a cargo del agente de la función notarial.¹²⁰

GIRALT FONT también hace hincapié en la doble connotación que posee la fe pública, por un lado la potestad legal atribuida a ciertos funcionarios y también se refiere a “la calidad jurídica que el ejercicio de la dación de fe incorpora al documento que contiene la actuación del agente”¹²¹.

Y como decíamos anteriormente, el mayor desafío está dado por el hecho de que la función notarial referida a la fe pública está basada en los documentos, cuyo soporte es el papel. Por tanto nos enfrentamos aquí a la más importante transformación, ya que la migración del documento escrito al informático constituye el mayor desafío.

El pasaje de un soporte material a un soporte virtual, tal como se produce en los casos de la contratación telemática, debe realizarse manteniendo los fines de permanencia, validez y eficacia propios del ejercicio notarial. Entran aquí a tallar los aspectos relativos a la seguridad que va a poseer el documento electrónico y a la forma de suscribirlos.

2.2 El Deber de Consejo

Este deber, si bien en si mismo no parece verse afectado por las nuevas tecnologías en cuanto a su ejercicio, entendemos que cobra relevancia en la medida en que los contratos se vuelven complejos.

¹²⁰ PEREZ MONTERO, Hugo. “Eficacia judicial y extrajudicial del documento notarial”. Ob. Cit., página 13.

¹²¹ GIRALT FONT Jaime. “Fe”. Ponencia presentada a la VI Jornada Notarial Iberoamericana. Quito, Ecuador, 25 al 29 de octubre de 1993. Tema IV Función del Notario. Página 13.

Y la complejidad tiene un doble aspecto, por un lado cuando se trata de contratos informáticos la misma se está referido a los sistemas informáticos como objeto de los mismos. Pero desde la óptica de la celebración de los negocios, la falta de presencialidad de las partes frente al Escribano, las distancias geográficas existentes entre las mismas, más allá de los cambios desde el punto de vista documental, cambian la forma de negociar, tornándose más impersonal.

El asesoramiento profesional, aún en la contratación privada, teniendo conocimiento de las connotaciones de determinadas cláusulas en los contratos de adhesión, que podamos realizar a través de sitios web, es fundamental para los consumidores. Pero también lo será para las empresas que poseen portales a través de los cuales ofrecen sus productos o servicios.

Puede ser también asesor jurídico en procesos de informatización, nadie mejor que es escribano para analizar los problemas jurídicos.

2.3 Control de Legalidad

El control de legalidad que realizan los escribanos de los negocios a realizarse es una labor preventiva, ya que permite detectar problemas que puedan afectar la validez del mismo.

“También en este entorno, la actividad del notario se ve potencializada en la transacción informática a distancia, porque ésta abre la posibilidad de su celebración con cualquier persona y su culminación en cualquier parte del mundo. Esta circunstancia exige un amplio conocimiento del Derecho que, de acuerdo al caso, resulte aplicable, a fin de prevenir su conculcación y evitar la anulación o nulidad del acuerdo”¹²².

¹²² SIRI GARCIA, Julia. “La incidencia del documento electrónico en el Derecho Notarial, ¿atenta o no contra sus principios?. VI Congreso Notarial del MERCOSUR. Cochabamba, 28 a 30 de setiembre de 2000. Tema 3. Página 46.

2.4 Control de Legitimación

El Notario realiza en los actos que autoriza el control de legitimidad del sujeto y su vinculación con el objeto de la transacción. Es un punto a destacar aquí la legitimidad en el caso de las personas jurídicas, el análisis de la representación, los alcances de las potestades atribuidas para un determinado otorgamiento y la vigencia de las mismas¹²³.

Es relevante también determinar quién se está obligando, quién es el sujeto de la relación jurídica. Este punto es trascendente en los contratos marcos en los cuales las relaciones telemáticas se realizan en forma automática, no perdiendo de vista que en última instancia la comunicación siempre se produce entre máquinas.

2.5 Autenticidad

“La autenticidad, tomada en su doble aspecto de autoría cierta y de fidelidad de la representación del acto, incluida su data correspondiente, tradicionalmente queda asegurada por la actuación notarial que registra en instrumento público la presencia, otorgamiento y suscripción que ante él se llevan a cabo, todo lo cual se refleja en papel”¹²⁴.

La necesidad de un tercero imparcial en la contratación tradicional, que se produce en un mismo ámbito espacial, signada por la materialidad del documento y la presencia de las partes, hace pensar que en el ámbito telemático, será aún más importante esta presencia.

¹²³ VIEGA María José. “La función notarial frente a la contratación electrónica”. Ponencia presentada al X Congreso Iberoamericano de Derecho e Informática. Chile, 6 al 9 de setiembre de 2004.

¹²⁴ SIRI GARCIA, Julia. “El Notariado en la Era de la Tecnología”. Ob. Cit, página 78.

Ejemplos de esta necesidad lo constituye el Cyber Notary, en Estados Unidos, concibiéndolo con una función notarial tal cual la concibe el Sistema de Notariado Latino. Otra manifestación de la necesidad de un tercero que de fe pública es el Fedatario Juramentado en Perú.

A este respecto manifiesta el Escribano De la Fuente: "Fundamentalmente - y este punto es el más interesante-, no existe en el negocio un tercero imparcial que dé certeza, forma y veracidad al negocio jurídico y a sus otorgantes, autenticando además todo lo que es la negociación. Aunque parezca mentira, hasta hoy ese ha sido el escollo más importante y es lo que ha trabado la contratación por vía telemática. Los otros puntos son muy interesantes y pueden resultar curiosos desde el punto de vista técnico: cómo se forma una firma digital, cómo se forma la clave pública, la clave privada, la dirección electrónica, los servidores, etc. Como decía, la traba más grande que ha tenido la contratación electrónica es que le ha sido muy difícil encontrar un tercero imparcial que dé confianza a las partes que están interviniendo en el negocio.- Es decir que, por un lado, tenemos cosas que pueden ser - y no quiero restar importancia a la tecnología de avanzada- resueltas aplicando tecnología de avanzada, pero la intervención de ese tercero imparcial, del Notario o del Escribano en ese negocio jurídico, y el "plus" que está agregando la actuación notarial al negocio jurídico, desde ya adelanto que no va a haber tecnología que pueda superarla.¹²⁵"

Pero, también están aquellos que entienden que las llamadas Autoridad de Certificación o Autoridades Certificantes emisoras de las claves que constituyen la firma digital, pueden estar en condiciones de suplir las funciones del Escribano.

2.6 Confidencialidad

¹²⁵ DE LA FUENTE Juan Angel. "La contratación electrónica y la intervención notarial". Ciclo de Conferencias. Instituto de Investigación y Técnica Notarial. 15 de octubre de 1998. Asociación de Escribanos del Uruguay, 1999. Página 3.

La confidencialidad de la información está solucionada a nivel informático por los procesos de encriptado y descencriptado, contando con determinadas prohibiciones en algunos países. A nivel Notarial rige el Secreto Profesional para la información comunicada al Escribano. En este ámbito es conveniente analizar las connotaciones de utilizar o no una red cerrada en la operativa de transmisión de documentación entre los Registros Públicos y los Notarios¹²⁶.

2.7 Registro y Conservación

Los fines a que apuntan los registros son¹²⁷:

a) conservación: asegura la *identidad* del documento (imposibilidad de sustitución), su *permanencia* (por todo el tiempo que el soporte papel y los ingredientes empleados para su grafía permitan) y su *inalterabilidad* (ya que por el régimen de custodia y archivo a que están sometidos los registros, es muy improbable su modificación);

b) reproducción: las matrices se retienen por el notario y para el tráfico jurídico se expiden traslados de ellas, con igual valor que los originales;

c) cotejo: mediante la comparación entre la matriz y su traslado, es posible, en caso de duda, determinar la fidelidad del contexto de éste;

d) fecha cierta: por aquellos documentos que por sí mismo no la tuvieran y cuya incorporación al Registro de Protocolizaciones se le confiere desde ese momento. En lenguaje informático, es el *time stamping* –sólo que con valor jurídico reconocido-.

¹²⁶ VIEGA María José. “La función notarial frente a la contratación electrónica”. Ob. Cit.

¹²⁷ SIRI GARCIA, Julia. “El Notariado en la Era de la Tecnología”. Ob. Cit, página 80.

2.8 Policía Jurídica

Vigilancia del cumplimiento de las formalidades. Equilibrio entre los contrayentes, principios de libertad, igualdad y seguridad.

Esto está vinculado a la desigualdad de las partes en los contratos informáticos, al desequilibrio entre el proveedor y el usuario, donde el deber de informar del proveedor es sumamente relevante.

2.9 Control Tributario

El Escribano puede perfectamente realizar los contralores tributarios en el comercio electrónico.

2.10 Internacionalización del Notariado

La eliminación de las fronteras en cuanto a la contratación se debe a las comunicaciones y contrataciones en simultáneo que nos permite Internet, con personas distantes geográficamente, por un lado, y a la negociación de bienes virtuales por otro, lleva a cuestionarnos cuales serán los límites de la función notarial.

Vinculado a este tema, la Esc. Julia Siri se ha preguntado en relación al proyecto Ciber-Notario, existente en Estados Unidos, si “el ámbito de competencia: ¿se limitarán a autenticar las transacciones internacionales a su llegada o a su salida de Estados Unidos o, con esa vocación expansiva propia de su idiosincrasia, esos profesionales serán los únicos habilitados para actuar

en sede de transacciones electrónicas internacionales, desplazando así a los demás notarios del Mundo?”¹²⁸.

El proyecto ciber-notario consiste en la preparación de abogados, a los cuales se los forma en el área de las nuevas tecnologías y con conocimientos de un notario de tipo latino. Un ejemplo similar es el caso del Fedatario Juramentado en Perú.

La fe pública constituye un monopolio inherente a la soberanía del Estado y éste la ejerce, por delegación, mediante la actuación de determinados funcionarios y oficiales públicos, a quienes inviste de la potestad fideifaciente respecto de los documentos que autorizan (instrumentos públicos)¹²⁹.

La función notarial una función pública ejercida por delegación del Estado, entendiéndose por tanto que la misma debe ser ejercida dentro de las fronteras del país en el cual el Escribano fue investido.

Tal como lo ha estimado el Parlamento Europeo (Resolución del 18 de enero de 1994), que el Notariado queda exceptuado de las disposiciones relativas al libre establecimiento y a la libre prestación de servicios. Antes de la Declaración de Madrid (23 de marzo de 1990) –refrendada por los Presidentes de los Notariados de Alemania, Bélgica, España, Francia, Grecia, Holanda, Italia y Luxemburgo-, había afirmado que la profesión notarial tiene carácter unitario, participa de la autoridad pública en su integridad y que la función asesora y documentadora son inescindibles, pues la primera es presupuesto indispensable para que el documento notarial produzca la plenitud de efectos¹³⁰.”

¹²⁸ SIRI GARCIA, Julia. “Los derechos fundamentales del hombre y la misión del Notario”. Ponencia presentada en el XXII Congreso Internacional del Notariado Latino. Buenos Aires, Argentina. 27 de setiembre al 2 de octubre de 1998. Tema II. Asociación de Escribanos del Uruguay, 1998. Página 18.

¹²⁹ GIRALT FONT Jaime. “Fe”. Ponencia presentada a la VI Jornada Notarial Iberoamericana. Ob. Cit, página 10.

¹³⁰ SIRI GARCIA, Julia. “El Notario frente a la globalización de las economías nacionales. Un enfoque de Derecho Notarial”. Página 5. VIII Jornada Notarial de Norteamérica, Centroamérica y el Caribe. Cancún, Quintana Roo, México, 8 al 11 de noviembre de 1995. AEU, 1995.

3. El Notario frente al Documento Electrónico

Los Escribanos debemos tener la creatividad suficiente para adaptarnos a la tecnología existente. De forma tal, que contamos con herramientas informáticas y telemáticas para pasar del soporte papel al soporte informático en lo que a los documentos públicos se refiere.

Será necesario realizar un cambio, el cual sin lugar a dudas deberá estar respaldado por la capacitación de los notarios, contar con la infraestructura necesarias, para así pasar a pensar en los cambios legislativos que permitirán que esto pueda ser posible.

Un primer aspecto a destacar en el Registro de Protocolizaciones es referente a la posibilidad que existe hoy día de dar fecha cierta a los contenidos existentes en Internet. Así es que, a través de Actas Notariales es posible probar la existencia de un sitio web, la ocupación de determinado dominio, los contenidos de una página web en un momento determinado. El procedimiento es sencillo, el Escribano se conecta a Internet en virtud a una solicitud específica de un cliente, ingresa al sitio requerido, imprime en papel notarial las diferentes páginas y las protocoliza, constatando la información contenida en el ciberespacio y dando fecha cierta a la misma.

Esta actividad todavía hoy día está signada por el elemento papel, estamos bajando a soporte papel la información, estamos transformando los bits de forma tal que puedan ser tangibles, teniendo la materialidad que ha signado a los documentos a través del tiempo.

También existe la posibilidad de labrar Actas en los contratos informáticos, como por ejemplo de las actividades de la etapa precontractual y relacionadas con el moderno concepto de entrega.

En la etapa precontractual, de gran importancia en los contratos telemáticos, resulta de gran interés:

Documentos Electrónicos Firma Digital

a) que el usuario realice un cuadro de necesidades, en el cual se determine cuales son sus objetivos y como llevará a cabo el proceso de informatización.

b) documentar su proceso, realizando actas de todas las reuniones entre las partes.

c) A los efectos de objetivar la evaluación en cuanto al funcionamiento del sistema, es importante determinar previamente algunos aspectos. Para ello ya sea en la etapa precontractual o en el contrato mismo, debe elaborarse una grilla en la que se establezcan los ítems que serán evaluados, el momento en que se hará dicha evaluación, el establecimiento de una escala a los efectos de realizar la calificación y la documentación que se obtendrá en cada caso.

Respecto al moderno concepto de entrega al que hacíamos referencia, el mismo surge frente a la adquisición de un sistema informático. En estos casos no es suficiente que lo entreguen en un lugar físico determinado, sino que es relevante, que el sistema funcione en forma correcta y de acuerdo a los parámetros solicitados.

Tenemos entonces un primer momento que será la entrega física de la cosa, en la cual se debe firmar un acta de recepción provisoria. Posteriormente deberá realizarse la instalación del sistema y en un tercer momento se producirá la verificación de su funcionamiento. Esta verificación se realiza a través del llamado test de aceptación, período que dura entre 30 y 60 días. Durante esta etapa el sistema debe funcionar normalmente de acuerdo a las condiciones y necesidades establecidas en el contrato. Una vez verificado este plazo se firma el acta de recepción definitiva.

Por supuesto, que todos los documentos enumerados son documentos privados, para los cuales no es imprescindible la presencia del escribano. Sin embargo entendemos que es necesaria, no solamente porque estaremos dando fecha cierta al documento y certificando las firmas de las partes, sino porque otorgaremos al negocio seguridad jurídica en general, asesorando a las partes sobre el alcance de las decisiones que van tomando, las cuales muchas

veces obedecen a necesidades técnicas, no estando respaldado por las responsabilidades civiles y/o incluso penales que pueden ocasionar las mismas.

4. Cibernotario y Fedatario Juramentado

Como hemos mencionado anteriormente, con las nuevas tecnologías han surgido nuevos profesionales del Derecho, uno de ellos es el Cibernotario y en la legislación peruana surge el Fedatario Juramentado.

El Comité de Seguridad Informática de la American Bar Association, examinó el tema de la firma digital en los documentos electrónicos y llegó a la conclusión que una operación con firma digital necesitaba un tercero de confianza que proporcionara un elemento de seguridad imparcial. Al pensar quién podría ser ese tercero imparcial se hizo evidente que ya existía una profesión que había estado proporcionando seguridad imparcial a las operaciones durante siglos, la profesional notarial.

La American Bar Association junto con la Unión Internacional del Notariado Latino desde 1993 iniciaron una serie de estudios que culminaron con la creación de la figura del Cibernotario.

Así nació el concepto del Cibernotario: “profesional del derecho que también estará versado en todos los aspectos técnicos”¹³¹.

La falta de fiabilidad del Notary Public norteamericano, significaba que el proyecto tenía que crear un tipo nuevo superior del notario en Estados Unidos, que fuera tanto un jurista como un técnico.

Para Mario Miccoli el Cibernotario no debe ser tenido como si se tratara de una película de ciencia ficción.

¹³¹“ El Escribano como Autoridad Certificante: con especial referencia a la contratación electrónica”. <http://www.cep.org.py/trabajos>. Página visitada el 28/10/04.

El Cibernotario cumple dos funciones, según el Notario Fernando Goma Lanzón, que son:¹³²

- a) “La primera es jurídica en el sentido de que desarrolla las funciones tradicionales de notario, entendiendo por tal, y esto es de gran importancia, no el mal llamado notario anglosajón, sino el notario oficial público reconocido en prácticamente todos los países de tipo latino. El de que el sistema americano se plantea adoptar algunos principios de notariado latino para conseguir una adecuada seguridad en las transacciones internacionales electrónicas, constituye incuestionablemente un argumento a favor de la institución notarial...”
- b) “La segunda función es de tipo electrónico: el cibernotario habrá de tener un nivel de especialización alto en cuanto a conocimientos informáticos, debiendo actuar como autoridad de registro (en sentido muy amplio, puesto que no sólo comprende el verificar la legalidad y capacidad del solicitante, sino que puede ser requerido para investigar sus datos económicos o penales) y tercero de confianza. Se le encomienda la llamada “notarización”, determinación fehaciente de la fecha y hora de su intervención, igualmente la certificación de la identidad del emisor de un mensaje comprobado con su firma digital. Y cuantas funciones se consideren adecuadas en el futuro...”

Mencionamos como otro profesional que surge con las nuevas tecnologías al Fedatario Juramentado.

Este nuevo personaje surge en el Estado de Perú, por Decreto Legislativo N°681, artículo 3, de fecha 11 de octubre de 1991.

¹³² IRABIEN, José Fernando: “México: ¿Querer o no querer?”. <http://www.alfa-redi.org/revista>.
Página visitada el 28/10/04.

El Fedatario Juramentado puede tener la calidad de funcionario público o privado, se consideran depositarios de la fe pública y mantienen en todo momento su independencia de las empresas a las que ofrecen sus servicios.

Este no podría mantener una relación laboral exclusiva con alguna institución o compañía, más si ofrecer sus servicios mediante el sistema de servicios no personales, lo que conllevaría a facturar sus ingresos y someterse al pago de tributos de cuarta categoría.¹³³

Mediante el decreto reglamentario del Decreto Legislativo, el Decreto Supremo N° 009-92-JUS, en su artículo 4 estableció que Los Fedatarios Públicos Juramentados serían: “aquellos que actúan adscriptos a una notaría pública; o que ejercen en las empresas que ofrecen sus servicios al público”; y que el Fedatario Particular Juramentado sería aquel que: “ofrece sus servicios profesionales a una o más de las empresas que organizan sus propios archivos”

Hasta 1997 en Perú fueron los notarios los encargados de dar fe de los documentos micrograbados y el Fedatario Juramentado era un personaje que no había sido tenido en cuenta por el medio comercial y público. A partir de febrero de 1997, el Colegio de Abogados de Lima implementó un curso de especialización destinado a la obtención del diploma de idoneidad para optar por el grado de Fedatario Juramentado, siguiendo estos cursos hasta nuestros días.

La Ley N° 26.612 estableció que el Fedatario Juramentado debía capacitarse periódicamente, con miras a su ratificación como funcionario dador de fe.

Podemos decir que el ámbito de actuación de estos profesionales es frente a actos realizados mediante el uso de equipos de nuevas tecnologías, como ser otorgar autenticidad a los actos digitales y creaciones de documentos

¹³³ VELARDE KOEHLIN, Carmen. “El Fedatario Particular Juramentado en Informática: Institución peruana al servicio de una solución global”. <http://www.derechotecnologico.com/estrado/estrado13.html>. Página visitada el 28 de octubre de 2004.

Documentos Electrónicos Firma Digital

electrónicos. No puede realizar escrituras públicas, ni actas de transferencias de bienes muebles registrales como los notarios.

El Fedatario Juramentado redacta cuatro tipos de actas: actas de apertura, de cierre, de retoma y de comprobación, además de otorgar los testimonios de dichas actas y autenticar las copias impresas de las microformas.

Si el Fedatario deja de actuar como tal, todos sus archivos deben ser entregados a una notaría del lugar para que ésta los conserve y administre, según lo establecido en el artículo 19 del reglamento.

Como vemos éste es un apoyo al notario, no sería un sustituto, sino que pueden convivir las dos instituciones al mismo tiempo.

“La Comisión de Informática y Seguridad Jurídica de la Unión Internacional del Notariado Latino (UINL) ha estudiado las cuestiones surgidas en torno a las transacciones jurídicas por vía electrónica y ha afirmado claramente que las mismas constituyen un tema de suma importancia para el notariado. La Comisión se ha propuesto las siguientes tareas: definir y difundir las funciones notariales en el marco de las transacciones jurídicas por vía electrónica; elaborar recomendaciones en procura de prácticas notariales uniformes en las transacciones jurídicas por vía electrónica a nivel mundial; elaborar propuestas para una formación notarial básica en materia de transacciones jurídicas por vía electrónica; proveer de información a todos los notariados que la soliciten; desarrollar el concepto de una infraestructura notarial de seguridad a nivel mundial basada en las estructuras internacionales (UINL) a la cabeza, y cuerpos nacionales (Consejos Nacionales) y Notarios de los Estados miembros como base”¹³⁴.

¹³⁴ LOPEZ Fernando Ernesto. “De la caligrafía a la criptografía”. Ponencia presentada al IX Congreso Iberoamericano de Derecho e Informática. Costa Rica, 2002.

APENDICE NORMATIVO

1. Código General del Proceso

Artículo 77. Formas de Notificación. La notificación se practicará por la oficina central de notificaciones y en su caso, por correo, por telegrama, por acta notarial, por la policía, por tribunal comisionado o por el medio idóneo que habilite la Suprema Corte de Justicia.

Artículo 140. Valoración de la prueba. Las pruebas se apreciarán tomando en cuenta cada una de las producidas y en su conjunto, racionalmente, de acuerdo con las reglas de la sana crítica, salvo texto legal que expresamente disponga una regla de apreciación diversa.

El tribunal indicará, concretamente, cuales medios de prueba fundan principalmente su decisión.

Artículo 146. Medios de prueba.

146.1 Son medios de prueba los documentos, la declaración de parte, la de testigos, el dictamen pericial, el examen judicial y las reproducciones de hecho.

146.2 También podrán utilizarse otros medios probatorios no prohibidos por la regla de derecho, aplicando analógicamente las normas que disciplinan a los expresamente prohibidos por la ley.

Artículo 170. Autenticidad de los documentos.

170.1 El documento público se presume auténtico mientras no se demuestre lo contrario mediante tacha de falsedad; igual regla se aplicará al documento privado cuyas firmas se encuentren autenticadas por notario o autoridad competente.

170.2 Los demás documentos privados emanados de las partes, se tendrán por auténticos, salvo que se desconozca su firma, sin están suscritos o la autoría, si no lo están, en las oportunidades que se indican en el artículo siguiente o se impugnen mediante tacha de falsedad.

2. Ley Nº 15921

CAPITULO I

Disposiciones Generales

Artículo 1. Declárase de Interés Nacional la promoción y desarrollo de las zonas francas, con los objetivos de promover inversiones, expandir las exportaciones, incrementar la utilización de mano de obra nacional e incentivar la integración económica internacional.

Artículo 2. Las zonas francas son áreas del territorio nacional de propiedad pública o privada, cercadas y aisladas eficientemente, las que serán determinadas por el Poder Ejecutivo previo asesoramiento de la Comisión Honoraria Asesora de Zonas Francas, con el fin de que se desarrollen en ellas con las exenciones tributarias y demás beneficios que se detallan en esta ley, toda clase de actividades industriales, comerciales o de servicios y entre ellas:

A) Comercialización, depósito, almacenamiento, acondicionamiento, selección, clasificación, fraccionamiento, armado, desarmado, manipulación o mezcla de mercancías o materias primas de procedencia extranjera o nacional.

B) Instalación y funcionamiento de establecimientos fabriles.

C) Prestación de servicios financieros, de informática, reparaciones y mantenimiento, profesionales y otros que se requieran para el mejor funcionamiento de las actividades instaladas y la venta de dichos servicios a terceros países.

D) Otras que a juicio del Poder Ejecutivo resultaren beneficiosas para la economía nacional o para la integración económica y social de los Estados.

El Poder Ejecutivo adoptará las medidas necesarias a los efectos de que estas actividades no perjudiquen la capacidad exportadora de las industrias ya instaladas en zonas no franca.

Artículo 3. Declárase de utilidad pública la expropiación de los inmuebles de propiedad privada para el establecimiento de las zonas francas y sus accesos.

Autorízase al Poder Ejecutivo para permutar inmuebles del dominio fiscal del Estado por inmuebles de propiedad municipal o de otras personas públicas estatales que sean adecuados para el establecimiento y acceso de las zonas francas o para ampliación de las ya existentes.

Artículo 4. Solamente podrán habitar dentro de las zonas francas las personas destinadas a la vigilancia y al mantenimiento de los servicios necesarios a las actividades allí desarrolladas y los funcionarios que determine por su parte el Poder Ejecutivo.

CAPITULO II

De la Administración, Control y Explotación de las Zonas Francas

Artículo 5. La administración, supervisión y control de las zonas francas estará a cargo del Ministerio de Economía y Finanzas a través de la Dirección de Zonas Francas a la cual se podrá conceder la desconcentración adecuada para el mejor cumplimiento de sus funciones.

Artículo 6. Créase una Comisión Honoraria Asesora en materia de Zonas Francas integrada por cinco miembros, designados de la siguiente forma:

A) Uno por el Poder Ejecutivo, que presidirá.

B) Los cuatro restantes serán elegidos por los integrantes del Directorio de la Corporación Nacional para el Desarrollo que representen al Estado, los cuales, a estos efectos, se constituirán en órgano elector y su decisión deberá

ser adoptada con un mínimo de cuatro votos conformes. Conjuntamente con la designación de los titulares, se designará por los mismos procedimientos igual número de suplentes respectivos.

Artículo 7. La Comisión Honoraria Asesora será convocada por el Ministerio de Economía y Finanzas o por su Presidente y tendrá el exclusivo cometido de asesorar en la determinación de las áreas del territorio nacional donde habrán de instalarse las zonas francas de explotación estatal o particular. La iniciativa corresponderá exclusivamente al Poder Ejecutivo, ante quien se presentarán las solicitudes, debiendo someter preceptivamente a consideración de la citada Comisión las solicitudes que considere convenientes.

La Comisión deberá expedirse fundadamente en el plazo perentorio de treinta días corridos contados a partir del momento en que el Poder Ejecutivo ponga la solicitud a su consideración. La misma será acompañada de la opinión fundada de la Dirección de Zonas Francas.

El asesoramiento de la Comisión deberá contar con un mínimo de cuatro votos conformes. En su defecto, en caso omiso, o en caso de pronunciamiento en contrario a la opinión del Poder Ejecutivo, los antecedentes deberán ser remitidos a consideración de la Asamblea General o de la Comisión Permanente en su caso, las cuales dispondrán del plazo de treinta días para expedirse. Vencido dicho plazo sin pronunciamiento, el Poder Ejecutivo podrá autorizar la solicitud.

Artículo 8. Cada área delimitada como zona franca podrá ser explotada por el Estado o por particulares debidamente autorizados.

A estos efectos entiéndese por explotación la operación por la cual a cambio de un precio convenido con cada usuario, una persona física o jurídica provee la infraestructura necesaria y suficiente para la instalación y funcionamiento de una zona franca.

Artículo 9. Las empresas particulares autorizadas a explotar una zona franca no estarán amparadas en las exenciones y beneficios que esta ley concede a los usuarios. Sin perjuicio de que puedan obtener -si correspondiere- la declaración a que se refiere el decreto ley 14.178, de 28 de marzo de 1974, (Promoción Industrial).

Artículo 10. La solicitud de autorización para explotación de zona franca por particulares deberá ser presentada al Poder Ejecutivo, acompañada de un proyecto de inversión que demuestre fehacientemente la viabilidad económica del mismo y los beneficios que reportará al país.

La autorización será onerosa, ya sea mediante el pago al Estado de una suma única o mediante el pago de un canon periódico según se convenga, sin perjuicio de lo establecido en el artículo 30 de esta ley.

Artículo 11. Las empresas a que se refiere el artículo 9º deberán realizar su explotación en los términos que resulten de su autorización y su violación o falta de cumplimiento podrán ser objeto de una multa, que se graduará de conformidad con la gravedad de la infracción, de hasta un máximo de N\$ 50:000.000 (cincuenta millones de nuevos pesos) que se reajustarán por el Índice de los Precios al Consumo establecido por la Dirección General de Estadística y Censos, sin perjuicio de la revocación de la autorización cuando correspondiere según la naturaleza de la violación.

Artículo 12. En caso de revocación de autorización u otras situaciones cuya gravedad así lo determine, el Poder Ejecutivo podrá disponer a través de la Dirección de Zonas Francas la adopción de las medidas necesarias a los efectos del mantenimiento y suministro de la infraestructura indispensable para el correcto funcionamiento de la zona franca.

Las resoluciones adoptadas para dicho fin no tendrán efecto suspensivo.

Artículo 13. En los propietarios de los predios en que se instalen zonas francas privadas deberán constituir en ellos una servidumbre que tendrá por objeto la afectación del o de los inmuebles a tal destino. Dicha servidumbre se

constituirá por un plazo igual al establecido en la autorización de explotación de la zona franca y se otorgará por el o los propietarios de los predios, compareciendo, en representación del Estado, el Director de Zonas Francas.

La servidumbre se mantendrá por el plazo estipulado aun en el caso en que se revoque la autorización.

CAPITULO III

De los usuarios de Zonas Francas

Artículo 14. Son usuarios de zonas francas todas las personas físicas o jurídicas que adquieran derecho a desarrollar en ellas cualquiera de las actividades a que se refiere el artículo 2º . Las empresas instaladas en zonas francas no podrán desarrollar actividades industriales, comerciales y de servicios, fuera de las mismas.

Artículo 15. Es usuario directo aquel que adquiere su derecho a operar en zona franca mediante contrato celebrado con quien explota la misma, sea el Estado o particular debidamente autorizado. En toda circunstancia, a estos efectos, el Estado podrá contratar directamente a través de la Dirección de Zonas Francas y el usuario prestar garantía.

Es usuario indirecto aquel que adquiere su derecho a operar en zona franca mediante contrato celebrado con el usuario directo utilizando o aprovechando sus instalaciones.

Los contratos por los cuales se adquiere la calidad de usuario, deberán ser registrados en la Dirección de Zonas Francas y una vez inscriptos serán oponibles a terceros.

Artículo 16. Las contratos que suscriban quienes exploten zonas francas con los usuarios directos, o los que suscriban los usuarios directos con los indirectos y que regulen derechos de uso de la zona franca se tendrán por inexistentes si no han sido aprobados previamente por la Dirección de Zonas Francas.

Artículo 17. Los fundadores de las sociedades anónimas cuyo único objeto sea el de realizar operaciones en calidad de usuarios de la zona franca podrán inscribir directamente ante el Registro Público y General de Comercio el acta de constitución y el estatuto, adjuntando a la solicitud de inscripción la constancia expedida por la Inspección General de Hacienda de que se ha suscrito como mínimo el 50% (cincuenta por ciento) del capital social por tres o más personas físicas o jurídicas y que se ha integrado en dinero o bienes susceptibles de estimación pecuniaria por lo menos un 60% (sesenta por ciento) del capital accionario suscrito. Hecha la inscripción y publicado por una sola vez en el "Diario Oficial" un extracto de dichos instrumentos, la sociedad se considerará legalmente constituida y podrá solicitar directamente ante el Director del Registro Público y General de Comercio su inscripción en la Matrícula de Comerciante. El Banco de la República Oriental del Uruguay liberará el depósito que se hubiera efectuado por integración en dinero, justificándose la inscripción del estatuto en el Registro Público y General de Comercio. De la misma manera procederá en el caso en que se desistiera de la constitución de la sociedad. No regirá respecto de estas sociedades la exigencia de integración de un nuevo 20% (veinte por ciento) de las acciones suscritas, prevista en el inciso segundo del artículo 405 del Código de Comercio, en la redacción dada por el artículo 208 de la ley 13.318, de 28 de diciembre de 1964.

Artículo 18. Los usuarios de las zonas francas emplearán en las actividades que desarrollen en las mismas, un mínimo de 75% (setenta y cinco por ciento) de personal constituido por ciudadanos uruguayos, naturales o legales, a fin de poder mantener su calidad de tales y las exoneraciones tributarias, franquicias, beneficios y derechos que esta ley les acuerda.

En casos excepcionales, este porcentaje podrá ser reducido previa autorización del Poder Ejecutivo, atendiendo a características especiales de la actividad a desarrollar y razones de interés general.

CAPITULO IV

De las exenciones y beneficios

Artículo 19. Los usuarios de las zonas francas están exentos de todo tributo nacional, creado o a crearse, incluso de aquellos en que por ley se requiera exoneración específica, respecto de las actividades que desarrollen en la misma.

Artículo 20. No estarán comprendidas en las precedentes exenciones tributarias las contribuciones especiales de seguridad social y las prestaciones legales de carácter pecuniario establecidas a favor de personas de derecho público no estatales de seguridad social.

Cuando el personal extranjero que trabaje en la zona franca exprese por escrito su deseo de no beneficiarse del sistema de seguridad social vigente en la República, no existirá obligación de realizar los aportes correspondientes.

Asimismo no estarán exonerados del Impuesto a las Rentas de la Industria y Comercio los dividendos o utilidades acreditados o pagados a personas físicas o jurídicas domiciliadas en el exterior, cuando se hallen gravados en el país del domicilio del titular y exista crédito fiscal en el mismo por impuesto abonado en la República (literal d) del artículo 2º del Título 4 del Texto Ordenado 1987).

Artículo 21. Los bienes, servicios, mercancías y las materias primas, cualquiera sea su origen, introducidos a las zonas francas estarán exentos de todo tributo o cualquier otro instrumento de efecto equivalente sobre la importación o de aplicación en ocasión de la misma, aun aquellos en que por ley se requiera exoneración específica cualquiera fuera su naturaleza.

Los bienes, servicios, mercancías y materias primas que procedan de territorio nacional no franco y sean introducidos a las zonas francas, lo serán de acuerdo a todas las normas vigentes para la exportación en ese momento.

Artículo 22. Los bienes, servicios, mercancías y materias primas introducidos en las zonas francas y los productos elaborados en ellas, podrán salir de las mismas en cualquier tiempo, exentos de todo tributo, o cualquier

otro instrumento de efecto equivalente, gravámenes y recargos creados o a crearse, incluso aquellos en que por ley se requiera exoneración específica cualquiera fuera su naturaleza.

Cuando fueren introducidos desde las zonas francas al territorio nacional no franco, bienes, servicios, mercancías y materias primas existentes en ellas o elaborados en las mismas se considerarán importaciones a todos sus efectos.

Artículo 23. La Administración Nacional de Puertos percibirá el importe de los servicios efectivamente prestados, por todos los bienes que tengan destino o provengan de la zona franca, no pudiendo las tarifas exceder del costo directo del servicio.

A los efectos de la aplicación de las tarifas de la Administración Nacional de Puertos, el ingreso o egreso de los bienes y su traslado a o desde las zonas francas, se considerará tránsito internacional pudiendo cobrarse el ingreso o egreso por tan sólo una vez.

Artículo 24. Los organismos públicos que suministren insumos o servicios a los usuarios de las zonas francas podrán establecer para éstos tarifas promocionales especiales.

Los monopolios de los servicios del dominio industrial y comercial del Estado no regirán en las zonas francas.

Artículo 25. El Estado, bajo responsabilidad de daños y perjuicios, asegura al usuario, durante la vigencia de su contrato, las exoneraciones tributarias, beneficios y derechos que esta ley le acuerda.

CAPITULO V

De los espacios y construcciones en zonas francas

Artículo 26. Las construcciones que realice el usuario directo se regirán por las reglas y condiciones técnicas que se establezcan por la Dirección de Zonas Francas.

Las mismas sólo podrán destinarse al cumplimiento de las actividades del usuario.

Artículo 27. Las prestaciones pecuniarias en moneda nacional o extranjera que deban abonar los usuarios a quienes exploten las mismas -ya sea el Estado o particulares autorizados- podrán ser reajustables de conformidad con lo que se establezca por las partes en el respectivo contrato; las mismas deberán ser abonadas por el usuario por todo el tiempo que dure su ocupación, aún cuando ésta se extienda más allá del plazo contractual y sus prórrogas.

Artículo 28. La falta de pago de tres prestaciones consecutivas si el mismo fuere mensual, o de una si lo fuere por períodos mayores, dará derecho al explotador -sea el Estado o un particular- a solicitar directamente la desocupación de la zona franca al usuario, previa intimación de pago con plazo de tres días mediante telegrama colacionado.

Se seguirá el procedimiento de entrega de la cosa previsto en los artículos 1309 y siguientes del Código de Procedimiento Civil, sin perjuicio de las sanciones que pudiere aplicar la Dirección de Zonas Francas.

Artículo 29. El cobro de las prestaciones adeudadas se tramitará por la vía del juicio ejecutivo, previa intimación mediante telegrama colacionado y no podrán oponerse otras excepciones que las previstas en el artículo 108 del decreto-ley 14.701, de 12 de setiembre de 1977, sin perjuicio de las sanciones a que alude el artículo anterior.

Artículo 30. La Dirección de Zonas Francas podrá convenir con el o los usuarios y los explotadores particulares, la compensación de las prestaciones pecuniarias establecidas, con obras de infraestructura y servicios prestados por éstos, que propendan a la mejora y al desarrollo de las zonas francas, pero en ningún caso podrá el usuario o el explotador particular invocar compensación alguna si así no se hubiera acordado por escrito.

Artículo 31. El producido de las prestaciones pecuniarias obtenidas por la Dirección de Zonas Francas de parte de los usuarios se destinará al mejoramiento de los servicios, promoción y publicidad y a obras para el desarrollo y mejoras de las mismas.

Artículo 32. El usuario directo podrá, durante el período de vigencia del contrato o sus prórrogas, ceder el mismo a un tercero, con el consentimiento de la Dirección de Zonas Francas y de su co-contratante en caso de explotación particular. Sólo se podrán enajenar las construcciones y las instalaciones realizadas o adquiridas al cesionario del referido contrato o a otros usuarios o al Estado.

Dichos contratos se considerarán inexistentes si no hubiesen sido aprobados previamente por la Dirección de Zonas Francas.

Artículo 33. Finalizado el plazo contractual o sus prórrogas, el usuario directo o indirecto deberá desocupar la zona franca. En caso negativo se seguirá el procedimiento de entrega de la cosa, previsto en los artículos 1309 y siguientes del Código de Procedimiento Civil. El mismo procedimiento se seguirá en todos los casos que corresponda la desocupación.

Artículo 34. El usuario sólo podrá realizar mejoras y construcciones con la autorización escrita de quien explote la zona.

Las realizadas sin autorización quedarán en beneficio del explotador, sin derecho del usuario a compensación o reembolso alguno, salvo la opción de aquél de compeler el retiro a costo del usuario y sin perjuicio de las sanciones que resulten aplicables. No regirán en las zonas francas las disposiciones del decreto ley 14.219, de 4 de julio de 1974, sus modificativos y concordantes.

Artículo 35. A falta de acuerdo entre las partes, las construcciones y mejoras realizadas por el usuario con autorización de quien explote la zona franca, sea el Estado o particular, deberán ser abonadas por éste al valor de la fecha de desocupación.

Las partes, incluso del Estado, podrán pactar que todos los conflictos que entre ellos se susciten en materia de mejoras, se diriman por la solución del arbitraje.

CAPITULO VI

De los bienes en zonas francas

Artículo 36. Los bienes, mercancías y materias primas de procedencia extranjera con destino a zonas francas deberán cumplir de inmediato con dicho destino una vez llegados al país. No podrán permanecer en ningún depósito, salvo en aquellos ubicados dentro de los recintos aduaneros y durante el lapso máximo que la reglamentación fije para cumplir con su introducción a la respectiva zona franca.

Artículo 37. No se permitirá dentro de las zonas francas el comercio al por menor.

Los usuarios de zonas francas podrán expedir "warrants" y certificados de depósito de las mercaderías, materias primas y productos depositados en las zonas que les hubieran sido asignadas.

Dichos certificados sólo serán negociables una vez refrendados por la Dirección de Zonas Francas.

Artículo 38. Serán enteramente libres el ingreso y egreso a las zonas francas de títulos valores, moneda nacional y extranjera, metales preciosos por cualquier concepto, su tenencia, comercialización, circulación y conversación o transferencia.

Artículo 39. En la reglamentación que establezca el Poder Ejecutivo se dictarán normas tendientes a resolver el caso de los bienes, mercaderías o materias primas, abandonados por los usuarios en las zonas francas o por los propietarios o consignatarios de los mismos, en los predios o galpones de los usuarios. Se entenderá que hay abandono una vez transcurrido el plazo de seis meses del vencimiento de la última obligación pecuniaria incumplida.

Facúltase al Poder Ejecutivo para vender dichos bienes, mercaderías o materias primas en subasta pública o directamente previa tasación. Si los bienes, mercaderías o materias primas fueran de propiedad de un usuario directo, las sumas obtenidas se aplicarán en primer lugar a la cancelación de las prestaciones pecuniarias pendientes de pago con el Estado o con el explotador privado; si fueran de propiedad de un usuario indirecto, a la cancelación de sus obligaciones con el respectivo usuario directo, originadas en el contrato a que se refiere el inciso segundo del artículo 15 de esta ley; si fueran de propiedad de terceros la cancelación de las obligaciones contraídas con el usuario como consecuencia de los respectivos contratos de depósito o consignación. El excedente, si lo hubiera, se depositará en el Banco de la República Oriental del Uruguay a la orden de los propietarios de los bienes vendidos según correspondiere. Los acreedores de cualquier naturaleza podrán hacer valer sus derechos sobre la suma depositada.

En el caso de introducirse a plaza dichos bienes, mercaderías o materias primas, abonarán los tributos, gravámenes o recargos, vigentes en el momento de su importación. El valor imponible será el que resulte de la tasación o subasta pública, certificado por el Poder Ejecutivo.

Artículo 40. No regirán para las actividades a desarrollarse en zonas francas los requisitos establecidos o que pudieren establecerse en materia de integración obligatoria de componentes nacionales a los bienes que allí se elaboren, así como cualquier otra exigencia que condicione o pudiere condicionar el ingreso o egreso de bienes en zona franca, salvo los relativos a su control.

Artículo 41. El Ministerio de Economía y Finanzas expedirá los certificados de origen en las condiciones y formalidades que establezca el Poder Ejecutivo, sin que pueda efectuarse en dichos certificados discriminación alguna en cuanto al origen de los productos elaborados en territorio no franco.

Los tratamientos preferenciales concedidos a las exportaciones uruguayas por otros países con relación a determinados productos y en volúmenes o valores limitados, serán aprovechados con preferencia por las industrias exportadoras de dichos productos ya instaladas en la zona no franca. El Poder Ejecutivo deberá adoptar las medidas necesarias a tal propósito.

CAPITULO VII

De las sanciones y disposiciones finales

Artículo 42. Las violaciones e infracciones de la presente ley, sus reglamentos y estipulaciones contractuales, serán sancionadas por el Poder Ejecutivo.

A) Con multa de hasta N\$ 50:000.000.00 (cincuenta millones de nuevos pesos) que se reajustarán por el Índice de los Precios al Consumo establecido por la Dirección General de Estadística y Censos.

B) Con prohibición de ingresos y egresos de mercaderías y/o la realización de cualquier operación en calidad de usuario por un tiempo determinado; y

C) Con la pérdida de las exenciones y demás beneficios que esta ley concede.

Artículo 43. El Poder Ejecutivo reglamentará la presente ley y dispondrá las medidas necesarias a los efectos de procurar la sencillez y simplificación de todos los servicios y trámites relativos a la exportación e importación de bienes de zonas francas, adoptando aquellas que, acordes con los beneficios que esta ley concede y los controles indispensables, permitan alcanzar la mayor eficiencia y celeridad de dichas operaciones.

Artículo 44. Declárase que las zonas francas de Colonia y Nueva Palmira, creadas por la ley 7.593, de 20 de junio de 1923, se encuentran comprendidas en las disposiciones de la presente ley.

Artículo 45. Los actuales usuarios de las zonas francas de Colonia y Nueva Palmira quedan sometidos a las disposiciones de la presente ley.

Los que desarrollen actividades simultáneamente fuera de zonas francas dispondrán de un plazo de ciento ochenta días desde la vigencia de esta ley para adecuarse a lo previsto en el artículo 14.

Artículo 46. El Poder Ejecutivo velará por la preservación del medio ambiente.

Artículo 47. Prohíbese la introducción a zonas francas de armas, pólvora, municiones y demás materias destinadas a usos bélicos, como así también las declaradas contrarias a los intereses del país por el Poder Ejecutivo.

Artículo 48. Deróganse los decretos leyes 14.498, de 19 de febrero de 1976 y 15.121, de 10 de abril de 1981, así como toda otra disposición que se oponga a la presente ley.

Artículo 49. Comuníquese, etc..

3. Ley Nº 16.002

Artículo 129. La documentación emergente de la transmisión a distancia, por medios electrónicos, entre dependencias oficiales, constituirá, de por sí, documentación auténtica y hará plena fe a todos sus efectos en cuanto a la existencia del original transmitido.

Artículo 130. El que voluntariamente transmitiere a distancia entre dependencias oficiales un texto del que resulte un documento infiel, incurrirá en los delitos previstos por los artículos 236 a 239 del Código Penal, según corresponda.

4. Ley N° 16.060

Artículo 11. (Legajo).- En el Registro Público de Comercio, realizada su inscripción, se formará un legajo para cada sociedad, con las copias del contrato social, sus modificaciones y demás documentos que disponga la ley o su reglamentación. Su consulta será pública.

La reglamentación podrá autorizar el empleo de todos los medios técnicos disponibles para el cumplimiento de lo dispuesto en el inciso anterior.

Artículo 91. (Norma especial).- La reglamentación establecerá las normas contables adecuadas a las que habrán de ajustarse los estados contables de las sociedades comerciales.

Asimismo podrá autorizar para estas sociedades, el empleo de todos los medios técnicos disponibles en reemplazo o complemento de los libros obligatorios impuestos a los comerciantes.

Artículo 418. (Legajo).- Sin perjuicio de lo dispuesto por el artículo 11, el órgano estatal de control formará su propio legajo de cada sociedad anónima con la copia del contrato social, sus modificaciones, los documentos que deban incorporarse al legajo del Registro Público de Comercio, los referidos en el artículo 414 y aquellos que disponga la reglamentación.

La reglamentación podrá autorizar el empleo de todos los medios técnicos disponibles para el cumplimiento de lo dispuesto en el inciso anterior.

El legajo podrá ser consultado por cualquier accionista.

5. Ley N° 16.170

Artículo 383. Suspéndese la aplicación del artículo 11 de la Ley N° 16.060, de 4 de setiembre de 1989, hasta que el Poder Ejecutivo proceda a su reglamentación, la cual deberá dictarse cuando a su juicio se disponga de los



medios técnicos apropiados, para la formación del legajo o soporte de información equivalente.

6. Decreto N° 500/991

Artículo 14. Es de interés pública, para el mejor cumplimiento de los servicios, el intercambio permanente y directo de datos e información entre todas las unidades y reparticiones de la Administración Pública, sea cual fuere su naturaleza jurídica o posición institucional, a través de cualquier medio hábil de comunicación, sin más limitación que lo dispuesto en el artículo 80.

A efectos de implantar sistemas de libre flujo de información, se propenderá a la interconexión de los equipos de procesamiento electrónico de información u otros medios similares.

Asimismo podrá la Administración brindar el servicio de acceso electrónico a sus bases de datos a las personas físicas o jurídicas, estatales, paraestatales o privadas que así lo solicitaren.

Artículo 19. Toda petición o exposición que se formule ante cualquier órgano administrativo, se efectuará en papel simple (florete, fanfold o de similares características), de acuerdo con las especificaciones contenidas en el artículo 44 del presente decreto.

Podrán utilizarse formularios proporcionados por la Administración, admitiéndose también los impresos que presenten las partes siempre que respeten las reglas referidas en el inciso anterior.

Asimismo las dependencias de la Administración Central podrán admitir la presentación de los particulares por fax u otros medios similares de transmisión a distancia, en los casos que determinan.

Artículo 32. La documentación emergente de la transmisión a distancia, por medios electrónicos, entre dependencias oficiales, constituirá, de por sí,



documentación auténtica y hará plena fe a todos sus efectos en cuanto a la existencia del original transmitido.

El que voluntariamente transmitiere a distancia entre dependencias oficiales un texto del que resulte un documento infiel, incurrirá en los delitos previstos por los artículos 236 a 239 del Código Penal, según corresponda. (Ley 16.002 de 25 de noviembre de 1988, arts. 129 y 130).

Artículo 33. En aplicación de lo dispuesto por el artículo 14, la Administración propiciará el uso de soportes de información electrónicos, magnéticos, audiovisuales, etc., siempre que faciliten la gestión pública.

Artículo 70. Los hechos relevantes para la decisión de un procedimiento podrán acreditarse por cualquier medio de prueba no prohibido por la ley.

La valoración de la prueba se efectuará de conformidad con las reglas contenidas en el Código General del Proceso.

Artículo 90. Autorízase la copia fotográfica y microfilmada de los expedientes y demás documentos archivados en todas las dependencias del Estado y demás Organismos Públicos, y la destrucción de los documentos originales cuando ello sea indispensable, de conformidad con las normas reglamentarias vigentes o a dictarse.

Dichas copias tendrá igual validez que los antecedentes originales a todos los efectos legales, siempre que fueren debidamente autenticadas por las Direcciones de las respectivas Oficinas. (Ley 14.106, de 14 de marzo de 1973, art. 688).

Artículo 91. Las resoluciones que den vistas de las actuaciones, decreten la apertura a prueba, las que culminen el procedimiento y, en general, todas aquellas que causen gravamen irreparable o que la autoridad disponga expresamente que así se haga, serán notificadas personalmente al interesado en la oficina o en el domicilio que corresponda, de acuerdo con el artículo 97.

La notificación personal en la oficina se practicará mediante la comparecencia del interesado, su apoderado, o persona debidamente autorizada para estos efectos.

Si el interesado no compareciese espontáneamente, se intimará su concurrencia a la oficina dentro del plazo de tres días hábiles, mediante telegrama colacionado certificado con aviso de entrega, carta certificada con aviso de retorno o por cualquier otro medio idóneo.

Si al vencimiento de dicho plazo el interesado no hubiese concurrido, se practicará la notificación personal en el domicilio correspondiente por medio de un funcionario comisionado, entendiéndose con el interesado o personal hábil que acreditará su identidad mediante el documento respectivo. La persona con quien se practique la diligencia deberá firmar la constancia respectiva. En el caso de no encontrarse ninguna de las personas indicadas, así como cuando éstas se negaren a firmar la constancia, el funcionario comisionado dejará cedulón en lugar visible, del modo que mejor asegure su recepción por el interesado, levantando acta de la diligencia.

También podrá practicarse la notificación a domicilio por telegrama colacionado certificado con aviso de entrega, por carta certificada con aviso de retorno, télex, fax o cualquier otro medio idóneo que proporcione certeza en cuanto a la efectiva realización de la diligencia y a su fecha, así como en cuanto a la persona a la que se ha practicado.

Artículo 154. Cualquiera sea la forma documental utilizada para la interposición de los recursos (escrito en papel simple, formulario o impreso, telegrama colacionado certificado con aviso de entrega, télex, fax, o cualquier otro medio idóneo), siempre deberá constar claramente el nombre y domicilio del recurrente y su voluntad de recurrir traducida en la manifestación de cuáles son los recursos que se interponen y la designación del acto administrativo que impugna.

Si se actúa en representación de otro, se procederá de conformidad con lo establecido en los arts. 20 y 24 del presente decreto.

Si la autoridad que dictó el acto estuviera radicada en los departamentos del Interior, el recurrente deberá, en caso de franquearse el recurso subsidiario, establecer domicilio en la radio de la Capital de la República, donde se realizarán los emplazamientos, citaciones, notificaciones e intimaciones que puedan disponerse en la tramitación del recurso jerárquico o de anulación correspondiente.

Artículo 157. En caso que los recursos se hayan interpuesto mediante telegrama colacionado certificado con aviso de entrega, télex, fax, u otro procedimiento similar, por razones de conservación de la documentación y seguridad jurídica, la Administración procederá de inmediato a su reproducción a través de los medios pertinentes y formará el correspondiente expediente. El jefe o encargo de la unidad de administración documental extenderá la correspondiente certificación de la reproducción realizada.

En los casos señalados precedentemente, el recurrente o su representante, dispondrá de un plazo de diez días hábiles a contar del siguiente a la recepción del correspondiente documento por la Administración, para comparecer en la oficina a efectos de ratificar por escrito su voluntad de recurrir, de cumplir con la exigencia legal de la firma letrada, para la agregación del mandato respectivo en caso de representación y, en general, para cumplir con todo otro requisito que para el caso sea exigible. Si no lo hiciere dentro del plazo señalado, sin justa causa, la Administración tendrá el recurso por no presentado.

Artículo 158. En los casos de utilización del procedimiento del telegrama colacionado certificado con aviso de entrega, se tendrá por fecha y hora de interposición del recurso la que estampe la oficina telegráfica al recibir el texto a remitir. En los demás procedimientos referidos en el artículo anterior, se tendrá por fecha y hora de recepción, la que luzca el reporte emitido por el equipo utilizado o, en su defecto, la que estampo el funcionario receptor.

Se entenderá que el recurso no fue presentado en tiempo cuando sea interpuesto el último día del término fijado por el artículo 142 después de vencido el horario de la oficina donde deba presentarse.

Artículo 195. Los hechos relevantes para la decisión del procedimiento disciplinario podrán acreditarse por cualquier medio lícito de prueba (fotografías, fotocopias, croquis, cintas magnetofónicas, así como por todo otro medio hábil que provea la técnica).

7. Ley Nº 16.226

Artículo 383. El Tribunal de lo Contencioso Administrativo podrá, en forma directa o por concesión a terceros, brindar el servicio de acceso electrónico digital a sus bases de datos de jurisprudencia y gestión, por medio de la red telefónica pública, a las personas físicas o jurídicas, estatales, paraestatales o privadas que así lo solicitaren. El Tribunal de lo Contencioso Administrativo fijará los precios de los servicios, que no podrán superar los precios del mercado.

El producido del servicio será aplicado a la mejora del citado servicio electrónico.

Artículo 384. Las comunicaciones procesales a las partes podrán efectuarse también por medios electrónicos o de similares características. Los documentos emergentes de la transmisión, constituirán documentación auténtica que hará plena fe a todos sus efectos, siendo de aplicación lo dispuesto por el artículo 130 de la ley 16.002, de 25 de noviembre de 1988. El tribunal de lo Contencioso Administrativo determinará y reglamentará la forma en que se practicarán las mismas.

Artículo 477. Las comunicaciones y notificaciones de las actuaciones administrativas podrán realizarse por medio de fax. (facsimil).



8. Ley N° 16.713

Título III - Del Banco de Previsión Social y del Registro de Historia Laboral

Capítulo I. Del Banco de Previsión Social

Artículo 84. (Emisión de Cheques). En los cheques emitidos por el Banco de Previsión Social, destinados al pago de jubilaciones, pensiones y otros beneficios, podrá sustituirse la firma autógrafa por signos o contraseñas impresos o impresos mecánica o electrónicamente.

9. Ley N° 16.736

Sección VIII – Normas de desregulación y reforma administrativa

Capítulo I - Normas Generales

Artículo 694. Las administraciones públicas impulsarán el empleo y aplicación de medios informáticos y telemáticos para el desarrollo de sus actividades y el ejercicio de sus competencias, garantizando a los administrados el pleno acceso a las informaciones de su interés.

Artículo 695. Los trámites y actuaciones que conforman el procedimiento administrativo así como los actos administrativos podrán realizarse por medios informáticos. Su validez jurídica y valor probatorio serán idénticos a los de las actuaciones administrativas que se tramiten por medios convencionales. La firma autógrafa podrá ser sustituida por contraseñas o signos informáticos adecuados.

Artículo 696. La notificación personal de los trámites y actos administrativos podrá realizarse válidamente por correo electrónico u otros medios informáticos o telemáticos, los cuales tendrán plena validez a todos los efectos siempre que proporcionen seguridad en cuanto a la efectiva realización de la diligencia y a su fecha.



Artículo 697. La documentación emergente de la transmisión por medios informáticos o telemáticos constituirá de por sí documentación auténtica y hará plena fe, a todos sus efectos, en cuanto a la existencia del original transmitido. El que voluntariamente transmitiere un texto del que resulte un documento infiel, adultere o destruya un documento almacenado en soporte magnético, o su respaldo, incurrirá en los delitos previstos por los artículos 236 a 239 del Código Penal, según corresponda.

Artículo 698. El Poder Ejecutivo reglamentará las disposiciones contenidas en los artículos precedentes, las que no podrán implicar costos presupuestales.

10. Decreto N° 65/998

Visto: el proyecto de decreto sobre "procedimiento administrativo electrónico" que eleva la Oficina Nacional del Servicio Civil.

Resultando: I) que la Ley de Presupuesto N° 16.736 de fecha 5 de enero de 1996, encomendó al Poder Ejecutivo la reglamentación de los artículos 694 a 697 del citado cuerpo normativo. II) que dichas normas contienen las disposiciones tendientes al empleo y aplicación de medios informáticos y telemáticos, para el desarrollo de las actividades y el ejercicio de las competencias de la Administración Pública. III) que estos medios son de uso corriente, tanto en el ámbito nacional como internacional.

Considerando: I) que el presente proyecto de decreto responde a la actual política de reforma del Estado, tendiente al logro de una mayor eficiencia en los trámites y procedimientos administrativos, reglamentando la implementación de medios electrónicos de transmisión, almacenamiento y manejo de documentos. II) que el empleo de dichos medios informáticos y telemáticos en la sustanciación de los expedientes administrativos, permitirá minimizar la utilización de documentos basados en papel, logrando así una mayor celeridad y simplificación en la gestión administrativa. III) que, asimismo,



la incorporación de la informática a la gestión administrativa, permitirá un mayor control del flujo de información que maneja el Estado, que redundará en beneficio de la Administración y de los administrados.

Que a tales fines, dada la diversidad de sistemas de información y de sus plataformas existentes en la Administración, es necesario establecer un estándar de comunicación electrónica de documentos que deberá ser compatible con los utilizado sen la actividad privada nacional e internacional.

Atento: a lo informado por el Director de la Oficina Nacional DEL Servicio Civil y a lo preceptuado por los artículos 694 a 698 de la Ley 16.736 de fecha 5 de enero de 1996.

EL PRESIDENTE DE LA REPÚBLICA

Actuando en Consejo de Ministros

DECRETA:

CAPÍTULO I

Disposiciones Generales

Artículo 1. La sustanciación de actuaciones en la Administración pública, así como los actos administrativos que se dicten en las mismas, podrán realizarse por medios informáticos.

Cuando dichos trámites o actos, revestidos de carácter oficial, hayan sido redactados o extendidos por funcionarios competentes, según las formas requeridas y dentro del límite de sus atribuciones, constituirán instrumentos públicos y como tales se tendrán como auténticos y harán plena fe, salvo desconocimiento o tacha de falsedad.

En tal sentido, constituirán instrumentos públicos, aquellos creados por medios informáticos que aseguren su inalterabilidad.

Documentos Electrónicos Firma Digital

Cuando la sustanciación de las actuaciones administrativas se realice por medios informáticos, las firmas autógrafas que la misma requiera podrán ser sustituidas por contraseñas o signos informáticos adecuados.

Artículo 2. Se entiende por expediente electrónico, la serie ordenada de documentos públicos registrados por vía informática, tendientes a la formación de la voluntad administrativa en un asunto determinado.

Artículo 3. El expediente electrónico tendrá la misma validez jurídica y probatoria que el expediente tradicional.

La documentación emergente de la trasmisión a distancia, por medios electrónicos, entre dependencias oficiales constituirá, de por sí, documentación auténtica y hará plena fe a todos sus efectos en cuanto a la existencia del original transmitido (art.129 de la Ley N° 16.002 de fecha 25 de noviembre de 1988).

Las formalidades relativas a la intervención notarial de certificación de firmas en actos, actas y contratos de la Administración, se seguirá regulando por las normas vigentes en la materia.

CAPÍTULO II

Normas sobre procedimiento

Artículo 4. Todas las normas sobre procedimiento administrativo serán de aplicación a los expedientes tramitados en forma electrónica, en la medida en que no sean incompatibles con la naturaleza del medio empleado.

Artículo 5. Toda petición o recurso administrativo que se presente ante la administración podrá realizarse por medio de documentos electrónicos. A tales efectos los mismos deberán ajustarse a los formatos o parámetros técnicos que oportunamente fije el Poder Ejecutivo, con el asesoramiento de la Oficina Nacional del Servicio Civil, en lo referente a componentes específicos y a la validez del documento electrónico, de la Comisión Nacional de Informática, en lo referente a aspectos informáticos y del Grupo Técnico Asesor, en lo que



respecta a las telecomunicaciones e integración de diferentes organismos de la Administración Pública.

En caso de incumplimiento de dichas especificaciones, tales documentos se tendrá por no recibidos.

No obstante lo expresado precedentemente, se respetará el principio del informalismo a favor del administrado, tanto para las peticiones como para los recursos administrativos.

Artículo 6. Los administrados podrán presentar sus peticiones y recursos administrativos por medio de documentos electrónicos, mediante la utilización de los programas de ordenador que satisfagan el estándar establecido por la Comisión Nacional de Informática.

Artículo 7. Toda vez que se presente un documento mediante transferencia electrónica, la Administración deberá expedir una constancia de su recepción. La constancia de recibo de un documento electrónico será prueba suficiente de su presentación.

Su contenido será la fecha, lugar y firma digital del receptor.

Para las hipótesis previstas en este artículo así como en el anterior, serán de aplicación en lo pertinente, las disposiciones contenidas en los artículos 157 a 159 del Decreto N°500/991 de fecha 27 de setiembre de 1991.

Artículo 8. La Administración admitirá la presentación de documentos registrados en papel para su utilización en un expediente electrónico. En tales casos podrá optar entre la digitalización de dichos documentos para su incorporación al expediente electrónico, o la formación de una pieza separada, o una combinación de ambas, fijando como meta deseable la digitalización total de los documentos.

En caso de proceder a la digitalización del documento registrado en papel, se certificará la copia mediante la firma digital del funcionario encargado del proceso, así como la fecha y lugar de recepción.

Documentos Electrónicos Firma Digital

Artículo 9. Autorízase la reproducción y almacenamiento por medios informáticos de los expedientes y demás documentos registrados sobre papel, existentes en todos los organismos públicos.

Artículo 10. Podrán reproducirse sobre papel los expedientes electrónicos, cuando sea del caso su sustanciación por ese medio, ya sea dentro o fuera de la repartición administrativa de que se trate, o para proceder a su archivo sobre papel. El funcionario responsable de dicha reproducción, certificará su autenticidad.

Artículo 11. Tratándose de expedientes totalmente digitalizados, el expediente original en papel, deberá radicarse en un archivo centralizado. En caso de la tramitación de un expediente parcialmente digitalizado, la pieza separada que contenga los documentos registrados en papel, se radicará en un archivo a determinar por la repartición respectiva. En ambos casos, el lugar dispuesto propenderá a facilitar la consulta, sin obstaculizar el trámite del expediente.

Artículo 12. Los plazos para la sustanciación de los expedientes electrónicos, se computarán a partir del día siguiente de su recepción efectiva por el funcionario designado.

Se entiende por recepción efectiva, la fecha de ingreso del documento al subsistema de información al cual tiene acceso el funcionario designado a tales efectos.

Artículo 13. Los sistemas de información de expedientes electrónicos deberán prever y controlar las demoras en cada etapa del trámite. A su vez, deberán permitir al jerarca modificar el trámite para sortear los obstáculos detectados, minimizando demoras.

Artículo 14. Los órganos administrativos que utilicen expedientes electrónicos, adoptarán procedimientos y tecnologías de respaldo o duplicación, a fin de asegurar su inalterabilidad y seguridad, los que serán definidos por la Oficina Nacional del Servicio Civil, con el asesoramiento de la

Documentos Electrónicos Firma Digital

Comisión Nacional del Servicio Civil, con el asesoramiento de la Comisión Nacional de Informática o eventualmente del Grupo técnico asesor, cuando involucre a más de un organismo.

Artículo 15. El Poder Ejecutivo, con el asesoramiento de la Oficina Nacional del Servicio Civil, de la Comisión Nacional de informática y del Grupo Técnico Asesor, en sus respectivas competencias, determinará periódicamente, en consideración a la evolución de la tecnología disponible, los medios técnicos de almacenamiento, reproducción y transmisión telemática de documentos que, por su naturaleza o por la eficacia de los procedimientos de control aplicables, ofrezcan protección adecuada contra la pérdida o adulteración de la información almacenada, reproducida y/o transmitida.

Artículo 16. Los documentos que hayan sido digitalizados en su totalidad, a través de los medios técnicos incluidos en el artículo anterior, podrán ser destruidos si ello conviene a las necesidades de cada organismo.

Los originales de valor histórico, cultural o de otro valor intrínseco, no podrán ser destruidos, por lo que luego de almacenados serán enviados para su guarda a la repartición pública que corresponda, en aplicación de las normas vigentes sobre conservación del patrimonio histórico y cultural del Estado.

Artículo 17. Las copias o reproducciones de documentos anteriormente referidos, tendrán la misma validez del documento original a todos los fines para los que éste fuese empleado, sustituyéndolo con idéntico valor legal, siempre que estuviesen debidamente autenticados.

CAPÍTULO III

Firma electrónica y digital

Artículo 18. Se entiende por firma electrónica, el resultado de obtener por medio de mecanismos o dispositivos un patrón que se asocie biunívocamente a un individuo y a su voluntad de firmar.

Documentos Electrónicos Firma Digital

Artículo 19. Se entiende por firma digital, un patrón creado mediante criptografía, debiendo utilizarse sistemas criptográficos "de clave pública" o "asimétricos", o los que determine la evolución de la tecnología.

Artículo 20. A efectos de dotar de seguridad y certeza la gestión del sistema que se reglamenta, será responsabilidad de cada organismo que dirija un proyecto que utilice la tecnología de "claves públicas" y "claves privadas", determinar y documentar la forma de administración de las mismas.

Artículo 21. La divulgación de la clave o contraseña personal de cualquier funcionario autorizado a documentar su actuación mediante firmas o contraseñas informáticas, constituirá falta gravísima, aún cuando la clave o contraseña no llegase a ser utilizada.

Artículo 22. Todo documento electrónico autenticado mediante firma digital, se considerará como de la autoría del usuario al que se haya asignado la clave privada correspondiente, salvo que medie prueba de la falsificación del documento electrónico o de la divulgación de la clave por terceros.

Quedan expresamente exceptuados de lo dispuesto anteriormente, la firma del Presidente de la República y de los ministros de Estado en los decretos y resoluciones del poder Ejecutivo, debiendo estamparse la firma en forma ológrafa (Arts. 168 numeral 25 y 181 ordinal 7° de la Constitución de la República).

Artículo 23. Cuando los documentos electrónicos que a continuación se detallan, sean registrados electrónicamente, deberán identificarse mediante la firma electrónica o la firma digital de su autor:

- a) los recursos administrativos, así como toda petición que se formule a la Administración;
- b) los actos administrativos definitivos;
- c) los actos administrativos de certificación o destinados a hacer fe pública;

d) los dictámenes o asesoramientos previos a una resolución definitiva.

Artículo 24. Los actos administrativos de mero trámite, no requerirán la firma electrónica del o los funcionarios intervinientes, pero deberán identificarse mediante una clave simple.

CAPÍTULO IV

Penalidades.

Artículo 25. El que voluntariamente transmitiere un texto del que resulte un documento infiel, adultere o destruya un documento almacenado en soporte magnético, o su respaldo, incurrirá en los delitos previstos por los artículos 236 a 239 del Código Penal, según corresponda (art.697 de la ley 16.736 de fecha 5 de enero de 1996).

Artículo 26: El que voluntariamente transmitiere a distancia entre dependencias oficiales un texto del que resulte un documento infiel, incurrirá en los delitos previstos por los artículos 236 a 239 del Código Pernal, según corresponda (art.120 de la Ley N° 16.002 de fecha 25 d e noviembre de 1988).

11. Decreto N° 312/998

VISTO: el Decreto N° 459/997, de 4 de diciembre de 19 97, por el cual se aprueba la Reformulación de la Estructura Organizativa de la Unidad Ejecutora Dirección Nacional de Aduanas, en el marco del régimen de modernización desregulación y reforma del Estado previsto en los artículos 694° a 707° y siguientes de la Ley N° 16.736, de 5 de enero de 1996 y Decretos Reglamentarios N° 186/996, de 16 de mayo de 1996 y 6 5/998, de 10 de marzo de 1998.

RESULTANDO: I) que el Contrato de Préstamo N° 996/OC -UR, Proyecto de Reforma del Estado, suscrito entre la República Oriental del Uruguay y el Banco Interamericano de Desarrollo, incluye como Sub-Proyecto B:

Modernización de la Administración de las Finanzas Públicas, el Sub-Componente B.2, Administración Aduanera.

II) que en dicho marco se celebró el Convenio de Cooperación Aduanera entre la Superintendencia Nacional de Aduanas del Perú y la Dirección Nacional de Aduanas.

III) que del referido régimen surge la necesidad de modernizar, entre otros aspectos, la estructura operativa de la Dirección Nacional de Aduanas.

IV) que las normas y procedimientos constituyen el marco para la desarrollo de las operaciones aduaneras, por lo que su racionalización y sistematización, son fundamentales para cumplir con las metas de modernización, la que constituye uno de los objetivos del Convenio celebrado entre la República y el Banco Interamericano de Desarrollo.

V) que las herramientas informáticas y de comunicación, aplicadas a los procedimientos racionalizados dentro del marco normativo, son un elemento imprescindible para obtener la agilidad, control y transparencia que requieren los operadores del Comercio Exterior.

CONSIDERANDO: I) que dentro del proceso del proceso racionalizador de las normas y procedimientos, la Dirección Nacional de Aduanas estimó la conveniencia de establecer un único formato estándar para la declaración de las operaciones aduaneras de entrada, salida y tránsito, reduciendo la multiplicidad de los mismos, lo cual constituye una indiscutible mejora tanto para el operador, como para el funcionario que debe efectuar la fiscalización.

II) que para la obtención de la agilidad y seguridad que exige el comercio exterior, se hace preciso integrar bajo la plataforma informática y de comunicaciones, el tratamiento de todas las operaciones aduaneras, la que tendrá como objetivo además facilitar la gestión de la Dirección Nacional de Aduanas, tanto en el aspecto técnico de la fiscalización, como en el del manejo de los recursos puestos a su disposición.



III) que en este sentido se está procediendo a la implantación de un nuevo Sistema Informático (nominado "Lucía"), para el control de las operaciones aduaneras.

ATENCIÓN: a lo expuesto precedentemente, a lo dispuesto en la Ley N° 16.736, de 5 de enero de 1996 y sus reglamentaciones y a lo establecido en el Decreto N° 459/997, de 4 de diciembre de 1997.

EL PRESIDENTE DE LA REPUBLICA

DECRETA:

Artículo 1. La declaración jurada de las mercaderías ante la Dirección Nacional de Aduanas, en las operaciones de entrada, salida y tránsito, se realizará y solicitará por el Declarante, en el Documento Unico Aduanero.

Artículo 2. La Dirección Nacional de Aduanas, atendiendo a situaciones especiales derivadas de la operativa del Comercio Exterior debidamente justificadas, podrá establecer con carácter general, la utilización del Documento Unico Aduanero Simplificado, para la declaración de dichas operaciones.

Artículo 3. La Dirección Nacional de Aduanas determinará los datos e informaciones que debe contener el Documento Unico Aduanero, así como los documentos que deben adjuntarse como justificación de los mismos y que acrediten los elementos de hecho exigibles para la aplicación del régimen aduanero solicitado.

Artículo 4. Las declaraciones aduaneras deberán ser fidedignas y realizarse de conformidad a las informaciones obtenidas de los documentos presentados, los cuales a todos los efectos forman parte integrante de la misma.

Artículo 5. La descripción de la mercadería en la declaración aduanera deberá ser hecha en términos que permitan a la Aduana su identificación y clasificación arancelaria al nivel de la correspondiente Sub-Partida de la

Documentos Electrónicos Firma Digital

Nomenclatura Común del Mercosur. Cuando por aplicación de lo establecido en un Acuerdo Internacional firmado por la República o, en una norma nacional, se establezca una tributación menor a la que correspondería si la operación se sujetara al régimen general aplicable, la descripción de la mercadería se ampliará de tal forma que permita a la Aduana identificarla sin ninguna duda, con el producto al que el Acuerdo o la norma otorga el beneficio correspondiente.

Artículo 6. La Dirección Nacional de Aduanas reglamentará la forma de impresión y presentación del Documento Unico Aduanero y de la Declaración de Valor en Aduanas, incluida la presentación por medios electrónicos. En el uso de la firma electrónica se estará a lo dispuesto en la normativa vigente.

Artículo 7. La intervención del Despachante de Aduana en la operación aduanera y las responsabilidades derivadas de ella que no le sean directamente imputables, quedarán respaldadas por la firma del importador, exportador o remitente de la Declaración Jurada de Responsabilidad, la que presentará junto a la declaración aduanera, en tanto no se haga uso de la firma electrónica.

Artículo 8. Ante las necesidades actuales y futuras de intercambio de información entre las distintas Autoridades Aduaneras, la Dirección Nacional de Aduanas propenderá a la introducción de criterios de estandarización internacional, en los mensajes electrónicos de intercambio de información.

Artículo 9. Los procedimientos aprobados por la Dirección Nacional de Aduanas serán informatizados en la medida en que sea posible. Cualquier actuación establecida en el procedimiento que realicen funcionarios sobre la Aplicación Informática de la Aduana, tendrá un efecto jurídico y probatorio equivalente a la que se venía realizando manualmente sobre los documentos. Será de plena aplicación en la materia lo establecido por el Decreto N° 65/998 citado.

Artículo 10. La Dirección Nacional de Aduanas establecerá, en coordinación con otros Organismos e Instituciones del Estado, los

procedimientos para racionalizar sus actuaciones en la operativa del Comercio Exterior y especialmente en lo que concierne a las autorizaciones que los mismos deben emitir preceptivamente. Los procedimientos aprobados tendrán carácter obligatorio para ambas Instituciones, siempre y cuando lo consientan y serán puestos en conocimiento de los operadores.

Artículo 11. El intercambio de datos de la Dirección Nacional de Aduanas con particulares y Organismos Públicos se hará utilizando las redes de valor agregado homologadas por el Instituto, de acuerdo a las normas técnicas establecidas por el mismo, sin perjuicio de los futuros avances tecnológicos que en el área de la informática o de las comunicaciones se puedan verificar.

Artículo 12. La Dirección Nacional de Aduanas comprobará que el operador está al día en sus obligaciones fiscales con la Dirección General Impositiva, Banco de Seguros del Estado, Banco de Previsión Social y la propia Dirección Nacional de Aduanas, no autorizando la realización de cualquier operación aduanera a aquellos que no estén en dicha situación.

Artículo 13. El pago de los tributos, precios o proventos liquidados en el Documento Unico Aduanero, será hecho efectivo en el lugar, tiempo y forma determinado por la Dirección Nacional de Aduanas, incluso por medios electrónicos.

Artículo 14. Cualquier tributo, precio o provento que se genere con motivo de la realización de las operaciones de entrada, salida o tránsito de las mercaderías, cuya cuantía pueda ser determinada al momento del registro del Documento Unico Aduanero, deberá ser declarado y liquidado en el mismo. En un plazo no superior a doce meses desde la aprobación de la presente norma, la Dirección Nacional de Aduanas establecerá de la presente norma, la Dirección Nacional de Aduanas establecerá de acuerdo con los respectivos Organismos el procedimiento para la declaración, liquidación y recaudación de los montos correspondientes.

Artículo 15. La solicitud para la autorización del fraccionamiento de los conocimientos a que se refiere el artículo 34° del Decreto N° 570/994, puede



ser hecho por vía electrónica, con el formalismo que la Dirección Nacional de Aduanas determine en su reglamentación.

Artículo 16. La selección de las declaraciones por la Aduana para su control parcial (documental o Canal Naranja) o total (comprobación documental, física y análisis de valor, o Canal Rojo), producirá los mismos efectos enunciados en el inciso segundo del artículo 249° de la Ley N° 13.318, para las detenciones de las declaraciones.

Artículo 17. En las declaraciones seleccionadas sin comprobación física y/o documental (Canal Verde) o en aquellas en las que se disponga de la documentación adjunta, por medios electrónicos (Canal Naranja, con documentos capturados y enviados por medios electrónicos –scanner-), la autorización para el desaduanamiento y retiro de la mercadería será hecha por vía electrónica mediante el envío de una contraseña por cada despacho. La contraseña enviada por el Organismo tendrá la misma validez jurídica y probatoria que las firmas autógrafas que sus funcionarios realizan sobre las declaraciones presentadas en papel.

Artículo 18. Para las declaraciones no solicitadas por el Organismo Central de Valoraciones al momento de su presentación, se entiende que la actuación “a priori” de esta Oficina no es preceptiva, aún en el caso de que el Canal de verificación fuese Rojo.

Artículo 19. El desaduanamiento y entrega de la mercadería no impide que dentro del período de prescripción de los tributos, la Dirección Nacional de Aduanas proceda a la revisión de las operaciones aduaneras, poniendo de manifiesto las irregularidades que detecte y tomando las acciones legales y judiciales correspondientes, sin que ello implique responsabilidad para el Organismo por el desaduanamiento efectuado, salvo que se probara fehacientemente la complicidad del mismo en la maniobra.

Artículo 20. El declarante concurrirá al despacho de la mercadería en el lugar en que se encuentre dentro de los cinco días hábiles siguientes a la presentación de la declaración en la Aduana. La falta de concurrencia facultará

al funcionario para actuar de oficio, sin que pueda admitirse posteriormente reclamo alguno del declarante por los derechos que hubiese dejado de ejercer.

Artículo 21. En las operaciones de tránsito de mercaderías, la Agencia de Transporte encargada del traslado de la mercadería será responsable del buen término de la operación de la mercadería declarada en la Aduana de destino, en el horario establecido, con los precintos impuestos sobre el medio de transporte intactos y cumpliendo el resto de requisitos inherentes a la operación de tránsito.

Artículo 22. Al efecto de la declaración y control de las operaciones de abastecimiento de naves y aeronaves con mercadería nacional, las mismas tendrán la consideración de operaciones asimiladas a la Exportación, siguiendo los procedimientos comunes, especiales o simplificados que la Dirección Nacional de Aduanas establezca.

Artículo 23. Derogado por Decreto N° 479/001 de 4/12/ 2001 artículo 5°.

Artículo 24. Derogado Decreto N° 479/001 de 4/12/2001 artículo 5.

Artículo 25. En la Exportación, cuando el medio de transporte en el cual van a salir las mercaderías del territorio aduanero, tuviere mayor capacidad que la de los medios de transporte en los que se presenta la mercadería a despacho ante la Aduana, se permitirá la realización de embarques parciales en dicho medio de transporte de las mercaderías incluidas en un mismo Documento Unico Aduanero.

Artículo 26. Cualquier referencia de la normativa vigente a Documento Unico de Importación o permiso de importación en las operaciones de Importación o Admisión Temporal o a Documento Unico de Exportación o permiso de exportación en las operaciones de Exportación, se entenderán hechas al Documento Unico Aduanero.

Artículo 27. La Dirección Nacional de Aduanas establecerá los procedimientos operativos que deben cumplir los Agentes Privados de Interés Público y los demás operadores relacionados con las operaciones aduaneras.

Artículo 28. Deróganse el artículo 8 del Decreto 756/968, de 18 de diciembre de 1968, los artículos 1º, 2º y 3º del Decreto N° 475/976, de 29 de julio de 1976, los artículos 2º y 3º del Decreto N° 565/994, de 29 de diciembre de 1994 y los artículos 2º y 7º del Decreto N° 477/995, de 29 de diciembre de 1995.

Artículo 29. Este decreto entrará en vigencia a partir de su publicación.

Artículo 30. Comuníquese, publíquese, etc.

12. Ley N° 17243

Sección 3ª

Sistema informático del Estado

Artículo 24. El Estado, los Entes Autónomos y los Servicios Descentralizados deberán implantar el expediente electrónico para la sustanciación de todas las actuaciones administrativas. A tal efecto dispondrán los actos jurídicos y operaciones materiales tendientes al cumplimiento de esta norma en el menor tiempo posible, dando cuenta a la Asamblea General.

El expediente electrónico es la serie ordenada de documentos registrados por vía informática, provenientes de la Administración o de terceros, tendientes a la formación de la voluntad administrativa en un asunto determinado, teniendo la misma validez jurídica y probatoria que el expediente tradicional.

Artículo 25. Autorízase en todo caso la firma electrónica y la firma digital, las que tendrán idéntica validez y eficacia a la firma autógrafa, siempre que estén debidamente autenticadas por claves u otros procedimientos seguros, de acuerdo a la tecnología informática.

La prestación de servicios de certificación no estará sujeta a autorización previa y se realizará en régimen de libre competencia, sin que ello implique sustituir o modificar las normas que regulan las funciones que corresponde realizar a las personas facultadas para dar fe pública o intervenir en documentos públicos.

Artículo 26. Los Gobiernos Departamentales podrán aplicar lo dispuesto en los dos artículos anteriores dando cuenta a sus respectivas Juntas Departamentales.

Artículo 27. Los actos administrativos y las órdenes de compra que adjudiquen la contratación de bienes o servicios, deberán estar acompañados de una constancia emitida por el Sistema Integrado de Información Financiera del Estado, que certifique la existencia de crédito suficiente para atender la erogación resultante. El Ministerio de Economía y Finanzas establecerá las formalidades requeridas para la emisión de la constancia.

El acto administrativo o la orden de compra deberán hacer referencia a la existencia de la referida constancia, debiendo incluir los datos identificatorios de la misma.

Los proveedores adjudicatarios, previo a la entrega de los bienes o a la prestación de los servicios, deberán exigir a la Administración la vía correspondiente de la constancia de existencia de crédito suficiente.

Las contrataciones que contravengan esta disposición son nulas (artículo 8º del Código Civil).

Las disposiciones de este artículo comprenden las adquisiciones de bienes y servicios realizadas por las unidades ejecutoras de los Incisos 02 al 15 del Presupuesto Nacional por montos superiores al límite de la contratación directa. Facúltase al Poder Ejecutivo a extender este régimen a las contrataciones efectuadas al amparo de lo dispuesto por el numeral 2) del inciso segundo del artículo 33 del TOCAF.

13. Ley Nº 17.292

SECCION XI

ZONAS FRANCAS

Artículo 65. Sustitúyese el ARTÍCULO 2º DE LA IEY nº 15.921, de 17 de diciembre de 1987, por el siguientes:

"ARTICULO 2º.- Las zonas francas son áreas del territorio nacional de propiedad pública o privada, cercadas y aisladas eficientemente, las que serán determinadas por el Poder Ejecutivo previo asesoramiento de la Comisión Honoraria Asesora de Zonas Francas, con el fin de que se desarrollen en ellas con las exenciones tributarias y demás beneficios que se detallan en la presente ley, toda clase de actividades industriales, comerciales o de servicios y entre ellas:

A) Comercialización de bienes, excepto los referidos en el artículo 47 de la presente ley, depósito, almacenamiento, acondicionamiento, selección, clasificación, fraccionamiento, armado, desarmado, manipulación o mezcla de mercancías o materias primas de procedencia extranjera o nacional. En todo caso que se produzca el ingreso de los bienes al territorio político nacional, será de estricta aplicación a lo dispuesto en el artículo 36 de la presente ley.

B) Instalación y funcionamiento de establecimientos fabriles.

C) Prestación de todo tipo de servicios, no restringidos por la normativa nacional, tanto dentro de la zona franca como desde ella a terceros países.

Asimismo, los usuarios de zonas francas podrán brindar los siguientes servicios telefónicos o informáticos desde zonas francas hacia el territorio nacional no franco, respetando los monopolios, exclusividades estatales y/o concesiones públicas:

Documentos Electrónicos Firma Digital

1) Centro Internacional de llamadas (International Call Centers), excluyéndose aquellos que tengan como único o principal destino el territorio nacional.

2) Casillas de correo electrónico.

3) Educación a distancia.

4) Emisión de certificados de firma electrónica.

Los servicios que anteceden recibirán el mismo tratamiento tributario que los servicios prestados desde el exterior ya sea en lo que refiere el prestador, así como a la deducibilidad del mismo por el prestatario.

D) Otras que, a juicio del Poder Ejecutivo, resultaren beneficiosos para la economía nacional o para la integración económica y social de los Estados.

En caso de que por este medio se habilite la prestación de nuevos servicios desde zona franca hacia el territorio no franco, los mismos estarán alcanzados por el régimen tributario vigente al momento de la habilitación, pudiendo establecerse el mismo en base a regímenes de retención de impuestos con carácter definitivo, de acuerdo a lo que establezca el Poder Ejecutivo.

El Poder Ejecutivo adoptará las medidas necesarias, a efectos de que estas actividades no perjudiquen la capacidad competitiva o exportadora de las empresas ya instaladas en zona no franca.

La Administración Nacional de Telecomunicaciones no podrá fijar tarifas diferenciales para los servicios de telecomunicaciones fundadas en la distancia entre Montevideo y el lugar en que se encuentre emplazada la zona franca, siendo de recibo diferencias basadas en otros motivos, como ser, volumen o tráfico."

14. Decreto N° 83/001

Visto: Lo dispuesto en el artículo 15 del Decreto N° 65/998 de 10 de marzo de 1998.

Resultando: I) que la citada norma encomendó al Poder Ejecutivo, con el asesoramiento de la Oficina Nacional del Servicio Civil, de la Comisión Nacional de informática y del Grupo Técnico Asesor en sus respectivas competencias, la determinación periódica de los medios técnicos de almacenamiento, reproducción y transmisión telemática de documentos. II) que en cumplimiento de dicha disposición, la Oficina Nacional del Servicio Civil, la Comisión Nacional de Informática y el Grupo Técnico Asesor, realizaron una serie de estudios de investigación con el objetivo de establecer la situación actual de las tecnologías de almacenamiento de información y su relación con la realidad y perspectivas de la Administración Pública uruguaya.

Considerando: I) que los medios de almacenamiento que el Poder Ejecutivo determine, deben asegurar una adecuada protección contra la pérdida o adulteración de la información almacenada, reproducida y/o transmitida; II) que de la investigación realizada surgió la inexistencia de estándares nacionales o internacionales que establezcan la estabilidad o la vida útil de los medios ópticos de almacenamiento digital de la información, de forma de asegurar el grado de eficacia de los mismos; III) que la tecnología de almacenamiento es esencialmente dinámica y por tanto requiere el estudio permanente de las herramientas disponibles, teniendo en cuenta consideraciones técnicas, económicas y estratégicas; IV) que a efectos de lograr la actualización periódica de las nuevas tecnologías, así como del material necesario para la toma de decisiones por parte de los organismos estatales, se entiende pertinente su publicación en el sitio de Internet de la Oficina Nacional del Servicio Civil; V) que se entiende oportuna la inclusión de recomendaciones que permitan a los centros de Cómputos de los distintos organismos del Estado, implementar medidas de seguridad y resguardo de la información, en especial para los archivos de documentos electrónicos que no

Documentos Electrónicos Firma Digital

cuenten con el correspondiente respaldo en papel; VI) que se considera necesario destacar la importancia de la calidad de los medios físicos a emplearse como soporte de los documentos almacenados a largo plazo, así como de las técnicas de control de calidad en el proceso de grabado y del monitoreo periódico de la calidad de lectura de las copias, con el objetivo de asegurar la recuperación de la información; VII) que en virtud de que los documentos electrónicos son conjuntos de datos digitales generados ya sea por vía de software específico o de software de gran divulgación, se establece la necesidad de almacenar no sólo los datos que conforman los documentos electrónicos, sino también el software empleado, de forma de acceder a los mismos desde sus propios archivos; VIII) que de las conclusiones de la investigación realizada por la Oficina Nacional del Servicio Civil, la Comisión Nacional de Informática y el Grupo Técnico Asesor, se desprende que ninguna tecnología es cien por ciento confiable o segura, por lo que se recomienda el empleo de tecnologías mixtas, combinadas de acuerdo con las necesidades de cada Organismo.

Atento: a lo precedentemente expuesto, a lo informado por la Oficina Nacional Del Servicio Civil y el grupo Técnico Asesor, y a lo dispuesto por el artículo 15 del Decreto N° 65/998 de 10 de marzo de 1 998:

EL PRESIDENTE DE LA REPÚBLICA

Actuando en consejo de Ministros

DECRETA:

Artículo 1. Los medios de almacenamiento de documentos electrónicos a mediano y largo plazo, podrán seleccionarse de la siguiente lista:

* Discos de Video Digital sólo de lectura (conocidos por sus siglas en inglés DVD-R "digital Video Disc Recordable")

* Discos Magneto Ópticos de escritura única y lectura múltiple (conocidos por sus siglas en inglés MO-WORM "Magneto Optical Disc Write Once Read Many")

Documentos Electrónicos Firma Digital

* Discos compactos de escritura única y lectura múltiple (conocido por sus siglas en inglés CD-R "Compact Disc Recordable").

Artículo 2. Los medios de soporte de la tecnología a emplearse deberán contar con la certificación de calidad ISO y deberán tener una vida útil mínima de 20 años. El control de calidad de dichos medios será responsabilidad de los Centros de Cómputos de cada organismo del Estado.

Artículo 3. Los registros de documentos electrónicos realizados a través de la utilización de alguno de los medios indicados en el artículo 1° del presente Decreto, deberán efectuarse en un mínimo de dos copias. Deberá emplearse siempre la misma copia para el uso periódico, quedando las restantes como archivo muerto. El archivo muerto deberá ubicarse en un lugar físico diferente al de la copia de uso periódico, asegurando sus condiciones de preservación.

Artículo 4. Será cometido de cada organismo del Estado la determinación del plazo para el registro de los documentos a través de alguno de los medios técnicos de almacenamiento previstos en el artículo 1° del presente decreto.

Artículo 5. La Oficina Nacional del Servicio Civil publicará en Internet y mantendrá actualizadas las recomendaciones necesarias, así como toda otra información que considere relevante o de utilidad que se relacione con el uso de estos medios. Asimismo, incorporará nuevas tecnologías, con el previo informe favorable de la comisión Nacional de Informática y del Grupo Técnico Asesor, de conformidad con los cometidos asignados en el Decreto N°. 65/9998 de 20 de marzo de 1998.

Artículo 6. El proceso de copiado de los documentos a los medios citados, deberá contar con una etapa previa de control de calidad, en la que se registrará la fecha y la hora del control, así como el nombre, apellido, documento de identidad y la firma digital o contraseña del funcionario responsable de dicho cometido.

Documentos Electrónicos Firma Digital

Artículo 7. A efectos del almacenamiento de documentos electrónicos a corto plazo, podrá utilizarse cualquier dispositivo de uso corriente en los equipos informáticos disponibles en cada organismo del Estado, debiendo contar los mismos con el correspondiente respaldo de acuerdo con las medidas de seguridad oportunamente adoptadas por los distintos Centros de Cómputos. El almacenamiento de dichos respaldos deberá realizarse de forma que asegure su protección e inalterabilidad y en lugares físicos alejados de los centros de procesamiento de la información.

Respaldo del software de acceso a los documentos

Artículo 8. Deberán almacenarse por lo menos dos copias de todas las herramientas de software necesarias para acceder a los mismos, junto con los datos almacenados en los medios descritos en el artículo 1° de este Decreto, excepto en el caso de que éstos fueran almacenados en formato estándar, tales como el formato ASCII (American Standard Code For Information Interchange), TIFF (Tagged Image File Format) o HTML (Hiper Text Markup Language)

Control de vida útil

Artículo 9. Los Organismos deberán controlar cada dos o tres años la estabilidad de la información almacenada, a través de muestreos estadísticos sobre medios que contengan datos almacenados desde un período no menor a dos años y luego de transcurridos por lo menos dos años desde el último control. Las muestras deberán ser representativas de los medios empleados, teniendo en cuenta el proveedor del medio y las condiciones de almacenamiento.

Artículo 10. Cuando se detecten deterioros o pérdida de la información, deberá recurrirse a las copias de respaldo - según se haya procedido de conformidad con lo establecido en el artículo 3° del presente Decreto - y generar una nueva copia de respaldo.

Artículo 11. Cumplido el 75% de la vida útil del medio de almacenamiento empleado, de conformidad con la certificación de las características técnicas de cada uno, deberá transferirse la información allí contenida a otro medio de almacenamiento que cumpla con los requisitos de seguridad e inalterabilidad que aseguren la calidad de la tecnología escogida.

Control de los cambios de la tecnología

Artículo 12. Cada organismo del Estado deberá contar con más de un dispositivo de lectura (hardware y software) para cada tipo de tecnología empleada, a fin de asegurar el acceso a la información almacenada. Dicho equipamiento deberá permitir la migración de los datos contenidos a un medio de almacenamiento temporal, a efectos de permitir la migración hacia nuevas tecnologías de almacenamiento.

Artículo 13. Los organismos estatales deberán asegurar en forma permanente el buen funcionamiento de los dispositivos de lectura de los medios empleados, atendiendo especialmente al posible desuso de los mismos, en cuyo caso, si es necesario, deberá establecerse en forma eficiente y prematura una migración de los documentos hacia otra tecnología.

Artículo 14. Cuando se adopte una nueva tecnología de almacenamiento, la misma deberá permitir la migración de los datos existentes de forma confiable y económica, previniéndose respecto de la posible pérdida de calidad, o bien, optar por la selección de otra tecnología compatible con la actual que involucre mejoras comparativas. La nueva tecnología deberá contar, además, con el aval de la Oficina Nacional del Servicio Civil y de la Comisión Nacional de Informática. Cada organismo deberá establecer mecanismos de migración para un eventual traspaso de la información de una tecnología a la otra, en caso de que no sean compatibles o de que se verifique el desuso de la actual.

Artículo 15. Se recomienda la duplicación de la información en distintas tecnologías a efectos de una mayor seguridad, en especial para el caso de



documentos que por su importancia requieran mayores exigencias en cuanto a su preservación.

Penalidades

Artículo 16. Serán de aplicación las disposiciones contenidas en los artículos 25 y 26 del Decreto N°65/998 de 20 de marzo de 1998.

Artículo 17. Comuníquese, publíquese, etc.

15. Decreto N° 382/003

VISTO: lo dispuesto por los artículos 129 de la Ley 16.002 de 24 de noviembre de 1988, los artículos 694 a 697 de la Ley 16.736 de 5 de enero de 1996 y el artículo 25 de la Ley 17.243 de 29 de junio de 2000, en cuanto prevén el uso de medios informáticos y telemáticos.

RESULTANDO: Que con la sanción del artículo 25 de la Ley 17.243 se reconoce el empleo de la firma digital y su eficacia jurídica para otorgar seguridad a las transacciones electrónicas, promoviendo el comercio electrónico seguro, de modo de permitir la identificación en forma confiable de las personas que realicen transacciones electrónicas.

Que asimismo, la sanción del artículo 129 de la ley 16.002 y de los artículos 694 a 697 de la ley N° 16.736 impulsa la progresiva despapelización del Estado, contribuyendo a mejorar su gestión, facilitar el acceso de la comunidad a la información y posibilitar la realización de trámites por Internet de forma segura.

CONSIDERANDO: Que resulta conveniente reglamentar las disposiciones legales precitadas.

ATENTO: a lo precedentemente expuesto y a lo dispuesto por el artículo 168 numeral 4° de la Constitución de la República.

EL PRESIDENTE DE LA REPÚBLICA



Actuando en Consejo de Ministros

DECRETA:

Artículo 1. El presente decreto reglamenta el uso de la firma digital y el reconocimiento de su eficacia jurídica.

Artículo 2. Definiciones.- A los efectos de este Decreto, se establecen las siguientes definiciones:

a) Firma Digital es el resultado de aplicar a un documento un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, de manera tal que dicha verificación permita, simultáneamente, identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

b) Prestador de servicios de certificación es una tercera parte que expide certificados digitales, pudiendo prestar además, otros servicios relacionados con la firma digital.

c) Certificado Digital es un documento digital firmado digitalmente por un Prestador de servicios de certificación, que vincula la identidad del titular del mismo con una clave pública y su correspondiente clave privada.

d) Clave Privada es la clave generada por un proceso matemático, que contiene datos únicos que el firmante utiliza para crear la firma digital. Su conocimiento y control es exclusivo del firmante. Si el firmante decidiera compartirla, se imputará como suyo todo aquello que fuera realizado mediante el uso de la misma.

e) Clave pública es aquella clave generada por el mismo proceso matemático que genera la clave privada. Contiene datos únicos que permiten verificar la firma digital del firmante. Su conocimiento es público.

f) Lista de Certificados Revocados de un prestador de servicios de certificación es un archivo firmado digitalmente por éste, en el que constan los



números de serie y fecha de revocación de todos los certificados revocados del Prestador de servicios de certificación.

g) Firmante o Signatario, es la persona física que cuenta con un Certificado Digital que utiliza para firmar digitalmente.

h) Periodo de Validez, es el período de vigencia del Certificado Digital.

Artículo 3. Validez y eficacia de la firma digital.- La firma digital tendrá idéntica validez y eficacia a la firma autógrafa, siempre que esté debidamente autenticada por claves u otros procedimientos seguros de acuerdo a la tecnología informática que:

1. garanticen que la firma digital se corresponde con el certificado digital emitido por un prestador de servicios de certificación de firma digital, que lo asocia con la identificación del signatario;

2. aseguren que la firma digital se corresponde con el documento respectivo y que el mismo no fue alterado ni pueda ser repudiado; y

3. garanticen que la firma digital ha sido creada usando medios que el signatario mantiene bajo su exclusivo control y durante la vigencia del certificado digital.

Artículo 4. Valor probatorio de la firma digital.- La firma digital tendrá respecto al documento respectivo, idéntico valor probatorio al que tiene la firma manuscrita con respecto al documento consignado en papel, siempre que la misma haya sido creada mediante mecanismos de clave pública y privada u otros procedimientos acordes a la evolución de estándares tecnológicos internacionalmente reconocidos como fiables que cumplan con las exigencias establecidas en el artículo precedente. .

Artículo 5. Requisitos del Certificado Digital.- El Certificado Digital del firmante deberá cumplir con los siguientes requisitos:

1. Contar como mínimo con la siguiente información del titular del certificado:

Documentos Electrónicos Firma Digital

- a. Nombre completo tal como aparece en el documento de identidad.
 - b. Número, tipo y país emisor del documento de identidad
 - c. La clave pública asociada a la clave privada.
2. Número de serie.
 3. Identificación del prestador de servicios de certificación.
 4. Período de validez.
 5. Firma Digital del prestador de servicios de certificación.
 6. Debe estar vigente.
 7. No debe estar revocado a la fecha de la firma.
 8. Haber sido creado de acuerdo a las políticas del prestador de servicios de certificación que cumplan con lo establecido en el artículo 6.

Artículo 6. Requisitos de emisión del Certificado Digital.- Los requisitos para la emisión de Certificados Digitales serán los siguientes:

a) Presencia física del solicitante del certificado con documento de identidad vigente y válido en la República Oriental del Uruguay.

b) Un contrato en soporte papel, con fecha de emisión, en el que se consigna la información exacta trasladada de la documentación presentada firmado en forma manuscrita en el que deberá constar:

I) Responsabilidades del Solicitante respecto de la clave Privada cuya clave pública correspondiente se consigna en el certificado y todos los usos que a la misma se le dieran.

II) Declaración del solicitante de su total conocimiento y aceptación de la Declaración de Prácticas de Certificación y/o Política de Certificación correspondientes al certificado solicitado.



III) Responsabilidades del solicitante y del prestador de servicios de certificación respecto a la solicitud de revocación de un certificado, consignando plazos de responsabilidad.

c) Generar la clave privada cuya clave pública correspondiente se consignará en el certificado.

Artículo 7. Cese de actividades del prestador de servicios de certificación.- Si el prestador de servicios de certificación cesara sus actividades está obligado a comunicar dicha situación a través del Diario Oficial y cualquier otro medio que considere pertinente, a mantener o derivar el servicio de recepción de solicitudes de revocación y a actualizar y publicar la Lista de Certificados Revocados hasta que haya vencido el último de los certificados emitidos.

Artículo 8. Actualización y publicación de la Lista de certificados Revocados.- El prestador de servicios de certificación deberá actualizar y publicar la Lista de Certificados Revocados al menos cada 24 horas.

Artículo 9. Equivalencia de certificados.- Los certificados que expidan los prestadores de servicios de certificación establecidos en otros Estados, de acuerdo con su respectiva legislación, se considerarán equivalentes a los expedidos por los establecidos en la República, siempre que los mismos hayan sido emitidos con garantías de confiabilidad similares a las exigidas por este decreto, y que exista reciprocidad del país de origen con respecto de los certificados emitidos en el Uruguay

Artículo 10. Comuníquese, publíquese, etc.-

16. Decreto N° 392/003

Artículo 10. Las empresas exportadoras (industrializadoras o no), previo a cada embarque, deberán depositar el monto de la retención del 5% correspondiente a cada operación de exportación en la cuenta que a tales



efectos se abrirá en el BROU, con el nombre MGAP/FFRAA, anexando la siguiente información: el volumen exportado, el precio declarado por los productos comprendidos en dicho documento, y el agente financiero a través del que se percibirá el producido de cada negociación de venta cursada.

Al recibo de cada pago realizado por las empresas o productores exportadores, el BROU expedirá un certificado en dos vías (una dirigida a la Dirección Nacional de Aduanas y otra a la Comisión de Contralor del FFRAA creada por el Art. 8º de la ley Nº 17.663, de 11 de julio de 2003), en el que se detallará la exportación a la que corresponde la retención y el importe efectivamente depositado. El BROU podrá sustituir, una o ambas vías de este certificado, por el documento electrónico que se considere adecuado.

La Dirección Nacional de Aduanas no aprobará ni numerará el Documento Unico de Exportación (DUA) correspondiente a exportaciones comprendidas en el Art. 2º de este decreto, ni permitirá que se cursen de ningún modo exportaciones de arroz alcanzadas por el Art. 2º de la ley Nº 17.663, de 11 de Julio de 2003, sin constatar, previamente, que el exportador haya abonado la retención correspondiente en la cuenta del MGAP/FFRAA, cuya apertura se ha dispuesto en el BROU.

En caso de anulación o cumplimiento parcial de una exportación, una vez recibida la información oficial de la Dirección Nacional de Aduanas, el BROU podrá aceptar que las retenciones pagadas en exceso sean consideradas como pagos de nuevas exportaciones del productor o empresa exportadora.

17. Decreto Nº 396/003

VISTO: la necesidad de reglamentar algunos aspectos referidos al manejo electrónico de información personal por parte de las instituciones asistenciales públicas y privadas;

RESULTANDO:



I) que por resolución de 17 de noviembre de 2000, a iniciativa de la Dirección General de la Salud, se creó un Grupo de Trabajo con el cometido de definir pautas relativas a integridad de datos, autenticación, disponibilidad de la información, conservación de la misma y transmisión por Internet u otros medios;

II) que dicho Grupo de Trabajo se ha expedido sugiriendo la adopción de una serie de normas mínimas que contemplen equilibradamente los derechos fundamentales de cada persona y el interés colectivo comprometido en la preservación de la higiene pública;

CONSIDERANDO:

I) que nuestro país ha reconocido tempranamente que los registros médicos llevados en ficha o historia clínica, en forma electrónica u otra, constituirán, de por sí, documentación auténtica y harán plena fe de su contenido a todos sus efectos (artículo 17 del Decreto N° 258/992 de 9 de junio de 1992, extendido por el Decreto N° 204/001 de 23 de mayo de 2001);

II) que es conveniente avanzar en la regulación jurídica del tema, siguiendo las recomendaciones del Grupo de Trabajo;

ATENTO: a lo precedentemente expuesto y a lo establecido en los artículos 72 y 168 de la Constitución de la República y en la Ley N° 9.202 de 12 de enero de 1934;

EL PRESIDENTE DE LA REPÚBLICA

D E C R E T A:

Capítulo I

Disposiciones Generales

Artículo 1. Declárase de interés público el establecimiento de la historia clínica electrónica única de cada persona, desde el registro perinatal hasta el fallecimiento.

Documentos Electrónicos Firma Digital

A los efectos de este Decreto, se entiende por historia clínica electrónica el conjunto de datos clínicos, sociales y financieros referidos a la salud de una persona, procesados a través de medios informáticos o telemáticos.

Artículo 2. A fin de lograr la máxima integración de la información relativa a cada persona, todas las instituciones de asistencia médica, públicas o privadas, particulares o colectivas, deberán mantener los datos respectivos, poniéndolos a disposición del titular de los mismos y de los profesionales de la salud que estén directamente implicados en el diagnóstico y tratamiento del mismo.

Artículo 3. Declárase, en concordancia con lo establecido en los artículos 129 y 130 de la Ley N° 16.002 de 25 de noviembre de 1998 y en el artículo 697 de la Ley N° 16.736 de 5 de enero de 1996, que toda historia clínica en medio electrónico constituye documentación auténtica y como tal, será válida y admisible como medio probatorio, haciendo plena fe a todos los efectos, siempre que esté debidamente autenticada.

Artículo 4. Declárase, en concordancia con lo establecido en el artículo 695, inc. 3° de la Ley N° 16.736 de 5 de enero de 1996 y en el artículo 25 de la Ley N° 17.243 de 29 de junio de 2000, que se considerará debidamente autenticada toda historia clínica en medio electrónico cuyo contenido esté validado por una o más firmas electrónicas mediante claves u otras técnicas seguras de acuerdo al estado de la tecnología informática.

Artículo 5. A efectos de dotar de seguridad a las historias clínicas electrónicas, será de responsabilidad de cada institución de asistencia médica, pública o privada, particular o colectiva, determinar las formas y procedimientos de administración y custodia de las claves de acceso y demás técnicas que se usen.

Artículo 6. La divulgación de la clave o contraseña personal de cualquier sujeto que disponga de la misma, constituirá falta gravísima, aún cuando la clave o contraseña no llegase a ser utilizada.

Artículo 7. A fin de alcanzar el objetivo de la historia clínica electrónica única de cada persona y de propender a la compatibilidad de las bases de datos, se deberán tener en cuenta los estándares incluidos en el Anexo al presente Decreto, cuyo contenido se considera parte integrante del mismo, sin perjuicio de las adecuaciones y complementos que disponga la Comisión a que refiere el artículo 19 de este reglamento.

Capítulo II

Principios y objetivos

Artículo 8. El sistema de historia clínica electrónica única de cada persona, deberá ajustarse en todo momento a los siguientes principios generales:

- a) finalidad;
- b) veracidad;
- c) confidencialidad;
- d) accesibilidad y;
- e) titularidad particular.

Dichos principios generales servirán también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de las disposiciones pertinentes.

Artículo 9. De acuerdo al principio de finalidad, los datos consignados en la historia clínica no podrán ser usados en forma nominada para otros fines que no sean los asistenciales. En su mérito, los datos relativos a la salud de la persona se consideran personales y sensibles, por lo que no podrán ser objeto de tratamiento nominado alguno por medios informáticos o telemáticos, a menos que medie para ello expreso consentimiento informado del interesado.

Artículo 10. El principio de veracidad impone incluir en la historia clínica electrónica todos los procedimientos, sean diagnósticos o terapéuticos, que se

indiquen al paciente, incluyendo la semiología realizada, la evolución del caso y todo otro dato referencial o gráfico que permita conocer la situación real del sujeto de que se trate.

La información contenida en la historia clínica electrónica deberá exponerse en forma inteligible para el paciente y no podrá ser alterada sin que quede registrada la modificación de que se trate, aún en el caso de que ella tuviera por objeto subsanar un error.

Artículo 11. El principio de confidencialidad obliga a tratar los datos relativos a la salud de la persona con la más absoluta reserva.

A tal efecto, la historia clínica electrónica deberá contar con una estructuración que separe la información de identificación del titular del resto de los datos consignados, pudiendo asociarse ambas únicamente en el ámbito de la atención médica del titular de la historia clínica.

Artículo 12. Sin perjuicio de lo establecido en la disposición precedente, el principio de confidencialidad podrá ceder: a) frente a la autoridad epidemiológica o judicial, sin otro trámite, b) podrá ser levantado también mediante el expreso consentimiento informado del interesado.

Artículo 13. En aplicación del principio de accesibilidad, el titular de los datos tendrá en todo momento derecho a conocerlos, a que le sean explicados y a que se rectifiquen si fueran probadamente erróneos.

No obstante, en casos excepcionales a juicio del médico tratante y bajo su responsabilidad como parte del proceso de atención, podrán establecerse restricciones parciales o temporales al acceso.

Artículo 14. La información contenida en la historia clínica electrónica deberá exponerse en forma inteligible por el paciente y no podrá ser alterada sin que quede registrada la modificación de que se trate, aún en el caso de que ella tuviera por objeto subsanar un error. Una vez validado, ningún dato de la historia clínica electrónica podrá ser eliminado y en caso de ser necesario su

corrección, se agregará el nuevo dato con la fecha, hora y contraseña del que hizo la corrección, sin suprimir lo corregido.

Artículo 15. Siendo los datos contenidos en la historia clínica electrónica de titularidad de la persona a que refieren, sólo ésta o sus derechos habientes podrán autorizar el uso por terceros de la información total o parcial en ella contenida.

Capítulo III

Normas de aplicación

Artículo 16. La implantación de la historia clínica electrónica única para cada persona no implica la derogación de las disposiciones vigentes en materia de historias y registros clínicos, en cuanto sea compatible con el soporte informático.

Artículo 17. Las instituciones que adopten la historia clínica electrónica, podrán proceder a la destrucción de los registros en soporte papel en las condiciones previstas para hacerlo con las historias clínicas pasivas.

Artículo 18. El cumplimiento de lo previsto en este Decreto será fiscalizado por la repartición competente del Ministerio de Salud Pública y la infracción a sus disposiciones será reprimida de conformidad con la normativa vigente en materia de control de las instituciones asistenciales públicas y privadas.

Artículo 19. Créase una Comisión de estándares uniformizadores de las historias clínicas electrónicas, la que estará integrada por cinco personas designadas por el Ministerio de Salud Pública a propuesta de las siguientes dependencias e instituciones:

- a) la Dirección General de la Salud, cuyo representante la presidirá;
- b) la Dirección General de la Administración de los Servicios de Salud del Estado;
- c) las instituciones de Asistencia Médica Colectiva;



d) los Seguros Parciales y;

e) la Universidad de la República;

Artículo 20. Las instituciones que ya hayan adoptado la historia clínica electrónica antes de la fecha de este Decreto, deberán adecuarse a sus disposiciones en el lapso máximo de seis meses a contar de su vigencia.

Artículo 21. El presente Decreto se aplica a cualquier sub conjunto de la historia clínica electrónica.

Artículo 22. Este Decreto entrará en vigencia el primer día del mes siguiente al de su publicación en el Diario Oficial.

Artículo 23. Comuníquese.

Anexo -Estándares

I. Estándares obligatorios

A. -Categoría: Identificación

A.1.- Subcategoría: Identificación del paciente: Documento de Identidad Nacional (Número de Cédula de Identidad)

A.2.- Subcategoría: Identificación del profesional de la salud con vínculo permanente o bajo contrato incluido en la estructura funcional: Documento de Identidad Nacional (Número de Cédula de Identidad)

A.3.- Subcategoría: Identificación de personas físicas o jurídicas proveedores de servicios asistenciales (Instituciones de Asistencia y profesionales externos sin vínculo con la estructura): RUC- Registro Único de Contribuyentes.

A.4.- Subcategoría: Identificación de proveedores de insumos: RUC -Registro Único de Contribuyentes

B.- Categoría: Intercambio de mensajes: No se define en esta instancia un estándar obligatorio en esta categoría.



C.- Categoría: Contenido y estructura de la historia clínica.

C.1.- Subcategoría: Información Perinatal: Sistema Informático Perinatal
(Centro Latinoamericano de Perinatología -CLAP/OPS/OMS)

D.- Categoría: Codificación y Terminología

D.1.- Subcategoría: Diagnósticos: Clasificación Internacional de
Enfermedades, 10ª Revisión (CIE-10)

E.- Será considerado estándar obligatorio todo aquel que sea definido por
la Comisión de Estándares prevista en el Art. 19º del presente Decreto.

II. Estándares recomendados

A. -Categoría: Identificación: Remitirse a "I. Estándares obligatorios"

B. -Categoría: Intercambio de mensajes

B. 1.- Subcategoría: Información médica: HL 7

B.2.- Subcategoría: Imágenes médicas: DICOM

C.- Categoría: Contenido y estructura de la historia clínica.

C. 1.- Subcategoría: Información Pediátrica: Sistema Informático del Niño
(Centro Latinoamericano de Perinatología -CLAP/OPS/OMS)

INDICE

Índice de contenido

PROLOGO.....	3
CAPITULO I	
INTRODUCCIÓN.....	8
1. Efectos de la Tecnología en la Sociedad.....	9
1.1 El Tiempo.....	9
1.2 El Espacio.....	11
1.3 El Acceso.....	12
2. La respuesta del Derecho al Fenómeno Tecnológico	13
CAPITULO II	
DOCUMENTO TRADICIONAL.....	15
1. Concepto.....	15
2. Evolución Histórica.....	18
3. Clases de Documentos.....	19
3.1 Según los aspectos que reúnen: externos e internos.....	20
3.2 Según los valores del documento: primarios, secundarios y terciarios. .	21
3.3 Según las edades y valores del documento: primera edad, edad intermedia y edad permanente.....	22
3.4 Según el emisor: públicos y privados.....	22

*Documentos Electrónicos
Firma Digital*

4. Caracteres.....23

CAPITULO III

DOCUMENTO ELECTRONICO.....26

1. Concepto.....26

2. Evolución Histórica.....32

3. Clases de Documentos Electrónicos.....37

3.1 Según el soporte: Documentos Electrónicos, Magnéticos, Digitales o Informáticos.....37

3.2 Según la forma en que son transmitidos: Electrónico, Telemático, Vía Telefax o Facsímile.....38

3.3 Según el emisor: Públicos y Privados.....39

4. Caracteres.....39

CAPITULO IV

DERECHO COMPARADO.....41

1. Estados Unidos.....41

1.1 Estado de UTAH.....41

1.2 Ley Federal43

2. Italia.....43

3. Alemania.....44

4. Directiva de la Unión Europea.....45

5. Portugal.....45

*Documentos Electrónicos
Firma Digital*

6. España.....	46
7. Perú.....	47
8. Argentina.....	49
9. Chile.....	52
10. Brasil.....	53
11. Paraguay.....	53
12. Ecuador.....	54
13. Venezuela.....	54
14. México.....	55
15. Cuadro Comparativo entre los Países del MERCOSUR.....	56
15.1 Documento Electrónico.....	56
15.2 Documento Electrónico en los Países Adheridos al MERCOSUR... ..	59
15.3 Firma Electrónica y Digital en los países del MERCOSUR.....	60

CAPITULO V

DERECHO URUGUAYO.....	63
1. Introducción.....	63
2. Código General del Proceso de fecha 18 de octubre de 1988.....	63
3. Ley N° 15921 de fecha 17 de diciembre 1987	65
4. Ley N° 16.002 de fecha 25 de noviembre de 1988.....	66
5. Ley N° 16.060 de fecha 5 de enero de 1990.....	66
6. Decreto N° 500/991 de fecha 27 de setiembre de 1991.....	68

*Documentos Electrónicos
Firma Digital*

7. Ley N° 16.226 de fecha 29 de octubre de 1991.....	71
8. Ley N° 16.713 de fecha 3 de setiembre de 1995.....	72
9. Ley N° 16.736 de fecha 5 de enero de 1996.....	72
10. Decreto N° 65/998 de fecha 10 de marzo de 1998.....	74
11. Decreto N° 312/998 de fecha 3 de noviembre de 1998.....	75
12. Ley N° 17.243 de fecha 29 de junio de 2000.....	76
13. Ley N° 17.292 de fecha 25 de enero de 2001.....	77
14. Decreto N° 83/2001 de fecha 8 de marzo de 2001.....	78
15. Decreto N° 382/2003 de fecha 17 de setiembre de 2003.....	79
16. Decreto N° 392/003 de fecha 26 de setiembre de 2003	80
17. Decreto N° 396/003 de fecha 30 de setiembre de 2003.....	81

CAPITULO VI

FIRMA ELECTRÓNICA Y DIGITAL.....	83
1. Introducción.....	83
2. Firma Ológrafa.....	85
3. Firma Electrónica.....	87
3.1 La Biometría.....	88
3.2 Sistemas de Cifrado.....	89
4. Firma Digital.....	91

CAPITULO VII

*Documentos Electrónicos
Firma Digital*

AUTORIDADES DE CERTIFICACION.....	94
1. Introducción.....	94
2. Componentes de una Infraestructura de Clave Pública.....	95
2.1 Autoridad Certificante Raíz (AC) o Certificate Authority (CA).....	95
2.1.1 Emisión de Certificados.....	96
2.1.2 Mantenimiento de la información y emisión de listas de revocación de certificados (CRL).....	99
2.1.3 Publicación de los certificados no vigentes y de las listas de revocación.....	99
2.1.4 Mantenimiento de Archivos.....	100
2.2 Autoridad de Registro (AR) o Registration Authority (RA).....	101
2.3 Archivo.....	102
3. Los elementos de la PKI.....	102
3.1 Sistema de autenticación.....	102
3.2 Políticas de Certificación.....	103
3.3 Personal Capacitado.....	103
4. Obtención de un Certificado Digital.....	104
5. Actualidad.....	106

CAPITULO VIII

EL NOTARIADO FRENTE A LAS NUEVAS TECNOLOGIAS.....	108
1. Introducción.....	108

*Documentos Electrónicos
Firma Digital*

2. La Función Notarial.....	110
2.1 La Fe Pública	111
2.2 El Deber de Consejo.....	112
2.3 Control de Legalidad	113
2.4 Control de Legitimación.....	114
2.5 Autenticidad.....	114
2.6 Confidencialidad.....	115
2.7 Registro y Conservación.....	116
2.8 Policía Jurídica.....	117
2.9 Control Tributario.....	117
2.10 Internacionalización del Notariado.....	117
3. El Notario frente al Documento Electrónico.....	119
4. Cibernotario y Fedatario Juramentado.....	121
APENDICE NORMATIVO.....	125
1. Código General del Proceso.....	125
2. Ley N° 15921.....	126
3. Ley N° 16.002.....	139
4. Ley N° 16.060.....	140
5. Ley N° 16.170.....	140
6. Decreto N° 500/991.....	141
7. Ley N° 16.226	145
8. Ley N° 16.713.....	146

*Documentos Electrónicos
Firma Digital*

9. Ley N° 16.736.....	146
10. Decreto N° 65/998.....	147
11. Decreto N° 312/998.....	154
12. Ley N° 17243.....	161
13. Ley N° 17.292.....	163
14. Decreto N° 83/001.....	165
15. Decreto N° 382/003.....	170
16. Decreto N° 392/003.....	174
17. Decreto N° 396/003	175
INDICE.....	183