UNIVERSIDAD DE BELGRANO

# Las tesinas de Belgrano

**Facultad de Derecho y Ciencias Sociales**
**Carrera de Abogacía**

## Firma y documento digital. Su desarrollo, teórico, técnico y legislativo.

**Nº 77** **Leonardo Miatello**

**Tutor: Alberto Ize**

**Departamento de Investigación**
Junio 2003

A mis padres y mis hermanas
que me enseñan cada día
el verdadero sentido de la vida.

No te des por vencido ni aún vencido;
No te sientas esclavo ni aún esclavo;
trémulo de pavor, piénsate bravo,
y acomete feroz, ya mal herido.

Ten el tesón del clavo enmohecido,
que ya viejo y ruin vuelve a ser clavo;
no la cobarde intrepidez del pavo
que amaina su plumaje al primer ruido.

Procede como Dios, que nunca llora;
o como Lucifer, que nunca reza;
o como el robledal, cuya grandeza
necesita del agua y no la implora…

¡Que muerda y vocifere, vengadora,
ya rodando en el polvo, tu cabeza!

(Almafuerte)

# Indice

# Capítulo 1. Generalidades

**1. Introducción**

El avance de la ciencia en las últimas décadas, y la gran injerencia que en la vida moderna tienen la informática y las telecomunicaciones han planteado ciertas situaciones que parece menester estudiar.

Este fenómeno, que medido a la luz de los tiempos del derecho es absolutamente nuevo, viene de la mano de un gran cambio que se está gestando en la sociedad y que comenzó en los últimos veinte o treinta años.

Así como con el nacimiento de las máquinas a vapor y el automóvil se revolucionó la forma de mover al mundo, el lanzamiento de la Computadora Personal en el año 1981 de la mano de la empresa IBM (International Business Machine Inc.), cambió las formas de trabajar, comerciar, comunicarse, e inclusive de entretenerse.

Amadas u odiadas, las Computadoras Personales y la Informática en general influyen de manera directa o indirecta en las vidas de cada uno de los habitantes del mundo. Es innegable que se trata de uno de los inventos que más transformaron a las sociedades en todos sus aspectos. Desde un simple entretenimiento, hasta operaciones quirúrgicas transoceánicas por medio de robots, pasando por sistemas de pronósticos de clima, comercio on-line y una infinidad de situaciones imposibles de enumerar, todo ha sido influenciado por el desarrollo increíble la Ciencia Informática y su indisoluble relación con las Telecomunicaciones.

Su cada día mayor capacidad de almacenamiento y procesamiento de datos y las posibilidades de interconexión las ha convertido en un elemento insustituible en las empresas y en los hogares.

Esta apasionante interacción del hombre con las máquinas, y de los hombres entre si a través de los canales de comunicación creados con ellas , han suscitado una serie de situaciones que no son ni fueron ajenas a los hombres de las ciencias del derecho.

**2. Objeto del Trabajo**

Este trabajo pretende plantear de manera conceptual el escenario contextual dónde se ve involucrado el *documento digital*, y de manera inseparable la *firma digital.*

Para ello, buscaremos apoyo en los conceptos tradicionales de instrumento y documento - en su relación de género a especie -, en el concepto de firma ológrafa, en la legislación doméstica y comparada, en la doctrina que se ha desarrollado sobre el documento y la firma digital, en el establecimiento de su necesaria vinculación conceptual, y en la escasa y errática jurisprudencia existente.

Los aspectos técnicos de la materia se abordarán de manera meramente ilustrativa por no ser propios del objeto de este trabajo, se ahondará solamente lo suficiente como para que el lector comprenda la dinámica del mismo.

Lo que pretende de alguna manera este estudio es determinar el contexto dónde el documento y la firma digital operan, teniendo en cuenta que ellos y el derecho positivo vigente se consideran piezas de un mundo que cambia a medida que se actualizan y potencian las tecnologías existentes.

**3. Justificación del estudio**

Todo cambio tecnológico trae aparejado de manera natural la resistencia de quien no lo conoce, no llega a entenderlo, o peor aún, no alcanza a asumirlo como propio de la sociedad en que vive.

Antes de calificar de manera positiva o negativa un cambio de las magnitudes que se está produciendo de la mano del desarrollo frenético de las Ciencias de la Información y las Telecomunicaciones, es menester echar luz sobre el asunto.

Es necesario, conocer las aplicaciones prácticas que el desarrollo de la tecnología puede tener, sin perder de vista el contexto en dónde se producen, para poder de esta manera analizar la influencia que tienen sobre las actividades sociales del hombre, y deducir, prevenir o solucionar los problemas que naturalmente se suscitan.

Sin lugar a dudas, en los últimos 20 años, y con mayor intensidad en el último lustro, se ha transformado el alcance del comercio y de los actos jurídicos que se involucran en el tráfico de mercaderías y servicios. Hemos presenciado en la última década del siglo XX el nacimiento de una nueva sociedad, la Sociedad de la Información y el Conocimiento, y el mundo ha entrado definitivamente en la era digital. La transformación más visible, más allá de la creación de un ilimitado mercado virtual a nivel mundial, se produjo en la manera en que estos actos se instrumentan y pueden llegar a probarse. La gran cantidad de problemas que esto genera, motiva el presente estudio.

Como es costumbre en la historia, el derecho sigue desde atrás los cambios que se producen en la sociedad, tratando de regularlos y estableciendo las soluciones para los problemas que de manera inevitable se producen entre los hombres. Esta vez sin embargo debemos estar atentos a no parcializar el estudio,

pues el cambio que se está gestando merece una recepción multidisciplinaria que tenga por finalidad sentar sólidas bases para el diseño de la infraestructura destinada a soportar de manera coherente e integradora los efectos que estos cambios tendrán sobre la sociedad en su conjunto.

En los últimos tiempos se ha generado en nuestro país y en el mundo legislación, doctrina y jurisprudencia relacionada con el documento y la firma digital que no podemos desconocer y que merecen un estudio que nos permita dilucidar hacia dónde corren las tendencias actuales y si es posible tomar otro rumbo y porqué.

# Capítulo 2
# Base Conceptual Legal y Doctrinaria

**4. Documento e Instrumento**

*a) Concepción tradicional y Concepto*

Desde un punto de vista material, puede decirse que documento e instrumento son cosas, demostrativas de la existencia de negocios o hechos jurídicos[1].

En un sentido amplio, diremos también que documento es toda cosa que sea producto de un acto humano, perceptible con los sentidos de la vista y el tacto, que sirve de prueba histórica indirecta y representativa de un hecho cualquiera.

A priori, podemos establecer entre documento e instrumento, siguiendo doctrina indiscutida, una relación de genero a especie, dónde el instrumento, por ser esencialmente escrito, abarca un ámbito más restringido.

Sintetiza magistralmente el concepto Chiovenda[2], para quien un documento es toda representación material destinada e idónea para reproducir una cierta manifestación del pensamiento. Los instrumentos son una clase especial de documentos pero a ellos deben agregarse las demás cosas también representativas (planos, cuadros, películas cinematográficas, discos, cintas grabadas, etcétera).

*b) Elemento Material*

Hemos dicho que desde el punto de vista material, tanto el documento como el instrumento son cosas, con lo cual no podemos dejar de considerar cuales son los materiales aptos para ser considerados soporte de un documento o instrumento.

Nuestro pensamiento, influenciado por siglos de historia, nos lleva a pensar naturalmente en el papel. Este es el soporte “natural” de los instrumentos y por ende de los documentos. Era el elemento más común al momento de la redacción de los códigos decimonónicos, entre los cuales incluimos a la obra de Vélez Sarsfield.

De todos modos, debemos pensar también que esto no siempre fue así, y debemos permitirnos arriesgar que tal vez no será siempre así.

Efectivamente, el soporte de los documentos fue adaptándose al desarrollo tecnológico del momento. Así durante mucho tiempo el soporte de los documentos fueron tablillas de arcilla, de cera, papiros o pergaminos. Podemos decir sin temor a equivocarnos, que la elección del soporte depende de la abundancia del elemento con el que está materializado y de su utilidad y ductilidad para alcanzar el propósito perseguido. Nada impide además que en la confección de un instrumento, se utilicen maquinarias. La escritura de por sí es un hecho tecnológico tan complejo como una grabación magnetofónica o el almacenamiento magnético u óptico de información.

*c) Clasificaciones*

Prácticamente de manera unánime la doctrina ha convenido en clasificar a los instrumentos, en públicos y privados. Sin embargo, por diferencias en la redacción en nuestro Código Civil, algunos autores han propuesto como una clasificación más acertada, la división entre instrumentos públicos e instrumentos particulares.

Quienes adscriben a la primera clasificación, seguramente han tenido en cuenta el Título 5 (De los Instrumentos Públicos) de la Sección Segunda (De los hechos y actos jurídicos que producen la adquisición, modificación transferencia o extinción de los derechos y obligaciones) del Libro Segundo (De los derechos personales en las relaciones civiles) del código de fondo dónde, en el texto del título y en varios Artículos, se hace referencia al instrumento privado (v.gr. Artículos 1013, 1015, 1027, 1029, 10311034, 1035)

1. RIVERA, Julio Cesar, “Instituciones del Derecho Civil” Tº II, Pág. 636, Ed. Abeledo Perrot (reimpresión año 1994)
2. ARAZI, ROLAD Y FENOCHIETTO, CARLOS, “Régimen del Código Procesal Civil y Comercial de la Nación”, Pág. 338, Ed. Astrea.

Por otra parte, los seguidores de la segunda clasificación, apoyan su postura en la letra del Artículo 978 (... La expresión por escrito puede tener lugar, o por instrumento público o por instrumentos particulares...), Artículo 1188 (... Los contratos que debiendo ser hechos por instrumento público o particular...), Artículo 1190 (... Los contratos se prueban..., ... Por instrumento público..., ... Por instrumentos particulares firmados o no firmados...)

Sin adherir expresamente a ninguna de las posturas reseñadas, por no ser el objeto de este trabajo, pasaremos ahora a las consideraciones pertinentes sobre cada tipo de instrumento.

*Instrumento público*

De manera preliminar podemos decir que es instrumento público, aquel efectuado por o ante un oficial público facultado por el Estado para dar fe de los actos que realiza o que se efectúan en su presencia. Cualquiera de los enumerados en el Artículo 979 del Código Civil constituye un ejemplo de esta categoría. Ossorio[3], con otras palabras, lo define como aquel documento "...otorgado o autorizado, con las solemnidades requeridas por la ley, por notario, escribano, secretario judicial u otro funcionario público competente, para acreditar algún hecho, la manifestación de una o varias voluntades y la fecha en que se producen."

Los instrumentos públicos pueden tener por finalidad acreditar la existencia de un hecho o acto, que constituye el presupuesto más frecuente; o constituir la forma de ejercicio de un poder público. En este supuesto no tienen por finalidad demostrar que se realizó tal acto, sino ordenar, como lo hace una sentencia judicial o un decreto del Poder Ejecutivo[4].

A pesar de lo expresado en el acápite del Artículo 979 (...Son instrumentos públicos respecto de los actos jurídicos... ) es unánimemente aceptado que los instrumentos públicos pueden acreditar todo tipo de hecho o acto.

Nuestra legislación, no nos proporciona un concepto normado de Instrumento Público, en su lugar, el Articulo 979 del Código Civil, nos proporciona una enumeración, que luego ha sido ampliada por los desarrollos doctrinarios:

1. Las escrituras públicas hechas por escribanos públicos en sus libros de protocolo, o por otros funcionarios con las mismas atribuciones, y las copias de esos libros sacadas en la forma que prescribe la ley.
2. Cualquier otro instrumento que extendieren los escribanos o funcionarios públicos en la forma que las leyes hubieren determinado.
3. Los asientos en los libros de los corredores, en los casos y en la forma que determine el Código de Comercio.
4. Las actas judiciales, hechas en los expedientes por los respectivos escribanos, y firmadas por las partes, en los casos y en las formas que determinen las leyes de procedimientos; y las copias que de esas actas se sacasen por orden de juez ante quien pasaron.
5. Las letras aceptadas por el gobierno o sus delegados, los billetes o cualquier título de crédito emitido por el tesoro público, las cuentas sacadas en libros fiscales, autorizadas por el encargado de llevarlas.
6. Las letras de particulares, dadas en pago de derechos de aduana con expresión o con la anotación correspondiente de que pertenecen al Tesoro público.
7. Las inscripciones de la deuda pública, tanto nacionales como provinciales.
8. Las acciones de las compañías autorizadas especialmente, emitida de conformidad con sus estatutos.
9. Los billetes, libretas, y toda cédula emitida por los bancos, autorizados para tales emisiones.
10. Los asientos de los matrimonios en los libros parroquiales, o en los registros municipales, y las copias sacadas de esos libros o registros.

Para que un documento sea considerado público deberá contener los siguientes requisitos: a) Ser extendido por un Oficial Público, b) que ese Oficial Público sea capaz de otorgarlo, c) que dicho oficial sea competente en razón de la materia y territorio, d) que satisfaga las formalidades que establece la ley.

De manera práctica, lo que caracteriza al instrumento público, es que hace plena fe, no solo entre las partes, sino frente a terceros, a menos que sea tachado de falso civil o criminalmente. Claro que esa plena fe esta referida a la realidad de la existencia material de los hechos que el oficial público hubiere anunciado como cumplidos por el mismo o pasados en su presencia[5].

3. OSSORIO, Manuel, Diccionario de las Ciencias Jurídicas, Políticas y Sociales. 21ª Ed. Actualizada, corregida y aumentada por Guillermo Cavanellas de las Cuevas. Ed. Heliasta. Pág. 356
4. RIVERA, Julio Cesar, Op. Citado, Pág. 642.
5. OSSORIO, Manuel, Op Citado, Pág. 519

**Instrumentos particulares o privados**

Para conceptuar al instrumento particular o privado, utilizaremos el método de definición por negación. Diremos entonces que el documento privado, es aquel que, reuniendo todas las características de un instrumento, no requiere de la intervención de un oficial público.

En lo atinente a la regulación de los actos entre particulares, nuestra normativa adhiere al principio de libertad de formas. En efecto, el Artículo 917 del Código Civil prescribe: “La expresión positiva de la voluntad será considerada como tal, cuando se manifieste verbalmente, o por escrito, o por otros signos inequívocos con referencia de determinados objetos.” Este principio se ve reproducido luego en el Artículo 974 y en el 1020, en los cuales se establece, que salvo prescripción en contrario, las partes pueden usar la forma que juzguen conveniente para materializar los actos privados, y que cuando la forma escrita sea la elegida, las partes pueden formularlas en el idioma y con las solemnidades que crean más convenientes respectivamente.

Este principio de total libertad de formas, es desplazado a los efectos probatorios, por lo preceptuado en los Artículos 1012 y 1021, la firma y el doble ejemplar.

**5. Firma**

*a) Concepto*

Tal como lo reseñamos en el punto anterior, la firma es según el Artículo 1012 del C.C. “... una condición esencial para la existencia de todo acto bajo forma privada. Ella no puede ser reemplazada por signos ni por las iniciales de los nombres o apellidos.”

Podemos afirmar, sostenidos en abundante doctrina, que la firma está constituida por trazos que constituyen el modo habitual que tiene una persona de escribir su nombre con la finalidad de manifestar la adhesión de su voluntad al texto a cuyo pie la pone.

Resulta ineludible, transcribir el último párrafo de la nota al Artículo 3639 del Código Civil, que de manera meridianamente clara explica el concepto de firma: “La firma no es la simple escritura que una persona hace de su nombre o apellido; es el nombre escrito de una manera particular, según el modo habitual seguido por la persona en diversos actos sometidos a esta formalidad. Regularmente la firma lleva el apellido de la familia; pero esto no es de rigor si el hábito constante de la persona no era firmar de esta manera. Los escritores franceses citan el testamento de un Obispo, que se declaró válido, aunque la firma consistía únicamente en una cruz seguida de sus iniciales, y de la enunciación de su dignidad.”

De lo dicho, podemos concluir, que en rigor de verdad, no es siquiera requerible que se trate de escritura (entendida esta como letras o dibujos que signifiquen sonidos en algún idioma), sino que basta con que consistan en trazos, es decir dibujos.

*b) Caracteres*

*- Ológrafa*

La firma, para encuadrar en el concepto vertido anteriormente, debe haber sido estampada de puño y letra por parte de la persona a quien se imputa su autoría.

Esto quiere decir que no son válidas las firmas estampadas por medios mecánicos, calcadas o copiadas de una original por terceros.

*- Manifestaciones de individualidad*

Debe ser una expresión de la individualidad de quien la escribe, lo que no significa que deba hacer referencia al nombre del firmante, ya que él mismo puede querer significar otras cosas como su seudónimo, apodo, sobrenombre, algún título o algún cargo. En todo caso lo que el firmante quiere expresar es algún rasgo de su individualidad.

*- Exclusiva*

Como referencia a la individualidad de cada persona, esta debe ser de su uso exclusivo.

*- Habitual*

Teniendo en cuenta lo dicho al momento de tratar el concepto de firma, este es su rasgo preponderante. Si bien la firma de los sujetos cambia a través del tiempo, y ninguna firma es idéntica a las demás, cada firma debe ser similar a la cronológicamente anterior.

No importa en sí si una firma es legible o no, pero si debe ser la manera habitual en que un sujeto expresa su conformidad por escrito.

*- Expresión de voluntad*

La firma debe ser estampada con la finalidad de adherir al contenido expresado en el texto, razón por la cual debe ubicarse al final del documento, siendo de ningún valor todo lo escrito debajo de ella.

Una de las excepciones a este principio está dada por los documentos compuestos por varias páginas, donde habitualmente se firman todas ellas en un margen, y se pone una firma al final del texto en la última carilla.

*c) Función*

Estamos aquí ante un punto clave, cual es la utilidad y la finalidad de todo elemento en la vida del hombre.

Clásicamente la firma ha servido a la obtención de dos objetivos:

- Imputación de autoría del acto
- Demostración de la voluntad de su autor.

Teniendo en cuenta estas dos funciones universalmente aceptadas para la firma, tendremos un norte que nos permitirá interpretar todos los caminos que encontremos en el estudio que nos ocupa.

*d) La impresión digital*

La doctrina y jurisprudencia mantienen posiciones encontradas con respecto a la validez de los instrumentos signados por la impresión de la huella digital. La Corte Suprema de la Provincia de Entre Ríos[6] ha reconocido este desencuentro cuando manifestó que "La impresión digital y la firma a ruego son asuntos que reconocen tesituras encontradas en la doctrina nacional. Existen tres posiciones que dan distinta significación jurídica a la impresión digital. La primera hace una interpretación literal del Artículo 1012 del Código Civil. Sostiene que la firma es la única forma válida para exteriorizar la voluntad en los instrumentos privados. Otra se ubica en las antípodas y equipara la impresión digital a la firma. La restante, es intermedia y le acuerda valor indiciario de forma tal que la impresión digital puesta por un analfabeto al pie del documento hace presumir —iuris tantum— la verdad de su contenido."

Según lo expuesto en el fallo vemos claramente que hay 3 posturas sostenidas por la doctrina y la jurisprudencia.

**Postura restringida:** Dentro de los que se enrolan en una interpretación literal del Artículo 1012 del C.C. podemos encontrar a Orgaz[7] quien sostiene que "mal puede aceptarse como manifestación válida de la voluntad de una persona la que aparece identificada por la impresión digital de ella, si por definición se trata de un analfabeto que no ha podido enterarse por sí mismo del contenido del documento.", a su vez Acuña Anzorena[8], basado en la interpretación literal del Artículo 1012 le ha negado el carácter de instrumentos privados a los documentos en los que obra la impresión digital del otorgante. Por lo expuesto surge claramente que para los sostenedores de esta teoría la impresión dactilar en el documento acredita identidad del sujeto pero no la manifestación de su voluntad. Esta postura también se encuentra avalada por una fallo de la Suprema Corte de Justicia de la Provincia de Buenos Aires[9] cuando manifestó que "la firma —conforme al Artículo 1012 del C.C.— es una condición esencial para la existencia de todo acto bajo la forma privada, la que no puede ser reemplazada por signos o iniciales, por lo que la impresión digital - aunque resulte útil como prueba de identidad - no es apta como expresión de voluntad contractual y no suple la falta de firma, aunque haya sido estampada en presencia de testigos."

**Postura intermedia:** En la postura intermedia encontramos enrolado a Días de Guijarro[10] quien sostiene que "si bien esos documentos no pueden ser considerados instrumentos privados en el carácter que enuncia el Artículo 1012, no se puede negar que son escritos no firmados, mencionados entre los medios de prueba por el Artículo 1190 inciso 2° del C.C.", por lo tanto el citado autor le otorga una presunción de validez

6. Luna de Jauregui, Eva Victoria c/Barnechea de Rojas, Margarita y/o sus herederos y/o sucesores y otro y/o responsable s/ sumario. S CCCO02 CO 0000 000816 16-02-95 SD SMALDONE.
7. ORGAZ A., La impresión digital en los documentos privados, Revista "Colegio Abogados de Buenos Aires", marzo-abril 1936, página 97.
8. ACUÑA ANZORENA A., "Efectos jurídicos de la impresión digital en los documentos privados», La Ley, tomo 23, página 904.
9. SCBA, Ac 36968 S 10-11-87, Juez SAN MARTIN (MA) - Lambermont, Roberto José y otro c/ Sucesión de Pura Reynafé y otra s/ Escrituración y cumplimiento boleto - AyS 1987-V-10 - MAG. VOTANTES: Negri - San Martín - Cavagna Martínez - Mercader - Laborde - Ghione
SCBA, Ac 46687 S 19-10-93, Juez SAN MARTIN (MA) - Orge Martínez, Jesús y otra c/ Martínez, María (suc.) s/ Escrituración - DJBA t. 145 p. 248 - LL t. 1994-D p. 477 - MAG. VOTANTES: San Martín - Negri - Mercader - Pisano - Vivanco - Laborde
10. DÍAZ DE GUIJARRO E., "La impresión digital en los documentos privados no firmados", Jurisprudencia Argentina, tomo 50, página 85.

iuris tantum. También adhiere a esta postura un fallo de la Corte Suprema de la Provincia de Entre Ríos[11] cuando manifiesta que "la falta de firma por parte del otorgante en un poder, en razón de no saber leer ni escribir, por lo que impusiera su impresión digital, previa lectura del contenido del instrumento, del cual se ratificara, no es causal de nulidad absoluta".

**Postura amplia:** Dentro de la postura amplia que admite la huella dactilar como firma encontramos el proyecto de reforma al Código Civil de 1936 que en su Artículo 275 disponía que "los instrumentos suscriptos por analfabetos con sus impresiones digitales, tendrán los mismos efectos que los instrumentos firmados.", sin embargo, esta asimilación de la firma ológrafa a la firma mediante la impresión de la huella dactilar a sido duramente castigada por Borda[12], ya que según este autor no se toma en cuenta la fundamental manifestación de Orgaz, puesto que incurre en la incongruencia de atribuirle a alguien una manifestación de voluntad de la que no ha podido enterarse por ser analfabeto. Debido a este planteo el anteproyecto de reforma al Código Civil de 1954 adopta una postura menos exagerada y se enrola en la postura intermedia ya que su Artículo 288 dice que "la impresión digital puesta por un analfabeto al pie de un documento hace presumir hasta prueba en contrario la verdad de su contenido en los términos del Artículo 300. En tal caso no regirá la limitación establecida en la primera parte de ese precepto".

Más recientemente la Ley de Contrato de Trabajo N° 20.744, modificada por la ley N° 21.297, en su Artículo 59 dice que "La firma es condición esencial en todos los actos extendidos bajo forma privada, con motivo del contrato de trabajo. Se exceptúan aquellos casos en que se demostrará que el trabajador no sabe o no ha podido firmar, en cuyo caso bastará la individualización mediante impresión digital, pero la validez del acto dependerá de los restantes elementos de prueba que acrediten la efectiva realización del mismo". Esta disposición admite expresamente a los fines del contrato de trabajo la impresión dactilar como firma en los casos en que el trabajador no supiese o no hubiese podido firmar. Un fallo de la Suprema Corte de la Provincia de Entre Ríos[13] ha sostenido lo mismo cuando el tribunal manifestó que "La impresión digital ha sido expresamente admitida como expresión de voluntad y consentimiento, en tanto otros elementos de prueba concurran a acreditar la efectiva realización del acto, Artículo 59 Ley de Contrato de Trabajo, requisito que en el caso quedó cumplimentado con la intervención del oficial público."

*e) La Firma a ruego*

Los documentos firmados a ruego son aquellos que aparecen firmados por un tercero a pedido del interesado.

Este tipo de firma ha sido prevista en las tres redacciones que el Artículo 1001 del Código Civil ha ostentado a lo largo de la historia (Original, Ley 9151 y 15.875). Este artículo regula los requisitos de validez de las escrituras públicas.

En el ámbito del derecho comercial también se ha aceptado la firma a ruego, en efecto, el Artículo 208 del Código de Comercio de la Nación, en su Inciso 3º dispone que los contratos comerciales pueden justificarse "... por documentos privados, firmados por los contratantes o algún testigo, a su ruego y en su nombre."

El problema por lo tanto se circunscribe a la validez de los instrumentos privados firmados de esta manera en el ámbito regido estrictamente por el derecho civil.

Según Llambías[14] en la posición negativa podemos encontrar a Segovia, Machado, Salvat y a Etcheverry Borneo, quienes niegan todo valor legal a la firma a ruego en los instrumentos privados por carecer los mismos de la firma de la parte interesada y violar el requisito establecido por el Artículo 1012 del C.C. que exige la firma de las partes como un requisito esencial. A su vez un fallo de la Suprema Corte de la Provincia de Buenos Aires[15] enrolándose en la posición negativa estipula que "La firma a ruego sólo resulta admisible en aquellos actos otorgados ante un funcionario público (Artículo.1001, C.C.)". A su vez en otro fallo el mismo tribunal[16] manifestó que "Si el documento carece del requisito esencial de la firma no tiene el valor de instrumento privado ni puede atribuírsele carácter de principio de prueba por escrito, conforme a lo dispuesto en los Artículos 1012 y 1192 del Código Civil, sin que la circunstancia de que aparezca suscripto a ruego de una de la partes y lleve su impresión digital, autorice a decidir lo contrario."

11. Torres, Emilio Pantaleón y otros c/Cooperativa de Prod. Alimenticios para Comerc. Min.»Gral. Sarmiento» Limitada y/o quien resulte responsable s/Indemnización por despido y otros. S CCCO03 CO 0000 003357 6500066 24-06-94 SD ROVIRA
12. BORDA, G. A., "Tratado de derecho civil, Parte General", 3ª edición, tomo II, N° 929, página 154.
13. Torres, Emilio Pantaleo y otros c/Cooperativa de Prod. Alimenticios para Comerc.Min.»Gral.Sarmiento» Limitada y/o quien resulte responsable s/Indemnización por despido y otros. S CCCO03 CO 0000 003357 6500066 24-06-94 SD ROVIRA.
14. Obra citada, página 398.
15. SCBA, Ac 36968 S 10-11-87, Juez SAN MARTIN (MA) - Lambermont, Roberto José y otro c/ Sucesión de Pura Reynafé y otra s/ Escrituración y cumplimiento boleto - AyS 1987-V-10 - MAG. VOTANTES: Negri - San Martín - Cavagna Martínez - Mercader - Laborde - Ghione.
16. Suprema Corte Buenos Aires, Febrero 25 1964. ED, 14-282.

Según Rivera[17] dentro de los que aceptan la firma a ruego en los instrumentos privados encontramos a Llerena, Llambías, Borda y Aráuz Castex, quienes para otorgarle validez al acto sustentan su posición en la teoría del mandato basándose para ello en el Artículo 1873 del C.C.. A su vez un fallo de la Cámara Nacional Civil[18] dispuso que "... aunque el Artículo 1012 del Código Civil exija la firma de las partes que intervienen para acreditar o probar la existencia del acto bajo forma privada, el reconocimiento de ese carácter de principio de prueba por escrito, de la firma a ruego, dependerá de la prueba que se acerque y que corrobore cual fue el exacto alcance del acto cuestionado, para llevar al juez la convicción de que el mismo fue efectivamente celebrado y que sus cláusulas eran la expresión de la voluntad de ellas, y en especial del que pidió que se firmara a ruego en su nombre.", lo cual lo enrola evidentemente en la teoría del mandato admitiendo su existencia. En otro fallo de la misma Cámara[19] se manifestó que "cabe otorgarle a la firma a ruego los efectos de un mandato, y en consecuencia, por esa vía, corresponde asignarle eficacia al instrumento suscripto en esos términos, siempre que se haya acreditado la existencia de esta última relación jurídica (en el caso, se trataba de un boleto de compraventa en el que la vendedora analfabeta, posteriormente fallecida, asentó su impresión dígito pulgar e hizo firmar a ruego a una amiga".

*f) Instrumentos privados sin firma.*

A fin de determinar la validez de los instrumentos privados sin firma, se propone analizar si las funciones de la firma ológrafa pueden se suplidas por otros medios.

Ya nuestra legislación recepciona algunos supuestos en los que la firma puede ser reemplazada por reproducciones facsimilares y otros dónde inclusive puede prescindirse de ella[20]

Rivera afirma, citando a Fernández Leiva[21] que si la imputación de autoría y la manifestación de voluntad, las dos principales funciones de la firma ológrafa, pueden ser satisfechas por otros elementos, entonces la misma se torna prescindible.

Los medios técnicos puestos a nuestro alcance hoy en día, han cambiado la manera en que nos identificamos y expresamos nuestra voluntad. En efecto, quien puede negar que cualquiera de nosotros puede identificarse mediante el uso de una tarjeta magnética y una clave ante un cajero automático, o en el portal de servicios por Internet de cualquier entidad bancaria y realizar prácticamente cualquier tipo de transacción sin necesidad de interactuar con otras personas sino con maquinas.

Podemos decir que hoy la declaración de voluntad no sólo se obtiene por los medios que nos brindan el artículo 917 y 918 del Código Civil[22], sino también por signos que resultan de la realización material de actos inequívocos.

La postura de los tribunales entorno de este tema es en nuestro días equilibrada, de hecho se viene afirmando que los instrumentos particulares no firmados, no están desprovistos de todo valor, pues valen como prueba de los contratos, de dónde el articulo 1012 admite morigeraciones.

# Capítulo 3
# Documento Digital

**6. Concepto**

Tal como lo hemos definido en el Capítulo 2, el documento, puede estar materialmente plasmado sobre papel, sobre cualquier otro tipo de soporte que resulte apto según su naturaleza.

Durante mucho tiempo, fueron considerados elementos esenciales del concepto de documento, su soporte más tradicional, el papel, la grafía tradicional como manera de plasmar un mensaje, y la firma ológrafa del emisor, o emisores del documento como manera de acreditar la autoría del mismo y la adhesión de su voluntad a lo expresado en el mismo. De esta forma se confundieron durante mucho tiempo el contenido con el continente.

17. Obra citada, página 737.
18. Cámara Nacional Civil, Sala F, Julio 28 1970, Mariani, Irineo, Suc. C. Cabañes de López, Manuela.
19. Cámara Nacional Civil, Sala B, Mayo 30 1986 - El Derecho, 121-432.
20. Artículo 212 de la Ley de sociedades para el primer caso y Artículo 59 de la Ley de Contrato de Trabajo.
21. Obra citada, página 738.
22. Artículo 917: La expresión positiva de la voluntad será considerada tala, cuando se manifieste verbalmente, o por escrito, o por otros signos inequívocos con referencia a determinados objetos.
Artículo 918: La expresión tácita de la voluntad resulta de aquellos actos, por los cuales se puede conocer con certidumbre la existencia de la voluntad, en los casos en que no se exija una expresión positiva, o cuando no haya una protesta o declaración expresa en contra.

El avance tecnológico, ha hecho que muchos doctrinarios intenten definir el concepto de documento digital.

Cuando en general se utiliza el término documento electrónico o digital, se lo hace con bastante ligereza, refiriéndose solamente al cambio de soporte. Así ha sido definido como una representación material apta de reproducir una manifestación de voluntad del hombre y que se materializa en soportes magnéticos, como un disquete, un CD-ROM, un disco zip, o que queda registrada en la memoria de la PC; y que consiste en un mensaje digital que requiere de determinados componentes de hardware para ser comprendido por el hombre, o que puede ser legible directamente sin necesidad de la intervención de máquinas traductoras, como sucede con un mensaje de correo electrónico[23].

Documento electrónico es la representación de un acto jurídico en un soporte magnético o digital que permita de algún modo la comprensión de su contenido, por parte de un ser humano. Es toda cosa susceptible de percepción sensorial y aprehensión mental, representativa de un hecho cualquiera, y que puede estar expresado en cualquier elemento material que sirva para tales fines[24].

Ettore Giannatonio[25] dice que, por documento electrónico se debe entender a aquel que es formado por el ordenador o el documento formado por medio de este. En el primer caso el ordenador no se limita a materializar una voluntad, una decisión, sino que, conforme a una serie de datos, parámetros y a unos programas[26], decide, en el caso concreto, el contenido de la regulación de intereses. Este es el caso de los contratos concluidos entre ordenadores, en virtud de intereses ya expresados, el ordenador se limita a comprobar si se dan ciertas circunstancias, en cuyo caso concreta la operación[27].

Rodolfo Herrera Bravo, jurista chileno, ha hecho una división entre los documentos electrónicos. Entiende por documento electrónico, en sentido estricto, a la representación material, destinada e idónea para reproducir una cierta manifestación de voluntad, materializada a través de las tecnologías de la información sobre soportes magnéticos, como un disquete, un CD-ROM, una tarjeta inteligente u otro, y que consisten en mensajes digitalizados que requieren de máquinas traductoras para ser percibidos y comprendidos por el hombre.

A su vez, tenemos a los documentos electrónicos en sentido amplio o también llamados documentos informáticos, que pueden ser caracterizados por la posibilidad de ser perceptibles y legibles directamente por el hombre sin necesidad de la intervención de máquinas traductoras, como sería el caso de la boleta que emite un cajero automático[28].

Por lo general los documentos electrónicos son la trascripción de una escritura sobre papel que, con frecuencia, se destruye después de registrarse digitalmente.

Los documentos electrónicos digitales han sido tradicionalmente entidades estáticas, una colección de bits que tienen sentido tomados como un todo. Eran además propiedad de una aplicación que le imponía al documento de la necesidad de un formato determinado y unas caprichosas propiedades para su almacenamiento. Esta situación ha cambiado en los últimos años. Por un lado, los ordenadores han dejado de ser maquinas orientadas al tratamiento numerativo y con el aumento de sus prestaciones se han aplicado al tratamiento de la información cognitiva. Por otro lado, las redes de ordenadores y necesidad creciente de compartir datos electrónicos han provocado la aparición de sistemas cada vez más inteligentes favorecidos por las nuevas tecnologías. Así, los documentos en los ordenadores han dejado de ser una replica del papel, para convertirse en entidades dinámicas y multimedia, tienen conocimiento de lo que son, que aplicación los creó y con cuales pueden compartir datos o como deben presentarse en función del entorno en que se invoquen.

Los documentos son actualmente una colección de vínculos o hipervínculos a objetos de cualquier tipo, ya sea texto, datos, programas, imágenes fijas o en movimiento, sonidos, fuentes de letras, otros documentos.

**7. Análisis de los conceptos**

Como podemos observar del conjunto de definiciones ofrecidas, es difícil encontrar pautas para conceptualizar al documento digital. Se producen enfoques disímiles que hacen que el mismo concepto de documento digital tenga acepciones totalmente contrarias o hasta contradictorias.

Se debe ser muy cuidadoso al momento de definir un concepto como este, tan técnico, pues es muy probable que de lo contrario se llegue a soluciones absurdas o ilógicas, o se incluyan algunas cosas y se

23. PICECH, Ariel Eduardo, “Prueba Penal y Documento Electrónico”.
24. RIBAS, Javier, “Comercio Electrónico en Internet: aspectos jurídicos”.
25. Consejero de la Suprema Corte de Casación de Italia. Profesor Universitario (Roma)
26. GIANNANTONIO, Ettore, “Informática y Derecho. Aportes de la doctrina Internacional. El valor jurídico del documento electrónico”. Volumen 1, Pág. 94, Ed. Depalma, Buenos Aires, 1991.
27. BARREIRA DELFINO, Eduardo, “Documento Electrónico”, Fascículo Nº 23, Cátedra de Derecho Empresario, Ed. de Belgrano.
28. HERRERA BRAVO, Rodolfo, “Documento electrónico: algunas vías de aplicación en el Derecho probatorio chileno”.

excluyan otras de manera arbitraria. Este es uno de los problemas que más a menudo podemos observar. En efecto, si por ejemplo decimos, haciendo sólo referencia al cambio de soporte, que un documento digital es aquel plasmado sobre un soporte magnético (entran dentro de esta categoría los disquetes, discos rígidos, tarjetas de memoria, chips de memoria, etc...) estamos dejando fuera de la definición a los medios de almacenamiento óptico (como los discos compactos), los magneto-ópticos (como puede ser un disco zip), o los que deriven del frenético avance de la industria informática. Si decimos que es necesario que el documento electrónico éste guardado en la memoria de una PC (Personal Computer) para ser tal, podríamos dejar afuera todos aquellos documentos guardados en medios de almacenamiento extraíbles, o en otras máquinas que técnicamente no pueden ser consideradas una PC, como por ejemplo una simple agenda electrónica o un complicado servidor Host.

Estas consideraciones que parecen no tener importancia en el ámbito del Derecho Civil o Comercial, dónde las omisiones o lagunas pueden ser completadas por vía de la analogía o interpretación, pueden presentar serios problemas y desatar largos debates doctrinarios al momento de tener que utilizar estos conceptos en el campo del Derecho Penal, que se tornan totalmente innecesarios desde el momento en que los mismos pueden ser evitados con la previsión necesaria.

Hechas estas salvedades sobre los recaudos que deben tomarse al momento de emitir la definición del concepto de un objeto de las características que nos ocupa, realizaremos algunas consideraciones sobre los distintos conceptos vertidos.

No nos parece del todo apropiado definir al documento electrónico, tal como lo hace Rivas, como la representación de un acto jurídico en soporte magnético o digital, por cuanto, siendo documento, no necesariamente debe contener la representación de un acto jurídico, podría bien contener hechos jurídicos, o inclusive sólo estar destinado a la transmisión de otros conocimientos, como es el caso de la gran cantidad de material publicado por casas académicas y universidades de todo el mundo en la Red Internet. Resulta asombroso ver cómo cada día aparece nuevo material firmado digitalmente en las páginas de estas instituciones y de muchas empresas de renombre internacional, a fin de evitar su adulteración por parte de personas inescrupulosas, tales los casos de Microsoft Inc. y Macromedia Inc. entre otros. Lo que puede resultar asombroso además es que las grandes compañías de software están firmando digitalmente los archivos que componen sus programas[29], con lo cual el producto lleva incorporado inseparablemente su certificado de integridad.

Continuando el análisis de los conceptos ofrecidos por los distintos autores, creemos que lo dicho por Ettore Giannatonio, se ajusta más a un concepto de contrato electrónico que al de documento electrónico. La representación de ese contrato electrónico, podría ser o no un documento electrónico, como por ejemplo la boleta de un cajero automático. En rigor de verdad, estamos inclinados a pensar que, cuando una máquina de acuerdo a una serie de parámetros que constituyen las reglas que las partes de manera bilateral o unilateral se han dado para la realización de un determinado negocio jurídico, decide la realización de determinada transacción, no se está realizando otra cosa que un contrato, por cierto de características especiales, pero un contrato sin lugar a dudas. No debemos confundir al contrato con el documento que lo representa, y que constituye en última instancia el medio por el que ha de ser probado el acuerdo de voluntades concretado. Claro que ello desde un punto de vista práctico no es algo sencillo. En efecto, la nota al Artículo 973 del Código Civil, con gran claridad comenta: "... La voluntad, como todo lo que no tiene cuerpo, es impalpable, penetra en el pensamiento, desaparece y se modifica en un instante. Para encadenarla era preciso revestirla de un cuerpo físico."

De manera análoga a lo dicho sobre la definición de Rivas, creemos poco feliz la inclusión de la "manifestación de voluntad" que hace el jurista chileno Rodolfo Herrera Bravo.

Descartaremos también, del concepto de documento electrónico, al llamado documento informático, o la materialización en papel de -por ejemplo-, una transacción realizada en un cajero automático. La boleta que la terminal electrónica imprime en un papel y nos entrega, no cabe duda, es un documento en soporte papel, sin firma, que por convenio entre las partes es reconocido como válido para probar la transacción realizada, pero que no escapa en lo más mínimo de los conceptos tradicionales. Debemos recordar que es nocivo para el método de las ciencias crear conceptos nuevos allí dónde no existen.

En general coinciden los autores, al momento de definir al documento electrónico, en el soporte digital de su almacenamiento, en la intervención de algún tipo de maquinaria, y en la intervención de uno o más programas, que no son en última instancia más que un conjunto de reglas de procesamiento de información.

Claro que esto no siempre fue así. A los estudiosos de la Informática Jurídica les ha costado más de una década de estudios diferenciar al documento electrónico con el documento elaborado por una computadora

29. MS-Windows XP, de Microsoft Inc. Tiene todos sus archivos troncales firmados digitalmente. De esta manera, con herramientas que el mismo sistema operativo brinda, se pueden detectar los archivos que hubieran sido modificados por la instalación de otros programas o por el ataque de virus o hackers, y que normalmente pueden causar la inestabilidad o mal funcionamiento del sistema.

y plasmado en papel. En efecto, muchos juristas, inclusive muchos de ellos destacados internacionalmente, han considerado al documento impreso mediante el uso de una impresora, un procesador de texto y una computadora como un documento electrónico en sentido amplio: "… Nada prohíbe, en cambio, que un documento electrónico en sentido amplio, esto es extendido con el auxilio del computer, pueda constituir una válida escritura privada. Así, por ejemplo, el caso de un tabulado formado mediante una impresora conectada con el sistema de elaboración y firmado por las partes…"[30]

El avance de la doctrina en este aspecto ha sido muy positivo y se ha rectificado el camino. Seguir en la misma línea de análisis nos debiera haber conducido a discriminar entre el documento mecanografiado del manuscrito, lo cual a todas luces un despropósito.

**8. Nuestra opinión**

En rigor, creemos que este afán por definir al documento electrónico, proviene de la dificultad que tenemos para individualizarlos en la práctica, dificultad ésta producto de varios siglos, dónde el papel y los documentos fueron prácticamente considerados las mismas cosas.

Hoy nadie puede negar que un contrato plasmado en un papel sea un documento, y que pertenezca al tipo especial de documentos que denominamos comúnmente instrumentos. Tampoco se podrá negar la calidad de documento al conjunto de páginas impresas en papel que constituyen este trabajo. Nadie negaría tampoco que un billete de curso legal es un documento, es más que es un instrumento público que inclusive tiene la curiosa particularidad de no estar firmado. Esto sucede de manera natural porque podemos tenerlos entre manos, percibirlos con nuestros sentidos, de la manera habitual en la que se ha hecho por siglos, y podemos aprehender su contenido aplicando reglas relativas a los signos que lo componen (alfabeto u otros signos), al idioma en que están redactados y a la sintaxis, que hemos internalizado desde muy pequeños, es decir, porque es algo que conocemos profundamente y de manera muy natural.

De la misma manera, nos preguntamos si, ese mismo contrato o este trabajo, cuando aún no habían sido impresos y eran sólo un archivo de un procesador de textos ¿podían ser considerados documentos? Si ese contrato se hubiera registrado en una base de datos, con reglas claras y precisas que luego nos permitan recuperar y aprehender su contenido, ¿sería un documento? El llamado "dinero electrónico", que no es más que un conjunto de registros que indican un determinado crédito en una cuenta bancaria, ¿es un documento?

Creemos que estas preguntas merecen respuestas afirmativas. Obviamente, podrán surgir todo tipo de objeciones respecto a la seguridad que tienen estos documentos. Indudablemente, el contrato que se encuentra en un procesador de texto, sin la aplicación de alguna técnica de seguridad informática, no merece la misma confianza que la versión impresa del mismo, dónde inclusive el ojo lego o inexperto puede detectar cualquier modificación, alteración o adulteración que haya sufrido.

De la misma manera el "Dinero electrónico" merece confianza por cuanto, vive en el espíritu de quien lo usa, la certeza de que se aplican rigurosas normas de seguridad en el manejo de este tipo de información.

De modo que, si logramos demostrar que existen hoy en día técnicas lo suficientemente seguras como para asegurar la autoría de un documento electrónico, su autenticidad y no repudiabilidad, estaríamos en condiciones de prescindir de un concepto de "documento electrónico". Llegado a este punto, todo se vería circunscrito a un problema de confianza en estas técnicas.

30. GIANNANTONIO, Ettore, Op. Citado, Pág. 113.

# Capítulo 4
# Firma digital

## 9. Introducción

Según lo vertido en el capitulo anterior, podemos inferir que es prácticamente imposible pensar en un sistema seguro de documentos electrónicos sin contar con un medio que nos brinde la confianza necesaria para creer en ellos.

En este capítulo analizaremos lo que a nuestro juicio constituye un medio seguro, eficiente y eficaz para generar la confianza que buscamos a fin de poder asimilar un documento digital con uno impreso en un tradicional soporte de papel.

## 10. Concepto

Definir un concepto de firma digital es tarea ardua. Nos permitimos afirmar esto, teniendo en cuenta la amplia gama de desarrollos técnicos y la velocidad con que caminan las ciencias de la computación.

Así y todo, cuando se trata de este tipo de conceptos, y a pesar de lo acertado de la afirmación del Dr. Vélez Sarsfield en cuanto las definiciones no son propias de los códigos y las leyes de fondo, creemos conveniente definir un concepto y creemos conveniente que lo incorporen las regulaciones que se dicten al efecto, aún a riesgo de que en poco tiempo resulten obsoletas o requieran de alguna actualización.

Los puntos en común entre la definición de firma digital y la de firma tradicional (ver supra § 5.a), son lamentablemente pocos. Podemos buscarlos si, afortunadamente en su finalidad que es esencialmente la misma, pero definitivamente la materialización de una y otra es totalmente diferente.

Con el desarrollo logrado actualmente en las ciencias informáticas, es prácticamente unánime el criterio según el cual, firmar digitalmente un documento requiere apoyarse en un sistema de criptografía de clave asimétrica o sistema de clave pública (PKI por sus siglas en inglés Public Key Infrastructure). Sobre los detalles técnicos del funcionamiento nos explayaremos más adelante.

Podemos afirmar, aquí sin temor a equivocarnos, que la firma digital es un *procedimiento matemático* que se aplica a un archivo o conjunto de datos digitales, y que desde la sanción de la Ley 25.506 en nuestro país debe cumplir con algunos requisitos detallados en la ley y otros que la normativa ha delegado en el decreto reglamentario y demás normas que dicte la Autoridad de Aplicación. En su aspecto meramente material, el resultado de este procedimiento matemático, es un conjunto de caracteres que acompaña a un documento o conjunto de datos digitales, acreditando quién es su autor (**autenticación**) y que no ha existido ninguna manipulación posterior de los datos (**integridad**). Para firmar un documento digital, su autor utiliza su propia clave secreta (sistema criptográfico asimétrico), a la que sólo él tiene acceso, lo que impide que pueda después negar su autoría **(no revocación o no repudio**). De esta forma, el autor queda vinculado al documento de la firma. La validez de dicha firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

Para firmar digitalmente un documento, según el método unánimemente seguido, el firmante utiliza su clave privada, que sólo él conoce y a la cual, recalcamos, sólo él tiene acceso. Luego cualquier persona utiliza la clave pública del autor para verificar la firma y la integridad del documento electrónico recibido.

## 11. Caracteres

Es necesario, cualquiera sea el sistema de firma digital que se utiliza, que esta cumpla con determinados requisitos, en función de garantizar ciertas pautas, que son las que nos permiten equiparar la firma digital a la firma ológrafa. Estos tienen que ver esencialmente con las finalidades que persigue la firma de todo documento.

*a) Autenticación o Autoría*

La firma digital, para ser eficaz, debe poseer un mecanismo tal que permita aseverar con un alto grado de certeza la identidad del autor de un documento firmado digitalmente.

Esta autenticación de autoría es imprescindible para el correcto funcionamiento del sistema, ya que endilga a un sujeto un compromiso por el cual deberá responder a todos sus efectos.

*b) Integridad*

Igual, o tal vez más significativo que lo anterior, es certificar que la información contenida en el documento electrónico sea la que su autor suscribió. Esto equivale a decir, que en el proceso de firmado de un documento digital, se debe asegurar que luego los datos no puedan ser alterados por terceros sin que esta acción quede posteriormente evidenciada.

*c) Ausencia de revocación*

Todo sistema de firma digital idóneo para los fines perseguidos, debe además garantizar que el firmante no pueda luego desconocer la firma puesta en un documento, desvirtuando de esta manera su adhesión de voluntad.

Si un sistema de firma digital no asegurara este tópico, la inseguridad jurídica no tendría límites y el sistema se tornaría meridianamente inútil.

*d) Adhesión*

Firmar digitalmente un documento, indica que el signatario expresa su adhesión de voluntad o conformidad con lo expresado o contenido en el documento digital. Esto nos lleva pensar que sería recomendable que las aplicaciones informáticas que se utilicen para signar digitalmente documentos, deberían de alguna manera recordar esto al usuario al momento de producir la firma.

## 12. Otros tipos de Firma Digital

*a) La firma digitalizada mediante dispositivos de captura de imagen.*

Nos referimos en este punto a las firmas manuscritas “escaneada”. Esta no puede considerarse en forma alguna firma digital pues carece de los requisitos mínimos para asegurar la autoría, la adhesión de voluntad y la integridad de los datos contenidos en un documento electrónico.

Aclaramos que algunas nuevas aplicaciones de software de manejo de documentos[31] están utilizando una imagen escaneada de la firma del usuario para “enmascarar” la firma digital verdadera, pero esto no deja de ser un detalle de estética que nada aporta a la seguridad del documento.

*b) Sistemas biométricos.*

Estos sistemas analizan alguna parte del cuerpo humano, que tiene la característica de ser genérica en todos los seres humanos, y de ser a la vez único para cada persona, como por ejemplo el patrón de voz, las huellas dactilares, el patrón vascular de la retina ocular, la estructura visible del iris.

Estos sistemas en una primera impresión pueden resultar de lo más atractivos, en efecto cada persona se constituye en su propia clave o llave para abrir pasos en sistemas de seguridad o para firmar algún documento. Sin embargo veremos continuación y brevemente que no sólo no son la panacea, sino que además tienen sus bemoles.

Las técnicas de identificación biométricas, decíamos, se basan en comparar alguna característica del cuerpo humano, con la información guardada en una base de datos. Aquí se empiezan a producir los primeros inconvenientes: la información debe ser previamente almacenada, esto importa la definición de un proceso de carga en las mismas, que debe respetar ciertos estándares de seguridad y calidad. Supone además la custodia y el mantenimiento de estas bases actualizadas. Por otra parte, la técnica planteada no difiere en mucho de un sistema de claves simétricas, pues en definitiva, la clave es única, y se heredan todas las debilidades que este supuesto origina.

Estos sistemas tienen un costo relativamente elevado, lo cual no los hace aún aptos para un uso masivo, así resulta interesante su aplicación para usos específicos, como por ejemplo para determinar el acceso a áreas o sistemas restringidos dónde la identidad de la persona resulta un tópico de alta sensibilidad y que normalmente no puede ser cubierta con el uso de tarjetas inteligentes u otro tipo de llaves. Un claro ejemplo de esta aplicación está dada en la Honorable Cámara de Diputados de la Nación, dónde se implementó el sistema de escáner de huella dactilar en las bancas para asegurar que los legisladores puedan emitir su voto para la sanción de las leyes sin que otras personas puedan tomar su lugar y asegurar un sistema de votación de alta transparencia. Cabe destacar que este sistema se implementó, luego de que fracasara el anteriormente implementado, que no tenía la finalidad de determinar la identidad de las personas, sino su asistencia en el recinto a los efectos de la determinación del quórum y que consistía en un sensor de peso que detectaba si el escaño esta ocupado.

*c) Sistemas de análisis de escritura.*

Este sistema consiste en el análisis del patrón de escritura de una persona. El sujeto, cuando pretende identificarse ante algún sistema de seguridad debe firmar o realizar un cuerpo de escritura normalmente sobre una tableta digitalizadora, que transmitirá los datos a una computadora dónde se realizará la comparación con un cuerpo de escritura previamente almacenado en una base de datos.

Se utiliza aquí un procedimiento similar al de los sistemas biométricos, y muchos autores de hecho la incluyen entre ellos. Sin embargo, debemos reseñar que esto es en principio conceptualmente incorrecto.

31. En este sentido podemos nombrar Adobe Acrobat 5.0 de Adobe Systems Incorporated. www.adobe.com

Pues la escritura no constituye un aspecto físico del individuo como lo son su voz, su huella dactilar o su iris, sino un aspecto psicológico en cuanto el modo de escribir, está generalmente aceptado, es un aspecto de la personalidad del sujeto.

Esto mismo debilita el sistema, pues la escritura como aspecto de la personalidad, tiende a cambiar de acuerdo al estado de ánimo de la persona lo que podría causar el rechazo de la autenticación pretendida. Además la escritura, se ve modificada por el paso del tiempo, según el sujeto vaya adquiriendo o perdiendo capacidades motrices, siendo esto algo del todo normal durante la vida de las personas, lo que ocasionaría la necesidad de actualizar las bases de datos en períodos muy cortos.

*d) Tarjetas inteligentes*

En rigor de verdad, este tampoco es un sistema de firma. Estas tarjetas, si bien se utilizan en un gran número de aplicaciones de seguridad (cajeros automáticos, tarjetas de crédito y débito, control acceso a áreas restringidas, asistencia puestos de trabajo y estudio, cajas de supermercados, etc...) y están ampliamente difundidas, no constituyen un sistema de firma, sino un medio de almacenamiento de datos que luego se utilizan para identificar a la persona ante un sistema de seguridad. Estas varían en capacidad, bastante reducida en las ya antiguas tarjetas de banda magnéticas, algo más importante en las tarjetas "inteligentes" que tienen un chip electrónico incrustado, y en el tope de línea las tarjetas PCMCIA que no sólo pueden contener datos, sino programas enteros.

En su funcionamiento, se las asocia con una clave, que el usuario debe mantener secreta y que le asegura ser la única persona que puede utilizar la misma para identificarse ante cualquier dispositivo apto para leer la tarjeta.

Debemos entonces tener cuidado de no confundir el contenido con el continente, estas tarjetas podrían eventualmente contener una clave de identificación, pero en sí no se constituyen en un sistema de firma o encripción.

El avance de la tecnología nos muestra cada día nuevas maravillas en este rubro, de hecho la compañía IOMEGA ha publicado el lanzamiento de un dispositivo del tamaño de un llavero, que munido de un puerto USB (Universal Serial Bus), permite el almacenamiento de hasta 1 gigabyte de información[32], sin necesidad de ningún tipo de conexión especial ni alimentación eléctrica, por un lapso de hasta 10 años.

**13. Criptología**

Se hace inevitable en este punto del trabajo, realizar algunas consideraciones sobre criptología, para dar algunas precisiones más que las ofrecidas en los puntos anteriores. Nótese, que nos referimos en este punto a **criptología** y no a **criptografía**, siendo la última uno de los dos capítulos principales de la primera.

En efecto, la criptología se compone de dos disciplinas distintas y complementarias, la **criptografía** por un lado, y el **criptoanálisis** por otro.

Mientras que la criptografía tiene por principal misión, convertir un texto inteligible o plano en un texto ininteligible o criptograma que sólo podrán interpretar las personas que poseen la clave, su técnica complementaria, el criptoanálisis, se dedica a buscar la forma de acceder a la versión descifrada de un criptograma, sin tener autorización para ello, es decir sin poseer la clave que resuelve el sistema.

*a) Criptografía*

Según podemos leer en el diccionario de la Real Academia de la Lengua Española, **criptografía.** (Del griego **kryptoz** (kryptos), «oculto» y **graptoz** (graptos), «escritura») f. Arte de escribir con clave secreta o de un modo enigmático.

Es una disciplina o técnica que busca transformar un texto mediante un método, que sólo pueden resolver inversamente las personas autorizadas.

Para esto se pueden utilizar algoritmos secretos o algoritmos públicos. Ambos pueden ser complementados con una palabra, llamada clave que es imprescindible en el proceso de encripción y desencripción.

Los sistemas de algoritmo público están hoy infinitamente más divulgados que los de algoritmo secreto, y esto obedece a razones que, a pesar de parecer muy claras, dieron origen a extensos debates, inclusive de índole ideológica. Los motivos que hicieron que se impongan los sistemas de algoritmos públicos son los siguientes:

- El nivel de seguridad es el mismo.
- Los algoritmos públicos se pueden fabricar de manera masiva, incluyéndolos en aplicaciones de software o en chips o circuitos integrados. Esto baja dramáticamente los costos.

32. A modo ilustrativo, el mismo volumen de información puede ser almacenado en 711 disquetes de 1.44 Mb (3 ¼) o en dos Discos Compactos. www.iomega.com

- Es más fácil y más seguro transmitir sólo una clave que todo el funcionamiento de un algoritmo.
- Los algoritmos públicos están mucho más probados, en efecto están a disposición de toda la comunidad científica para que los pruebe y detecte en él fallas o "agujeros".

Apoyándose en estos puntos, son muchas las voces que claman por la disponibilidad pública de la criptografía y por su uso libre. El último tal vez sea el argumento más fuerte, pues la experiencia ha demostrado que la única manera de obtener buenos algoritmos de encripción, es que estos sean publicados para el escrutinio de toda la comunidad científica. La seguridad no debe basarse en mantener secreto el algoritmo, pues estos tarde o temprano acaban siendo descubiertos y descritos, sino en su resistencia demostrada tanto teórica como prácticamente, y la única manera de demostrar la fortaleza de un algoritmo es sometiéndolo a ataques de todo tipo.

Como estudiosos de las ciencias sociales, debemos hacer notar que es imposible desligar a la criptografía de todas las consideraciones políticas, filosóficas y morares que suscita. Recordemos por ejemplo, que el software criptográfico está sujeto en Estado Unidos de Norte América a las mismas leyes que el armamento nuclear, y que en muchos países de Europa se pretende elaborar legislaciones parecidas. Su exportación está sujeta en los Estados Unidos de Norte América a serias restricciones determinadas por su inclusión en la International Traffic in Arms Regulation (ITAR). En efecto, las versiones exportables de los navegadores de redes y clientes de correo electrónico más difundidas (como el Internet Explorer y Outlook de Microsoft INC. o el Netscape Navigator) incorporan módulos de seguridad y de encripción de datos débiles, que utilizan longitudes de claves que no son realmente seguras para los propósitos para los que se ofrecen esos productos. Esta situación, si bien es advertida al usuario, no lo es en forma clara y contundente, y figura circunstancialmente en la documentación de ayuda que acompaña a esos programas.

Mientras tanto, los representantes de la industria de la informática y telecomunicaciones en los EE.UU. aducen que estas restricciones causan pérdida de mercados a manos de competidores de otros países dónde la criptografía no sufre estas restricciones.

Otra línea de debate, es la pretensión de algunos gobiernos de constituirse en guardián de todas las claves de sus ciudadanos y considerar ilegales aquellas no registradas, so pretexto de luchar contra el terrorismo y narcotráfico.

Quienes resisten el uso ilimitado de la criptografía, insinúan que cualquiera que abogue por su uso libre es poco menos que un delincuente que la necesita para encubrir sus crímenes. Sin embargo, defender el ámbito de lo privado es un derecho inalienable de las personas, que inclusive debe prevalecer sobre la obligación que tienen los estados de perseguir a los delincuentes.

De todos modos, no creemos estar equivocados al decir que el derecho a utilizar la criptografía está indirectamente recepcionado como parte de los derechos humanos, y esto sin lugar a dudas achicaría el margen de discusión sobre el tema. En efecto el Artículo 12 de la Declaración Universal de los Derechos Humanos de la Naciones Unidas reza:

**"Artículo 12** Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."

*b) Criptoanálisis*

El criptoanálisis se conforma de muchas técnicas diversas. Cualquiera de ella es válida si sirve en definitiva para lograr el objetivo: descifrar un criptograma sin estar autorizado para ello. A la luz de lo expuesto, nos damos cuenta que la criptografía y el criptoanálisis son técnicas complementarias y que se necesitan la una a la otra para evolucionar y perfeccionarse. A modo de ilustrativo, podemos recordar textuales palabras de Ronald Rivest, uno de los inventores del método RSA del que hablaremos más adelante, en una entrevista periodística: "… Recuerdo que Shamir y yo elaborábamos permanentemente métodos de criptografía pública, y Adleman siempre conseguía descifrarlos. Finalmente, sin embargo, dimos con uno que ninguno pudo descodificar…[33]"

La dificultad para el criptoanalista, está dada por la cantidad de información disponible en el problema que debe resolver. Cuanto menos información, mayor dificultad. En efecto no es lo mismo tener sólo un criptograma para resolver, que contar con un texto en claro, con su criptograma, y el algoritmo que hace que a partir de uno se genere el otro.

En todos los casos, el analista busca la clave, o el método práctico para obtener la clave que proporciona la solución de todo el sistema de seguridad.

Las técnicas, como decíamos, pueden ser de lo más variadas, desde las más primitivas, conocidas como "ataque de fuerza bruta" o "prueba y error" que consisten en probar en la menor cantidad de tiempo,

33. "El arte de escribir en clave", en Suplemento Informática del Diario Clarín, Buenos Aires, 13 de febrero de 2002.

todas las claves posibles, a otras más complicadas y refinadas, como las aproximaciones matemáticas y la aplicación de métodos estadísticos.

Suelen distinguirse las siguientes formas de emprender un criptoanálisis[34]:

1. *Ataque sólo con texto cifrado*: el atacante tiene acceso solamente a uno o varios textos cifrados con el mismo algoritmo. El adversario se concentra entonces en descifrar todos los textos posibles o mejor aún la clave (o claves) utilizadas. Esta es la peor situación para el criptoanalista.
2. *Ataque sólo con texto original conocido*: el criptoanalista tiene acceso a uno o varios mensajes sin cifrar y sus correspondientes cifrados. Su trabajo consiste en deducir la clave o claves usadas o bien en conseguir un algoritmo para desencriptar cualquier mensaje que utilice la misma clave. Este caso se da también cuando se conoce el tema del que trata el mensaje o parte de él como por ejemplo las cabeceras de los mensajes de correo o si se trata de código fuente buscando las palabras claves frecuentes.
3. *Ataque con texto original escogido*: en este caso el atacante puede obtener cifrado cualquier texto que él desee con la misma clave que el mensaje que trata de descifrar. Este ataque es más fuerte que el anterior porque permite al criptoanalista elegir ciertos patrones que le aporten información para elegir o descartar claves posibles.
4. *Ataque con texto original adaptativo*: una variación del anterior, y más fuerte todavía, el atacante puede elegir los textos que quiere ver cifrados en función de los resultados obtenidos al cifrar textos anteriormente elegidos.
5. *Ataque con texto cifrado elegido*: el criptoanalista puede obtener los textos originales correspondientes a ciertos textos cifrados de su elección.

Además y aunque menos 'académicos' a menudo los métodos más eficaces y temibles: amenazas, sobornos, chantajes o torturas.

*«Nihil tam munitum quod non expugnari pecuna possit.» (Ningún lugar está tan fuertemente defendido que no pueda ser conquistado mediante el dinero).* Marco Tulio Cicerón, 106-43 a.C.

Para concluir estas consideraciones sobre criptoanálisis, reseñaremos algunos conceptos utilizados de manera uniforme en el criptoanálisis científico.

*Distancia unívoca:* Es la cantidad mínima de mensaje necesaria para poder descifrar la clave. Cuanto mayor sea la distancia unívoca, más seguro es el sistema, el sistema ideal debería tener una distancia unívoca infinita.

*Romper un sistema:* Conseguir un método práctico para descifrar la clave de un sistema criptográfico. En base a esto se califican los sistemas de la manera que sigue.

*Sistema incondicionalmente seguro:* El criptograma que genera tiene una longitud menor a la distancia unívoca.

*Sistema probablemente seguro:* No se ha probado, al momento de la calificación, como romperlo.

*Sistema condicionalmente seguro:* Los analistas potenciales, al momento de la calificación, no poseen medios para romperlo.

Debemos aclarar aquí que no existen los sistemas completamente seguros, pues siempre un sistema puede ser roto probando todas las claves posibles. Dada esta premisa, la criptografía, busca siempre que los sistemas cumplan con una de las siguientes condiciones:

- El precio para romper un sistema es más grande que el valor de la información que resguarda.
- El tiempo necesario para romper un sistema es más extenso que el tiempo de vida útil de la información.

*c) Sistemas Criptográficos*

Se sabe que ya indios, chinos, persas y babilonios poseían desde la antigüedad signos equivalentes a las letras de sus alfabetos con los que comunicaban órdenes secretas a sus emisarios, en especial en tiempos de guerra[35].

Un método original consistía en afeitar la cabeza de un esclavo y escribir sobre su piel el mensaje que quería enviarse, esperando a que el pelo creciera podía enviarse al emisario sin que nadie sospechase que era transmisor de información, claro está que algunos estudiosos incluyen a este tipo de técnicas dentro de la estenografía y no entre las técnicas de criptografía, aunque su finalidad sea la misma.

También en Esparta durante los enfrentamientos de ésta con Atenas se utilizaban largas tiras de papel sobre las que escribían una vez enrolladas sobre un bastón. Al desenrollar la tira, resultaba ilegible para cualquiera que desconociera el método o no tuviera un bastón del mismo grosor.

34. MundoCripto. www.mundocripto.com. Jaime Suárez Martínez. Agosto 2000.
35. MundoCripto. www.mundocripto.com.

En la edad media, los copistas camuflaban a veces su nombre en los manuscritos, sustituyendo vocales por puntos (al modo 'fuga de vocales') o consonantes arbitrarias.

La República Veneciana en continuos conflictos con sus vecinos mezclaba caracteres griegos o hebraicos con los latinos al transmitir mensajes en tiempos de guerra.

Los primeros sistemas de criptografía no incluían en su modelo la utilización de una clave o llave que resolviera el sistema. En efecto, primitivamente los sistemas de encripción de texto, se basaban en la transposición de las palabras, sílabas o letras que componían el mensaje de acuerdo a reglas preestablecidas que tanto el emisor como el receptor del mensaje conocían. Este conjunto de reglas es lo que podemos llamar un algoritmo.

El más clásico de todos los métodos de los cuales hemos tenido noticia, es tal vez el método Julio César, que consistía en sustituir las letras que componían las palabras del mensaje, por las que ocupaban tres posiciones más adelante en el alfabeto del latín.

Con el tiempo los sistemas transposiciones se fueron haciendo cada vez más complicados, primero surgieron los sistemas monoalfabéticos, que se basan en sustituir cada letra por otra que ocupa la misma posición en un alfabeto desordenado. El principal inconveniente está dado por lo dificultoso de recordar un alfabeto desordenado. Es aquí entonces dónde hace aparición en el esquema de los sistemas criptográficos la utilización de las palabras claves, que a todas luces son más fáciles de recordar que un alfabeto desordenado. Mediante el uso de un algoritmo conocido, y la palabra clave, se podían determinar tantos alfabetos desordenados como palabras claves existieran.

A mediados del siglo XV, se publicaron los primeros sistemas polialfabéticos. En estos, ya no se utilizaban un único alfabeto desordenado para todo el mensaje, sino que a cada letra del mensaje le correspondía un alfabeto desordenado, que se determinaba por conjunción de un algoritmo conocido, una palabra clave y la letra del criptograma.

Recién a mediados del siglo XIX se logró publicar una solución generalizada para los métodos polialfabéticos, poniendo fin a cuatro siglos de silencio.

Como ocurrió a lo largo de la historia con muchos avances científicos, eran las guerras las que impulsaban el desarrollo de los sistemas criptográficos y del criptoanálisis, y el nacimiento de las primeras máquinas para realizar cálculos automáticos y veloces hicieron que la criptología diera un gran salto durante el siglo XX.

Sin embargo recién en la década del setenta, podemos anunciar el nacimiento de la criptografía moderna, y no hubiera sido esto posible sin el nacimiento de las computadoras digitales.

Fue durante la década del setenta, dónde nacieron los sistemas criptográficos que conocemos y utilizamos en la actualidad. A partir de allí, la criptología se dividió en dos grandes grupos, sistemas de clave única o simétrica, y sistemas de clave doble o asimétrica, que nunca dejaron de avanzar, y que en algunos momentos, lejos de competir, se han complementado y potenciado mutuamente.

*d) Sistemas de Criptografía Simétrica*

Hablamos de sistema de clave simétrica, cuando es la misma clave la que se utiliza para resolver el cifrado y descifrado de los datos, esto equivale a decir que el algoritmo que produce la encripción y desencripción de la información, es único. Este sistema requiere entonces, que tanto el emisor del dato, como su receptor utilicen el mismo algoritmo (método de cálculo) y la misma clave.

Justamente, en este punto se encuentra la debilidad más grande del sistema de clave simétrica. De hecho, para mantener la seguridad, es necesario que sólo el emisor y el receptor del mensaje conozcan la clave, si no se cumple esta premisa el sistema de seguridad se derrumba.

En su funcionamiento el sistema se debilita al ser necesario en ciertos supuestos la transmisión de la clave, que no está exenta de ser interceptada por terceros. Si bien existirían medios para transmitir una clave por canales seguros (siempre es menos costoso en término de esfuerzos transmitir una clave por canal seguro que un mensaje entero) nos hallamos siempre con el problema de la identidad del sujeto a los efectos de utilizar el sistema como método de firma digital. En efecto al ser esta una clave compartida no habría manera de imputar inequívocamente la identidad del sujeto que emitió el mensaje o información, ya que todo lo que puede hacer uno de ellos lo puede hacer el otro.

Nos damos cuenta entonces, que durante varios siglos, estos sistemas han sido aptos para mantener en secreto un mensaje, información o dato, pero no lo son para cumplir con los requisitos necesarios de una firma digital.

Claro está que los sistemas de cifrado simétrico no tienen todas las de perder. De hecho, los algoritmos de cifrado simétrico son más simples de desarrollar y su ejecución o cálculo es infinitamente más rápida que los de cifrado asimétrico que se basan en operaciones matemáticas mucho más complejas, esto permite el uso de claves más largas, que hacen más compleja la ruptura del sistema. Además su simplici-

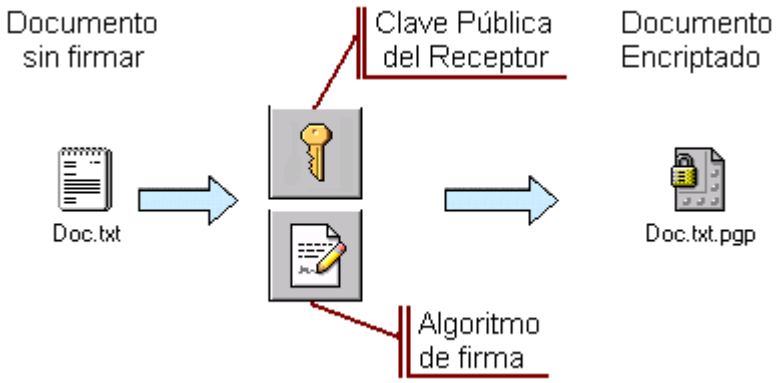
dad y velocidad hacen que sean más baratos, siendo el costo de la seguridad un punto que nunca debe dejarse de tener en cuenta. Es por esto que la criptografía simétrica no ha sido dejada completamente de lado, y muchas aplicaciones de firma digital la utilizan en combinación con métodos de cifrado asimétrico.

*e) Sistemas de Criptografía Asimétrica*

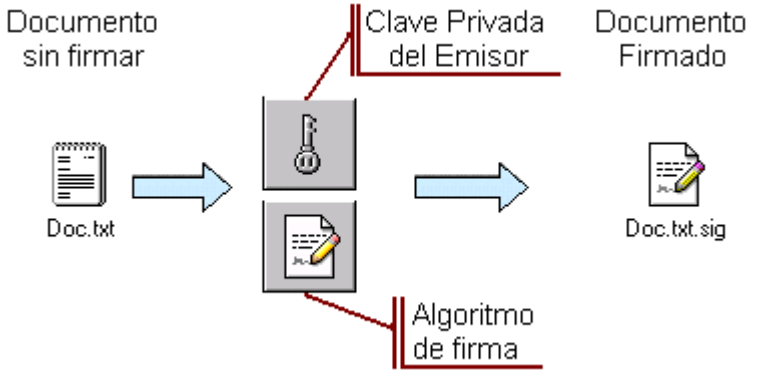
En términos históricos, son estos sistemas absolutamente nuevos, pues se han descubierto y desarrollado a partir de la segunda mitad de la década del setenta. Conceptualmente resuelven mediante distintos cálculos matemáticos, el problema de la clave única, o dicho de otra manera, el problema del secreto compartido del que adolecen los sistemas de cifrado simétrico. De hecho, todos los sistemas de clave asimétrica desarrollados (tal vez más de una treintena a los que deben sumarse sus variantes y combinaciones), utilizan un par de claves para su funcionamiento, dónde una es utilizada por el emisor para cifrar el mensaje y otra por el receptor para descifrarlo.

Estas claves tienen la propiedad de que cada una de ellas invierte la acción de la otra pero, y aquí está el punto más relevante, a partir de una no se puede obtener la otra. Estas claves son normalmente números muy largos que estructuralmente no difieren en lo absoluto el uno del otro, y de manera convencional se mantiene una de ellas secreta, y se la denomina clave privada, mientras se da a conocer la otra a toda la comunidad, denominándola clave privada.

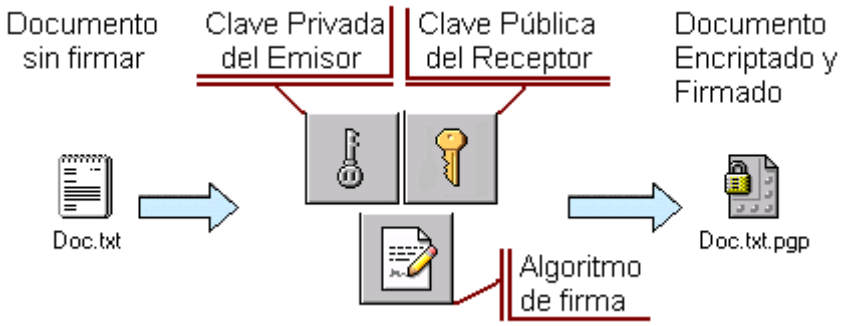
La clave privada deberá ser custodiada por el usuario y es imprescindible que se mantenga en secreto. La clave pública, por el contrario, se publicará junto con la identidad del usuario. Así cuando se quiera enviar un mensaje seguro a un usuario se tomará la clave pública de este y se utilizará para cifrar el mensaje que se quiera enviar. El resultado de esta operación será el texto cifrado que sólo el propietario de la clave privada correspondiente a esa clave pública podrá descifrar (Ver figura siguiente).




De otra forma, podríamos aplicar a ese mensaje la clave privada del emisor, esto si bien no asegura la confidencialidad del mensaje, pues cualquier persona que tenga acceso al mensaje y a la clave pública del emisor – todas por definición del sistema – podrá saber sobre el contenido del mismo, nos asegura si, la identidad de su emisor, pues el hecho de que una firma digital sea verificable por medio de una cierta clave pública implica necesariamente que esa firma fue creada por la correspondiente clave privada que, necesariamente, el firmante siempre mantuvo secreta y nunca divulgó (Ver figura siguiente).



Finalmente, podríamos aplicar a ese mensaje sucesivamente la clave privada del emisor y la clave pública del receptor, esto nos brindaría los dos servicios para los que fueron pensados los sistemas de criptografía de clave asimétrica, es decir confidencialidad, pues sólo podrá abrir el mensaje el destinatario con su clave privada, y autenticación, pues solo podrá verificarse la autenticidad con la clave pública del emisor (Ver figura siguiente).




Llegados a este punto, alguien podría preguntase si existen dos claves tan íntimamente ligadas de manera tal que inviertan sus acciones pero donde el hecho de conocer una no implique conocer la otra.

La respuesta a esta pregunta es si y la herramienta para obtenerlas son los números primos. Si bien hemos dicho que “no se puede” obtener la clave privada a través de la pública, debemos matizar éste “no se puede”.

Cuando nos referimos a ”no poder” queremos decir que no existen algoritmos ni ordenadores suficientemente eficientes para obtener una clave a partir de la otra en un tiempo razonable (de nuevo el calificativo “razonable” dependerá en cada caso del periodo de validez que se quiera que tengan las claves), en definitiva no resulta computacionalmente posible. En buen romance diremos entonces que la imposibilidad es práctica y no metafísica. El problema básico que se utiliza en los sistemas de clave pública es el de la factorización.

Factorizar un número es descomponerlo en producto de números primos y esta operación, cuando tratamos de números grandes, resulta un problema difícil de resolver.

Existen diferentes sistemas de clave pública pero el más extendido y el que se considera un estándar de facto es el RSA. Este criptosistema, creado en 1978 por Rivest, Shamir y Adleman (de las iniciales de ellos deriva su nombre), se basa justamente en el hecho de que, hasta ahora, la tarea de factorizar es muy difícil.

Así pues, parece que el problema de la seguridad quedaría del todo solucionado con los sistemas de clave pública. Sin embargo resta el problema de la suplantación de identidad, es decir, cómo asegurarnos que la clave pública que utilizamos para validar la firma digital, realmente pertenece a la persona al que se dice pertenecer.

Aquí entra a jugar un papel importante la Infraestructura de Firma Digital (PKI por sus siglas en inglés: Public Key Infraestructure)

**14. Confianza**

Tal vez, sea este uno de los puntos más arduos de tratar cuando hablamos de sistemas de firma digital y de documentos digitales. Si bien queda objetivamente claro que con el desarrollo actual de las ciencias de la informática, el sistema de claves asimétricas es seguro y práctico para los fines en que se lo pretende usar, en el aspecto subjetivo de la cuestión, podemos decir sin temor a equivocarnos, que por naturaleza el hombre tiende a desconfiar de lo que no conoce plenamente, y de aquello que no puede aprehender con sus sentidos.

Tal como lo reseñáramos antes, el sistema de escritura por medio de trazos sobre papel o algún medio similar, es un hecho culturalmente asimilado a lo largo de siglos de historia, que no podemos pretender suplantar en poco más de una década de desarrollos informáticos. Nos referimos a este lapso, porque, si bien las computadoras existen desde hace algunas décadas más, recién a partir de fines de la década de 1980 las computadoras comenzaron a irrumpir masivamente en los hogares, siendo antes un reinado exclusivos de grandes corporaciones o altos centros de estudio.

A pesar de lo subjetivo del asunto, existen métodos para determinar la confiabilidad de un sistema de firma digital, análogos al que se utiliza para determinar la confiabilidad de cualquier sistema informático.

Para esto es necesario establecer una *Cadena de Confiabilidad*, que se compone esencialmente de tres piezas que tienen todas ellas igual importancia y que son a saber, a) criptosistema seguro, b) implementa-

ción segura y c) la utilización a conciencia por parte de los usuarios.

Se considera que un criptosistema es seguro cuando no es posible acceder a los datos que protege, sin poseer la clave adecuada, y tampoco es posible crear una firma sin poseer la clave privada pertinente, es decir, cuando no es posible "falsificar" la firma digital.

Es generalmente aceptado en la actualidad que los criptosistemas de clave asimétrica, cumplen, bajo determinadas condiciones, con estos requisitos indispensables. Es necesario que ese criptosistema cuente con algoritmos de reconocida resistencia, tanto teórica como práctica, es decir que haya recibido la suficiente atención y exhaustivo análisis por parte de la comunidad científica especializada, y que haya resistido también los ataques a los que normalmente puede ser sometido. El algoritmo de clave asimétrica más popular de la actualidad, el RSA, con claves superiores a los 2048 bytes de longitud, ha resistido hasta ahora todo tipo de ataques, en efecto aún no ha sido posible quebrarlo mediante un ataque de "fuerza bruta" (no es computacionalmente posible) y el problema sobre el que se basa, la factorización de números primos grandes, no ha sido resuelto de manera práctica.

Por implementación segura, se entiende el respeto de todas las normas de seguridad informática y calidad de software y hardware. Por ejemplo, la implementación maligna de un mecanismo de firma digital en un programa de computadora podría hacer que fuera posible capturar la clave secreta de firma y guardarla sin que el usuario se percate en un archivo, perdiendo así este el control absoluto de su clave, lo que haría que el sistema deje de ser confiable, pues nos hallaríamos ante la posibilidad de que alguien más utilice esa clave para falsificar la firma.

El punto de la implementación segura, puede ser cubierto únicamente utilizando software elaborado por empresas serias y conocidas, con suficiente solvencia moral y económica.

En el concepto de Implementación segura, podemos incluir lo que la Ley de Firma digital del Estado de Utah define como "Sistema Confiable", y que exige que los equipos y programas de computación sean razonablemente confiables contra la posibilidad de intrusión o uso indebido, que brinden un razonable grado de disponibilidad, confiabilidad y correcto funcionamiento, y que se adapten debidamente al desempeño de sus funciones específicas[36].

Finalmente, el usuario también tiene su cuota de participación al momento de establecer la Cadena de Confiabilidad a la que estamos haciendo referencia. En efecto, es necesario que el sistema sea utilizado a conciencia por parte de todos los partícipes. Aunque contemos con el mejor algoritmo de firma que las ciencias exactas puedan elaborar, y la implementación realizada respetando los más altos estándares de seguridad y calidad en software y equipos de computación e infraestructura de comunicación, el sistema se debilita sustancialmente si cada usuario no protege debidamente su clave privada. Las claves nunca deben ser dejadas a disposición de terceros, por mucha confianza que ellos nos merezcan, y no deben ser compartidas por los usuarios.

Por ello la confiabilidad de un mecanismo de firma digital depende de los eslabones del criptosistema, su implementación y su utilización que, conjuntamente, forman una cadena cuyo grado de confiabilidad está dado por la resistencia de su eslabón más débil.

**15. Infraestructura de firma digital - Dinámica**

Como lo planteamos al final del punto 13-e, si bien el sistema de firma digital basado en claves simétricas ha demostrado su seguridad y utilidad práctica, restaba todavía el problema de la suplantación de identidades.

*a) Antecedentes*

En la medida en que la firma digital de clave asimétrica se utilizó informalmente, el problema de la suplantación de identidad no parecía un inconveniente insuperable ni demasiado grave. El esquema de firma adoptó y logró la evolución natural del el concepto de la certificación. Dijimos antes, que una clave privada está indisolublemente asociada a una clave publica. Ahora bien, como esta clave pública puede ser incorporada en un documento digital estándar (certificado) este puede recibir tantas firmas como sean necesarias, es decir, se puede firmar una clave. Basándose en esta posibilidad, se fueron construyendo las primeras redes de confianza. Cada comunidad fue constituyendo sus repositorios (depósitos) de claves públicas. Cuando una persona estaba segura de la pertenencia de una clave a otra determinada persona (porque tal vez había recibido una copia de la misma por una canal seguro o personalmente) aplicaba a esa clave pública su firma, es decir la certificaba. Cuanta mayor cantidad de firmas acumulaba una clave pública en su certificado, más confiable resultaba la identidad de la persona a la que pertenecía la clave privada correlativa.

36. Ley de Firma Digital de Utah. Título 1. Título abreviado, interpretación y definiciones, Artículo 103. Ítem 37.

Luego, la evolución del sistema llevó a que se incorporara al esquema el concepto de **transmisión de confianza,** que se resume en la posibilidad que tiene cualquier usuario de establecer que confía en las claves en las que confía determinada persona o grupo de personas.

Mientras no existieron legislaciones que dieran a la firma digital los mismos efectos que tiene la firma ológrafa, este sistema fue sobradamente suficiente. En la medida en que se pretendió regular el sistema para otorgarle efectos legales, fue necesaria la creación de entidades certificadoras, es decir, entes ubicados un escalón más arriba que los usuarios, que certifican las claves públicas y en las que todos podemos, o deberíamos poder, confiar.

Claro que el debate en este punto es de los más arduos, pues no fue fácil, ni es fácil determinar quien es tan confiable como para que la sociedad toda confíe en él. Pero antes de entrar en las consideraciones de este debate, expondremos el modelo teórico de la Infraestructura de Firma Digital (PKI).

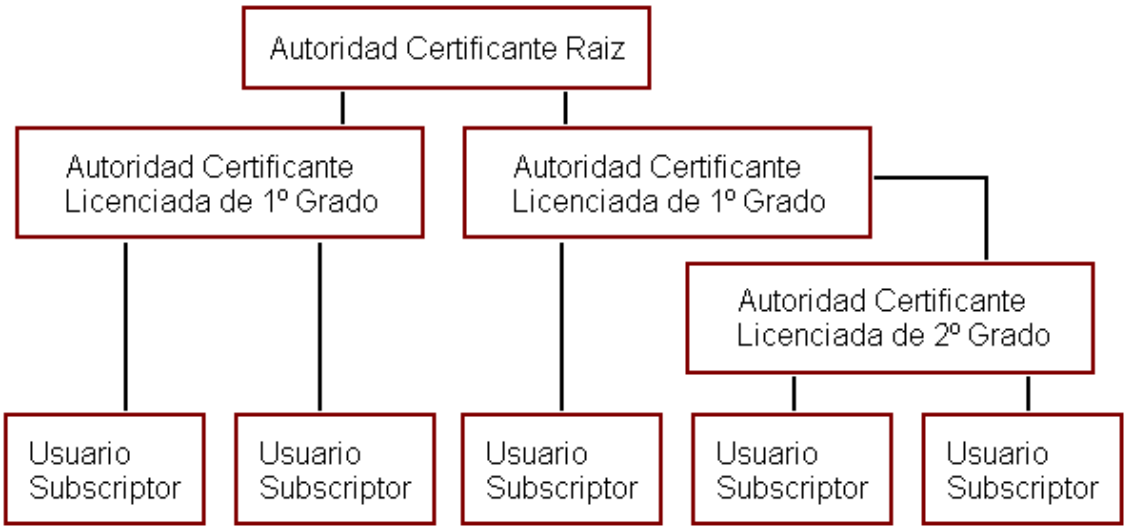
*b) Terceras partes confiables*

Una Infraestructura de Firma Digital es un conjunto de hardware, software, bases de datos, redes, procedimientos y obligaciones legales, que permite que las personas físicas y jurídicas se identifiquen entre si al realizar transacciones o intercambiar documentos electrónicos.

Sin perjuicio de las diferentes variantes que pueden plantearse un esquema teórico de base podemos encontrar en ella a los siguientes actores: una Autoridad Certificante Raíz, una o varias Autoridades Certificantes Licenciadas dispuestas en uno o más grados, y finalmente los usuarios suscriptores. Se ha observado también, pero con menos frecuencia la presencia de otras entidades intermedias, entre el usuario y las Autoridades Certificantes Licenciadas, que funcionan como intermediarias de la oferta y demanda de certificados digitales. La difusión de este tipo de actor en la Infraestructura de Firma Digital se vuelve particularmente interesante en nuestro país, dónde la gran dispersión geográfica dificulta el asentamiento de empresas o sucursales de las mismas que brinden este tipo de servicio en el Interior del país, tarea que podría ser delegada en entidades públicas o privadas a nivel local como lo podrían ser las cámaras de comercio o agrupaciones civiles de distinto tipo.

Aunque parezca paradójico, en la era de la información y las telecomunicaciones, dónde los mercados se han vuelto virtuales, intemporales y geográficamente ilimitados, es necesaria la presencia local de la Autoridad Certificante Licenciada o un delegado de la misma, a fin de otorgar certificados confiables, pues dependiendo del tipo de certificado que se otorgue al usuario puede ser necesario constatar personalmente datos como su identidad, su domicilio o su teléfono, no alcanzando a veces una simple declaración jurada del usuario acerca de estos datos.

En definitiva, lo que se plantea es la necesidad de que exista una infraestructura de terceras partes confiables *(trusted third party)*. Estas son las encargadas de mantener registros de claves públicas en línea y de prestar otros tipos de servicios relacionados con la firma digital, como el *time-stamping*, que equivale a una firma digital que además da fecha cierta a un documento digital.




*c) Certificados.*

Son registros electrónicos que atestiguan que una clave pública pertenece a determinado individuo o entidad, y que al momento de solicitarlo este era poseedor de la clave privada que se corresponde unívocamente con ella.

Su finalidad, como ya lo hemos entrevisto a lo largo del desarrollo, es identificar el par de claves con el usuario o firmante. Este es en definitiva el servicio más importante que debe prestar la Autoridad Certificante.

En su aspecto material se trata de un archivo digital que contiene una clave pública, el nombre o denominación de su propietario, la fecha de vencimiento del certificado (y correlativamente de las claves que certifica), el nombre de la autoridad certificante, el número de serie del certificado, el todo firmado con la clave privada de la autoridad que lo emitió.

Quien quiera obtener uno de estos certificados deberá seguir los siguientes pasos. En primer lugar generar el par de claves en su computadora utilizando un software apropiado[37], hacemos notar, que está prohibido para las autoridades certificantes generar el par de claves que ha de certificar, para evitar todo tipo de sospecha sobre quien posiblemente posea la clave privada. Luego esta persona deberá presentarse ante una autoridad certificante para registrar su clave pública acreditando su identidad, y esta expedirá el correspondiente certificado. Normalmente la Autoridad Certificante entrega al firmante el certificado de firma digital a la vez que lo publica en un sitio de Internet accesible al público.

Basándose en este modelo de funcionamiento, muchos países, entre ellos el nuestro, están elaborando las normas necesarias para otorgar validez al uso de la firma digital, equiparándola en sus efectos a la firma ológrafa. Analizaremos a continuación la Ley 25.506 de diciembre de 2001, para la cual en la actualidad se está elaborando el Proyecto de Decreto Reglamentario.

# Capítulo 5
# Análisis de Legislación

**16. Legislación doméstica - Ley de Firma Digital 25.506**

Con fecha 14 de noviembre de 2001 fue sancionada la Ley 25.506 de Firma Digital, y con fecha 11 de diciembre del mismo año fue promulgada por el Poder Ejecutivo Nacional. Con ella, Argentina se sumó al grupo de países que han reconocido y regulado la validez jurídica de la firma digital.

Distintas han sido en el mundo las actitudes legislativas que se han tenido respecto de este tema, al respecto se ha observado:

a) una postura amplia en que el legislador establece la validez del documento electrónico, sin hacer referencia a su soporte material ni al tipo de lenguaje a utilizar. Tampoco se analiza o se ajustan otras normas que hacen referencia al documento tradicional (es el caso del Proyecto del Estado de California, y de la Electronic Signature Act of 1996, del Estado de Florida);
b) una postura restringida en que el legislador se preocupa no sólo de establecer la validez jurídica del documento electrónico sino también de reglamentar su uso, a la vez que determina detalladamente la infraestructura técnica y operacional que se utilizará para la inserción del mismo en la práctica comercial (como en Utah Digital Signature Act, de 1995; y Georgia Digital Signature Act de 1996);
c) una postura detallista en que el legislador revisa todo el cuerpo legal para derogar, modificar o agregar normas que hagan compatibles el sistema con el documento electrónico (como en el caso del Proyecto del Gobierno de Alemania); y por último,
d) algunas combinaciones, donde se encuentra un sistema de intervención junto con algunas características de las posturas antes referidas. (como en el Proyecto de Ley sobre Documento Electrónico realizado por Ediforum Italia y Proyecto de Ley sobre Documentos Electrónicos de Chile)[38].

Podríamos incluir la norma Argentina en el primer grupo, dado que no se modifica ni se revisan otras partes del cuerpo normativo vigente, con la salvedad del artículo 78 bis del Código Penal, dónde se introduce la equiparación de la firma digital a la firma ológrafa, la acción de suscribir a la de crear una firma digital, y los términos documento, instrumento privado y certificado al documento digital firmado digitalmente.

A lo largo de 53 artículos dispuestos en once breves capítulos y un Anexo, se regula el régimen jurídico de la firma digital, otorgándole – salvo exclusiones taxativamente determinadas en el artículo 4º – los mismos efectos que la firma ológrafa (artículo 3º).

La manera en que está redactada la norma, nos hace pensar que el legislador proyectó una ley a largo plazo, ya que se ha evitado establecer en ella los estándares tecnológicos de funcionamiento que pueden

37. Contienen esta funcionalidad entre otros: a) Internet Explorer de Microsft Inc. desde su versión 4.0 en adelante, b) los clientes de correo electrónico Outlook Express desde la versión 4.0 en adelante y MS-Outlook desde la versión 97 en adelante de Microsoft Inc. y Lotus Notes de IBM Inc. c) PGP (Pretty Good Privacy) en todas sus versiones. d) Acrobat desde la versión 5.0 en delante de Adobe Inc.

38. DEVOTO Mauricio y LYNCH Horacio M., “Banca, comercio, moneda electrónica y la firma digital”. En www.notaríadigital.com

devenir obsoletos, dejando esta tarea a cargo de la Autoridad de Aplicación, según se prevé en el último párrafo del artículo 2º.

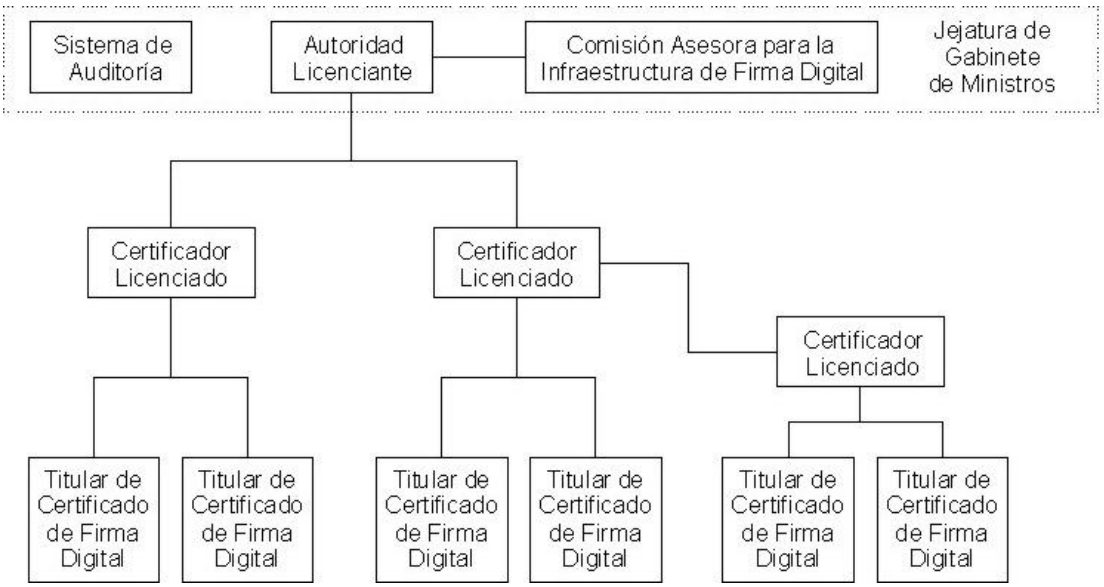
Sin embargo, la norma no ha logrado abstraerse totalmente en este plano, y encontramos a lo largo de su redacción variadas referencias al **sistema de firma digital de clave asimétrica** sin que éste sea nombrado expresamente. Prueba de ello, existe en el Anexo dónde en la definición de una variada gama de términos, se incluyen las definiciones de "Clave Criptográfica Pública" y "Clave Criptográfica Privada".

Por otra parte, a lo largo de la norma se hace referencia también a "*información de exclusivo conocimiento del firmante*" (artículo 2º), "*datos de creación de firma digital*" (artículo 21 incisos b, c y p, artículo 25 incisos a y c, artículo 31 inciso c), "*datos utilizados para generar la firma digital*" (artículo 31 inciso a y b), dónde la alusión a una clave criptográfica privada es clara y las referencias a "datos de verificación de firma" (artículo 9 inciso b, artículo 13, artículo 19 inciso a), "*Información necesaria para la verificación de la firma*" (artículo 14 inciso b subítem 4) dónde se refieren a la clave criptográfica pública.

La norma intenta ajustarse a estándares internacionales, pero como veremos a lo largo de su análisis hay varios puntos que pueden ser objetables.

*a) Infraestructura*

Como marco general, se establece que la Jefatura de Gabinetes de Ministros será la Autoridad de Aplicación de la norma (Capítulo VI), y se la constituye en la Entidad Licenciante Raíz, se determina la existencia de Certificadores Licenciados (Capítulo III), y se deja en manos de la autoridad de aplicación la determinación de cuantos niveles de licenciamiento van existir (artículo 30 inciso g), para completar lo que se considera la estructura básica de lo que conocemos con la sigla PKI o Infraestructura de Clave Pública se regulan los derechos y obligaciones del titular del certificado digital. Adicionalmente, se establecen dos figuras más, un sistema de Auditoria (Capítulo VII), cuyo diseño está a cargo de la Autoridad de Aplicación, y una Comisión Asesora para la Infraestructura de Firma Digital (capítulo VIII).




*b) Efectos legales*

El artículo 1º, no agrega mucho a lo que luego dirá el resto de la ley, en efecto se limita a decir que reconoce le empleo de la firma electrónica y la firma digital (debería citarlas en orden inverso pues la primera es un subgénero de la segunda) y su eficacia jurídica en las condiciones que establece la ley.

En el artículo 3º equipara la firma digital a la firma ológrafa, estableciendo que esta satisface el requisito de firma, cuando cualquier normativa establece la obligación de firmar o prescribe consecuencias para su ausencia.

El artículo 12º – último del Capitulo I – establece que queda satisfecha la obligación de conservar documentos, registros y datos, con la conservación de los correspondientes documentos firmados digitalmente. Establece que para producirse este efecto, además de cumplirse con los requisitos que determine la reglamentación, estos deberán ser accesibles para la consulta posterior, y permitir mínimamente determinar su origen, fecha y hora de generación, envío y/o recepción.

Este último artículo es tan importante como los demás, pues a medida que el sistema entre en funciona-

miento permitirá reducir considerablemente el volumen de papel archivado y hacer más fácil la recuperación de los documentos para su posterior consulta, debido a las naturales ventajas de los sistemas informáticos por sobre el archivo tradicional.

Debemos recordar que el archivo de legajos y documentos en general está causando serios problemas de infraestructura edilicia en muchas reparticiones públicas, dónde inclusive está en peligro la integridad estructural de algunos de los edificios que las alojan. Por lo general estos archivos se encuentran en un pésimo estado de conservación, produciéndose la pérdida de documentos muchas veces valiosos por el deterioro producido por las malas condiciones ambientales de almacenamiento o simplemente porque es imposible acceder físicamente a ellos.

*c) Exclusiones.*

En su artículo 4º la ley enumera las materias a las que no es aplicable el uso de la firma digital. Estimamos que este artículo ha sido incluido por el legislador para proteger a quien no conoce debidamente el funcionamiento de la firma digital, pues los estándares de seguridad que brinda hoy en día no la hacen incompatible con las materias citadas en la enumeración que realiza el mismo.

Se excluyen en los primeros tres incisos a las disposiciones por causa de muerte, a los actos jurídicos del derecho de familia (aquí el legislador debería haber sido más preciso, pues por ejemplo no vemos ningún inconveniente en que un acto del derecho de familia de contenido patrimonial como un convenio de alimentos sea firmado digitalmente por las partes) y los actos personalísimos en general.

En el cuarto y último inciso, tal vez a nuestro juicio el más importante, se hace referencia a los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes. Un ejemplo de esto lo constituyen entre otras cosas las escrituras públicas que necesariamente deben ser escritas y plasmadas en papel en cuanto luego deben ser incorporadas a un protocolo, entre otras reglas de procedimiento que deben cumplir de manera estricta los escribanos públicos.

Si la materia tiene finalmente la recepción esperada, creemos que cada día serán menos los casos que entren en las exclusiones por vía de este inciso, pues es de esperar que paulatinamente se vayan adaptando las leyes a la recepción de este novedoso método de firmar y autenticar documentos.

*d) Documento digital.*

En el artículo 6º – probablemente debería haber sido uno de los primeros – el legislador ha definido el concepto de Documento Digital. La redacción del artículo merece una pequeña crítica por el método que utiliza para realizar la definición, en efecto dice que "… se entiende por documento digital a la representación digital de hechos o actos…" , lo que a todas luces es una definición redundante dado que remite al objeto definido.

Ya hemos dicho en el Capítulo 2 de este mismo trabajo que un documento es según la definición dada por Chiovenda "toda representación material destinada e idónea para reproducir una cierta manifestación del pensamiento". Decir que un documento digital es una representación digital no agrega por lo tanto nada de esclarecedor al objeto de estudio que se nos presenta.

Finalmente creemos conveniente reemplazar *actos y hechos* por *datos,* en cuanto resulta una locución más amplia, pero no menos útil o precisa para los fines en que se la pretende utilizar.

*e) Presunción de autoría e integridad*

Los artículos 7º y 8º de la ley establecen presunción de autoría e integridad. Estas presunciones son *iuris tantum* y por lo tanto pueden ser desvirtuadas con las pruebas correspondientes a cargo de quien afirme lo contrario.

La principal condición para que estas presunciones tengan efectos está dada por la validez de la firma digital, que está regulada en el artículo 9º de la misma ley.

Los efectos prácticos de estas presunciones no son menores, entre ellos tenemos por ejemplo que se torna innecesario el reconocimiento judicial de firma en los documentos privados. De hecho, en un documento firmado digitalmente, ya no será la contraparte la encargada de probar que la firma pertenece al firmante que ella señala como tal, sino que será el titular del certificado de firma digital quién deberá probar apropiadamente que no es él quien firmó digitalmente el documento que se le endilga.

*f) Firma electrónica*

En el artículo 5º de la ley, se ha dado recepción al concepto de firma electrónica. Esta es una firma digital a la que le falta alguno de los requisitos legales para ser considerada como tal. En algunos proyectos de ley de otros países (por ejemplo el español) esta clase de firma es llamada firma digital, mientras que lo que en nuestra legislación se llama así, es nombrada como firma digital avanzada.

Creemos que el concepto debería ser afinado y hacer referencia a la falta de algún requisito no esencial, ya que de faltar alguno de estos, el objeto no debería ser considerado siquiera como una firma electrónica.

Más allá de la manera de llamarlo y de su alcance ideal, el concepto no debe ser menospreciado por sus implicancias prácticas. En efecto, cuando nos encontremos ante una firma electrónica, se revierten las presunciones de las que hablamos en el acápite anterior, y de ser desconocida, será tarea de quien la invoca, probar su validez. También se deberá dar el lugar apropiado a la autonomía de la voluntad en cuanto no se afecten normas de orden público.

Sin contar aún con la aplicación práctica del sistema, puede resultar difícil imaginar situaciones en las que nos hallemos ante una firma electrónica, sin embargo entre otras podemos prever las siguientes:

- Firmas creadas utilizando claves amparadas en certificados emitidos por Entidades Certificantes nacionales no reconocidas por la Autoridad de Aplicación.
- Firmas creadas utilizando claves amparadas en certificados emitidos por Entidades Certificantes extranjeras que no estén incluidos en los supuestos del Artículo 16.
- Firmas creadas utilizando claves amparadas en certificados vencidos.
- Firmas realizadas en operaciones por montos mayores a los autorizados por el certificado (artículo 23 inciso b)

*g) Validez de la firma digital*

El artículo 9º de la ley establece los requisitos de validez de la firma digital, y si bien responde a los estándares en la materia, parece interesante dedicar algunas líneas al análisis de su redacción.

Establece el mismo en su inciso C que una firma digital es válida cuando el "…certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado…".

Debe tenerse en cuenta que el artículo 16 hace referencia al reconocimiento de certificados emitidos en el extranjero. Es por esto que creemos que se debe interpretar, que cuando hace mención de la *emisión*, se refiere a Autoridades Certificantes nacionales (emisión según lo establecido en los artículos 13 y 14), mientras que el *reconocimiento* hace referencia aquellos certificados incluidos en el artículo 16 y que han sido emitidos por Autoridades Certificantes extranjeras.

*h) Original*

Regula la Ley lo referido a los originales en su artículo 11º. Establece este artículo que las copias o reproducciones de documentos electrónicos firmados digitalmente – agregamos: archivos o registros digitales – realizadas a partir de originales de primera generación serán considerados también originales y poseerán por lo tanto el mismo valor probatorio.

Hay entorno a este artículo varias cuestiones que considerar. En primer lugar no establece claramente el concepto de "original de primera generación". Por otra parte este no es tampoco un concepto común en la ciencia informática, que sería la primer fuente dónde buscar ayuda para esclarecer concepto técnicos o cuasi técnicos como este. Suponiendo que este concepto se refiere al archivo originado por el usuario de una computadora mediante una aplicación cualquiera y firmado digitalmente, tampoco queda claro si las copias o reproducciones de este archivo serán originales de primera generación o si serán originales de segunda generación, si es que este concepto existe. Menos claro aún resulta la situación de las reproducciones o copias de los segundos.

Más allá de tener en cuenta estas imprecisiones conceptuales que seguramente podrán ser neutralizadas por adecuadas interpretaciones doctrinarias y jurisprudenciales cuando el sistema entre en efectivo funcionamiento, hay un punto aún de mayor interés por sus efectos prácticos.

Nuestra normativa en efecto no contempla, la posibilidad de que se designe una instancia del documento para que sea original único. Esta omisión, excluye la posibilidad de utilizar la firma digital para todos aquellos documentos dónde la multiplicidad de copias hace que este pierda su utilidad.

De hecho, las consecuencias prácticas de este artículo hacen que sea imposible generar documentos que incorporen la vía ejecutiva para ser firmados digitalmente, pues nadie querrá que existan múltiples copias, todas con la misma validez legal, de un documento con estas características, como puede ser un cheque o un pagaré entre los ejemplos más clásicos y simples.

Este tópico merece una pronta revisión, teniendo en cuenta además que existen hoy los medios técnicos para designar un documento electrónico firmado digitalmente como único original, válido, efectivo y ejecutable.

*i) Certificados digitales*

En cuatro artículos – desde el 13 hasta el 16 inclusive – se regulan las pautas básicas sobre certificados digitales.

El concepto vertido sobre el mismo es suficientemente preciso para determinar su naturaleza, así como también suficientemente amplio para adaptarse a un cambio de tecnología. En efecto se refiere a este como el medio para vincular al titular del certificado con sus datos de verificación de firma digital. En el estado actual esto equivale a su clave pública.

En los Artículos 14 y 15 regula lo referente a los requisitos de validez y al período de validez del certificado de firma digital.

Lo referente a las causas que motivan la revocación de los certificados, ha sido incluido inciso e del Artículo 19. Esta ubicación es metodológicamente objetable, por cuanto el capítulo dónde se encuentra este artículo regula lo relativo al Certificador Licenciado y específicamente el artículo 19 regula sus funciones como tal. Pensamos que esta materia debería haberse regulado dentro del mismo Capítulo II que se dedica a los Certificados Digitales.

Otro aspecto que no contempla la ley, y que podría haberse previsto en la regulación del período de vigencia o los motivos de revocación, es el referente a la validez del certificado a partir del momento del fallecimiento de su titular (si fuese una persona física) o su disolución (si fuese una persona jurídica). Es de esperar que este tópico sea aclarado por la reglamentación de la ley y por las políticas de certificación de las Autoridades Certificantes que se designen, pues si bien es fácilmente subsanable a través de una coherente interpretación por parte de los magistrados del sistema normativo en su conjunto, no deja de ser un punto de conflicto que podría evitarse y que en honor a la precisión y calidad jurídica de la norma debería haber sido tomado en cuenta.

Más adelante, en el Artículo 23°, titulado Desconocimiento de la Validez de un Certificado, se establecen los motivos que determinan la invalidez de un Certificado Digital. Este artículo merece dos críticas puntuales.

La primera derivada de su ubicación dentro de la ley, en efecto el artículo 23° pertenece al Capítulo III que regula tópicos referentes al Certificador Licenciado. Si el artículo se refiere a la validez o invalidez de un Certificado Digital, debería haber sido incluido, junto con las demás reglas para este tema en el Capítulo II.

La segunda en cambio tiene que ver con su contenido mismo. En efecto, en los incisos a y b, lo que debería considerarse inválido en sí no es el Certificado Digital, sino la Firma Digital creada mediante la utilización del Certificado Digital en esas condiciones (finalidad diferente a la prevista cuando fue extendido y operaciones que superen el monto máximo autorizado).

Se desprende de una coherente interpretación que el Certificado Digital continúa siendo válido si se lo utilizara dentro de las condiciones de emisión, y que en caso contrario, según lo dispuesto en el artículo 5°, dará lugar a la creación de una firma electrónica en vez de una firma digital.

*j) Certificador Licenciado*

Al hablar del Certificador licenciado, debemos decir que estamos ante una de las caras más visibles de la Infraestructura de Firma Digital. Nuestra ley trata el tema en su Capítulo III y los define en el artículo 17º como toda "…persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante".

Se determina que en el ámbito del sector privado esta actividad se desarrollará bajo el régimen de competencia y que los aranceles serán libremente establecidos por los prestadores. Este concepto aunque parezca redundante, pues es una de las características de la libre competencia que los participantes establezcan las condiciones generales de contratación, nos sugiere un amplio régimen de libre competencia dónde el Estado renuncia inclusive a la fijación de tarifas mínimas o máximas.

En el artículo siguiente incluye entre quienes pueden emitir certificados digitales a las entidades que controlan las matrículas profesionales, aunque limita su actuación a la emisión de certificados en lo referido a esta función.

Si bien en el mismo artículo, somete a estas entidades al cumplimiento de los requisitos para ser certificador licenciado, no exige explícitamente, como en el artículo anterior que obtengan una licencia otorgada por el ente licenciante. De todos modos, a la luz de una interpretación coherente pareciera que deben tramitar tal licencia, pues es la única manera de probar el cumplimiento de los requisitos para ser certificador licenciado. Por otra parte pareciera incongruente que un organismo público, como podría serlo la AFIP al emitir certificados de firma digital para los contribuyentes o cualquier otra repartición pública al hacerlo para sus dependientes deba obtener tal licencia y una de estas entidades esté exenta.

En el artículo 19º se regulan las funciones del certificador licenciado. Establece en este punto la normativa algunos estándares de servicio que luego serán completados por las propias políticas de certificación y por la reglamentación que dicte la autoridad de aplicación en la reglamentación de la ley. A modo de ejemplo podemos citar las condiciones de emisión y revocación de los certificados, la obligación de información

pública del estado de los certificados por él emitidos, la obligación de identificar unívocamente a los certificados emitidos y de mantener copia de los mismos.

El artículo 20° establece las obligaciones básicas del Certificador Licenciado, sin perjuicio de las que luego pudiera establecer la Autoridad de Aplicación.

Se hace mucho hincapié en la obligación de información, la protección de claves privadas, la operación de un sistema técnicamente confiable que luego es definido en el anexo de la ley, la confidencialidad de los datos, la existencia de un plan de contingencias y de cese de actividades. Dispone también el artículo que los Certificadores Licenciados deberán constituir domicilio legal en la República Argentina.

Se establece que deberá mantenerse la confidencialidad de los datos que no se publican en el certificado digital. Debemos advertir, que respecto a los datos que si se publican, si bien son de público conocimiento, pues los certificados por definición deben estar disponibles en línea para la consulta de terceros interesados en verificar una firma digital, debería ser recabada de manera expresa la autorización del usuario para que estos sean utilizados de otra manera, como ser su inclusión en bases de datos destinadas a la comercialización o puesta a disposición de terceros.

Otro tema a tener en cuenta, es que si bien los Certificadores Licenciados están obligados a informar la manera en que garantizan su posible responsabilidad patrimonial con relación a los servicios prestados, no se establece en la normativa ningún parámetro para determinar la garantía mínima que deben prestar. Esperamos que este punto sea debidamente cubierto en la reglamentación de la Ley o en la normativa que deberá emitir la Autoridad de Aplicación.

*k) Titular de un certificado*

Respecto del Titular de un Certificado de Firma Digital, la ley establece en dos artículos sus derechos y obligaciones respecto de la utilización del sistema. Es de destacar, que incluso las obligaciones que están a su cargo tienen por fin último protegerlo e inducirlo a realizar una utilización a conciencia y segura de los servicios que presta la infraestructura de firma digital.

## 17. Legislación Comparada

*a) Ley de Firma Digital del Estado de Utah*

La elección de esta norma para su análisis no es casual ni arbitraria, sino que fue realizada teniendo en cuenta que fue esta la primera en dictarse sobre la materia en el mundo, y que en muchos aspectos, en poco se parece a las normas que se han dictado recientemente en otros países del mundo, entre ellos el nuestro.

Esta norma está estructurada en cinco Títulos a saber:

a) Título 1. Título Abreviado, interpretación y definiciones
b) Título 2. Acreditación y reglamentación de las Autoridades Certificantes
   Se regula en este título sobre la acreditación de las autoridades certificantes y los requisitos para que esto se produzca, la emisión de las licencias (inciso 201), las auditorias de gestión (inciso 202), la fiscalización de los requisitos para las autoridades certificantes acreditadas (inciso 203) y las actividades peligrosas prohibidas para cualquier autoridad certificante (inciso 204)
c) Título 3. Obligaciones de las Autoridades Certificantes y los Suscriptores
   En esta parte se establecen reglas que regirán la práctica de las autoridades certificantes acreditadas, específicamente reglas para la emisión, suspensión y revocación de certificados, los registros que vinculan un par de claves de firma digital a una persona, empresa o entidad comercial identificada por una autoridad de certificación. También se prohíben las declaraciones inexactas en los certificados, y se exige que el suscriptor mantenga el carácter confidencial de la clave privada. Asimismo, se limita la responsabilidad de la autoridad certificante hasta el límite de confianza recomendado que se especifica en el certificado pertinente.
d) Título 4. Efectos de la firma digital.
e) Título 5. Repositorios.
   Esta parte permite que la División (equivalente a la Autoridad Certificante Raíz en el esquema básico de PKI) reconozca repositorios a pedido. Limita la responsabilidad de los repositorios a su función de información, y elimina cualquier responsabilidad que podrían asumir por la veracidad de certificados o de otra información publicada en ellos por terceros.

De la lectura de la norma se desprende que, a pesar de ser la primera normativa en dictarse en su tipo, quienes la han elaborado tenían un conocimiento muy amplio, preciso y maduro de la materia a tratar. De hecho esta norma a más de seis años de su promulgación y a pesar de tratar temas que sufren una

evolución vertiginosa, no se ha tornado en absoluto obsoleta en ninguno de los tópicos que regula, lo que demuestra lo acertado del tratamiento que han recibido.

Cómo se desprende del nombre de su primer título, esta normativa contiene ya desde el inicio un pormenorizado glosario de términos, para evitar todo tipo de ambigüedad o mala interpretación. Este estilo de redacción preciso y analítico es luego es trasladado al resto de los títulos que la componen, dónde se realiza un exhaustivo y coherente análisis de cada uno de los temas tratados, sin dejan ningún punto librado al azar.

Hacemos notar que, por ejemplo, nuestra Ley 25.506 de Firma Digital, contiene un Glosario similar en su Anexo, que lamentablemente no es tan completo y preciso como el de la normativa en análisis. Lo que queremos destacar con esta mención, más allá de la completitud y precisión de los glosarios comprendidos en ambas normas, es la diferente técnica legislativa utilizada. Pues en la normativa local, el lector recién llega al Glosario luego de haber leído toda la normativa, tal vez sin comprenderla cabalmente, mientras que en la Ley de Firma Digital de Utah el mismo lector, es introducido en la temática, por cierto muy técnica, *ab initio,* lo que luego le permite continuar la lectura del resto de la normativa con mayor solvencia sobre los conceptos técnicos.

Nos detendremos brevemente en el análisis del Título 4 por ser el que se encarga de determinar los efectos jurídicos de la firma digital.

El inciso 401, es el que establece en sus párrafos iniciales el esquema general. En efecto establece: *"Cuando el régimen jurídico requiere una firma, o prevé ciertas consecuencias de la falta de firma, dicho sistema de derecho queda cumplido con una firma digital…"* y a renglón seguido, establece la condiciones: "*1. Si la firma digital se verifica por referencia a la clave pública mencionada en un certificado válido emitido por una autoridad certificante acreditada; 2. Si la firma digital fue suscripta por el firmante con la intención de firmar el mensaje, y 3. Si el destinatario no tiene conocimiento de que el firmante: 1. haya infringido un deber en su calidad de suscriptor, o bien 2. no posea legalmente la clave privada usada para suscribir la firma digital.*"

En este inciso, podemos observar de manera patente cómo se encuentran reflejados los requisitos de la firma, pues en la primera condición citada se acredita la identidad del firmante, y en el segundo su adhesión de voluntad.

Dentro del mismo artículo 401, se establece que no se limita ni desvaloriza la aplicación de las definiciones de firma vertidos en otras normas aunque no sean firmas digitales, en definitiva esta ley crea una nueva forma de firmar sin contraponerse a los existentes ni disminuirlos en su eficacia.

El artículo 402, establece una presunción de validez de las *Firmas digitales no confiables*, dejando en manos del receptor de un mensaje firmado de manera no confiable, aceptarlo y por lo tanto confirmar su validez de manera implícita y de acuerdo a lo que luego se establece en el inciso 406, o notificar inmediatamente al firmante del mensaje su decisión de no confiar en el mensaje firmado digitalmente de esta manera.

Este artículo mediante las posibilidades que otorga al receptor de un mensaje o documento firmado digitalmente, brinda un buen cierre en el sistema, reafirmando la seguridad jurídica del mismo.

El inciso 403, tiene similar efecto que el 401, y de hecho podrían haber sido consecutivos o se podría haber incluido ambos conceptos bajo el mismo numeral. De hecho, establece que un mensaje completamente firmado digitalmente cuya firma supere el proceso de verificación satisfactoriamente tiene la misma validez y puede ser exigido judicialmente como si fuera un documento escrito. Ha de notarse, que generalmente los casos que exigen documentos escritos, son los mismos que exigen firma de una o más de las partes intervinientes.

En su párrafo final, este artículo vuelve a reafirmar el concepto vertido en la última parte del artículo anterior, diciendo que *"…Sin embargo, el presente capítulo no impide que un mensaje, documento o registro sea considerado escrito bajo alguna otra ley aplicable.*

El siguiente artículo se ocupa de la validez de las copias de los mensajes firmados digitalmente, estableciendo como principio general que poseen la misma validez que los originales. A renglón seguido establece una excepción que si bien no desvirtúa el sentido de la norma, es importante mencionar, y que se relaciona con aquellos documentos en que "…sea evidente que el firmante designó una instancia del mensaje para que sea original único…".

Si bien para la mayoría de los documentos, la existencia de una o más copias no afecta en nada su operatividad, debemos recordar a los documentos negociables y títulos de créditos, dónde la exigencia de un único original, no sólo es implícita, sino necesaria por la naturaleza misma de estos papeles.

El inciso 405 y 406 establecen principios relativos a la materia probatoria, el primero trata sobre la calidad de reconocimiento de firma digital que posee un certificado firmado por una autoridad certificante acreditada. El artículo 406 en cambio se ocupa de establecer las presunciones acerca de determinados tópicos de la firma digital, que debe tener en cuenta un magistrado al resolver un litigio dónde se vea

involucrado un certificado de firma digital. En líneas generales, los efectos de los cuatro incisos de este artículo son establecer la carga de la prueba sobre quien desconozca una firma digital, debiendo por lo tanto probar los puntos sobre los que sustenta dicho repudio.

# Capítulo 6
# Conclusiones

**18. Estado actual teórico y práctico.**

A lo largo del trabajo ha quedado demostrado que existe la posibilidad práctica de implementar un sistema de firma digital. Esta posibilidad se sustenta teóricamente en el uso de técnicas criptográficas de clave asimétrica, sobre las cuales nos hemos explayado en el punto 13 del capítulo 4.

A continuación veremos que el sistema de firma digital además tiene en nuestro país sustento legal y que por otra parte su pronta puesta en marcha se justifica también desde el plano económico, el social y hasta el ecológico.

**19. Situación Legal**

Nuestro país ha ingresado a fines del año 2001 al grupo de naciones que recepcionó en sus regímenes legales a la firma digital.

Al momento de elaboración de este trabajo está pendiente el dictado de la normativa complementaria a la **Ley 25.506** a cargo de la Autoridad de Aplicación de esta norma, que es la Jefatura de Gabinete de Ministros, hasta ahora la norma sólo ha sido promulgada por el Poder Ejecutivo Nacional con fecha 11 de Diciembre de 2001, pero no tiene aplicación práctica.

La primera normativa que existió en el país sobre firma digital fue la **Resolución Nº 45/97** de la ex-Secretaría de la Función Pública (SFP) que establece las pautas mínimas a considerar para la elaboración de una normativa sobre firma digital en el país. Luego en función de esa normativa se elaboró el **Decreto Nº 427/98** que crea en el país la Infraestructura de Firma Digital para la Administración Pública Nacional (APN) a modo de prueba por un período de dos años prorrogables y establece la equivalencia entre la firma digital y la firma hológrafa siempre que se utilice para trámites internos de la APN que no involucre el derecho de terceros. Posteriormente se elaboró la **Resolución Nº 194/98 SFP** que establece los estándares tecnológicos para la implementación de la firma digital y la **Resolución Nº 212/98 SFP** que establece la Política de Certificación para la emisión de Certificados dentro de la APN.

En una línea de acción paralela y con la finalidad de acompañar el impulso inicial que aportó la ex-Secretaría de la Función Pública, con fecha 6 de Septiembre de 2001, se firmó el **Convenio sobre Sistema de Información para la Justicia Argentina** y el **Convenio de Comunicación Electrónica Interjurisdiccional**. Ambos fueron suscriptos por el Ministerio de Justicia y Derechos Humanos de la Nación, la Procuración General de la Nación, la Defensoría General de la Nación, la Secretaría para la Modernización del Estado dependiente de la Jefatura de Gabinetes de Ministros y representantes de los poderes judiciales de todas las provincias.

En el primero de ellos se establece el compromiso de las partes a realizar acciones tendientes a mejorar el Sistema de Información sobre la Justicia Argentina, mediante la publicación en sitios de acceso publico de la información acerca de cada uno de los órganos que componen cada uno de los poderes judiciales (tanto el nacional como los provinciales) y la realización de estadísticas y estudios que permitan brindar datos suficientes y confiables de modo tal que se puedan elaborar planes de mejoramiento.

El segundo de los convenios nombrados, se firma con el objetivo de complementar lo dispuesto en la Ley 22.172, y de incorporar progresivamente las tecnologías de la información a las comunicaciones interjurisdiccionales. Para ello se promueve un amplio marco de colaboración entre sus áreas informáticas y de comunicaciones, en lo que hace a conocimientos, herramientas y capacitación en general. También se acuerda uniformar los nombres de dominio (direcciones de Internet) de los participantes en el convenio con la finalidad de aportar claridad e impulsar un uso racional de las tecnologías de la información y en el plazo de un año homogeneizar las direcciones de correo electrónico, como así también mantenerlas debidamente actualizadas y publicadas en sus respectivos sitios de Internet y Guías Judiciales.

Por otra parte se están estudiando proyectos de reforma al Código de Procedimientos Civil y Comercial de la Nación, que tienen por objetivo adecuar la normativa de rito con la finalidad de poder utilizar las herramientas que brinda la Ley 25.506 de Firma Digital y que serán directamente operativas cuando la Jefatura de Gabinetes de Ministros dicte la normativa que termine de regular la Infraestructura de Firma Digital. Se pretende mediante estas reformas brindar la posibilidad de constituir un domicilio procesal elec-

trónico dónde serán válidas las notificaciones y traslados que deban producirse en el trámite de un proceso. Esto nos acerca un poco al anhelado expediente electrónico y a la posibilidad de presentar escritos firmados digitalmente inclusive sin ser necesaria la concurrencia a nuestros ya abarrotados tribunales.

**20. El nacimiento de la sociedad de la información**

Sin dejar de considerar la importancia de tener un marco normativo adecuado, creemos firmemente que debe ampliarse el ámbito de acción de quienes queremos que este sistema continúe su desarrollo y puesta en marcha.

Lamentablemente muchas veces se cae en la falsa creencia de que tener una ley pone en marcha de manera automática, crea o da existencia a institutos que deben primero ser asumidos por la sociedad como herramientas a ser utilizadas por sus implicancias prácticas positivas. Existen en nuestro país y en todo el sistema jurídico continental variados ejemplos de figuras jurídicas que quisieron ser impuestas mediante una creación legislativa y que han fracasado rotundamente. Entre los más cercanos a nuestra memoria está la tristemente célere Factura de Crédito, que no logra popularizarse entre nuestros comerciantes a pesar de que ha sido regulada ya de manera sucesiva por distintas leyes. Por el contrario, uno de los pocos ejemplos que podemos citar en sentido contrario lo constituye la figura jurídica de la Sociedad de Responsabilidad Limitada, que resulto de una creación legislativa germánica de principios de siglo, e incorporada a la Ley de Sociedades Nº 11.645 en el año 1932[39], tuvo una amplia aceptación sobre todo entre quienes emprendían la formación de pequeñas y medianas empresas a pesar de su origen “artificial”.

Se torna necesario crear un ámbito de difusión y debate. Es necesaria la intervención de todos para poner en marcha este sistema, pero sería de especial interés que tres actores fundamentales de todo cambio se coordinen y entren en acción armónicamente:

*a) El Estado*

El Estado es uno de los actores fundamentales, y hoy uno de los que más prestamente debe realizar las acciones necesarias para que el sistema deje de existir en un plano teórico e informal para cobrar vida propia. Recordemos que aún está pendiente la reglamentación completa del sistema a cargo de la Jefatura de Gabinetes de Ministros sin la cual la Ley 25.506 no tiene aplicación práctica.

Pero más allá del adecuado marco normativo, es responsabilidad del Estado brindar su infraestructura como punto de apoyo del sistema, a fin de que a partir de su difusión, este resulte económico y confiable.

También deben ponerse en marcha los mecanismos para lograr acuerdos con otros países que hayan regulado la materia a fin de que los certificados emitidos por Autoridades Certificantes licenciadas en nuestro país sean aceptados en el extranjero, y recíprocamente, los emitidos en el extranjero en condiciones asimilables a las que nuestra legislación requiere, tengan plena validez en nuestro país. Esto podría convertirse en una herramienta más de fomento del comercio internacional.

Comenzada la resolución de estos asuntos de fondo, paralelamente debería adaptarse la legislación ritual a fin de dotar a nuestros tribunales con la posibilidad de usar esta herramienta en la tramitación de los expedientes.

*b) El Sector Académico*

Como vehículos de formación, investigación y difusión, las casas de estudio, y específicamente las Universidades, no pueden estar ausentes en el debate y puesta en marcha del sistema.

Lamentablemente muchas de las investigaciones que conocemos y los conocimientos sobre los que ha de basarse el sistema de firma digital, por no decir casi la totalidad, provienen del extranjero.

Si bien es poca la participación que desde el plano técnico se ha tenido, no debemos dejar de lado la importancia que tienen los centros académicos como lugares de difusión y debate. Es imprescindible que aporten su capacidad de comprensión e investigación para realizar las recomendaciones necesarias para poner en marcha el sistema de la manera más eficiente y económica, sin dejar de lado la seguridad.

En la faz técnica nuestras Universidades pueden proveernos, como lo han hecho en más de una oportunidad, de excelentes especialistas en todas las ramas de las ciencias informáticas que nada tienen que envidiar a los formados en el extranjero y que están en condiciones de representarnos ante los foros internacionales con ideas propias.

Si bien, de la manera en que están planteadas las reglas de juego internacional y las del mercado informático en particular es impensable tomar una posición de liderazgo, no resulta igual de utópico pensar en aportar ideas y desarrollos que nos posicionen dignamente en el plano internacional

39. NISSEN, Ricardo Augusto, “Curso de Derecho Societario”, Pág.367, Ed. AD-HOC, Buenos Aires, 1º Edición, 1998.

*c) El Sector Privado*

Las empresas que componen el sector privado, tal vez sean las que más cambios necesitan hacer para incorporar y usar con todo su potencialidad el sistema de firma digital. Paralelamente tal vez sean las que mayores beneficios obtengan si lo hacen con la suficiente inteligencia y creatividad.

Tal vez uno de los puntos más delicados tiene que ver con la necesaria reingeniería de sus procesos productivos y administrativos.

El parque informático actual de las empresas argentinas puede ser considerado bueno, pues la mayoría de ellas han incorporado tecnología en los últimos diez años y el período de estabilidad económica de la década del noventa les permitió mantenerlo actualizado. Por otro lado no es necesaria una PC de última generación para producir una firma digital.

Teniendo en cuenta esto, llegamos a la conclusión de que el principal cambio estará centrado en la difusión de esta nueva tecnología entre sus recursos humanos, no para capacitarlos en el uso, sino para generar conciencia de las ventajas que esta ofrece, y cuales son las implicancias prácticas y legales que su incorporación tiene.

No resulta simple a veces explicar el concepto de firma digital a quien no se interesa mínimamente en la informática. Por otra parte puede resultar difícil hacer comprender que el correo electrónico, del cual se hace uso y abuso dentro de las grandes organizaciones, dejará de ser una herramienta cualquiera para convertirse en uno de los posibles vehículos de nuestra propia firma.

**21. Vislumbrando el camino.**

Las aplicaciones informáticas en su diseño conceptual, deben ser herramientas capaces de contener adecuadamente las necesidades del negocio o proceso en que se pretenden aplicar a fin de que aporten su capacidad de almacenamiento o procesamiento.

Así como no es posible cavar los cimientos de un gran edificio con el trabajo de un solo hombre y una pala, ni es recomendable intentar matar una mosca con un arma de fuego, aunque ambas cosas en definitiva fueran posible, debe tenerse en cuenta que la falta de armonía o proporcionalidad entre los recursos informáticos y las organizaciones implica una asignación ineficiente de los recursos presupuestarios de cualquier organización, sea esta un ente público o una empresa privada.

La desproporcionalidad finalmente conduce de manera inexorable al fracaso en relación con las metas de eficacia esperadas. Cualquier presupuesto debe tener en cuenta no sólo la instalación y puesta en marcha del sistema, sino también algunos otros aspectos no menores como su futuro soporte técnico, la formación de las personas que han de utilizarlo, el mantenimiento de licencias, las actualizaciones, y la adaptación y reingeniería de los procesos en que han de participar a fin de realizar una asignación de recursos humanos y económicos acorde a los cambios que la aplicación de tecnología de procesamiento de datos implica dentro de una organización cualquiera.

Claro que esto no supone el pase a disponibilidad o despido de las personas que son reemplazadas en algunas de sus funciones por un sistema informático. Si con la utilización de aplicaciones informáticas, se reemplaza el trabajo manual, debe pensarse inmediatamente en la reutilización de esos recursos humanos dentro de la organización de manera más eficiente, en la realización de tareas con alto valor agregado que muchas veces un sistema informático no puede realizar o que de realizarlas significaría la incorporación al mismo de inteligencia de procesamiento que normalmente los hace crecer de manera desproporcionada y encarecer a niveles que muchas veces resultan ridículos.

Son variados los motivos que pueden llevarnos a impulsar la adopción de un sistema de firma digital, y aunque para muchas personas puede parecer un capricho de fanáticos de las ciencias de la informática, podemos verter a continuación motivos de índole económico, ecológico y también por qué no, de corte netamente social que ya de manera individual sostienen la necesidad de poner en funcionamiento el sistema con premura y que tomados en consideración de manera conjunta resultan demoledores por su propio peso.

Analistas económicos y políticos han señalado de manera reiterada que muchos de los males que sufre nuestro país son producto de una pésima administración de los recursos económicos en el sector público. Generalmente señalan, con razón, gastos desproporcionados en todas las áreas que componen los tres poderes del Estado en su nivel nacional, provincial y municipal. Hasta aquí nada novedoso ni objetable, puesto que estas observaciones también pueden ser llevadas a cabo por personas comunes. Sin embargo a pesar de que variada parte de estas fundadas críticas provienen del sector privado, pocos son los que observan que la mayoría de las grandes empresas del país están sentadas sobre la punta de un volcán a punto de entrar en erupción.

Alcanzan los dedos de una mano para contar las empresas que han realizado genuinamente una reingeniería de sus procesos productivos y administrativos a fin de reducir costos de manera eficiente y eficaz. La más de las veces, son los empleados y sus sueldos las variables de ajuste presupuestario, sin ver cuanto podría ahorrarse en muchos otros puntos del proceso.

Podemos traer a colación el ejemplo de las entidades bancarias que operan en nuestro país. Salvo raras excepciones en la mayoría de ellas existe una arraigada cultura del papel. Este se utiliza abundantemente no sólo en algunas tareas dónde resulta recomendable que así se lo haga, sino también en otras dónde es absolutamente contraproducente e inútil, como la impresión de interminables listados de clientes con el pretendido fin de controlar datos y saldos de una manera a todas luces ineficiente y que a la postre nadie mirará ni utilizará.

Se dilapidan fortunas además en la impresión de libros rubricados a fin de cumplir con reglamentaciones tendientes a proteger quien sabe bien que derechos, amontonando interminables volúmenes de libros de costosa y elegante encuadernación que luego nunca nadie consultará. Cabe aclarar que realizamos esta afirmación, no porque no creamos en la utilidad de los datos que se almacenan, sino por la inviabilidad de encontrar luego en ellos la información que necesitamos.

Para ser más claros en cuanto a la idea que queremos transmitir, imaginemos todos los volúmenes de una revista de publicaciones jurídicas publicados desde sus primeros lanzamientos a principios del siglo XX hasta nuestros días, todas ellas ocuparían una biblioteca de dos metros de alto y más de diez metros de ancho. Imaginémoslas sin un índice sistemático de búsqueda como los que esas importantes editoriales se han preocupado en desarrollar ¿Alguien podría negar la importancia de los fallos y comentarios en ellos publicados? ¿Alguien más podría negar la inutilidad de la información guardada de esa manera?

Todo esto podría ser evitado mediante la utilización, entre otros elementos, de un mecanismo confiable de firma digital. No sólo se podría reducir drásticamente el gasto, algo ya de por si interesante en cualquier planteo, sino que se puede ayudar que además ese gasto reducido muchas veces resulte además útil.

Los niveles de gastos en papel e insumos de impresión rara vez pueden ser imaginados. Una de las primeras diez entidades bancarias del país en término de tamaño y posicionamiento de cartera, en el último rubro gasta aproximadamente la suma de treinta mil dólares estadounidenses por mes (U$S 30.000). Si nos damos cuenta de la real dimensión que esta cifra tiene, tomaremos conciencia de que, del plano económico podemos pasar al plano social del asunto, pues con ese dinero a los valores actuales puede pagarse el sueldo de cien empleados administrativos de planta permanente en cualquiera de las entidades bancarias del país, abonándole un sueldo que supera la media del mercado.

Hechas estas consideraciones en un momento dónde el mercado laboral está en constante contracción, cobran una entidad aún mayor a las que tendría en épocas de bonanza económica. El mismo análisis puede ser llevado con toda estructuración lógica a las áreas administrativas del Estado, dónde la asignación de recursos es en muchos casos aún más deficiente que la que hemos reseñado.

# Anexo 1
# Apéndice Legislativo

**22. Legislación doméstica**

*a) Ley de Firma Digital 25.506*

**FIRMA DIGITAL**
Ley 25.506

Consideraciones generales. Certificados digitales. Certificador licenciado. Titular de un certificado digital. Organización institucional. Autoridad de aplicación. Sistema de auditoria. Comisión Asesora para la Infraestructura de Firma Digital. Responsabilidad. Sanciones. Disposiciones Complementarias.

Sancionada: Noviembre 14 de 2001.

Promulgada de Hecho: Diciembre 11 de 2001.

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

**LEY DE FIRMA DIGITAL**
**CAPITULO I**
**Consideraciones generales**

**ARTICULO 1º** — *Objeto.*

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 2º** — *Firma Digital*.

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

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

**ARTICULO 3º** — *Del requerimiento de firma*.

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

**ARTÍCULO 4º** — *Exclusiones*.

Las disposiciones de esta ley no son aplicables:

a) A las disposiciones por causa de muerte;
b) A los actos jurídicos del derecho de familia;
c) A los actos personalísimos en general;
d) A los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes.

**ARTÍCULO 5º** — *Firma electrónica.*

Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

**ARTÍCULO 6º** — *Documento digital*.

Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.

**ARTÍCULO 7º** — *Presunción de autoría*.

Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma.

**ARTÍCULO 8º** — *Presunción de integridad*.

Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma.

**ARTÍCULO 9º** — *Validez*.

Una firma digital es válida si cumple con los siguientes requisitos:

a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante;
b) Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente;
c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado.

**ARTICULO 10.** — *Remitente. Presunción.*

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

**ARTICULO 11.** — *Original*.

Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados

originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación.

**ARTICULO 12.** — *Conservación*.

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

**CAPITULO II**
**De los certificados digitales**

**ARTICULO 13.** — *Certificado digital*.

Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.

**ARTICULO 14.** — *Requisitos de validez de los certificados digitales*.

Los certificados digitales para ser válidos deben:

a) Ser emitidos por un certificador licenciado por el ente licenciante;
b) Responder a formatos estándares reconocidos internacionalmente, fijados por la autoridad de aplicación, y contener, como mínimo, los datos que permitan:
   1. Identificar indubitablemente a su titular y al certificador licenciado que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única;
   2. Ser susceptible de verificación respecto de su estado de revocación;
   3. Diferenciar claramente la información verificada de la no verificada incluidas en el certificado;
   4. Contemplar la información necesaria para la verificación de la firma;
   5. Identificar la política de certificación bajo la cual fue emitido.

**ARTICULO 15.** — *Período de vigencia del certificado digital*.

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

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

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

**ARTICULO 16.** — *Reconocimiento de certificados extranjeros*.

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

a) Reúnan las condiciones que establece la presente ley y la reglamentación correspondiente para los certificados emitidos por certificadores nacionales y se encuentre vigente un acuerdo de reciprocidad firmado por la República Argentina y el país de origen del certificador extranjero, o
**b)** Tales certificados sean reconocidos por un certificador licenciado en el país, que garantice su validez y vigencia conforme a la presente ley. A fin de tener efectos, estereconocimiento deberá ser validado por la autoridad de aplicación.

**CAPITULO III**
**Del certificador licenciado**

**ARTICULO 17.** — *Del certificador licenciado*.

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

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

**ARTICULO 18.** — *Certificados por profesión*.

Las entidades que controlan la matrícula, en relación a la prestación de servicios profesionales, podrán emitir certificados digitales en lo referido a esta función, con igual validez y alcance jurídico que las firmas efectuadas en forma manuscrita. A ese efecto deberán cumplir los requisitos para ser certificador licenciado.

**ARTICULO 19.** — *Funciones*.

El certificador licenciado tiene las siguientes funciones:

a) Recibir una solicitud de emisión de certificado digital, firmada digitalmente con los correspondientes datos de verificación de firma digital del solicitante;
b) Emitir certificados digitales de acuerdo a lo establecido en sus políticas de certificación, y a las condiciones que la autoridad de aplicación indique en la reglamentación de la presente ley;
c) Identificar inequívocamente los certificados digitales emitidos;
d) Mantener copia de todos los certificados digitales emitidos, consignando su fecha deemisión y de vencimiento si correspondiere, y de sus correspondientes solicitudes de emisión;
e) Revocar los certificados digitales por él emitidos en los siguientes casos, entre otros que serán determinados por la reglamentación:
   1) A solicitud del titular del certificado digital.
   2) Si determinara que un certificado digital fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación.
   3) Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.
   4) Por condiciones especiales definidas en su política de certificación.
   5) Por resolución judicial o de la autoridad de aplicación.
f) Informar públicamente el estado de los certificados digitales por él emitidos. Los certificados digitales revocados deben ser incluidos en una lista de certificados revocados indicando fecha y hora de la revocación. La validez y autoría de dicha lista de certificados revocados deben ser garantizadas.

**ARTICULO 20.** — *Licencia*.

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

**ARTICULO 21.** — *Obligaciones*.

Son obligaciones del certificador licenciado:

a) Informar a quien solicita un certificado con carácter previo a su emisión y utilizando un medio de comunicación las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de un sistema de licenciamiento y los procedimientos, forma que garantiza su posible responsabilidad patrimonial y los efectos de la revocación de su propio certificado digital y de la licencia que le otorga el ente licenciante. Esa información deberá estar libremente accesible en lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;
b) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de firma digital de los titulares decertificados digitales por él emitidos;
c) Mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación;
d) Operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la autoridad de aplicación;
e) Notificar al solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable, y las obligaciones que asume por el solo hecho de ser titular de un certificado digital;
f) Recabar únicamente aquellos datos personales del titular del certificado digital que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional;
g) Mantener la confidencialidad de toda información que no figure en el certificado digital;
h) Poner a disposición del solicitante de un certificado digital toda la información relativa a su tramitación;
i) Mantener la documentación respaldatoria de los certificados digitales emitidos, por diez (10) años a partir de su fecha de vencimiento o revocación;

j) Incorporar en su política de certificación los efectos de la revocación de su propio certificado digital y/o de la licencia que le otorgara la autoridad de aplicación;
k) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados digitales revocados, las políticas de certificación, la información relevante de los informes de la última auditoria de que hubiera sido objeto, su manual de procedimientos y toda información que determine la autoridad de aplicación;
l) Publicar en el Boletín Oficial aquellos datos que la autoridad de aplicación determine;
m) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas;
n) Informar en las políticas de certificación si los certificados digitales por él emitidos requieren la verificación de la identidad del titular;
o) Verificar, de acuerdo con lo dispuesto en su manual de procedimientos, toda otra información que deba ser objeto de verificación, la que debe figurar en las políticas de certificación y en los certificados digitales;
p) Solicitar inmediatamente al ente licenciante la revocación de su certificado, o informarle la revocación del mismo, cuando existieren indicios de que los datos de creación de firma digital que utiliza hubiesen sido comprometidos o cuando el uso de los procedimientos de aplicación de los datos de verificación de firma digital en él contenidos hayan dejado de ser seguros;
q) Informar inmediatamente al ente licenciante sobre cualquier cambio en los datos relativos a su licencia;
r) Permitir el ingreso de los funcionarios autorizados de la autoridad de aplicación, del ente licenciante o de los auditores a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso;
s) Emplear personal idóneo que tenga los conocimientos específicos, la experiencia necesaria para proveer los servicios ofrecidos y en particular, competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma digital y experiencia adecuada en los procedimientos de seguridad pertinentes;
t) Someter a aprobación del ente licenciante el manual de procedimientos, el plan de seguridad y el de cese de actividades, así como el detalle de los componentes técnicos a utilizar;
u) Constituir domicilio legal en la República Argentina;
v) Disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la presente ley y su reglamentación;
w) Cumplir con toda otra obligación emergente de su calidad de titular de la licencia adjudicada por el ente licenciante.

**ARTICULO 22.** — *Cese del certificador*.
El certificador licenciado cesa en tal calidad:
a) Por decisión unilateral comunicada al ente licenciante;
b) Por cancelación de su personería jurídica;
c) Por cancelación de su licencia dispuesta por el ente licenciante.
La autoridad de aplicación determinará los procedimientos de revocación aplicables en estos casos.

**ARTICULO 23.** — *Desconocimiento de la validez de un certificado digital*.
Un certificado digital no es válido si es utilizado:
a) Para alguna finalidad diferente a los fines para los cuales fue extendido;
b) Para operaciones que superen el valor máximo autorizado cuando corresponda;
c) Una vez revocado.

**CAPITULO IV**
**Del titular de un certificado digital**

**ARTICULO 24.** — *Derechos del titular de un certificado digital*.
El titular de un certificado digital tiene los siguientes derechos:
a) A ser informado por el certificador licenciado, con carácter previo a la emisión del certificado digital, y utilizando un medio de comunicación sobre las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de este sistema de licenciamiento y los procedi-

mientos asociados. Esa información deberá darse por escrito en un lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;
b) A que el certificador licenciado emplee los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por él, y a ser informado sobre ello;
c) A ser informado, previamente a la emisión del certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago;
d) A que el certificador licenciado le informe sobre su domicilio en la República Argentina, y sobre los medios a los que puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema, o presentar sus reclamos;
e) A que el certificador licenciado proporcione los servicios pactados, y a no recibir publicidad comercial de ningún tipo por intermedio del certificador licenciado.

**ARTICULO 25.** — *Obligaciones del titular del certificado digital*.
Son obligaciones del titular de un certificado digital:
a) Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;
b) Utilizar un dispositivo de creación de firma digital técnicamente confiable;
c) Solicitar la revocación de su certificado al certificador licenciado ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;
d) Informar sin demora al certificador licenciado el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.

**CAPITULO V**
**De la organización institucional**

**ARTICULO 26.** — *Infraestructura de Firma Digital*.
Los certificados digitales regulados por esta ley deben ser emitidos o reconocidos, según lo establecido por el artículo 16, por un certificador licenciado.

**ARTICULO 27.** — *Sistema de Auditoría*.
La autoridad de aplicación, con el concurso de la Comisión Asesora para la Infraestructura de Firma Digital, diseñará un sistema de auditoría para evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, así como también el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y de contingencia aprobados por el ente licenciante.

**ARTICULO 28.** — *Comisión Asesora para la Infraestructura de Firma Digital*.
Créase en el ámbito jurisdiccional de la Autoridad de Aplicación, la Comisión Asesora para la Infraestructura de Firma Digital.

**CAPITULO VI**
**De la autoridad de aplicación**

**ARTICULO 29.** — *Autoridad de Aplicación*.
La autoridad de aplicación de la presente ley será la Jefatura de Gabinete de Ministros.

**ARTICULO 30.** — *Funciones*.
La autoridad de aplicación tiene las siguientes funciones:
a) Dictar las normas reglamentarias y de aplicación de la presente;
b) Establecer, previa recomendación de la Comisión Asesora para la Infraestructura de la Firma Digital, los estándares tecnológicos y operativos de la Infraestructura de Firma Digital;
c) Determinar los efectos de la revocación de los certificados de los certificadores licenciados o del ente licenciante;
d) Instrumentar acuerdos nacionales e internacionales a fin de otorgar validez jurídica a las firmas digitales creadas sobre la base de certificados emitidos por certificadores de otros países;
e) Determinar las pautas de auditoría, incluyendo los dictámenes tipo que deban emitirse como conclusión de las revisiones;
f) Actualizar los valores monetarios previstos en el régimen de sanciones de la presente ley;

g) Determinar los niveles de licenciamiento;
h) Otorgar o revocar las licencias a los certificadores licenciados y supervisar su actividad, según las exigencias instituidas por la reglamentación;
i) Fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los certificadores licenciados;
j) Homologar los dispositivos de creación y verificación de firmas digitales, con ajuste alas normas y procedimientos establecidos por la reglamentación;
k) Aplicar las sanciones previstas en la presente ley.

**ARTICULO 31.** — *Obligaciones*.

En su calidad de titular de certificado digital, la autoridad de aplicación tiene las mismas obligaciones que los titulares de certificados y que los certificadores licenciados. En especial y en particular debe:

a) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder, bajo ninguna circunstancia, a los datos utilizados para generar la firma digital de los certificadores licenciados;
b) Mantener el control exclusivo de los datos utilizados para generar su propia firma digital e impedir su divulgación;
c) Revocar su propio certificado frente al compromiso de la privacidad de los datos de creación de firma digital;
d) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, números telefónicos y direcciones de Internet tanto de los certificadores licenciados como los propios y su certificado digital;
e) Supervisar la ejecución del plan de cese de actividades de los certificadores licenciados que discontinúan sus funciones.

**ARTICULO 32.** — *Arancelamiento*.

La autoridad de aplicación podrá cobrar un arancel de licenciamiento para cubrir su costo operativo y el de las auditorías realizadas por sí o por terceros contratados a tal efecto.

**CAPITULO VII**
**Del sistema de auditoría**

**ARTICULO 33.** — *Sujetos a auditar*.

El ente licenciante y los certificadores licenciados, deben ser auditados periódicamente, de acuerdo al sistema de auditoría que diseñe y apruebe la autoridad de aplicación.

La autoridad de aplicación podrá implementar el sistema de auditoría por sí o por terceros habilitados a tal efecto. Las auditorías deben como mínimo evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y, disponibilidad de los datos, así como también el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y, de contingencia aprobados por el ente licenciante.

**ARTICULO 34.** — *Requisitos de habilitación*.

Podrán ser terceros habilitados para efectuar las auditorías las Universidades y organismos científicos y/o tecnológicos nacionales o provinciales, los Colegios y Consejos profesionales que acrediten experiencia profesional acorde en la materia.

**CAPITULO VIII**
**De la Comisión Asesora para la Infraestructura de Firma Digital**

**ARTICULO 35**. — *Integración y funcionamiento*.

La Comisión Asesora para la Infraestructura de Firma Digital estará integrada multidisciplinariamente por un máximo de 7 (siete) profesionales de carreras afines a la actividad de reconocida trayectoria y experiencia, provenientes de Organismos del Estado nacional, Universidades Nacionales y Provinciales, Cámaras, Colegios u otros entes representativos de profesionales.

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

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

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

**ARTICULO 36.** — *Funciones*.

La Comisión debe emitir recomendaciones por iniciativa propia o a solicitud de la autoridad de aplicación, sobre los siguientes aspectos:

a) Estándares tecnológicos;
b) Sistema de registro de toda la información relativa a la emisión de certificados digitales;
c) Requisitos mínimos de información que se debe suministrar a los potenciales titulares de certificados digitales de los términos de las políticas de certificación;
d) Metodología y requerimiento del resguardo físico de la información;
e) Otros que le sean requeridos por la autoridad de aplicación.

**CAPITULO IX**
**Responsabilidad**

**ARTICULO 37.** — *Convenio de partes*.

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

**ARTICULO 38.** — *Responsabilidad de los certificadores licenciados ante terceros*.

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

**ARTICULO 39.** — *Limitaciones de responsabilidad*.

Los certificadores licenciados no son responsables en los siguientes casos:

a) Por los casos que se excluyan taxativamente en las condiciones de emisión yutilización de sus certificados y que no estén expresamente previstos en la ley;
b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;
c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el certificador pueda demostrar que ha tomado todas las medidas razonables.

**CAPITULO X**
**Sanciones**

**ARTICULO 40.** — *Procedimiento*.

La instrucción sumarial y la aplicación de sanciones por violación a disposiciones de la presente ley serán realizadas por el ente licenciante. Es aplicable la Ley de Procedimientos Administrativos 19.549 y sus normas reglamentarias.

**ARTICULO 41.** — *Sanciones*.

El incumplimiento de las obligaciones establecidas en la presente ley para los certificadores licenciados dará lugar a la aplicación de las siguientes sanciones:

a) Apercibimiento;
b) Multa de pesos diez mil ($ 10.000) a pesos quinientos mil ($ 500.000);
c) Caducidad de la licencia.

Su gradación según reincidencia y/u oportunidad serán establecidas por la reglamentación.

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

**ARTICULO 42.** — *Apercibimiento*.

Podrá aplicarse sanción de apercibimiento en los siguientes casos:

a) Emisión de certificados sin contar con la totalidad de los datos requeridos, cuando su omisión no invalidare el certificado;
b) No facilitar los datos requeridos por el ente licenciante en ejercicio de sus funciones;
c) Cualquier otra infracción a la presente ley que no tenga una sanción mayor.

**ARTICULO 43.** — *Multa*.

Podrá aplicarse sanción de multa en los siguientes casos:

a) Incumplimiento de las obligaciones previstas en el artículo 21;
b) Si la emisión de certificados se realizare sin cumplimentar las políticas de certificación comprometida y causare perjuicios a los usuarios, signatarios o terceros, o se afectare gravemente la seguridad de los servicios de certificación;
c) Omisión de llevar el registro de los certificados expedidos;
d) Omisión de revocar en forma o tiempo oportuno un certificado cuando así correspondiere;
e) Cualquier impedimento u obstrucción a la realización de inspecciones o auditorías por parte de la autoridad de aplicación y del ente licenciante;
f) Incumplimiento de las normas dictadas por la autoridad de aplicación;
g) Reincidencia en la comisión de infracciones que dieran lugar a la sanción de apercibimiento.

**ARTICULO 44.** — *Caducidad*.

Podrá aplicarse la sanción de caducidad de la licencia en caso de:

a) No tomar los debidos recaudos de seguridad en los servicios de certificación;
b) Expedición de certificados falsos;
c) Transferencia no autorizada o fraude en la titularidad de la licencia;
d) Reincidencia en la comisión de infracciones que dieran lugar a la sanción de multa;
e) Quiebra del titular.

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

**ARTICULO 45.** — *Recurribilidad*.

Las sanciones aplicadas podrán ser recurridas ante los Tribunales Federales con competencia en lo Contencioso Administrativo correspondientes al domicilio de la entidad, una vez agotada la vía administrativa pertinente.

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

**ARTICULO 46.** — *Jurisdicción*.

En los conflictos entre particulares y certificadores licenciados es competente la Justicia en lo Civil y Comercial Federal. En los conflictos en que sea parte un organismo público certificador licenciado, es competente la Justicia en lo Contencioso-administrativo Federal.

**CAPITULO XI**
**Disposiciones Complementarias**

**ARTICULO 47.** — *Utilización por el Estado Nacional*.

El Estado nacional utilizará las tecnologías y previsiones de la presente ley en su ámbito interno y en relación con los administrados de acuerdo con las condiciones que se fijen reglamentariamente en cada uno de sus poderes.

**ARTICULO 48.** — *Implementación*.

El Estado nacional, dentro de las jurisdicciones y entidades comprendidas en el artículo 8º de la Ley 24.156, promoverá el uso masivo de la firma digital de tal forma que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a la progresiva despapelización.

En un plazo máximo de 5 (cinco) años contados a partir de la entrada en vigencia de la presente ley, se aplicará la tecnología de firma digital a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanados de las jurisdicciones y entidades comprendidas en el artículo 8º de la Ley 24.156.

**ARTICULO 49.** — *Reglamentación*.
El Poder Ejecutivo deberá reglamentar esta ley en un plazo no mayor a los 180 (ciento ochenta) días de su publicación en el Boletín Oficial de la Nación.

**ARTICULO 50.** — *Invitación*.
Invítase a las jurisdicciones provinciales a dictar los instrumentos legales pertinentes para adherir a la presente ley.

**ARTICULO 51.** — *Equiparación a los efectos del derecho penal*.
Incorpórase el siguiente texto corno artículo 78 (bis) del Código Penal:
Los términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos documento, instrumento privado y certificado comprenden el documento digital firmado digitalmente.

**ARTICULO 52.** — *Autorización al Poder Ejecutivo*.
Autorízase al Poder Ejecutivo para que por la vía del artículo 99, inciso 2, de la Constitución Nacional actualice los contenidos del Anexo de la presente ley a fin de evitar su obsolescencia.

**ARTICULO 53.** — *Comuníquese al Poder Ejecutivo*.
DADA EN LA SALA DE SESIONES DEL CONGRESO ARGENTINO, EN BUENOS AIRES, A LOS CATORCE DÍAS DEL MES DE NOVIEMBRE DEL AÑO DOS MIL UNO.

— REGISTRADA BAJO EL Nº 25.506 —
Rafael Pascual. — Eduardo Menem. — Guillermo Aramburu. — Juan C. Oyarzún.

**ANEXO**

***Información*:** conocimiento adquirido acerca de algo o alguien.

***Procedimiento de verificación*:** proceso utilizado para determinar la validez de una firma digital. Dicho proceso debe considerar al menos:

**a)** que dicha firma digital ha sido creada durante el período de validez del certificado digital del firmante;
**b)** que dicha firma digital ha sido creada utilizando los datos de creación de firma digital correspondientes a los datos de verificación de firma digital indicados en el certificado del firmante;
**c)** la verificación de la autenticidad y la validez de los certificados involucrados.

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

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

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

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

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

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

1. Resguardar contra la posibilidad de intrusión y/o uso no autorizado;
2. Asegurar la disponibilidad, confiabilidad, confidencialidad y correcto funcionamiento;
3. Ser apto para el desempeño de sus funciones específicas;
4. Cumplir las normas de seguridad apropiadas, acordes a estándares internacionales en la materia;
5. Cumplir con los estándares técnicos y de auditoría que establezca la Autoridad de Aplicación.

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

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

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

***Criptosistema asimétrico*:** Algoritmo que utiliza un par de claves, una clave privada para firmar digitalmente y su correspondiente clave pública para verificar dicha firma digital.

**23. Legislación Comparada**

*b) Ley de Firma Digital del Estado de Utah*
**LEY DEL ESTADO DE UTAH SOBRE LA FIRMA DIGITAL.**
**CÓDIGO COMENTADO. TÍTULO 46, CAPÍTULO 3 (1996)**

**TÍTULO 1. Título Abreviado, Interpretación y Definiciones**

101. **Título abreviado**
Podrá citarse el presente capítulo llamándoselo Ley de Firma Digital de Utah.

102. **Objetivos e interpretación**
Se interpretará a este capítulo en coherencia con lo que se considere razonable en ciertas circunstancias, para lograr los siguientes fines:
Facilitar las transacciones mediante mensajes electrónicos confiables;
Reducir al mínimo la posibilidad de fraguar firmas digitales y el fraude en las transacciones electrónicas.
Instrumentar jurídicamente la incorporación de normas pertinentes, tales como la X.509 de la Unión Internacional de Telecomunicaciones (antiguamente Comité Consultor de Telégrafos y Teléfonos, o CCITT), y
Establecer, en coordinación con diversos Estados, normas uniformes relativas a la autenticación y confiabilidad de los mensajes electrónicos.

103. **Definiciones**
A los fines del presente capítulo, y salvo que se indique lo contrario, las siguientes expresiones significan:

1. **"Aceptar un certificado":**
   1. Manifestar que se aprueba un certificado, porque se conoce o se tiene noticia de su contenido; o bien,
   2. Solicitar un certificado a una autoridad certificante autorizada, sin cancelar ni revocar la solicitud notificando la cancelación o revocación a la autoridad certificante y obteniendo de ésta un recibo escrito y firmado, si la autoridad certificante subsiguientemente emite un certificado respondiendo a dicha solicitud.
2. **"Criptosistema asimétrico"**: algoritmo o serie de algoritmos que brindan un par de claves confiable.
3. **"Certificado"**: registro basado en la computadora, que:
   1. Identifica a la autoridad certificante que lo emite;
   2. Nombra o identifica a quien lo suscribe;
   3. Contiene la clave pública de quien lo suscribe, y
   4. Está firmado digitalmente por la autoridad certificante que lo emite.
4. **"Autoridad certificante"**: persona que emite un certificado.
5. **"Registro de publicidad de la autoridad certificante"**: registro en línea de acceso público, que lleva la División, relativo a la autoridad certificante acreditada.

6. **"Fórmula de certificación"**: declaración de las prácticas que emplea una autoridad certificante al emitir certificados.
7. **"Certificar"**: con referencia a un certificado, significa declarar que refleja todos los hechos relevantes.
8. **"Confirmar"**: verificar mediante un adecuado examen e investigación
9. **"Corresponder"**: con referencia a las claves, significa pertenecer al mismo par de claves.
10. **"Firma digital"**: transformación de un mensaje empleando un criptosistema asimétrico tal, que una persona que posea el mensaje inicial y la clave pública del firmante pueda determinar con certeza:
    1. Si la transformación se creó usando la clave privada que corresponde a la clave pública del firmante, y
    2. Si el mensaje ha sido modificado desde que se efectuó la transformación.
11. **"División"**: División Empresas y Código Comercial, del Departamento Comercial de Utah.
12. **"Falsificar una firma digital"**:
    1. Crear una firma digital sin autorización del tenedor legítimo de la clave privada, o bien
    2. Crear una firma digital verificable mediante un certificado donde aparezca incluida una persona inexistente o que no posea la clave privada correspondiente a la clave pública mencionada en él.
13. **"Poseer una clave privada"**: tener la posibilidad de utilizar una clave privada.
14. **"Incorporar por referencia"**: hacer que un mensaje pase a formar parte de otro identificando el mensaje que será incorporado y expresando la intención de que resulte incorporado.
15. **"Emitir un certificado"**: actos que realiza la autoridad certificante para crear un certificado y notificar al suscriptor mencionado en el certificado sobre el contenido de dicho certificado.
16. **"Par de claves"**: clave privada y su correspondiente clave pública en un criptosistema asimétrico, claves que tienen la propiedad de que la clave pública puede verificar una firma digital que crea la clave privada.
17. **"Autoridad certificante acreditada"**: autoridad certificante a quien la División le ha extendido una acreditación. Dicha acreditación debe estar vigente.
18. **"Mensaje"**: representación digital de información.
19. **"Notificar"**: comunicar un hecho a otra persona de una manera que fehacientemente se parezca, dadas las circunstancias, a lo que sería ponerla al tanto de la información.
20. **"Personal operativo"**: una o más personas físicas que actúan como autoridad certificante o como representante de ella, que sean empleadas de una autoridad certificante o las ligue a ellas un contrato, y que cumplan:
    1. Responsabilidades gerenciales o de determinación de políticas para la autoridad certificante, o bien
    2. Deberes que involucren la emisión de certificados, la creación de claves privadas o el manejo de los servicios de computación de la autoridad certificante.
21. **"Persona"**: persona física o jurídica capaz de firmar un documento, sea legalmente o como cuestión de hecho.
22. **"Clave privada"**: de dos claves, una de ellas, que se usa para crear una firma digital.
23. **"Clave pública"**: de dos claves, una de ellas, que se usa para verificar una firma digital.
24. **"Publicar"**: registrar o archivar en un repositorio.
25. **"Derecho limitado de pago"**: sentencia condenatoria al pago de daños y perjuicios contra una autoridad certificante, por un tribunal que tenga jurisdicción sobre dicha autoridad, en una acción civil promovida por violación del presente capítulo
26. **"Receptor"**: persona que recibe o tiene una firma digital y está en condiciones de confiar en ella.
27. **"Repositorio reconocido"**: repositorio reconocido por la División conforme al artículo 501 del presente capítulo.
28. **"Límite de confianza recomendado"**: cifra monetaria recomendada hasta donde confiar en un certificado de conformidad con el artículo 309 (1).
29. **"Repositorio"**: sistema para almacenar y recuperar certificados y demás información pertinente a las firmas digitales.
30. **"Revocar un certificado"**: volverlo ineficaz en forma permanente a partir de cierta fecha especificada. La revocación se efectúa mediante anotación o inclusión dentro de un conjunto de certificados revocados, y no implica que haya que destruir ni volver ilegible dicho certificado.
31. **"Poseer legalmente una clave privada"**: estar habilitado para utilizar una clave privada
    1. que el tenedor o sus representantes no han revelado a persona alguna en violación al art. 305 (1), y
    2. que el tenedor no hubiese obtenido mediante robo, engaño, intercepción u otro medio ilegal.
32. **"Suscriptor"**: persona que:
    1. es el sujeto cuyo nombre figura en un certificado;
    2. acepta el certificado, y
    3. tiene una clave privada que corresponde a la clave pública mencionada en dicho certificado.

33. **"Suficiente garantía"**: garantía de cumplimiento de obligaciones contractuales otorgada por un garante autorizado por el Departamento de Seguros de Utah a realizar operaciones comerciales en dicho Estado, o bien una carta de crédito irrevocable emitida por una institución financiera autorizada por el Departamento de Instituciones Financieras de Utah para funcionar en ese Estado, la cual, en cualquiera de los dos casos, debe cumplir con los siguientes requisitos:
    1. Que sea pagadera a la División, a favor de personas que tengan derechos de cobro limitados contra la autoridad certificante que figura como obligado principal o emitente de la carta de crédito.
    2. Que se libre por un monto especificado por una norma de la División, conforme al artículo....
    3. Que en ella se mencione que se la libra de conformidad con el presente capítulo.
    4. Que especifique un plazo de vigencia que se extienda por lo menos durante la vigencia de la acreditación que se otorgue a la autoridad certificante, y
    5. Que se ajuste a una forma prescripta o aprobada por norma de la División.
    6. La suficiente garantía también puede establecer que la responsabilidad anual total sobre la garantía a todas las personas que presenten un reclamo amparándose en ella no puede exceder el importe nominal de la garantía
34. **"Suspender un certificado"**: volverlo temporariamente ineficaz a partir de determinada fecha.
35. **"Timbre fechador"**: Significa:
    1. Agregar a un mensaje, a una firma digital o a un certificado una anotación firmada digitalmente donde se indique como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación, o bien
    2. La anotación así agregada.
36. **"Certificado de transacción"**: certificado válido, que incorpore por referencia una o más firmas digitales.
37. **"Sistema confiable"**: equipos y programas de computación:
    1. Que sean razonablemente confiables contra la posibilidad de intrusión o uso indebido;
    2. Que brinden un razonable grado de disponibilidad, confiabilidad y correcto funcionamiento, y
    3. Que se adapten debidamente al desempeño de sus funciones específicas.
38. **"Certificado válido"**: Certificado:
    1. Que ha sido emitido por una autoridad certificante;
    2. Que ha sido aceptado por el suscriptor allí mencionado;
    3. Que no ha sido revocado ni suspendido;
    4. Que no ha vencido.

    Se establece que un certificado de transacción constituye un certificado válido sólo en relación con la firma digital incorporada en él por referencia.
39. **"Verificar una firma digital"**: En relación con una firma digital, mensaje o clave pública, determinar fehacientemente:
    1. Que la firma digital fue creada por la clave privada correspondiente a la clave pública, y
    2. Que el mensaje no ha sufrido modificaciones con posterioridad a la creación de la firma digital.

104. Papel que le cabe a la División

**Autoridad certificante**

La División será la autoridad certificante, y está facultada para emitir, suspender y revocar certificados en la manera prescripta para las autoridades certificantes acreditadas. La Parte 3 rige para la División respecto de los certificados que emite.

**Base de datos de los registros de publicidad de la autoridad certificante**

La División mantendrá una base de datos a la cual pueda acceder el público, que contenga el registro de publicidad de cada autoridad certificante acreditada. También publicará el contenido de dicha base de datos en por lo menos un repositorio reconocido.

**Reglas**

La División establecerá reglas compatibles con el presente capítulo, para conseguir sus objetivos:

1. Para regir a las autoridades certificantes acreditadas, el ejercicio de su labor y la cancelación del ejercicio de la labor de tales autoridades;
2. Para determinar el monto apropiado que se considere suficiente garantía, teniendo en cuenta:
    a) el costo que dicha garantía representa para las autoridades certificantes acreditadas, y
    b) la garantía de responsabilidad financiera que brinda a las personas que confían en los certificados emitidos por autoridades certificantes acreditadas;
3. Para supervisar los soportes lógicos a usarse en la creación de firmas digitales y publicar informes relativos a ellos;

4. Para determinar los requisitos que debe reunir la forma de los certificados emitidos por autoridades certificantes acreditadas;
5. Para determinar los requisitos que deben cumplir las autoridades certificantes al llevar sus registros;
6. Para determinar los requisitos de contenido, forma y fuentes de información de los registros de publicidad de la autoridad certificante, la puesta al día de tal información, como también otras prácticas y políticas relativas a los registros de publicidad de las autoridades certificantes;
7. Para especificar la forma de las fórmulas de certificación, y
8. Para cualquier otro acto tendiente a dar validez e implementar la presente Ley de Firma Digital.

**TÍTULO 2. Acreditación y reglamentación de las autoridades certificantes**

201. **Acreditación y requisitos para las autoridades certificantes**
**Requisitos**

Para obtener o retener una licencia de autoridad certificante, quien pretenda serlo
1. Debe ser suscriptor de un certificado publicado en un repositorio reconocido
2. Debe emplear como personal operativo sólo a personas que no hubiesen sido condenadas en los últimos quince años por delitos de fraude, falso testimonio o engaño.
3. Debe emplear como personal operativo sólo a personas que hubiesen demostrado tener conocimientos y la capacidad de cumplir con los requisitos del presente capítulo.
4. Debe presentar en la División una suficiente garantía, a menos que la autoridad certificante sea el gobernador, algún organismo del gobierno estadual, la Fiscalía de Estado, el Consejo Judicial de Utah, una ciudad o una municipalidad, siempre y cuando los mencionados actuaran a través de funcionarios designados, autorizados por ley o reglamento, a ejercer las funciones de autoridad certificante; y este Estado o uno de los organismos mencionados sea el suscriptor de todos los certificados emitidos por dicha autoridad certificante.
5. Debe tener la posibilidad de usar un sistema confiable, incluso un método seguro para controlar el uso de su clave privada.
6. Debe presentar a la División prueba de poseer un suficiente capital de explotación que le permita realizar negocios en calidad de autoridad certificante.
7. Debe tener oficinas en este Estado o contar con un representante matriculado para la notificación de actos procesales en este Estado, y
8. Debe cumplir con todos los demás requisitos exigidos por la reglamentación de la División.

**Emisión de la licencia**

La División emitirá una licencia de acreditación a la autoridad certificante:
1. Que esté calificada conforme al apartado (1) de el presente artículo:
2. Que presente por escrito una solicitud de licencia a la División, y
3. Que abone una tasa estipulada por la División.

**Licencias restringidas**

La División puede clasificar las licencias de acuerdo con ciertas limitaciones específicas, tales como número máximo de certificados pendientes, máximo total de límites de confianza recomendados en certificados emitidos por la autoridad certificante o bien emisión sólo dentro de una única organización, y puede emitir licencias restringidas dentro de los límites de cada clasificación. Si la autoridad certificante emite un certificado que exceda las restricciones de la licencia, actúa como autoridad certificante no acreditada. (unlicensed).

**Suspensión o revocación de la licencia**

La División puede revocar o suspender la licencia a una autoridad certificante si ésta no cumple con lo dispuesto en el presente capítulo o si no sigue siendo calificada según lo establece el apartado (1) de este artículo, de conformidad con los procedimientos judiciales estipulados en la Ley de Procedimientos Administrativos, título 63, capítulo 46b.

**Reconocimiento de otras licencias**

La División puede reconocer la acreditación o autorización de autoridades certificantes que realicen otros organismos gubernamentales, siempre y cuando los requisitos para la acreditación sean substancialmente similares a los que rigen en este Estado. En tal caso:

1. La parte 4 del presente capítulo, relacionada con las presunciones y efectos legales, regirá para los certificados emitidos por autoridades certificantes acreditadas por dicho organismo gubernamental de la misma manera que rige para las autoridades certificantes de este Estado, y
2. Los límites de responsabilidad de El artículo 309 se aplicarán a las autoridades certificantes acreditadas o autorizadas por dicho organismo gubernamental del mismo modo que rigen para las de este Estado.

**Efectos de la falta de acreditación (licensing)**

Salvo que las partes estipulen lo contrario por contrato suscripto entre ellas, los requisitos para la acreditación que establece este artículo no afectan la efectividad, aplicabilidad ni la validez de una firma digital, salvo que la parte 4 del presente capítulo no regirá en relación con la firma digital que no pueda ser verificada por un certificado emitido por autoridad certificante acreditada. Más aún, los límites de responsabilidad establecidos por El artículo 309 no rigen para las autoridades certificantes no acreditadas.

**202. Auditorías de gestión**

**Evaluación anual de gestión**

Por lo menos una vez al año, un contador público con experiencia en temas de seguridad informática, o bien un acreditado profesional de la computación, evaluarán las operaciones de cada autoridad certificante acreditada con el fin de determinar si se cumplen las normas exigidas por este capítulo. La División puede especificar con mayor lujo de detalles los requisitos para los auditores.

**Categorización y publicación de los resultados**

Tomando en cuenta la información recogida en la auditoría, el auditor clasificará el desempeño de la autoridad certificante como de:

1. Cumplimiento total: La autoridad certificante cumple razonablemente con todos los requisitos regulatorios y establecidos por la ley.
2. Cumplimiento satisfactorio: La autoridad certificante cumple razonablemente con todos los requisitos regulatorios y establecidos por la ley; sin embargo, se advierte uno o más casos de incumplimiento o de incapacidad de demostrar el cumplimiento, pero se los considera de escasa importancia.
3. Cumplimiento parcial: La autoridad certificante cumple con algunos de los requisitos regulatorios y establecidos por la ley, pero se le comprueba incumplimiento, o incapacidad de demostrar cumplimiento, de uno o más resguardos importantes.
4. Incumplimiento: La autoridad certificante cumple muy pocos o ninguno de los requisitos regulatorios establecidos por ley, no lleva registros adecuados para demostrar cumplimiento de numerosos requisitos, o bien se negó a permitir la auditoría.
5. La División publicará en el registro de publicidad de la autoridad certificante la fecha de la auditoría y la resultante clasificación que recibió la autoridad.

**Excepciones de la obligación de realizar la evaluación de gestión**

La División puede eximir a la autoridad certificante acreditada de las exigencias fijadas por el apartado (1) de el presente artículo:

1. Si la autoridad certificante solicita por escrito ser eximida;
2. Si en la última auditoría que se le hubiera practicado hubiese obtenido la calificación de cumplimiento total o cumplimiento satisfactorio, y
3. Si la autoridad certificante declara bajo juramento una de las siguientes tres alternativas:
    1. que hubiera emitido menos de seis certificados durante el año anterior, y el total de los límites de confianza recomendados, de todos esos certificados, no excediera los U$S 10.000;
    2. que la vigencia total de todos los certificados emitidos por dicha autoridad durante el año anterior fuera inferior a 30 días, y el total de los límites de confianza recomendados, de todos esos certificados, no excediera los U$S 10.000;
    3. que los límites de confianza recomendados de todos los certificados pendientes y emitidos por la autoridad certificante totalizaran menos de U$S 1.000.

Si la declaración que presenta la autoridad certificante conforme a este apartado falsea algún dato relevante, se considerará que dicha autoridad no cumplió con la obligación de auditoría exigida por este artículo.

Si la autoridad certificante acreditada resultara eximida conforme a este apartado, la División publicará en el registro de publicidad que dicha autoridad ha sido eximida del requerimiento de una auditoría de gestión.

**203. Fiscalización de los requisitos para las autoridades certificantes acreditadas**

**Tareas fiscalizadoras de la División**

La División puede investigar las actividades de una autoridad certificante relativas al cumplimiento de lo prescripto por el presente capítulo y ordenarle que profundice su investigación y garantice el cumplimiento de lo dispuesto en el presente capítulo.

**Restricción, suspensión o revocación de la licencia (acreditación)**

La División puede restringir la licencia de una autoridad certificante tal como se establece en El artículo 3 si la autoridad no cumple alguna orden emanada de la División; también puede suspenderle o revocarle la licencia según se establece en El artículo 4

**Sanción civil**

Toda persona que a sabiendas o intencionalmente viole alguna cláusula del presente capítulo, o alguna disposición emanada de la División conforme a este artículo, será pasible de una penalidad civil que no sobrepasará los U$S 5.000 por infracción, o el 90% del límite recomendado de confianza, la cifra que sea menor.

**Costo de las tareas de fiscalización**

Si la División determina que una autoridad certificante ha infringido lo dispuesto por el presente capítulo, puede ordenarle el pago de las costas en que se hubiere incurrido en los procedimientos relativos a la orden.

**Procedimiento - Resoluciones**

La División puede ejercer la autoridad que le otorga este artículo de conformidad con las facultades que le otorga la Ley de Procedimientos Administrativos, título 63, capítulo 46b, y la autoridad certificante acreditada puede lograr judicialmente que se revisen los actos de la División tal como lo prescribe la misma Ley de Procedimientos Administrativos. La División a su vez puede solicitar una orden judicial para exigir el cumplimiento de cualquiera de sus resoluciones, y puede recaudar todos los montos adeudados conforme a este artículo, de la manera estipulada para la ejecución civil de órdenes por la Ley de Procedimientos Administrativos, título 63, capítulo 46b.

**204. Actividades peligrosas prohibidas para cualquier autoridad certificante**

**Prohibición de correr riesgos comerciales no razonables**

Ninguna autoridad, acreditada o no, realizará su actividad de negocios de manera tal de generar un riesgo elevado y no razonable de pérdida a sus suscriptores, a personas que confían en certificados por ella emitidos o en un repositorio.

**Publicación de boletines de advertencia**

La División puede publicar en uno o más repositorios reconocidos breves anuncios advirtiendo a suscriptores, a personas que confían en firmas digitales y/o repositorios respecto de cualquier actividad de una autoridad certificante, acreditada o no, que genere un riesgo no razonable conforme al apartado (1) de el presente artículo. La autoridad certificante acusada de crear dicho riesgo puede impugnar la publicación de la nota presentando una breve defensa por escrito. Al recibir la impugnación, la División la publicará junto con la nota de la División, y de inmediato notificará a la autoridad certificante la fecha de una audiencia. Celebrada la audiencia, la División la anulará de la lista de autoridades certificantes autorizadas objetadas por generar un riesgo no razonable, si dicha publicación no estuviera justificada por este artículo; y asimismo, cancelará su publicación si ya no estuviera más justificada, ó la continuará o enmendará si permaneciera justificada, o bien proseguirá las acciones judiciales para eliminar o reducir un riesgo no razonable por el apartado 1 de este artículo. La División publicará su decisión en uno o más repositorios reconocidos.

**Órdenes y prohibiciones**

En la manera prevista por la Ley de Procedimientos Administrativos, título 63, capítulo 46b, la División puede emitir órdenes y obtener prohibiciones u otra medida cautelar para impedir que una autoridad certificante viole lo dispuesto por el presente artículo, ya sea que dicha autoridad esté, o no, acreditada. Este artículo no acuerda a ninguna otra persona que no sea a la División el derecho de entablar acciones.

## TÍTULO 3. Obligaciones de las autoridades certificantes y los suscriptores

### 301. Requisitos generales para las autoridades certificantes

**Sistemas confiables**

La autoridad certificante o el suscriptor debe utilizar únicamente un sistema confiable:

1. Para emitir, suspender o revocar un certificado;
2. Para publicar o notificar la emisión, suspensión o revocación de un certificado, o
3. Para crear una clave privada.

**La publicidad ante una solicitud de información**

La autoridad certificante acreditada dará a publicidad toda declaración de procedimientos significativa, y todo hecho pertinente a la confiabilidad de un certificado emitido o a su capacidad de cumplir con su finalidad. Para efectuar la publicidad, la autoridad certificante puede requerir que se le haga un pedido escrito, razonablemente específico y firmado por una persona identificada, además del pago de un razonable arancel.

### 302. Emisión de un certificado

**Requisitos previos a la emisión de un certificado**

La autoridad certificante puede emitir un certificado a un suscriptor sólo si previamente se cumplen las siguientes condiciones:

1. La Autoridad Certificante ha recibido un requerimiento de emisión firmado por quien será el suscriptor; y
2. La Autoridad Certificante ha confirmado que:
    1. el eventual suscriptor es la persona cuyo nombre figurará en el certificado a emitirse;
    2. Si el eventual suscriptor actúa a través de uno o más representantes, que los haya autorizado debidamente a tener la custodia de su clave privada y a requerir la emisión de un certificado donde aparezca mencionada la correspondiente clave pública;
    3. información que aparece en el certificado es fidedigna;
    4. el eventual suscriptor posee legalmente la clave privada correspondiente a la clave pública mencionada en el certificado;
    5. el eventual suscriptor posee una clave privada capaz de crear una firma digital, y
    6. la clave pública a mencionarse en el certificado pueda utilizarse para verificar una firma digital generada por la clave privada que tiene el eventual suscriptor.

Los requisitos exigidos en el presente apartado son irrenunciables para la autoridad certificante acreditada, el suscriptor o ambos, según sea el caso.

**Publicación del certificado emitido y aceptado**

Si el suscriptor acepta el certificado emitido, la autoridad certificante publicará una copia firmada del mismo en un repositorio reconocido, salvo que las partes estipulen lo contrario. Si el suscriptor no acepta el certificado, la autoridad certificante acreditada no lo publicará, o bien cancelará su publicación si ya hubiese sido publicado.

**Se permiten requisitos más rigurosos**

Los términos del presente artículo no impiden que la autoridad certificante acreditada se rija por normas, procedimientos de certificación, planes de seguridad o requisitos contractuales más rigurosos, pero coherentes con el presente capítulo.

**Suspensión o revocación de un certificado por emisión deficiente**

Luego de emitido un certificado, la autoridad certificante puede revocarlo de inmediato si constata que no lo emitió conforme a los términos de el presente artículo. También puede suspender un certificado por un período razonable que no exceda las 48 horas para que, mediante una investigación, se confirme que existen fundamentos para revocarlo conforme al presente apartado. Cuando la autoridad certificante revoque o suspenda un certificado conforme a este apartado, notificará de inmediato al suscriptor.

**Orden de suspensión o revocación**

La División puede ordenar a la autoridad certificante acreditada la suspensión o revocación de un certificado emitido por esta última si, luego de notificar debidamente a la autoridad certificante y al suscriptor y

haberles otorgado la oportunidad de ser escuchados de acuerdo con la Ley de Procedimientos Administrativos, título 63, capítulo 46b, la División determinara que:
1. El certificado fue emitido sin cumplir substancialmente con las pautas de la presente sección, y
2. Si dicho incumplimiento implica un riesgo importante para personas que puedan confiar razonablemente en tal certificado.

Si se determina que, dada la urgencia, hace falta una solución inmediata conforme lo estipula la Ley de Procedimientos Administrativos, la División puede ella misma suspender un certificado por un período que no exceda las 48 horas.

**303. Garantías y obligaciones de la autoridad certificante al emitir un certificado**

**Garantías al suscriptor**

Mediante la emisión de un certificado, la autoridad certificante acreditada garantiza al suscriptor cuyo nombre figura en el certificado que:
1. el certificado no contiene información que a juicio de la autoridad certificante es falsa;
2. el certificado cumple con todos los requisitos pertinentes del presente capítulo, y
3. no se ha excedido en sus funciones específicas al emitir tal certificado.

La autoridad certificante no puede deslindar responsabilidades ni limitar las garantías previstas por este apartado.

**Obligaciones para con el suscriptor**

A menos que el suscriptor y la autoridad certificante convengan lo contrario, al emitir un certificado la autoridad promete al suscriptor:
1. Actuar de inmediato para suspender o revocar un certificado de conformidad con las secciones 306 ó 307, y
2. Notificar al suscriptor en tiempo razonable de cualquier hecho sobre el cual tenga conocimiento y que pueda afectar significativamente la validez o confiabilidad del certificado, luego de ser éste emitido.

**Consecuencias legales de la emisión de un Certificado**

Al emitir un certificado, la autoridad certificante autorizada certifica ante todos aquellos que confían razonablemente en la información contenida en el certificado que:
1. la información contenida en el certificado, que aparece como confirmada por la autoridad certificante autorizada, es válida;
2. toda la información significativa a los fines de la confiabilidad del certificado se halla mencionada o referenciada dentro del certificado;
3. el suscriptor ha aceptado el certificado, y que
4. la autoridad certificante ha cumplido con todas las leyes aplicables de este Estado relativas a la emisión del certificado.

**Consecuencias legales de la publicación**

Al publicar un certificado, la autoridad certificante autorizada certifica al repositorio en el cual éste se publica, y a todos los que razonablemente confían en la información contenida en el certificado, que ha emitido el certificado al suscriptor.

**304. Implicancias derivadas de la aceptación de un certificado**

**Declaraciones implícitas por parte del suscriptor**

Por el hecho de aceptar un certificado emanado de autoridad certificante acreditada, el suscriptor cuyo nombre figura en él garantiza a todos los que razonablemente confíen en la información allí contenida que:
1. posee legalmente la clave privada correspondiente a la clave pública mencionada en el certificado;
2. todas las declaraciones hechas por él a la autoridad certificante, relativas a la información del certificado, son verdaderas;
3. todas las declaraciones significativas hechas a la autoridad certificante, o hechas en el certificado y no confirmadas por la autoridad certificante al emitir el certificado, son verdaderas.

**Por parte de un representante o supuesto representante del suscriptor**

Al solicitar, en nombre de un mandante, la emisión de un certificado donde figure el mandante como suscriptor, el solicitante certifica, en nombre del mandante a todos aquellos que confían razonablemente en

la información contenida en el certificado que le solicitante:
1. tiene la autoridad legal requerida para solicitar la emisión de un certificado donde figure su mandato como suscriptor, y
2. tiene mandato para firmar digitalmente en nombre de su mandante y, si dicho mandato fuere limitado de alguna manera, que existen los adecuados resguardos para impedir que una firma digital exceda los límites del mandato otorgado.

**Limitaciones a la renuncia de responsabilidad o a la obligación de indemnizar**

Ninguna persona puede negar ni desconocer contractualmente la aplicación de este artículo, como tampoco obtener indemnización por sus efectos, si la negación, limitación o indemnización restringiera la responsabilidad por declaraciones inexactas frente a personas que razonablemente confíen en el certificado.

**Indemnización a la autoridad certificante por parte del suscriptor**

Al aceptar un certificado, el suscriptor se compromete a indemnizar a la autoridad certificante por daños y perjuicios en la emisión o publicación de un certificado, en base a:

1. Una declaración falsa y significativa realizada por el suscriptor; o bien
2. Un hecho significativo no revelado por el suscriptor;

si la falsedad o la no revelación se hubiesen hecho con la intención de engañar a la autoridad certificante o persona que confíe en el certificado, o con negligencia. Si la autoridad certificante emitió el certificado a pedido de uno o más representantes del suscriptor, dichos representantes asumen personalmente la obligación de indemnizar a la autoridad conforme a este apartado, como si fueran ellos los suscriptores que aceptan el certificado por propio derecho. No se puede renunciar a la indemnización que prevé este apartado ni limitar contractualmente su alcance; sin embargo, mediante un contrato se pueden prever términos adicionales, compatibles con esta indemnización.

**Declaraciones falsas**

Al obtener información del suscriptor pertinente a la emisión de un certificado, la autoridad certificante puede requerirle al suscriptor que certifique la veracidad de dicha información bajo juramento, so pena de iniciar procedimientos penales por haber suscripto declaraciones juradas falsas.

**305. Control de la clave privada**

**Obligación del suscriptor de mantener segura la clave privada**

Al aceptar un certificado emitido de una autoridad certificante autorizada, el suscriptor cuyo nombre figura en él asume la obligación de procurar razonablemente mantener el control de la clave privada e impedir su divulgación a persona alguna no autorizada para crear la firma digital del suscriptor.

**La clave privada es propiedad del suscriptor**

La clave privada es propiedad personal del suscriptor que la posee legalmente.

**Autoridad certificante fiduciaria si posee la clave privada del suscriptor**

Si una autoridad certificante posee la clave privada correspondiente a la clave pública mencionada en el certificado por ella emitido, lo hace en calidad de representante del suscriptor mencionado en el certificado, y sólo puede usar la clave privada con el previo consentimiento escrito del suscriptor, a menos que el suscriptor le otorgue expresamente su clave privada o permita a la autoridad certificante su uso según otros términos.

**306. Suspensión de un certificado**

**Suspensión por parte de la autoridad certificante emisora**

Salvo que la autoridad certificante y el suscriptor convengan lo contrario, la autoridad certificante autorizada que emitió el certificado que no sea un certificado transaccional puede suspenderlo por un lapso que no exceda las 48 horas:

1. A pedido de una persona que se identifique como el suscriptor cuyo nombre aparece en el certificado, o una persona que se encuentre en una posición tal que le permita saber que se ha comprometido la seguridad de la clave privada de algún suscriptor, como por ejemplo, un representante suyo, socio comercial, empleado o familiar inmediato, o bien

2. Por orden de la División conforme a lo que dispone el apartado 302(5).

La autoridad certificante no necesita confirmar la identidad o el mandato de la persona que solicita la suspensión.

**Suspensión dispuesta por la División o por un tribunal o por un secretario de condado**

A menos que el certificado especifique lo contrario, o que se trate de un certificado transaccional, la División, un tribunal o un secretario de condado puede suspender por 48 horas un certificado emitido por una autoridad certificante acreditada si:

1. una persona que se identifique como el suscriptor a cuyo nombre se emitió el certificado, o como un representante suyo, socio comercial, empleado o familiar inmediato suyo, solicita la suspensión, y
2. el solicitante declara que es imposible dar con la autoridad que emitió el certificado.

La División, un tribunal o el secretario de condado pueden exigir al solicitante que requiere la suspensión, que demuestre fehacientemente, incluso bajo declaración jurada, su identidad, la autorización y/o la indisponibilidad de la autoridad certificante, y puede negarse a efectuar la suspensión a su arbitrio. La División y/o entidades de fuerza pública pueden investigar las suspensiones ordenadas por la División o un tribunal o los secretarios de condado por posible acto ilícito que pueda haber cometido la persona que solicitó la suspensión.

**Nota**

Inmediatamente después de producida la suspensión de un certificado, la autoridad certificante autorizada publicará un aviso firmado de la suspensión en el repositorio que menciona el certificado, donde se deben publicar los avisos de suspensión. Si se mencionara más de un repositorio, lo publicará en todos ellos. Si alguno de tales repositorios no existiera más o se negara a aceptar la publicación, o si no se reconoce ningún repositorio conforme a lo que dispone el artículo 501 del presente capítulo, la autoridad certificante publicará la suspensión en algún otro repositorio reconocido. Si el certificado fuese suspendido por la División o por tribunal o por un secretario de condado, la División, el tribunal o el secretario efectuarán la notificación, siempre y cuando la persona que solicite la suspensión abone por adelantado el arancel que exija el repositorio para dicha publicación.

**Terminación de la suspensión solicitada**

Una autoridad certificante levantará una suspensión solicitada sólo si:

1. el suscriptor nombrado en el certificado suspendido solicita el levantamiento de la suspensión, si la autoridad certificante confirmó que el solicitante es el suscriptor o un representante suyo autorizado a levantar la suspensión, o bien
2. la autoridad certificante descubre y confirma que el pedido de suspensión se realizó sin autorización del suscriptor, siempre y cuando este apartado no exija que la autoridad certificante debe confirmar un pedido de suspensión

**Procedimientos contractuales alternativos**

El contrato entre suscriptor y autoridad certificante acreditada puede limitar o prohibir la suspensión solicitada por la autoridad certificante, o bien puede establecer otra forma de levantar una suspensión solicitada. Sin embargo, si el contrato limita o impide la suspensión por parte de la División o de tribunal o de un secretario de condado cuando no se dispone de autoridad certificante, la limitación o prohibición será efectiva sólo si se informa de ella en el certificado.

**Prohibición de presentar un pedido de suspensión falso o no autorizado**

Ninguna persona puede, a sabiendas o intencionalmente, declarar en forma inexacta ante una autoridad certificante su identidad o su autorización para solicitar la suspensión de un certificado. Toda violación a este apartado se considerará una contravención de clase B (contravención o delito menor).

**Efecto de la suspensión**

Durante el lapso que el certificado esté suspendido, el suscriptor queda relevado de su obligación de mantener confidencial la clave privada, de conformidad con lo establecido en el apartado 305(1).

**307. Revocación de un certificado**

**Revocación por pedido**

Una autoridad certificante autorizada revocará un certificado que emitió, siempre que no sea un certificado transaccional, después de:

1. recibir una solicitud de revocación de parte del suscriptor mencionado en el certificado; y
2. confirmar que la persona que solicita la revocación es el suscriptor o es un mandatario del suscriptor con autoridad para requerir la revocación.

**Plazos para que la revocación requerida tenga efecto**

La autoridad certificante autorizada confirmará un pedido de revocación, y revocará un certificado en el término de un día hábil cuando reciba un pedido escrito del suscriptor y tenga muestras suficientes para confirmar la identidad o representación del solicitante.

**Revocación a la muerte del suscriptor**

La autoridad certificante autorizada revocará un certificado por ella emitido en caso de:

1. Recibir una copia legalizada de la partida de defunción del suscripto, o de confirmar por algún otro medio que el suscriptor ha fallecido, o
2. Recibir documentos causantes de la disolución del suscriptor, o bien al confirmar por algún otro medio que el suscriptor se disolvió o dejó de existir.

**Revocación de certificados no confiables sin que medie un pedido**

La autoridad certificante puede revocar uno o más certificados por ella emitidos si fueran o llegaran a ser no confiables, con independencia de que el suscriptor consienta o no la disolución, y pese a lo que pueda establecer cualquier disposición en contrario acordada mediante contrato entre el suscriptor y la autoridad certificante autorizada.

**Notificación**

Ni bien la autoridad certificante revoca un certificado, debe publicar una notificación firmada de la revocación en el repositorio que menciona el certificado. Si figurara más de uno, la publicación deberá hacerse en todos ellos. Si el repositorio allí mencionado no existiera más o se negara a aceptar la publicación, o si no estuviera reconocido conforme lo establece el art. 501 de este capítulo, la autoridad certificante publicará la notificación en otro repositorio reconocido.

**Efecto del pedido de revocación sobre el suscriptor**

El suscriptor deja de certificar según lo establece el art. 304, y cesa su obligación de resguardar la clave privada tal como lo exige el art. 305 en relación con un certificado cuya revocación ha solicitado el suscriptor, desde

1. la fecha de publicación de la notificación de revocación según lo exige el apartado (5) del presente artículo, o bien
2. dos días hábiles después de que el suscripto solicite por escrito la revocación, brinde a la autoridad certificante información suficiente para confirmar el pedido y abone el arancel estipulado por contrato, lo primero que ocurra.

**Efecto de la notificación en la Autoridad Certificante**

Luego de producida la notificación requerida en el apartado 5 de este artículo, una Autoridad Certificante Autorizada es liberada de su responsabilidad emanada de la emisión del certificado revocado y deja de certificar según lo previsto en los apartados 303 (2) y 303 (3) respecto del certificado revocado.

**308. Vencimiento del certificado**

**Requisitos generales**

El certificado deberá indicar su fecha de vencimiento, que no excederá los tres años posteriores a su emisión, salvo que el certificado especifique que tendrá una vigencia superior.

**Efecto**

Cuando vence un certificado, el suscriptor y la autoridad certificante dejan de certificar según lo dispone este capítulo, y la autoridad certificante queda relevada de sus obligaciones provenientes de la emisión, en relación con el certificado que ha expirado.

**309. Límites de confianza y de responsabilidad recomendados**

**Significación del límite de confianza recomendado**

Al especificar en un certificado un límite de confianza, la autoridad que lo emitió y el suscriptor que lo acepta recomiendan que las personas confíen en él en tanto y en cuanto el monto en juego no exceda el límite de confianza recomendado.

**Límites de responsabilidad para las autoridades certificantes acreditadas**

Salvo que la autoridad certificante renuncie a la aplicación del presente apartado, se considerará:

1. Que no será responsable por pérdidas causadas por haberse confiado en una firma falsa o fraguada de un suscriptor si, con respecto a dicha firma, la autoridad hubiera cumplido con todos los requisitos pertinentes establecidos en el presente capítulo;
2. Que no será responsable por un monto mayor al que se menciona en el certificado como límite recomendado de confianza en caso de:
    1. una pérdida causada por haber confiado en una dato falso contenido en el certificado que a la autoridad certificante se le requiera confirmar, o
    2. incumplimiento con el art. 302 en la emisión del certificado;
    3. Será responsable sólo por daños directos emergentes de una acción promovida por resarcimiento de daños debido a haber confiado en el certificado.

Los daños directos compensatorios no incluyen:

1. daños ejemplares o punitivos;
2. daños por lucro cesante, ahorros u oportunidad, ni
3. daños físicos y morales.

**310. Cobranza basada en suficiente garantía**

**Derecho de cobro del reclamante**

Pese a cualquier disposición en contrario que pueda contener la garantía,

1. Si la garantía es una fianza, la persona puede recuperar el monto total de un derecho limitado de pago contra el obligado principal que figura en la fianza, y si hay más de uno de tales derechos limitados de pago durante la vigencia de la fianza, una participación proporcional, hasta un máximo equivalente al monto de la fianza, o bien
2. Si la garantía es una carta de crédito, una persona puede recuperar de la institución financiera emisora el monto total de un derecho limitado de pago contra el cliente cuyo nombre figura en la carta de crédito. Si hubiere más de un derecho limitado de pago durante la vigencia de la carta de crédito, una participación proporcional, hasta una responsabilidad máxima del emisor equivalente al monto del crédito.

Los reclamantes pueden recuperar sucesivamente de la misma garantía, siempre y cuando la responsabilidad total frente a todas las personas que esgriman derechos limitados de pago durante su vigencia no exceda del monto de la garantía.

**Honorarios de abogados**

Además de recuperar el monto de un derecho limitado de pago, el reclamante puede recuperar del producido de la garantía, hasta que se agote, una suma razonable en concepto de honorarios de abogados, y las costas judiciales en que hubiera incurrido para percibir el reclamo, siempre y cuando la responsabilidad total que figure en la garantía para todas las personas que esgriman derechos limitados de pago o que recuperen honorarios para abogados no exceda el monto total de la garantía.

**Procedimiento del reclamo**

Para recuperar un derecho limitado de pago contra un fiador o emisor de garantía, el reclamante deberá:

1. Notificar por escrito a la División consignando su propio nombre y domicilio, la suma reclamada y los fundamentos para el pago, y cualquier otra información que requiriera las normas de la División, y
2. Adjuntar a la notificación una copia certificada de la sentencia sobre la cual se basa el pago limitado.

La recuperación del derecho de pago limitado con el producido de la suficiente garantía no podrá efectuarse si el reclamante no cumple integralmente con el presente artículo.

**Plazo para la presentación de reclamos**

La recuperación del derecho de pago limitado con el producido de la garantía prescribirá para siempre a menos que se notifique el reclamo como lo exige el apartado (3) dentro de los dos o tres(??) años de ocurrida la violación del presente capítulo, base del reclamo.

## TÍTULO 4. Efecto de la firma digital

### 401. Cumplimiento de los requisitos de la firma

**General**

Cuando el régimen jurídico requiere una firma, o prevé ciertas consecuencias de la falta de firma, dicho sistema de derecho queda cumplido con una firma digital en los siguientes casos:

1. Si la firma digital se verifica por referencia a la clave pública mencionada en un certificado válido emitido por una autoridad certificante acreditada;
2. Si la firma digital fue suscripta por el firmante con la intención de firmar el mensaje, y
3. Si el destinatario no tiene conocimiento de que el firmante:
   1. haya infringido un deber en su calidad de suscriptor, o bien
   2. no posea legalmente la clave privada usada para suscribir la firma digital.

**Otras firmas**

Sin embargo, las disposiciones del presente capítulo no impiden que un símbolo sea válido como firma bajo otra ley aplicable, tal como el Código Comercial Uniforme de Utah, artículo 70A-1-201(39).

**Comisión impositiva**

El presente artículo no limita la facultad de la Comisión Impositiva del Estado para establecer la forma de las declaraciones de impuestos u otros documentos que se presenten a dicha Comisión.

### 402. Firmas digitales no confiables

Salvo que se establezca lo contrario por ley o contrato, si la firma digital no fuera confiable, en determinadas circunstancias el receptor de una firma digital asume el riesgo de que dicha firma sea fraguada. Si el receptor decide no confiar en una firma digital de conformidad con el presente artículo, deberá notificar cuanto antes al firmante su decisión, como también los fundamentos de tal decisión.

### 403. El documento que lleva firma digital se considera documento escrito

Un mensaje tiene la misma validez y puede ser exigido judicialmente y es efectivo como si estuviera escrito en papel, en los siguientes casos:

1. Si porta en su totalidad una firma digital, y
2. Si dicha firma digital es verificada mediante la clave pública mencionada en un certificado que:
   1. haya sido emitido por una autoridad certificante acreditada, y
   2. haya sido válido al momento en que se efectuó la firma digital.

Si embargo, el presente capítulo no impide que un mensaje, documento o registro sea considerado escrito bajo alguna otra ley aplicable.

### 404. Originales firmados digitalmente

Una copia de un mensaje firmado digitalmente tiene la misma validez legal que el original del mensaje, salvo que sea evidente que el firmante designó una instancia del mensaje firmado digitalmente para que sea original único, caso en el cual sólo dicha instancia constituye el mensaje válido, efectivo y ejecutable.

### 405. El certificado como un reconocimiento

Salvo que se establezca lo contrario por ley o contrato, un certificado emitido por autoridad certificante acreditada constituye un reconocimiento de una firma digital autenticada cotejándola con la clave pública mencionada en el certificado, con independencia de si aparecen, o no, palabras de reconocimiento con la firma digital, y de si el firmante se presentó físicamente ante la autoridad certificante cuando se creó la firma digital, siempre y cuando dicha firma cumpla con dos requisitos:

1. Que sea verificable mediante ese certificado, y
2. Que haya sido suscripta cuando el certificado era válido.

### 406. Presunciones en la resolución de litigios.

Al resolver un litigio que involucre una firma digital, un tribunal de este Estado deberá presumir:

1. Que un certificado firmado digitalmente, autenticado por una autoridad certificante autorizada y publicado en un repositorio conocido, o bien facilitado por la autoridad certificante o por el suscriptor cuyo nombre figura en el certificado, ha sido emitido por la autoridad que lo firmó digitalmente y aceptado por el suscriptor mencionado en él.

2. Que la información mencionada en un certificado válido y confirmado por una autoridad certificante acreditada emisora del certificado es fidedigna.
3. Si una firma digital está autenticada por la clave pública mencionada en un certificado válido emitido por una autoridad acreditada,
   1. Que esa firma digital es la del suscriptor cuyo nombre figura en el certificado;
   2. Que esa firma digital fue suscripta por el suscriptor con la intención de firmar el mensaje, y
   3. Que el receptor de esa firma digital no tiene noticia de:
      1. que el firmante hubiese infringido alguno de sus deberes de suscriptor, o
      2. que el firmante no tuviera legalmente la clave privada suscripta a la firma digital.
   4. Que la firma digital fue creada antes de haber sido marcada con sello fechador por un tercero no interesado utilizando un sistema confiable.

**TÍTULO 5. Repositorios**

**501. Reconocimiento de los repositorios**
**Condiciones para el reconocimiento**

La División reconocerá a uno o más repositorios, cuando haya constatado:

1. Que el repositorio a ser reconocido opera bajo la dirección de una autoridad certificante acreditada;
2. Que incluye una base de datos que a su vez contiene:
   1. Certificados publicados en el mismo;
   2. Notificaciones de certificados suspendidos o revocados, publicadas por las autoridades certificantes acreditadas u otras personas que suspenden o revocan certificados;
   3. Registros de publicidad de autoridades certificantes acreditadas;
   4. Todas las órdenes o recomendaciones publicadas por la División para regular a las autoridades certificantes, y
   5. Toda otra información que determinen las normas de la División.
3. Que opera mediante un sistema confiable;
4. Que no contiene una cantidad significativa de información que la división considere que es, o puede ser, no fidedigna o insuficientemente confiable.
5. Que contiene certificados publicados por autoridades certificantes a quienes se les requiere cumplir con las normas de uso que la División considera substancialmente similares, o más estrictas hacia las autoridades certificantes, que las de este Estado;
6. Que lleva un archivo de los certificados que han sido suspendidos o revocados, que han expirado, por lo menos en el término de los últimos 3 años, y
7. Que cumple con todo otro requisito razonable prescripto por las normas de la División.

**Procedimiento para el reconocimiento**

Un repositorio puede solicitar su reconocimiento a la División. Para ello deberá presentar una solicitud escrita adjuntando pruebas suficientes de haber satisfecho los requisitos que impone la División. La División decidirá si debe conceder o denegar el pedido en la manera que prevé la Ley de Procedimientos Administrativos, título 63), capítulo 46b.

**Revocación del reconocimiento**

El repositorio puede dejar sin efecto el reconocimiento notificando por escrito a la División con 30 días de anticipación. Asimismo, la División puede revocar el reconocimiento de un repositorio:

1. al haber pasado la fecha de expiración especificada por la División al conceder el reconocimiento, o
2. en cumplimiento de los procedimientos prescriptos por la Ley de Procedimientos Administrativos, título 63, capítulo 46b, si llega a la conclusión de que el repositorio ya no cumple con los requisitos para el reconocimiento establecidos por el presente artículo o por las normas de la División.

**502. Responsabilidad de los repositorios**

**Publicación del aviso de suspensión o de revocación**

Pese a cualquier declinación de responsabilidad que efectúe el repositorio, o a cualquier contrato suscripto entre el repositorio, la autoridad certificante o un suscriptor, el repositorio será responsable por la pérdida en que hubiese incurrido una persona que confiara razonablemente en una firma digital verificada por la clave pública mencionada en un certificado suspendido o revocado, si la pérdida se produjo más de un día hábil después de recibir el repositorio un pedido de publicar el aviso de la suspensión o revocación, y si el repositorio no hubiese publicado el aviso cuando la persona confió en la firma digital.

**Limitaciones de la responsabilidad**

A menos que se renuncie al derecho, el repositorio reconocido, el propietario o el operador de un repositorio reconocido:

1. No será responsable en caso de que no se hubiese registrado la publicación de una suspensión o revocación, salvo cuando el repositorio haya recibido el aviso de publicación y hubiera pasado un día hábil desde el momento en que lo recibió;
2. No será responsable conforme al inciso (1) de este artículo por un monto superior a la cifra consignada en el certificado como límite reconocido de confianza.
3. Será responsable conforme al inciso (1) de este articulo sólo por daños emergentes, que no incluyen:
    1. daños y perjuicios punitivos o ejemplares;
    2. daños por lucro cesante, ahorros o costo de oportunidad, ni
    3. daños físicos y morales.
    4. No será responsable por declaración inexacta o falsa en un certificado publicado por una autoridad certificante acreditada;
    5. No será responsable por registrar fidedignamente información que una autoridad certificante, un secretario de condado o un tribunal o la División hubiesen publicado tal como lo establece o lo permite este capítulo, inclusive información respecto de la suspensión o revocación de un certificado.
    6. No será responsable por publicar información sobre una autoridad certificante, un certificado o un suscriptor si lo hace de conformidad con lo que establece o permite el presente capítulo o una norma de la División, o si se publica por orden de la División en ejercicio de sus funciones regulatorias que le confiere este capítulo.

**Enmiendas propuestas al Código Penal de Utah Cód. Anot. Título 76 (1996)**

Las siguientes enmiendas se proponen para garantizar que el Código Penal de Utah pueda encarar adecuadamente el fraude y la falsificación en el comercio electrónico.

**Definiciones Generales**

La Subsección 76-1-601(12) fue enmendada para quedar en forma completa de la siguiente manera:

(12) “Escribir” o “escrita” incluye cualquier información manuscrita, tipiada, impresa, guardada o transmitida electrónicamente o cualquier otro método de grabado o fijado de información en una forma susceptible de ser preservada.

**Casos de prohibición de falsificación**

Se enmienda el apartado 76-6-501(12) de la siguiente manera:

(2) Tal como se lo usa en este artículo, el “escrito” incluye la impresión, el almacenamiento electrónico, la transmisión o cualquier otro método de registrar información valiosa, incluyendo formas tales como:
    (a) un cheque, cospel, estampilla, sello, tarjeta de crédito, marca comercial o cualquier otro símbolo de valor, derecho, privilegio o identificación;
    (b) una fianza, timbre fiscal o cualquier otro instrumento o escrito emitido por un gobierno o cualquier organismo;
    (c) una garantía (security), acción, bono, pagaré o cualquier otro instrumento escrito que represente un interés o un derecho sobre propiedad, o un interés pecuniario contra cualquier persona o empresa.

# Anexo 2
# Bibliografía


- Acuña Anzorena A., Efectos jurídicos de la impresión digital en los documentos privados, La Ley, tomo 23, página 904, Argentina.
- Altmark Daniel R., Informática y Derecho - La Etapa Precontractual en los Contratos Informáticos, Editorial Dipalma, Buenos Aires, 1991.
- Aracama Zorraquín, El Know how Técnico. Tentativa Sistemática Jurídica, Editorial Troyan, Argentina.
- Borda, G. A., Tratado de derecho civil, Parte General, 3ª edición, tomo II, Argentina.
- Bielsa, Rafael A., Informática y Derecho - Método de Análisis para una aplicación de Informática Jurídica Documental, Editorial Dipalma, Buenos Aires, 1991.
- Correa, Carlos María, Informática y Derecho - El Derecho Informático en América Latina, Editorial Dipalma, Buenos Aires, 1991.
- Devoto Mauricio, La Hoja, Revista quincenal del Colegio de Abogados de la Ciudad de Buenos Aires, año 4°, N° 58, página 6, Argentina.
- Devoto Mauricio, Comercio Electrónico y Firma Digital. La Regulación del Ciberespacio y las Estratégias Globales. Editorial La Ley, 2001.
- Devoto Mauricio, La Economía Digital, el dinero electrónico y el lavado de dinero. En http://www.itcenit.org.ar/Publicac/Lavado
- Devoto Mauricio y Horacio M. Lynch, Banca, comercio, moneda electrónica y la firma digital. En www.notaríadigital.com
- Diffie W., Hellman M.E., New Directions in Cryptography, Transactions on Information Theory Vol IT22 No 6, pp 644-654, USA, 1976.
- Farina, Juan M., Contratos Comerciales Modernos, Editorial Astrea, Argentina, 1998.
- Farjat Gérard, LAQUIS Manuel A. Y otros, El Derecho y las Nuevas Tecnologías, Editorial Depalma, Argentina.
- Friedman W., Cryptology, Encyclopedia Britannica, 6, pp 844-851, Inglaterra, 1967.
- Giannantonio Ettore, Informática y Derecho - El Valor Jurídico del Documento Electrónico, Editorial Dipalma, Buenos Aires, 1991.
- Hernández Claudio, Hackers, Los clanes de la ReD 2000, Kriptopolis, España, 1999.
- Hernández Claudio, Hackers, piratas tecnológicos, Coelma, España, 1998.
- Hernández Claudio, Hacking en Internet, Luis A.Iñigo e Israel Robla, España, 1998.
- Klander Lars, A prueba de Hackers, Anaya Multimedia, España, 1998.
- La Ley, Jurisprudencia y Fallos de Cámara, Editorial La Ley, Argentina.
- Llambías Jorge Joaquín, Tratado de Derecho Civil parte general, tomo II, Editorial Perrot, Argentina, 1975.
- Losano Mario G., Informática y Derecho - De la Pluma de Ganso al Rayo Laser: Nuevas tecnologías para los bancos de datos y las editoriales, Editorial Dipalma, Buenos Aires, 1991.
- Lucena López Manuel José, Criptografía y Seguridad en Computadores, Segunda Edición, Departamento de Informática Escuela Politécnica Superior Universidad de Jaén, España, 1999.
- Martino Antonio, Informática y Derecho - Sistemas Expertos Legales, Editorial Dipalma, Buenos Aires, 1991.
- Orgaz A., La impresión digital en los documentos privados, Revista “Colegio Abogados de Buenos Aires”, Argentina, marzo-abril 1936.
- Otamendi Jorge, Transferencia de tecnología: una cuestión que exige realismo en Derechos Intelectuales, Editorial Astrea, Argentina.
- Paul Fahn, Respuestas a las Preguntas más frecuentes sobre Criptografía actual. RSA Laboratories. RSA Data Security Inc. EEUU, 1993. Traducción por Lic. Andrés Hall y Cynthia R. Neme, Buenos Aires, 1996. www.cvn.gov.ar
- Rivera Julio César, Instituciones de Derecho Civil parte general, tomo II, Abeledo-Perrot, Argentina, 1995.
- Rivest R.L., Shamir A., Adleman L., A Method for Obtaining Digital Signature and Public-Key Cryptosystems, Communication of the ACM Vol 21 No 2 pp 120-126, USA, 1978
- Velázquez Juan Manuel y Quirantes Arturo, Manual de PGP 5.53i, España, 1998.

# Anexo 3
# Internet

**24. Argentina**

- Comisión Nacional de Valores.
  www.cnv.gov.ar
- PKI Argentina – Infraestructura de Firma Digital.
  http://www.pki.gov.ar
- IT-Cenit
  http://www.it-cenit.org.ar
- Universidad Nacional de Buenos Aires. Programa EcomDer - Congreso Internacional por Internet sobre Aspectos Jurídicos del Comercio Electrónico.
  http://www.ecomder.com.ar
  - Diario Judicial
    http://www.diariojudicial.com
  - Certisur S.A. Representante para el Mercosur de Verisign Trust Network Inc.
    http://www.certisur.com

**25. España**

- Criptonomicon – Criptografía y Seguridad en Internet
  Publicación del Departamento de Tratamiento de la Información y Codificación del Instituto de Física Aplicada del Consejo Superior de Investigaciones Científicas de España
  http://www.iec.csic.es/criptonomicon
- Hispasec – Instituto para la Seguridad en Internet
  http://www.hispasec.com
- R.E.D.I. – Revista Electrónica de Derecho Informático
  http://publicaciones/derecho.org/redi
- vLEX Networks
  http://vlex.com
- Kriptopolis – Seguridad en Internet
  Información independiente sobre seguridad y libertades en Internet
  http://www.kriptopolis.com
- MC – Mundo Cripto
  http://webs.ono.com/usr005/jsuarez/index.htm
- Enigma – Boletín del Taller de Criptografía de Arturo Quirantes Sierra
  http://www.ugr.es/~aquiran/cripto/cripto.htm
- Asociación de Internautas
  http://www.internautas.org

**26. Otros**

- México – UNAM - Universidad Autónoma de México
  http://www.mcc.unam.mx/index.html
- México – eVoBo.net – Representante para México de Entrust Inc.
  http://www.evobo.net
- Italia - Autoritá per l'Informatica nella Pubblica Amministrazione
  http://www.aipa.it