



PROYECTO DE LEY

Texto facilitado por los firmantes del proyecto. Debe tenerse en cuenta que solamente podrá ser tenido por auténtico el texto publicado en el respectivo Trámite Parlamentario, editado por la Imprenta del Congreso de la Nación.

Nº de Expediente	4991-D-2006
Trámite Parlamentario	122

El Senado y Cámara de Diputados,...

Art. 1º.- Creación. Créase con carácter exclusivo el "Servicio Nacional de Estampado de fecha y hora por Internet" a cargo del Observatorio Buenos Aires del Servicio de Hidrografía Naval.

Art. 2º.- Modalidad de prestación del servicio. El Servicio Nacional de Estampado de fecha y hora por Internet se prestará con carácter gratuito y en general, a través de la emisión de la fecha y hora por medio de un sitio tecnológicamente seguro de acuerdo a los estándares más actualizados de la tecnología de seguridad.

Art. 3º.- Solicitud de particulares. Emisión de certificados. Los particulares que requieran el estampado de fecha y hora oficial en documentos electrónicos lo solicitarán por medios informáticos al Servicio Nacional de Estampado de fecha y hora por Internet, el que emitirá un certificado digital de acuerdo a las condiciones del Capítulo II de la Ley 25.506, sus Decretos Reglamentarios y disposiciones de la autoridad de aplicación.

Art. 4º.- Licencia como certificador. Para cumplir con las prestaciones del artículo anterior, el Servicio Nacional de Hidrografía Naval deberá obtener licenciamiento como certificador según lo dispuesto en el Capítulo III de la ley 25.506, sus Decretos Reglamentarios y disposiciones de la autoridad de aplicación.

Art. 5º.- Otros servicios de seguridad. Prestación. El Servicio Nacional de Estampado de fecha y hora por Internet podrá prestar cualquier otro tipo servicios de seguridad a los documentos electrónicos, que sean permitidos por la Ley 25.506, sus Decretos Reglamentarios y disposiciones de la autoridad de aplicación.

Art. 6º.- Medidas transitorias. Facúltase al Poder Ejecutivo Nacional para disponer medidas transitorias que garanticen la prestación de este servicio conforme a los artículos anteriores, hasta tanto del Servicio de Hidrografía Naval obtenga el licenciamiento de ley.

Art. 7º.- Comuníquese al Poder Ejecutivo.

Fundamentos

Señor presidente:



El Proyecto de ley y estos fundamentos, que hago míos, han sido elaborados por el Grupo Firma Digital Tucumán integrado por las Universidades del Norte "Santo Tomás de Aquino", Nacional de Tucumán y Tecnológica Nacional-Facultad Regional Tucumán, por el Consejo Profesional de la Ingeniería, el Colegio de Graduados en Ciencias Económicas y la empresa proveedora de Internet Jet Net, todos de Tucumán.

Son abundantes las noticias del crecimiento del comercio concretado por medio de Internet, que se conoce como e-commerce o comercio electrónico por las características del medio de comunicación y el soporte de los actos jurídicos que implica.

Sin embargo, la contratación electrónica comprende un arco de posibilidades que van desde la inclusión de todos los contratos que se celebran por medios electrónicos o telemáticos hasta considerar tales al intercambio electrónico de datos de ordenador a ordenador, lo que ha llevado a la doctrina nacional a sostener que ha surgido una nueva categoría de contratos que no son ni literis ni verbis.

Pueden distinguirse claramente los celebrados a través de un sitio web de los que, por otros medios de comunicación dentro de la red, permiten negociar voluntariamente el acuerdo entre las partes.

Los primeros, instalados como estándar por las modalidades de comercio electrónico en Internet, contienen una oferta general e innominada, durante un tiempo. Le corresponde al interesado en aceptar la oferta introducirse en las condiciones predispuestas que se despliegan a continuación mediante sucesivas aceptaciones a pasos que conducen gradualmente a los términos y condiciones.

Como en esta modalidad no existe la posibilidad de realizar contraofertas las partes se vinculan a través de un contrato de adhesión, de la especie de contrato entre ausentes.

Existen otros tipos de contratos que culminan luego de una clásica etapa pre contractual de "regateo" de términos, por las que se concretan numerosas operaciones comerciales corrientes, tal como ocurre diariamente en el mundo en soporte papel nada más que por correo electrónico y según se domicilien las partes, se regirán por normas del derecho nacional o internacional privado.

En cuanto a lo que debe considerarse "escrito", documento en sentido jurídico y la firma en los contratos electrónicos, la ley 25.506 (Ver Anexo), regula toda la materia.

Como es obvio, cualquier cómputo de plazos que dé nacimiento, modifique o extinga el contrato mismo o relaciones jurídicas emergentes de su ejecución, requerirá de absoluta precisión en la determinación de la fecha (día y hora exactos).

En el mundo conectado mediante una red como Internet, coexisten distintas fechas por la misma razón que el planeta está dividido en husos horarios diferentes, por lo que el día calendario para una de las partes puede resultar posterior o anterior al de la otra, más esto puede resolverse mediante convenciones residentes en el mismo contrato.



Lo que no puede suceder es que la hora dentro del mismo día convenido, sea distinta, a menos que los relojes de los ordenadores intervinientes no estuvieran ajustados a un solo patrón horario o fueran deliberadamente manipulados.

La seguridad en la determinación exacta de la hora tiene la misma importancia que la de la fecha. Tanto en el mundo papel como en el on line, cuando se llega a un acuerdo, las partes procuran que sea ejecutable legalmente.

La "no repudiación" en la contratación electrónica consiste básicamente en la imposibilidad o inhabilidad de una parte para negar falsamente que ha enviado un particular documento o mensaje mediante el cual se ha alcanzado un acuerdo legal. Para ello debe ser autenticable ante un juez, jurado o un tercero juzgador, que la negativa de una contraparte respecto al quién, qué o cuándo del documento, es falsa.

Dentro de una estructura PKI como la que implementa la ley argentina, al solicitar un certificado para firmar digitalmente un correo electrónico, el certificador licenciado emitirá un Certificado Digital (art. 13 L 25.506) que pone en evidencia las dos primeras condiciones y tiene día y hora de fecha cierta del certificado, basando su vigencia en esa fecha (art. 15), más no acredita la fecha del documento.

Sin embargo, cuando se firma un correo, la hora que tendrá esa firma es la que tiene la máquina del remitente en el momento del envío, que puede ser distinto del momento en que lo escribió e indicó que lo firmaba.

Un Servicio de Sellado Digital de Fecha y Hora (SSDFH, "Digital Time-Stamping Service") o Autoridad de Certificación de Tiempo emite un sello fechador que asocia una fecha digital con un documento en un modo criptográficamente seguro. El sellado digital de fecha y hora se puede utilizar con posterioridad para probar que un documento electrónico existía en el momento que indican la fecha y hora digital.

Otra manera para agregar la fecha a un documento consiste en procesar el resumen del documento ("message digest") utilizando una función de "hash" de seguridad y enviar éste al servicio de registro digital de fecha y hora y recibe un registro digital de fecha y hora que consiste en el digesto del mensaje, la fecha y la hora en que fue recibido en el servicio de registro de fecha y hora, y la firma de ese servicio de registro digital de fecha y hora. Como el resumen del documento no revela la información que contiene el documento, el servicio de registro de fecha y hora no puede conocer el contenido de los documentos.

Más tarde, puede presentarse el documento y ese registro con la fecha y hora: un verificador procesará el resumen del documento y comprobará que concuerde con el resumen del documento sellado con la fecha y hora y así se verifica la firma del servicio de registro digital de fecha y hora.

En la etapa pre contractual puede suceder que dos partes han estado intercambiando correos electrónicos negociando los términos de un contrato extenso; como es corriente, se han resaltado en colores las modificaciones propuestas, tachando otras. Al final de las negociaciones se envían un borrador "definitivo" para que cada uno lo lea, aprobada la



cual una de las partes le envía firmada la versión definitiva para que la otra haga lo propio. La que lo recibe firmado asume que el contenido no ha sido modificado.

Consideremos la posibilidad que una de ellas ha introducido una leve pero sustancial modificación destinada a pasar desapercibida en un texto largo de cuya versión final corregida la otra confía de buena fe, por lo que no ha tomado la precaución de revisar línea por línea su contenido. La firma digital de la parte maliciosa no está destinada a avisar del cambio y la parte confiada que lo firma, lo advierte después durante la ejecución del contrato. En tal caso estará imposibilitado de demostrarlo.

Si la versión mutuamente aceptada antes de su firma digital hubiera estado sometida a un servicio de certificación de tiempo, el fraude hubiera podido ser detectado mediante comparaciones de hash ya que estos servicios aseguran la integridad del contenido del documento conjuntamente con la determinación de la fecha exacta.

Considérese un documento que debe ser firmado por varias personas. En algunos casos, esas firmas pueden tener sentido horizontal, es decir que no importa en qué secuencia se firme sino que estén todas las que tienen que estar. En otros, existen documentos que deben firmarse verticalmente o jerárquicamente, como una resolución donde debe firmar primero un secretario, luego el tesorero, una vez que estos dos firmaron recién firma el presidente. En estos, la Autoridad de Certificación puede emitir Sellos de Tiempo con cada firma para garantizar la secuencia pero no la fecha y hora en que se efectuaron las firmas, por no ser Autoridad de Time Stamping (ATS) reconocida.

Estos ejemplos revelan que es la combinación de una estructura PKI con la de una autoridad de sellado de contenido y tiempo la que mejor asegura la no repudiación de un contrato perfeccionado por medios electrónicos.

Para que sea confiable, el registro de fecha y hora tendrá que evitar ser falsificado.

Como requisitos, este tipo de servicio de registro deberá utilizar una clave de gran longitud si quiere que el sellado sea confiable por varias décadas. Segundo, la clave privada del servicio de registro debe ser conservada con máxima seguridad. Tercero, las fechas y horas deben provenir de un reloj también inviolable, que no puede ser reprogramado y que mantendrá la hora exacta durante muchos años. Cuarto, tiene que ser difícil crear sellos digitales de fecha y hora sin utilizar esa clave y reloj.

Este tipo de servicios de constatación de contenido y estampado electrónico de fecha y hora no ha sido regulado por la legislación argentina.

Revisando la ley 25.506, se encuentra solo en su art. 12, referido a la exigencia legal de conservar documentos, registros o datos, que "...también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permita determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción."



En el Decreto 2628/02 reglamentario de la ley también se encuentra solo una mención en el art. 16 que se refiere a los recursos del Ente Administrador: "El Ente Administrador podrá arancelar los servicios que preste para cubrir total o parcialmente sus costos. Los recursos propios del Ente Administrador se integrarán con: a) Los importes provenientes de los aranceles que se abonen por la provisión de los siguientes servicios: ... 2.- Servicios de certificación digital de fecha y hora,..."

Finalmente en el Anexo I (glosario): "...12.- Certificación digital de fecha y hora: Indicación de la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella.

Por Dec. 1792/83 el Observatorio Naval Bs. As. actualmente un organismo dependiente del Servicio de Hidrografía Naval tiene las misiones de conservar y difundir la Hora Oficial Argentina y el brindar apoyo a la navegación, la astronomía y la geodesia. El Servicio Público de la Hora Oficial se cumple mediante las emisiones de Hora y Frecuencias Patronas, los tops horarios emitidos por radiotelefonía y la hora telefónica que llega a los usuarios mediante el número 113.

La conservación de la hora está asegurada con los relojes atómicos del Observatorio Naval, cuya principal característica es la regularidad de su marcha, ya que el máximo error que se puede acumular es de un segundo en más de 3000 años con la precisión de un milésimo de segundo.

La determinación de la hora se realiza mediante la intercomparación de tiempo con la Oficina Internacional de la Hora, ya sea por comparación a distancia o en forma directa por transporte de reloj. En los últimos años se ha desarrollado la técnica de determinación de la hora mediante la transferencia de tiempo que provee la red satelital GPS (Global Positioning System), método que se implementó en el Observatorio Naval durante el corriente año.

Si se consulta su página web, proporciona el servicio de información de la hora oficial argentina pero sin perjuicio de la exactitud tecnológica de sus instrumentos de medición, la seguridad informática de dicha página y la imposibilidad de emitir certificados de tiempo como los que comentamos, no la habilitan para llenar el vacío legislativo en la materia.

Cuando se necesita de una fecha y hora cierta, es necesario que exista una autoridad de Time Stamping o un certificador de tiempo licenciado, lo que no ha sido contemplado hasta ahora en la República Argentina y puede obligar a los contratante nativos previsores a tener que recurrir a los servicios de un certificador extranjero.

Es por ello que se propone la creación de dicho servicio en forma exclusiva a cargo del Observatorio Naval Buenos Aires como organismo certificante licenciado, en cuyo caso no se requerirá que el que lo utiliza deba demostrar su validez, como ocurre con la firma digital, sino que la carga de dicha prueba correrá por cuenta de quien impugna sus datos.

Para el caso de las contrataciones internacionales, se admiten certificados de fecha emitidos por certificadores extranjeros, los que, salvo la suscripción de tratados



específicos, serán pasibles de imputación de falsedad con prueba a cargo del sospechado.

Sin más queda así fundamentado el presente proyecto, instando a su pronto tratamiento y aprobación.

ANEXO

Ley 25.506 sobre FIRMA DIGITAL

(Sancionada: Noviembre 14 de 2001, promulgada en Diciembre 11 de 2001.

CAPITULO I

Consideraciones generales

ARTICULO 1° - 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.

ARTICULO 2° - 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 3° - 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.

ARTICULO 4° - 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.

ARTICULO 5° - 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.

ARTICULO 6° - 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.

ARTICULO 7° - 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.

ARTICULO 8° - 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.

ARTICULO 9° - 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.



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:

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;

Ser susceptible de verificación respecto de su estado de revocación;

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

Contemplar la información necesaria para la verificación de la firma;

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, este reconocimiento 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 de emisión y de vencimiento si correspondiere, y de sus correspondientes solicitudes de emisión;
- e) Revocar los certificados digitales por él emitidos en los siguientes casos, entre otros que serán determinados por la reglamentación:
 - 1) A solicitud del titular del certificado digital.
 - 2) Si determinara que un certificado digital fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación.
 - 3) Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.



- 4) Por condiciones especiales definidas en su política de certificación.
- 5) Por resolución judicial o de la autoridad de aplicación.

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

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 de certificados digitales por él emitidos;

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

d) Operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la autoridad de aplicación;

e) Notificar al solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable, y 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 auditoría 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 procedimientos asociados. Esa información deberá darse por escrito en un lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;
- b) A que el certificador licenciado emplee los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por él, y a ser informado sobre ello;
- c) A ser informado, previamente a la emisión del certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago;



d) A que el certificador licenciado le informe sobre su domicilio en la República Argentina, y sobre los medios a los que 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.

(Nota Infoleg: Por art. 8° del Decreto N° 624/2003 B.O. 22/8/2003 se establece que la Comisión creada por el presente artículo actuará en la órbita de la SUBSECRETARIA DE LA GESTION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS.)

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 a las 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 y utilización de sus certificados y que no estén expresamente previstos en la ley;



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

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

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 8° 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 8° 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 como 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.