

LEY A N° 3997

Artículo 1º - La Provincia de Río Negro, interpretando el Artículo 50 de la Ley Nacional 25.506 #, adhiere a la misma en general invocando para ello lo previsto en el inciso 2º del artículo 12 de la Constitución Provincial #.

Artículo 2º - Se faculta al Señor Gobernador para que nombre a la autoridad de aplicación de la presente Ley.

Artículo 3º - El Poder Ejecutivo deberá dictar la respectiva reglamentación.

Artículo 4º - Las disposiciones de la presente Ley serán de aplicación en toda la jurisdicción del sector público provincial, el cual comprende la administración centralizada y descentralizada, los organismos de la Constitución, los entes autárquicos y todo otro ente en que el Estado provincial o sus organismos descentralizados tengan participación suficiente para la formación de sus decisiones.

Artículo 5º - Se crea en el ámbito de la Provincia de Río Negro la Comisión Asesora Multidisciplinaria para: la puesta en marcha y seguimiento de la aplicación de la presente Ley.

Artículo 6º - La Comisión Asesora estará integrada por ocho (8) miembros de los cuales dos (2) serán legisladores, dos (2) representantes del Poder Ejecutivo (uno (1) designado por la Subsecretaría de Ciencia y Tecnología), dos (2) del Poder Judicial y dos (2) serán expertos en informática, especialmente en claves públicas y privadas y sistemas de encriptación asimétrica, designados por el Poder Ejecutivo y que no tendrán ningún tipo de vínculo con el gobierno. Todos los integrantes de esta Comisión se ajustarán a lo siguiente:

- a) La Comisión Asesora tendrá ese carácter y deliberará y se pronunciará reportando a la autoridad de aplicación.
- b) La Comisión Asesora se dictará su propio reglamento de responsabilidades y funciones, el que no se podrá apartar de lo que la reglamentación de la Ley dicte como así también las instrucciones de la autoridad de aplicación.
- c) A solicitud de simple mayoría de sus miembros podrá pedir a la autoridad de aplicación incrementar el número de integrantes o conseguir el auxilio de profesionales que, a juicio de la Comisión, sea necesario para dilucidar cuestiones de su competencia.
- d) Las designaciones y remociones deberán ser todas aprobadas por la Legislatura de la Provincia de Río Negro, incluyendo a los representantes de ese cuerpo gubernamental.
- e) La duración en sus funciones será de dos (2) años y podrán continuar en sus cargos mientras la autoridad de aplicación así lo estime conveniente.
- f) Todos los cargos en la Comisión Asesora serán ad honorem y los reemplazos que se estimen realizar se ajustarán a las directivas de la autoridad de aplicación y al reglamento que la Comisión se dicte.

- g) Se exceptúa de lo prescripto en el inciso anterior a los expertos en informática. Será facultad de la autoridad de aplicación la modalidad de contratación de los mismos.
- h) La Comisión Asesora, a iniciativa propia o de terceros, propondrá a la autoridad de aplicación normas en el plano jurídico, en el de la puesta en marcha en el ámbito de la administración pública, en el de las contrataciones por parte del gobierno, en el de los sistemas de interacción entre reparticiones nacionales y de la provincia, en la estandarización y la adecuación a cambios fruto de la experiencia y en la implementación en la órbita de las actividades de los particulares.
- i) La Comisión trabajará en forma permanente y de acuerdo a su reglamento, no obstante la misma tendrá la obligación de producir informes periódicos a la autoridad de aplicación, siendo también responsabilidad de su área la difusión de sus acciones ante quien lo reclame.

Artículo 7º - Se autoriza a emplear la firma digital o en su defecto la firma electrónica en los actos internos de la administración pública provincial y en aquellos actos que excediendo la órbita interna se celebren con instituciones, organismos o cualquier otro tipo de institución con los que exista convenio de reciprocidad o que ya tengan sancionada una norma legal de adhesión a la Ley Nacional 25.506 #. También se registrá por este artículo el intercambio de información institucional.

Artículo 8º - Una vez puesta en marcha la presente Ley, la administración pública en general y la autoridad de aplicación en particular, llevarán adelante toda clase de medidas que propugnen la aplicación de la firma digital orientándose a la despapelización.

Artículo 9º - Reivindicando la autonomía federal, la Provincia de Río Negro se reserva el derecho de aplicar cualquier tipo de gravamen que estime conveniente del empleo de la firma digital en tanto no se oponga a lo establecido por el Gobierno Nacional, pudiendo ser éste de origen temporal (vigencia del certificado digital) o permanente, (impuesto a las transacciones digitales).

Artículo 10 - A los efectos de la aplicación de esta Ley, el gobierno reconocerá como certificador licenciado a aquéllos que contando con la aprobación nacional (Artículo 17 del capítulo III de la Ley Nacional 25.506 #) se avengan a encuadrarse en la presente Ley.

Artículo 11 - La radicación de certificadores licenciados que se desempeñen fuera de la órbita de la administración pública lo harán en términos de libre competencia, reservándose el Gobierno provincial la delimitación de cupos, áreas geográficas o cualquier otro tipo de segmentación que aseguren que los eventuales usuarios estarán debidamente protegidos por la legislación en materia de defensa del consumidor.

Artículo 12 - La autoridad de aplicación, con el concurso de la Comisión Asesora para la puesta en marcha y seguimiento de la firma digital, sin perjuicio de lo establecido en la Ley Nacional 25.506 #, establecerá un sistema de registro, métodos y mecanismos para la evaluación y constatación de la confiabilidad,

integridad, confidencialidad y disponibilidad de los esquemas utilizados por los registrados para la realización de identificaciones fehacientes dentro del marco de la infraestructura de firma digital.

Artículo 13 - Atento a lo establecido en el artículo anterior, la Provincia de Río Negro, a través de la autoridad de aplicación se reserva el derecho de adoptar todo cambio tecnológico que no oponiéndose a la Ley Nacional ni a los estándares internacionales, tienda a optimizar, adecuar y ampliar el uso de la firma digital.

Artículo 14 - La autoridad de aplicación, sin perjuicio de lo que indiquen las Leyes tanto penales como civiles, establecerá un sistema de multas y sanciones para quienes incumplan con los métodos y mecanismos dispuestos por la autoridad de aplicación.

En este sentido, la autoridad de aplicación se subrogará el derecho de informar a la autoridad de aplicación nacional el resultado de los controles realizados.

Artículo 15. - Dado que la aplicación de la presente Ley tiene directas implicancias sobre la identificación de las personas, la autoridad de aplicación constatará el cumplimiento de la Ley Nacional 25.326 # (Protección de Datos Personales) ya que la misma se encuadra en lo prescripto por el artículo 20 de la Constitución de la Provincia #. Por ello, será su obligación la de informar a la Dirección Nacional de Protección de Datos Personales, los incumplimientos constatados que pudieran derivar en perjuicios de índole particular.

Artículo 16 - Atento a que la puesta en vigencia de la presente Ley se inscribe en los términos: de adoptar nuevas tecnologías y modernizar los actos de gobierno, éstos deberán encuadrarse en lo previsto en el artículo 35 de la Constitución de la Provincia # (Derechos de la Tercera Edad) y el artículo 36 # (Discapacitados Excepcionales), es decir, será nula toda normativa, resolución o disposición emergente de esta Ley que genere algún tipo de discriminación que afecte tanto a personas de la tercera edad o a aquellas que puedan padecer algún tipo de discapacidad, debiendo la autoridad de aplicación tomar los recaudos pertinentes.

ANEXO A

LEY NACIONAL N° 25506

CAPITULO I

Consideraciones generales

Artículo 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.

Artículo 3° - Del requerimiento de la 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 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.

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 9° - 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.

Artículo 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.

Artículo 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.

Artículo 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

Artículo 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.

Artículo 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 indubitavelmente 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.

Artículo 15 - Período de vigencia el 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.

Artículo 16 - Reconocimiento de los 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

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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

Artículo 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.

Artículo 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

Artículo 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.

Artículo 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.

Artículo 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

Artículo 29 - Autoridad de aplicación. La autoridad de aplicación de la presente Ley será la Jefatura de Gabinete de Ministros.

Artículo 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.

Artículo 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.

Artículo 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

Artículo 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.

Artículo 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

Artículo 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.

Artículo 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

Artículo 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.

Artículo 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.

Artículo 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

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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

Artículo 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.

Artículo 48.- Implementación. El Estado nacional, dentro de las jurisdicciones y entidades comprendidas en el artículo 8° de la Ley Nacional N° 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 Nacional N° 24.156.

Artículo 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.

Artículo 50 - Invitación. Invítase a las jurisdicciones provinciales a dictar los instrumentos legales pertinentes para adherir a la presente Ley.

Artículo 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.

Artículo 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.

Artículo 53 - Comuníquese al Poder Ejecutivo.

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.