

# SESIONES ORDINARIAS

## 2001

# ORDEN DEL DIA N° 2651

### COMISION DE COMUNICACIONES E INFORMATICA Y DE LEGISLACION GENERAL

Impreso el día 3 de agosto de 2001

Término del artículo 113: 14 de agosto de 2001

**SUMARIO: Régimen** de habilitación y regulación del uso de la firma digital. **Fontdevila y otros.** (3.534-D.-2000.)

#### Dictamen de las comisiones

*Honorable Cámara:*

Las comisiones de Comunicaciones e Informática y de Legislación General han considerado el proyecto de ley del señor diputado Fontdevila y otros señores diputados, y han tenido a la vista el proyecto de ley del señor diputado Corchuelo Blasco y otros señores diputados (4.175-D.-00), el proyecto de ley de la señora diputada Puiggrós (5.460-D.-00), el proyecto de ley del señor diputado Cardesa y otros señores diputados (7.099-D.-00) y el proyecto de ley del señor diputado Atanasof y de la señora diputada Camaño (G.) (7.331-D.-00), por los que se establece el régimen de habilitación y regulación del empleo de la firma digital; y, por las razones expuestas en el informe que se acompaña y las que dará el miembro informante, aconsejan la sanción del siguiente

#### PROYECTO DE LEY

*El Senado y Cámara de Diputados,...*

#### LEY DE FIRMA DIGITAL

##### CAPÍTULO I

##### *Consideraciones generales*

Artículo 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.

Art. 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.

Art. 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.

Art. 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.

Art. 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.

Art. 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.

Art. 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.

Art. 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.

Art. 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.

Art. 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.

Art. 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.

Art. 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.

## CAPÍTULO II

### *De los certificados digitales*

Art. 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.

Art. 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.

Art. 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.

Art. 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 establecen 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.

## CAPÍTULO III

*Del certificador licenciado*

Art. 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.

Art. 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.

Art. 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.

Art. 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.

Art. 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.
- Art. 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.
- Art. 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.
- ## CAPÍTULO IV
- ### *Del titular de un certificado digital*
- Art. 24. – *Derechos del titular de un certificado digital.* El titular de un certificado digital tiene los siguientes derechos:
- a) A ser informado por el certificador licenciado, con carácter previo a la emisión del certificado digital, y utilizando un medio de comunicación, sobre las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de este sistema de licenciamiento y los procedimientos asociados. Esa información deberá darse por escrito en un lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;
  - b) A que el certificador licenciado emplee los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por él, y a ser informado sobre ello;

- c) A ser informado, previamente a la emisión del certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago;
- d) A que el certificador licenciado le informe sobre su domicilio en la República Argentina y sobre los medios a los que 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.

Art. 25. – *Obligaciones del titular del certificado digital.* Son obligaciones del titular de un certificado digital:

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

## CAPÍTULO V

### *De la organización institucional*

Art. 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.

Art. 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.

Art. 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.

## CAPÍTULO VI

### *De la autoridad de aplicación*

Art. 29. – *Autoridad de aplicación.* La autoridad de aplicación de la presente ley será la Jefatura de Gabinete de Ministros.

Art. 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.

Art. 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;

Art. 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.

## CAPÍTULO VII

### *Del sistema de auditoría*

Art. 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.

Art. 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.

## CAPÍTULO VIII

### *De la Comisión Asesora para la Infraestructura de Firma Digital*

Art. 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.

Art. 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.

## CAPÍTULO IX

### *Responsabilidad*

Art. 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.

Art. 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.

Art. 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 de-

mostrar que ha tomado todas las medidas razonables.

## CAPÍTULO X

### *Sanciones*

Art. 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.

Art. 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 llevará 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.

Art. 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.

Art. 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;

Art. 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.

Art. 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.

Art. 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.

## CAPÍTULO XI

### *Disposiciones complementarias*

Art. 47. – *Utilización por el Estado nacional.* El Estado nacional utilizará las tecnologías y provisiones 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.

Art. 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.

Art. 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.

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

Art. 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.

Art. 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.

Art. 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:* Calidad del conjunto de equipos de computación, software, protocolos de comunicación y de seguridad y procedimientos administrativos relacionados que cumpla 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.

Sala de las comisiones, 24 de julio de 2001.

Pedro J. Calvo. – José G. Dumón. – María S. Mayans. – Arturo R. Etchevehere. – Enrique G. Cardesa. – Pablo A. Fontdevila. – María del Carmen Falbo. – Miguel A. Giubergia. – Miguel A. Abella. – Manuel J. Baladrón. – Alejandro Balian. – Osvaldo M. Borrelli. – Adalberto L. Brandoni. – Carlos A. Castellani. – Carlos Caballero Martín. – Guillermo E. Corfield. – Graciela M. Giannettasio. – Simón F. G. Hernández. – Miguel A. Insfran. – Guillermo R. Jenefes. – Roberto I. Lix Klett. – Antonio A. Lorenzo. – Fernando R. Montoya. – Norberto R. Nicotra. – Alejandra B. Oviedo. – Irma F. Parentella. – Héctor T. Polino. – Ricardo C. Quintela. – Fernando O. Salim. – Margarita R. Stolbizer. – Atilio P. Tazzioli. – Julio A. Tejerina. – Luis A. Trejo. – Juan M. Urtubey. – Alfredo Villalba.



## INFORME

*Honorable Cámara:*

Las comisiones de Comunicaciones e Informática y de Legislación General han considerado el proyecto de ley del señor diputado Fontdevila y otros señores diputados, y teniendo a la vista los proyectos de ley de la señora diputada Puiggrós, del señor diputado Cardesa y otros señores diputados, del señor diputado Corchuelo Blasco y otros señores diputados, del señor diputado Atanasof y la señora diputada Camaño, por el que se habilita y regula el empleo de la firma digital. Al término, de su análisis, concluyeron que el avance hacia una progresiva digitalización, como consecuencia del desarrollo y convergencia de la computación y las telecomunicaciones, es un fenómeno mundial incontestable e insoslayable.

En este marco es indiscutible que las nuevas tecnologías de la información se presentan como una oportunidad para que los países menos desarrollados puedan achicar la brecha que los separa con los denominados países del primer mundo, teniendo la clase dirigente la responsabilidad de hacer uso de ella.

Por otra parte, este proceso de digitalización y la existencias de redes abiertas –tal como Internet– exigen poder identificar en forma fehaciente a las personas de modo tal de permitirles realizar todo tipo de transacciones: comercio electrónico, gestiones ante distintos organismos del Estado, trabajar en forma remota y hasta ejercer el derecho democrático de votar.

Es indudable que el Estado tiene un rol de liderazgo que cumplir en la incorporación de la cultura digital en la sociedad argentina.

Algunos esfuerzos aislados se realizaron, pero, indudablemente son insuficientes.

Las experiencias en la Argentina del uso de firma digital por parte de organismos públicos y privados que se pueden citar son: el sistema interbancario y bancos diversos, la Caja de Valores, la Comisión Nacional de Valores, empresas de telefonía, PAMI, ANMAT, etcétera.

La única legislación vigente es el decreto 427/98, que esencialmente equipara los efectos de la firma digital con la firma ológrafa en el ámbito de la Administración Pública Nacional. También, se pueden citar, como antecedentes, la resolución MTSS 555/97 del Ministerio de Trabajo y Seguridad Social que determina los procedimientos para la incorporación de documentos digitales y la firma digital; la resolución 45/97, 212/97 y 194/98 de la Secretaría de la Función Pública que reglamentó la incorporación de la tecnología de la firma digital, estándares e infraestructura de la misma, en la Administración Pública Nacional, y la resolución SAFJP 293/97 de la Superintendencia de Administradoras de Fondos de Jubilaciones y Pensiones, sobre incorporación del correo electrónico con firma digital.

Por último, se puede citar el decreto 677/2001, que establece el régimen de transparencia de la oferta pública, que acepta la posibilidad de celebrar reuniones de directorio y asambleas a través de medios no presenciales y modifica la ley 24.083 estableciendo una serie de pautas referidas a la designación de la Comisión Nacional de Valores como autoridad de aplicación del decreto, otorgando a ese organismo expresas facultades para establecer regímenes de información y requisitos diferenciales, previendo el sistema de la firma digital.

La Comisión de Comunicaciones e Informática constituyó en su seno una subcomisión especial de firma digital, integrada con asesores de los señores diputados de la comisión, asesores de diputados autores de los proyectos tenidos a la vista, así como por el asesor del senador de la Nación, don Pedro del Piero, autor de un proyecto presentado en esa Honorable Cámara, y representantes del Poder Ejecutivo nacional.

El 20 de septiembre de 2000, se llevó a cabo una audiencia pública a fin de recabar las opiniones y las experiencias de los diversos ámbitos en los que se utiliza este sistema. Los diputados de la Comisión de Comunicaciones e Informática recibieron las ponencias presentadas por: el licenciado Leandro Popik, de la Subsecretaría de la Gestión Pública; el licenciado Andrés Hall, de la Comisión Nacional de Valores; el doctor Mauricio Devoto, del Consejo Federal del Notariado Argentino; el doctor Guillermo Cosentino, del Superior Tribunal de la Provincia de Chubut; el licenciado Francisco Díaz, decano de la Facultad de Informática de la Universidad de La Plata; el ingeniero Pablo Viale, del Copitec; la doctora Beatriz García, del Banco Central de la República Argentina; el doctor Hugo Scolnik, profesor titular del Departamento de Computación de la UBA e integrante del Centro de Investigaciones en Información y Tecnología; el licenciado Ricardo Riva, de la Administración Nacional de Medicamentos, Alimentos y Tecnología Médica; y el doctor Eduardo Molinero, de la Cámara Argentina de Comercio Electrónico.

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

Las recomendaciones de Uncitral prevé en su artículo 7° (Firma) que cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos cuando:

a) Se utilice un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y

b) Ese método sea tan fiable y apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente. Estos requisitos están contemplados en el dictamen en los artículos 2° y 3°.

El dictamen de firma digital intenta legislar para el presente y para el futuro, evitando el condicionamiento a la tecnología que se utiliza hoy en día pues ello obligaría a modificarla, quizás, a breve plazo, atento que la rama de la ciencia que estudia estos temas es la criptografía y, contra lo que habitualmente se supone, existe un marco teórico muy desarrollado con respecto a los esquemas de firma digital no relacionados a un caso particular, como es el de la tecnología actualmente vigente.

El proyecto que sometemos a vuestra consideración establece una organización institucional que prevé la existencia de una autoridad de aplicación en sede de la Jefatura de Gabinete de Ministros, una comisión asesora integrada por representantes provenientes de organismos del Estado nacional, universidades nacionales, colegios profesionales; y la existencia de certificadores licenciados que expedirán los certificados y prestarán otros servicios en relación con la firma digital.

Se prevé, además, que la actividad de los certificadores licenciados no pertenecientes al sector público, presten el servicio en régimen de competencia.

A fin de facilitar el comercio electrónico internacional, se reconoce la validez de certificados digitales emitidos por certificadores extranjeros cuando los mismos reúnan las condiciones que establece esta ley y se encuentre vigente un convenio de reciprocidad firmado por la República Argentina y el país de origen del certificador extranjero, o los certificados sean reconocidos por un certificador licenciado en el país que garantice su validez y vigencia.

A fin de promover la masificación del uso de esta herramienta e impulsar la despapelización creciente del sector público nacional, el artículo 48 establece un plazo máximo de 5 años para que se aplique la tecnología de firma digital a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanadas de las respectivas jurisdicciones.

Todos estas consideraciones son fundamentos más que suficientes para producir un dictamen favorable y aconsejar su sanción.

*Pablo A. Fontdevila.*

## ANTECEDENTE

### PROYECTO DE LEY

*El Senado y Cámara de Diputados, ...*

## LEY DE FIRMA DIGITAL

### CAPÍTULO I

#### *Definiciones – Objeto*

Artículo 1° – *Utilización de términos.* A los efectos de esta ley se entiende por:

11.1 *UIT:* Unión Internacional de Telecomunicaciones, organismo especializado de las Naciones Unidas para las telecomunicaciones.

11.2 *ISO:* Organización Internacional de Estándares.

11.3 *ANSI:* Instituto Americano de Estándares Nacionales.

11.4 *Uncitral:* Comisión de las Naciones Unidas para el Derecho Mercantil Internacional.

11.5 *Documento digital:* La información (mensaje, registro o archivo informático), representada mediante dígitos o números, sin hacer referencia a su medio de almacenamiento o soporte, susceptible de ser firmada digitalmente.

11.6 *Firma digital:* La firma digital es el resultado de la transformación de un documento digital, por medio de un sistema informático, que cumple con los siguientes requisitos:

- a) Ser exclusiva del signatario;
- b) Ser susceptible de verificación;
- c) Estar bajo resguardo y control absoluto del signatario;
- d) Que el documento digital esté encriptado con la clave privada del signatario, de manera tal, que si el mensaje sufre alguna modificación, la firma quede invalidada;
- e) Que la persona que posea el documento digital inicial, el digesto encriptado y la clave pública del signatario, pueda determinar con certeza que la transformación fue realizada utilizando la clave privada correspondiente a dicha clave pública y que el documento digital no ha sido modificado desde que se efectuó;
- f) Que haya sido adoptado como norma por no menos de dos de las siguientes organizaciones:

I. La UIT.

II. La ANSI.

III. La ISO.

IV. La Uncitral;

- g) Que la transformación del mensaje se haya realizado empleando un criptosistema asimétrico.
- 11.7 *Criptografía*: Rama de las matemáticas aplicadas que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlos a su forma original.
- 11.8 *Criptosistema asimétrico*: Algoritmo o serie de algoritmos que brindan un par de claves seguras. Utiliza un par de claves compuesto por una clave privada utilizada para firmar digitalmente y su correspondiente clave pública utilizada para verificar esa firma digital, de forma tal que, con las longitudes de claves utilizadas, sea computacionalmente factible tanto obtener o inferir la clave privada a partir de la correspondiente clave pública como descryptar aquello que ha sido encriptado con una clave privada sin la utilización de la correspondiente clave pública.
- 11.9 *Par de claves*: Clave privada y su correspondiente clave pública en un criptosistema asimétrico seguro.
- 11.10 *Clave privada*: Clave que se utiliza para firmar digitalmente, mediante un dispositivo de creación de firma digital, en un criptosistema asimétrico seguro. Es una familia de métodos matemáticos, algoritmos, que admite distintas implementaciones tanto en hardware cuanto en software.
- 11.11 *Clave pública*: Clave que se utiliza para verificar una firma digital, en un criptosistema asimétrico seguro. Es una familia de métodos matemáticos, algoritmos, que admite distintas implementaciones tanto en hardware cuanto en software.
- 11.12 *Certificado de clave pública*: Documento digital firmado digitalmente por una autoridad certificante, que asocia una clave pública con su titular durante el período de vigencia del certificado.
- 11.13 *Condiciones de emisión y utilización de los certificados*: Documento que emite la autoridad certificante que contiene los términos de emisión de sus certificados.
- 11.14 *Sellado digital de fecha y hora*: Constancia, firmada digitalmente, de fecha, hora, minutos y segundos, como mínimo, que la autoridad certificante adiciona a un documento digital o a su digesto de mensaje.
- 11.15 *Dispositivo de creación de firma*: Conjunto de hardware o software, técnicamente confiable, que permite que los datos utilizados para la generación de la firma digital no sean deducidos o derivados de la propia firma, puedan producirse sólo una vez y que asegure, razonablemente, su secreto.
- 11.16 *Dispositivo de verificación de firma digital*: Dispositivo de hardware o software técnicamente confiable que verifica una firma digital utilizando la clave pública del firmante.
- 11.17 *SopORTE*: Medio en el cual se almacena la información de un documento digital, tal como memoria electrónica, disco magnético, magneto-óptico u óptico, cinta magnética, tarjeta inteligente, microchip.
- 11.18 *Ente Licenciante*: Organismo que otorga las licencias a las autoridades certificadoras.
- 11.19 *Autoridad Certificante*: Tercero confiable que firma el certificado de clave pública y pone en conocimiento público los certificados.
- 11.20 *Signatario*: Persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa.
- 11.21 *Computacionalmente no factible*: Cualidad de aquellos cálculos matemáticos asistidos por computadora que para ser llevados a cabo requieren de tiempo y recursos informáticos que superan ampliamente a los disponibles al momento de efectuar aquellos cálculos.
- 11.22 *Técnicamente confiable*: Cualidad del conjunto de equipos de computación, software, protocolos de comunicación y de seguridad y procedimientos administrativos relacionados, en tanto reúna los siguientes requisitos:
- a) Ser confiable para resguardar contra la posibilidad de intrusión o de uso no autorizado;
  - b) Brindar disponibilidad, confiabilidad, confidencialidad y correcto funcionamiento;
  - c) Ser apto para el desempeño de sus funciones específicas;
  - d) Cumplir con requisitos de seguridad apropiados, acordes a estándares internacionales en la materia;
  - e) Cumplir con los estándares tecnológicos que al efecto dicte la autoridad de aplicación.
- Art. 2º – *Objeto*. La presente ley habilita y regula el empleo de la firma digital, el reconocimiento de su eficacia jurídica dentro del principio de la libertad de las formas, y la prestación del servicio público de certificación.

## CAPÍTULO II

### Organización institucional

Art. 3º – *Infraestructura de firma digital*. Los certificados de clave pública deben ser emitidos por una autoridad certificante adjudicataria de una licencia otorgada por el ente licenciante.

Art. 4° – *Ente licenciante*. En el ámbito jurisdiccional de la autoridad de aplicación se constituirá el ente licenciante que entenderá en la adjudicación de licencias, vigilancia y control de las autoridades certificadoras. El ente licenciante estará dirigido por 3 (tres) directores designados por el Poder Ejecutivo nacional, a propuesta de la autoridad de aplicación. Los directores deberán tener título universitario y acreditar amplia experiencia en el campo de la informática.

Art. 5° – *Sistema de auditoria*. La autoridad de aplicación, con el concurso de la Comisión Asesora para la Infraestructura de la Firma Digital, diseñará un sistema de auditoria para evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, así como también el cumplimiento con las especificaciones del manual de procedimientos y los planes de seguridad y de contingencia aprobados por el ente licenciante.

Art. 6° – *Comisión Asesora para la Infraestructura de la Firma Digital*. Créase en el ámbito jurisdiccional de la autoridad de aplicación, la Comisión Asesora para la Infraestructura de la Firma Digital.

### CAPÍTULO III

#### *Certificado de clave pública*

Art. 7° – *Contenido*. El certificado de clave pública debe responder a formatos estándares reconocidos internacionalmente y contener, como mínimo, los siguientes datos:

- 7.1 Datos que identifiquen indubitadamente al suscriptor.
- 7.2 Clave pública del titular con identificación del algoritmo utilizado, y la metodología para verificar la firma digital del suscriptor impresa a un mensaje de datos.
- 7.3 Número de serie del certificado.
- 7.4 Período de vigencia del certificado (con aclaración de la fecha y hora del comienzo y fin de la validez).
- 7.5 La dirección de Internet donde se publique:
  - a) Las condiciones de emisión y utilización del certificado;
  - b) La lista de certificados revocados que mantiene la autoridad certificante que lo emitió;
  - c) Los informes de auditoria de la autoridad certificante, producidos por la Auditoría de Firma Digital.
- 7.6 Datos que identifiquen indubitadamente a la autoridad certificante emisora del certificado.
- 7.7 Firma digital de la autoridad certificante que emite el certificado, identificando los algoritmos utilizados.

7.8 Información acerca de la limitación de uso del certificado a determinados tipos y ámbitos de aplicación.

7.9 Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

Art. 8° – *Validez*. El certificado de clave pública es válido únicamente si está dentro del período de vigencia del respectivo certificado de clave pública. La fecha de vencimiento del certificado de clave pública en ningún caso puede ser posterior a la del vencimiento del certificado de clave pública de la autoridad certificante que lo emitió. Sin embargo, la fecha de expiración de un certificado en ningún caso podrá ser superior a 2 (dos) años, contados desde la fecha en que se haya expedido. Los certificados perderán validez, además, bajo alguna de las siguientes circunstancias:

- a) Revocación por cualquiera de las causales invocadas en el inciso b) del artículo 9° de la presente ley;
- b) Orden judicial emanada de juez competente;
- c) Fallecimiento del signatario o de su representante, incapacidad declarada, total o parcial, de cualquiera de ellos, disolución de la persona jurídica representada.

### CAPÍTULO IV

#### *Autoridad certificante*

Art. 9° – *Funciones*. Los servicios de habilitación del uso de la firma digital y emisión del certificado de clave pública serán prestados por personas físicas o jurídicas titulares de licencias, adjudicadas de acuerdo con las condiciones y los procedimientos establecidos por esta ley. Las licencias son intransferibles. La adjudicataria de la licencia o autoridad certificante, tiene las siguientes funciones:

- a) Emitir certificados de clave pública de acuerdo a la reglamentación;
- b) Revocar los certificados de clave pública que hubiera emitido con ajuste a las causas previstas en la reglamentación.

Art. 10. – *Obligaciones*. La autoridad certificante debe cumplir con las siguientes obligaciones:

- a) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a la clave privada de los titulares de certificados emitidos;
- b) Mantener el control exclusivo de su propia clave privada e impedir su divulgación;
- c) Operar utilizando un sistema técnicamente confiable;
- d) Identificar fehacientemente, según la normativa legal vigente, al suscriptor de firma digital;

- e) Recabar únicamente aquellos datos personales del titular del certificado que sean necesarios para su emisión de acuerdo a la reglamentación. Mantener la confidencialidad de toda información que no figure en el certificado;
- f) Diseñar un sistema de numeración correlativo de los certificados emitidos, que permita determinar biunívocamente la correlación entre el número del certificado y el titular del mismo;
- g) Mantener copia de todos los certificados emitidos, consignando la fecha de emisión y de la documentación exigida por la reglamentación;
- h) Mantener la documentación respaldatoria de los certificados emitidos por diez (10) años a partir de su fecha de vencimiento o revocación;
- i) Mantener el acceso al registro de certificados, válidos y revocados, en todo momento y para cualquier persona, a través de conexiones de telecomunicaciones accesibles públicamente de una manera verificable, y publicar estos listados en Internet en forma permanente e ininterrumpida;
- j) Solicitar sin demora al ente licenciante la revocación de su propio certificado, cuando tuviera sospechas fundadas de que la privacidad de su clave privada hubiese sido comprometida, o cuando el criptosistema asimétrico de la clave pública en él contenida haya dejado de ser seguro;
- k) Permitir el ingreso de los funcionarios autorizados por ente licenciante o de los auditores habilitados a su local operativo. Poner a su disposición toda la información necesaria y proveer la asistencia del caso;
- l) 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;
- m) Disponer de recursos económicos suficientes para operar de conformidad con lo dispuesto en la presente ley, en particular, para afrontar el riesgo de responsabilidad por daños.

Art. 11. – *Limitaciones de responsabilidad.* Las autoridades certificantes 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, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;
- c) Por los daños y perjuicios que excedan el valor límite por transacción, o por el total de transacciones, si tales valores límites constan en las correspondientes condiciones de emisión y utilización de sus certificados;
- d) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en su manual de procedimientos, deba ser objeto de verificación, siempre que la autoridad certificante pueda demostrar que ha tomado todas las medidas razonables para verificar tal información, de acuerdo con las circunstancias y el tipo de certificado que se trate.

Art. 12. – *Requisitos para obtener la licencia.* La licencia de autoridad certificante será otorgada a solicitud del interesado. Para obtener una licencia de autoridad certificante se debe cumplir con los siguientes requisitos:

- a) Ser persona física o jurídica regularmente constituida en el país;
- b) Tanto la persona física, como los integrantes de las personas jurídicas, no podrán estar incapacitados o inhabilitados civil ni penalmente para contratar o ejercer el comercio, ni haber sido condenados o estar sometidos a proceso por delito doloso, ni ser deudores morosos de obligaciones fiscales o previsionales;
- c) Tener capacidad patrimonial acorde con la inversión a realizar y el compromiso a asumir y poder demostrar el origen de los fondos;
- d) Cumplir con las exigencias técnicas de la reglamentación;

La certificación de firma digital es un servicio público oneroso prestado en régimen de competencia. Excepcional y subsidiariamente algún organismo del Estado podrá obtener una licencia de autoridad certificante para prestar dicho servicio a sus propios agentes o a terceros que, bajo circunstancias determinadas, lo soliciten.

Art. 13. – *Cese de actividades.* La autoridad certificante cesa en tal calidad:

- a) Por decisión unilateral comunicada al ente licenciante;
- b) Por revocación de su personería jurídica o por cualquier otra causal legal de disolución;
- e) Por revocación de su licencia dispuesta por el ente licenciante.

Los certificados emitidos por una autoridad certificante que cesa en sus actividades deben ser revocados a partir del día y la hora en que cesa su actividad. La autoridad certificante debe notificar al ente licenciante y hacer saber, mediante publicación en el Boletín Oficial de la Nación por 3 (tres) días consecutivos, y en la dirección de Internet donde publica el registro de certificados, la fecha y hora de cese de sus actividades, la que no puede ser anterior a los 90 (noventa) días corridos contados desde la fecha de la última publicación.

## CAPÍTULO V

### *Titular de un certificado de clave pública*

Art. 14. – *Requisitos.* El titular de un certificado de clave pública debe ser persona de existencia visible, excepto en los casos de autoridades certificantes o del ente licenciante.

Art. 15. – *Obligaciones.* El titular de un certificado de clave pública debe:

- a) Mantener el control exclusivo de su clave privada, no compartirla, e impedir su divulgación;
- b) Utilizar un dispositivo de creación de firma digital técnicamente confiable;
- c) Informar sin demora a la autoridad certificante sobre cualquier circunstancia que pueda haber comprometido la privacidad de su clave privada;
- d) Informar sin demora a la autoridad certificante el cambio de alguno de los datos contenidos en el certificado que hubiera sido objeto de verificación.

## CAPÍTULO VI

### *Ente licenciante*

Art. 16. – *Objeto y adjudicación.* El ente licenciante es el órgano técnico administrativo encargado de otorgar las licencias a las autoridades certificantes y de supervisar su actividad, según las exigencias instituidas por la reglamentación.

Art. 17. – *Funciones.* El ente licenciante tiene las siguientes funciones:

- a) Otorgar las licencias habilitantes a las autoridades certificantes y emitir los correspondientes certificados de clave pública, que permiten verificar las firmas digitales de los certificados que éstos emitan;
- b) Revocar las licencias otorgadas a las autoridades certificantes que dejan de cumplir con los requisitos establecidos para su autorización;
- c) Homologar dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la reglamentación;

- d) Fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de las autoridades certificantes;
- e) Verificar que las autoridades certificantes utilicen sistemas técnicamente confiables;
- f) Acordar con la Auditoría de Firma Digital el plan de auditoría para las autoridades certificantes;
- g) Efectuar las tareas de control del cumplimiento de las recomendaciones formuladas en los dictámenes de auditoría de las autoridades certificantes, para determinar, en su caso, si el auditado ha tomado las acciones correctivas.

Art. 18. – *Obligaciones.* En su calidad de titular del certificado emitido y de autoridad certificante, el ente licenciante tiene las mismas obligaciones que los titulares de certificados y las autoridades certificantes. Además debe:

- a) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a la clave privada de cualquier autoridades certificantes;
- b) Mantener el control exclusivo de su propia clave privada e impedir su divulgación;
- c) Revocar su propio certificado de clave pública frente al compromiso de la privacidad de su clave privada, o si el criptosistema asimétrico de la clave pública en el contenido deja de ser seguro, o si la función de digesto seguro utilizada para crear la firma digital del certificado deja de ser segura;
- d) Publicar en Internet en forma permanente e ininterrumpida los domicilios, números telefónicos y direcciones de Internet tanto de las autoridades certificantes como los propios y su certificado de clave pública;
- e) Supervisar la ejecución del plan de cese de actividades de las autoridades certificantes que discontinúan sus funciones;
- f) Abstenerse de emitir certificados de clave pública a personas que no sean autoridades certificantes.

Art. 19. – *Arancelamiento.* El ente licenciante cobrará un arancel de licenciamiento para cubrir su costo operativo y de las auditorías realizadas por sí o por terceros contratados a tal efecto.

El arancel por los servicios de las autoridades de certificación será establecido libremente por éstas.

## CAPÍTULO VII

### *Auditorías*

Art. 20. – *Sujetos a auditar.* El ente licenciante y las autoridades certificantes, deben ser auditados periódicamente, de acuerdo del sistema de auditoría que diseñe y apruebe la autoridad de aplicación.

La autoridad de aplicación podrá aplicar el sistema de auditoría por sí o por terceros habilitados a tal efecto.

Art. 21. – *Requisitos de habilitación.* A los efectos de su habilitación y del desarrollo de sus actividades, la Auditoría de Firma Digital debe cumplir los siguientes requisitos, sin perjuicio de los que establezca la reglamentación:

- a) Ser profesional, o asociación de profesionales, universitario con experiencia, demostrable objetivamente, en auditorías semejantes;
- b) Utilizar técnicas de auditoría apropiadas en sus evaluaciones;
- c) Prever su participación en los simulacros de emergencia destinados a probar el plan de contingencia.

#### CAPÍTULO VIII

##### *Comisión Asesora para la Infraestructura de Firma Digital*

Art. 22. – *Integración y funcionamiento.* La comisión estará integrada por 6 (seis) profesionales en informática y/o criptografía de reconocida trayectoria y experiencia, provenientes de las Secretarías de Comunicaciones; Secretaría para la Tecnología, la Ciencia y la Innovación Productiva; Subsecretaría de la Gestión Pública; Secretaría de Industria, Comercio y Minería; Secretaría para la Modernización del Estado y universidades nacionales.

- a) Los integrantes serán designados por el Poder Ejecutivo nacional por un período de cinco (5) años renovables por única vez;
- b) Se reunirá como mínimo trimestralmente;
- c) Deberá expedirse prontamente a solicitud de la autoridad de aplicación y sus dictámenes y disidencias se incluirán en las actas de la comisión, las que se publicarán en el Boletín Oficial de la Nación;
- d) Consultará periódicamente mediante audiencias públicas con la industria, los usuarios y las asociaciones de consumidores y mantendrá a la autoridad de aplicación regularmente informada de los resultados de dichas consultas.

Art. 23. – *Funciones.* La comisión debe emitir dictamen, por iniciativa propia o a solicitud de la autoridad de aplicación, sobre los siguientes aspectos:

- a) Tipos de algoritmos que se pueden implementar;
- b) Dispositivos de creación y verificación de firmas digitales, aconsejables de instalar;
- c) Longitudes mínimas aceptables de claves públicas y de digestos de mensaje y fecha límite de vencimiento de los certificados que las utilizan;
- d) Sistema de registro de toda la información relativa a la emisión de certificados de clave pública;

- e) Requisitos mínimos de información que debe contener el informe por escrito a los potenciales titulares de certificados de clave pública de los términos de las condiciones de emisión y utilización de sus certificados;
- f) Determinación de los efectos de la revocación de los certificados de clave pública de las autoridades certificantes y del ente licenciante.

#### CAPÍTULO IX

##### *Autoridad de aplicación*

Art. 24. – *Autoridad de aplicación.* La autoridad de aplicación de la presente ley es el Ministerio de Justicia y Derechos Humanos, quien ejercerá la función de superintendencia.

Art. 25. – *Funciones.* La autoridad de aplicación tiene las siguientes funciones:

- a) Establecer, previo dictamen de la Comisión Asesora para la Infraestructura de Firma Digital, los estándares tecnológicos y operativos de la Infraestructura de Firma Digital;
- b) Determinar los efectos de la revocación de los certificados de las autoridades certificantes o del ente licenciante;
- c) Instrumentar acuerdos nacionales, multinationales y regionales a fin de otorgar validez jurídica a las firmas digitales creadas sobre la base de certificados emitidos por autoridades certificantes de otros países;
- d) Determinar las pautas de auditoría, incluyendo los dictámenes tipo que deban emitirse como conclusión de las revisiones;
- e) Dictar un régimen de sanciones gradual a fin de su aplicación por parte del ente licenciante.

#### CAPÍTULO X

##### *Sanciones*

Art. 26. – *Sanciones.* El ente licenciante es competente para calificar y sancionar las conductas de las autoridades certificantes que infrinjan las disposiciones de esta ley y de las normas que dicte la autoridad de aplicación.

Aplicará las multas correspondientes según el régimen gradual de sanciones aprobado por la autoridad de aplicación.

Art. 27. – *Procedimiento.* Las sanciones se aplicarán mediante resolución fundada, previo sumario administrativo, y son recurribles ante la autoridad de aplicación.

El ente licenciante puede, una vez iniciado el sumario, suspender preventivamente a la autoridad certificante y, complementariamente, disponer las medidas conducentes para el resguardo de los derechos de los titulares de certificados.

## CAPÍTULO XI

*Normas de derecho internacional privado*

Art. 28. – *Equivalencia.* Los certificados de firmas digitales emitidos por entidades extranjeras, tendrán la misma validez y eficacia jurídica reconocida en la presente ley, siempre y cuando se cumplan con uno de los siguientes requisitos:

- a) Si la autoridad certificante extranjera cumple requisitos análogos a los de la presente ley y ha sido licenciada en el marco de un sistema voluntario de licenciamiento establecido por el gobierno de un país miembro del Mercosur;
- b) Si el certificado o la autoridad certificante están reconocidos en virtud de un acuerdo bilateral o multilateral entre la República Argentina y terceros países u organizaciones internacionales.

## CAPÍTULO XII

*Disposiciones generales*

Art. 29. – *Ámbito de aplicación.* La utilización de la firma digital es facultativa para las personas físicas o jurídicas de carácter privado, y de uso obligatorio para el sector público nacional definido en los términos del artículo 8 de la ley 24.156 (Ley de Administración Financiera y Sistemas de Control del Sector Público Nacional), el Poder Legislativo nacional y el Poder Judicial de la Nación, con arreglo a lo dispuesto en el artículo 34 de la presente ley.

Art. 30. – *Efectos jurídicos de la forma digital.* La firma digital, con los recaudos y exigencias que esta ley dispone, satisface el requerimiento de firma que las leyes establecen y tiene sus mismos efectos, siendo su empleo una alternativa de la firma manuscrita.

Esta ley no sustituye ni modifica las normas que regulan las funciones que corresponde realizar a las personas facultadas, con arreglo a derecho, para dar fe de la firma en documentos o para intervenir en la certificación de su carácter público.

Art. 31. – *Instrumento privado.* El documento digital firmado digitalmente, con los recaudos y exigencias que esta ley dispone, es instrumento privado siempre que su contenido pueda ser representado como texto inteligible.

## CAPÍTULO XIII

*Disposiciones modificatorias y derogatorias*

Art. 32. – *Modificación.* Sustituyese el artículo 8 de la ley 19.549 (Ley Nacional de Procedimientos Administrativos) por el siguiente texto:

Artículo 8°: El acto administrativo se manifestará expresamente y por escrito; indicará el lugar y fecha en que se lo dicta y contendrá la firma de la autoridad que lo emite, y si las circunstancias lo permitieren podrá utilizarse una

forma distinta. El documento firmado mediante el empleo del procedimiento de la firma digital, conforme a los términos y bajo las condiciones habilitantes dispuestas por la ley específica y las reglamentaciones vigentes, cumple con los requisitos de escritura y de firma del párrafo anterior.

Art. 33. – *Derogación.* Derógase el artículo 61 de la ley 25.237 (Ley de Presupuesto Nacional 2000).

## CAPÍTULO XIV

*Plazos – Disposiciones finales*

Art. 34. – *Implementación.* La autoridad de aplicación, en representación del Poder Ejecutivo nacional, convocará a representantes del Poder Judicial de la Nación y del Poder Legislativo nacional, a fin de determinar para cada ámbito los plazos máximos para iniciar la incorporación de la tecnología de digitalización de expedientes y firma digital, en forma gradual y obligatoria, en el ámbito de aplicación identificado en el artículo 29 de la presente ley.

En un plazo máximo de cinco (5) años contados a partir de la entrada en vigencia de la presente ley, se deberá llegar, como mínimo, a un nivel de despapelización del 50 % (cincuenta por ciento), respecto al estado actual dentro del ámbito de aplicación establecido en el artículo 29 de la presente ley, y uso masivo de la firma digital que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado desde su propia computadora.

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 los instrumentos jurídicos emanados del ámbito de aplicación establecido en el artículo 29 de la presente ley.

Art. 35. – *Reglamentación.* El Poder Ejecutivo nacional deberá reglamentar esta ley en un plazo no mayor a los 120 (ciento veinte) días de su publicación en el Boletín Oficial de la Nación. La autoridad de aplicación convocará a representantes del Poder Legislativo nacional y del Poder Judicial de la Nación para que en forma conjunta elaboren el proyecto de reglamentación de la presente ley, el que será elevado al Poder Ejecutivo nacional para su análisis.

Art. 36. – *Vigencia.* La presente ley entrará en vigencia desde la fecha de la publicación de su decreto reglamentario en el Boletín Oficial de la Nación.

Art. 37. – *Invitación.* Invítase a las jurisdicciones provinciales a dictar los instrumentos legales pertinentes para adherir a la presente ley.

Art. 38. – Comuníquese al Poder Ejecutivo.

Pablo A. Fontdevila. – Norberto R. Nicotra. – Irma F. Parentella.