PODER LEGISLATIVO
LEY Nº 4.017

DE VALIDEZ JURÍDICA DE LA FIRMA ELECTRÓNICA, LA FIRMA DIGITAL, LOS MENSAJES DE DATOS Y EL EXPEDIENTE ELECTRÓNICO.

EL CONGRESO DE LA NACION PARAGUAYA SANCIONA CON FUERZA DE

LEY

TÍTULO PRIMERO
Disposiciones Generales

Artículo 1°.- Objeto y ámbito de aplicación. La presente Ley reconoce la validez jurídica de la firma electrónica, la firma digital, los mensajes de datos, el expediente electrónico y regula la utilización de los mismos, las empresas certificadoras, su habilitación y la prestación de los servicios de certificación.

Artículo 2°.- Definiciones. A efectos de la presente Ley, se entenderá por:

Firma electrónica: es el 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.

Firma digital: es una firma electrónica certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría.

Mensaje de datos: es toda información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax, siendo esta enumeración meramente enunciativa y no limitativa.

Documento Digital: es un mensaje de datos que representa actos o hechos, con independencia del soporte utilizado para su creación, fijación, almacenamiento, comunicación o archivo.

Firmante, suscriptor o signatario: es toda persona física o jurídica titular de la firma electrónica o digital. Cuando el titular sea una persona jurídica, ésta es responsable de determinar las personas físicas a quienes se autorizarán a administrar los datos de creación de la firma electrónica o digital.

Remitente de un mensaje de datos: es toda persona que haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar o generar un mensaje de datos.

LEY N° 4017

Certificado digital: es todo mensaje de datos u otro registro emitido por una entidad legalmente habilitada para el efecto y que confirme la vinculación entre el titular de una firma digital y los datos de creación de la misma.

Prestador de servicios de certificación: entidad prestadora de servicios de certificación de firmas digitales.

Expediente electrónico: se entiende por “expediente electrónico”, la serie ordenada de documentos públicos registrados por vía informática, tendientes a la formación de la voluntad administrativa en un asunto determinado.

Parte que confía: es toda persona que pueda actuar sobre la base de un certificado o de una firma electrónica.

Artículo 3°.- Principios Generales. En la aplicación de la presente Ley, deberán observarse los siguientes principios:

a) Neutralidad tecnológica: Ninguna de las disposiciones de la presente Ley podrá ser aplicada de forma que excluya, restrinja o prive de efectos jurídicos a cualquier otro sistema o método técnico conocido o por conocerse que reúna los requisitos establecidos en la presente Ley.

b) Interoperabilidad: Las tecnologías utilizadas en la aplicación de la presente Ley se basarán en estándares internacionales.

c) Interpretación funcional: Los términos técnicos y conceptos utilizados serán interpretados en base a la buena fe, de manera que no sean negados efectos jurídicos a un proceso o tecnología utilizado por otro Estado por el solo hecho de que se le atribuya una nomenclatura diferente a la prevista en la presente Ley.

TÍTULO SEGUNDO

Sección I
De los Mensajes de Datos

Artículo 4°.- Valor jurídico de los mensajes de datos. Se reconoce el valor jurídico de los mensajes de datos y no se negarán efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos.

Tampoco se negarán efectos jurídicos, validez ni fuerza obligatoria a la información por la sola razón de que no esté contenida en el mensaje de datos que se supone ha de dar lugar a este efecto jurídico, sino que figure simplemente en el mensaje de datos en forma de remisión.

Artículo 5°.- Empleo de mensajes de datos en la formación de los contratos. La oferta, aceptación así como cualquier negociación, declaración o acuerdo realizado por las partes en todo contrato, podrá ser expresada por medio de un mensaje de datos, no pudiendo negarse validez a un contrato por la sola razón de que en su formación se ha utilizado este sistema, siempre y cuando concurran el consentimiento y los demás requisitos necesarios para su validez previstos en el Código Civil.

LEY N° 4017

Para que sea válida la celebración de contratos por vía electrónica, no será necesario el previo acuerdo de las partes sobre la utilización de medios electrónicos.

Artículo 6°.- Cumplimiento del requisito de escritura. Cuando en el ámbito de aplicación de la presente Ley, la normativa vigente requiera que la información conste por escrito o si las normas prevean consecuencias en el caso de que la información no sea presentada o conservada en su forma original; ese requisito quedará satisfecho con un mensaje de datos firmado digitalmente que permita que la información que éste contiene sea accesible para su ulterior consulta.

En caso de que el mensaje de datos no estuviere vinculado con una firma digital, el mismo será considerado válido, en los términos del parágrafo anterior; si fuera posible determinar por algún medio inequívoco su autenticidad e integridad.

Artículo 7°.- Admisibilidad y fuerza probatoria de los mensajes de datos. Toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria, siempre y cuando el mismo tenga una firma digital válida de acuerdo con la presente Ley.

Los actos y contratos suscritos por medio de firma digital, otorgados o celebrados por personas naturales o jurídicas, públicas o privadas en el ámbito de aplicación de la presente Ley, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel. Dichos actos y contratos se reputarán como escritos, en los casos en que la ley exija que los mismos consten por escrito, a los efectos de que surtan consecuencias jurídicas.

Artículo 8°.- Conservación de los mensajes de datos. Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados en su forma original, ese requisito quedará satisfecho con un mensaje de datos que los reproduzca, si:

a) existe una garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez su forma definitiva, como mensaje de datos u otra forma. Esta garantía quedará cumplida si al mensaje de datos resultante se aplica la firma digital del responsable de la conservación;

b) la información que contenga sea accesible para su ulterior consulta;

c) el mensaje de datos sea conservado con el formato que se haya generado, enviado o recibido o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida; y,

d) se conserve, de haber alguno, todo dato que permita determinar el origen y el destino del mensaje, la fecha y la hora que fue enviado o recibido.

Artículo 9°.- Integridad del documento digital o mensaje de datos. Para efectos del artículo anterior, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

Artículo 10.- De la reproducción de documentos originales por medios electrónicos. Cuando sea necesario almacenar documentos y datos de cualquier especie, se podrá almacenar la reproducción de los mismos en mensajes de datos. La reproducción del documento o dato deberá ser realizada en la forma y en los lugares indicados por la reglamentación de la presente Ley.

LEY N° 4017

La reproducción, a la que hace mención el presente artículo, no afectará ni modificará de modo alguno los plazos individualizados en el documento reproducido, ni tampoco implica reconocimiento expreso o tácito de que el contenido sea válido.

Artículo 11.- De la digitalización de los archivos públicos. El Estado y sus órganos dependientes podrán proceder a la digitalización total o parcial de sus archivos almacenados, para lo cual cada organismo del Estado o el Poder Ejecutivo podrá dictar el reglamento aplicable al proceso de digitalización mencionado, siempre y cuando los mensajes de datos resultantes cumplan con las condiciones mínimas establecidas en la presente Ley y estuvieran firmados digitalmente por el funcionario autorizado para realizar las citadas reproducciones.

Sección II
Del Envío y Recepción de los Mensajes de Datos

Artículo 12.- Remitente de los mensajes de datos. A los efectos de la presente Ley, se entenderá que un mensaje de datos:

a) proviene del remitente, si:

i) ha sido enviado por el propio remitente;

ii) ha sido enviado por alguna persona facultada para actuar en nombre del remitente respecto de ese mensaje;

iii) ha sido enviado por un sistema de información programado por el remitente o en su nombre para que opere automáticamente, o

iv) el mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el remitente, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el remitente para identificar un mensaje de datos como propio, aun cuando esta persona no hubiese estado debidamente autorizada por el mismo para ese efecto.

Los numerales ii, iii y iv del presente artículo no se aplicarán entre remitente y destinatario, a partir del momento en que el destinatario haya sido informado por el remitente de que los mensajes de datos que provengan en su nombre y/o con su firma digital pueden ser emitidos por personas no autorizadas para el efecto, quedando automáticamente inhabilitada la firma digital entre el remitente y el destinatario debidamente notificado. La notificación aquí mencionada no exime al titular de la firma digital de la obligación de notificar a la autoridad certificadora de esta situación.

Artículo 13.- Acuse de recibo. El remitente de un mensaje de datos podrá solicitar o acordar con el destinatario que se acuse recibo del mensaje de datos.

1) Cuando el remitente no haya acordado con el destinatario que el acuse de recibo se dé en alguna forma determinada o utilizando un método determinado, se podrá acusar recibo mediante:

a) toda comunicación del destinatario, automatizada o no, o

b) todo acto del destinatario, que baste para indicar al remitente que se ha recibido el mensaje de datos.

2) Cuando el remitente haya indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, se considerará que el mensaje de datos no ha sido enviado en tanto que no se haya recibido el acuse de recibo.

3) Cuando el remitente no haya indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, si no ha recibido acuse en el plazo fijado o convenido, o no se ha fijado o convenido ningún plazo, en un plazo razonable el remitente:

a) podrá dar aviso al destinatario de que no ha recibido acuse de recibo y fijar un plazo razonable para su recepción; y,

b) de no recibirse acuse dentro del plazo fijado conforme al inciso a), podrá, dando aviso de ello al destinatario, considerar que el mensaje de datos no ha sido enviado o ejercer cualquier otro derecho que pueda tener.

4) Cuando el remitente reciba acuse de recibo del destinatario, se presumirá que éste ha recibido el mensaje de datos correspondiente. Esa presunción no implicará que el mensaje de datos corresponda al mensaje recibido.

5) Cuando en el acuse de recibo se indique que el mensaje de datos recibido cumple con los requisitos técnicos convenidos o enunciados en alguna norma técnica aplicable, se presumirá que ello es así.

Salvo en lo que se refiere al envío o recepción del mensaje de datos, el presente artículo no obedece al propósito de regir las consecuencias jurídicas que puedan derivarse de ese mensaje de datos o de su acuse de recibo.

Artículo 14.- Tiempo y lugar del envío y la recepción de un mensaje de datos.

1) De no convenir otra cosa el remitente y el destinatario, el mensaje de datos se tendrá por expedido cuando entre en un sistema de información que no esté bajo el control del remitente o de la persona que envió el mensaje de datos en nombre del remitente.

2) De no convenir otra cosa el remitente y el destinatario, el momento de recepción de un mensaje de datos se determinará como sigue:

a) si el destinatario ha designado un sistema de información para la recepción de mensajes de datos, la recepción tendrá lugar:

i) en el momento en que entre el mensaje de datos en el sistema de información designado; o

ii) de enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, en el momento en que el destinatario recupere el mensaje de datos.

b) si el destinatario no ha designado un sistema de información, la recepción tendrá lugar en el momento en que el destinatario recupere el mensaje de datos de un sistema de información que no esté bajo su control.

3) El párrafo 2) será aplicable aun cuando el sistema de información esté ubicado en un lugar distinto de donde se tenga por recibido el mensaje conforme al párrafo 4).

4) De no convenir otra cosa el remitente y el destinatario, el mensaje de datos se tendrá por expedido en el lugar donde el remitente tenga su establecimiento y por recibido en el lugar donde el destinatario tenga el suyo. Para los fines del presente párrafo:

a) si el remitente o el destinatario tienen más de un establecimiento, será válido el que guarde una relación más estrecha con la operación subyacente o, de no haber una operación subyacente, será válido su establecimiento principal; y,

LEY N° 4017

b) si el remitente o el destinatario no tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.

TÍTULO TERCERO
De la Firma Electrónica

Sección I
Disposiciones Generales

Artículo 15.- Titulares de una firma electrónica. Podrán ser titulares de una firma electrónica personas físicas o jurídicas.

Para el caso de las personas jurídicas, la aplicación o utilización de la firma electrónica por sus representantes se considerará como efectuada por la persona jurídica con todos los alcances previstos en los estatutos o normas correspondientes a su funcionamiento que se encuentren vigentes al momento de la firma.

Corresponde a la persona jurídica, a través de sus órganos directivos, determinar las personas autorizadas para emplear la firma electrónica que le fuera asignada.

Artículo 16.- Obligaciones de los titulares de firmas electrónicas. Los titulares de firmas electrónicas deberán:

a) actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma;

b) dar aviso sin dilación indebida a cualquier persona que, según pueda razonablemente prever el titular, que puedan considerar fiable la firma electrónica o que puedan prestar servicios que la apoyen si:

i) sabe que los datos de creación de la firma han quedado en entredicho; o

ii) las circunstancias de que tiene conocimiento dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho.

c) cuando se emplee un certificado para refrendar la firma electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con su período de validez o que hayan de consignarse en él sean exactas y cabales.

El titular de la firma electrónica incurrirá en responsabilidad personal, solidaria e intransferible por el incumplimiento de los requisitos enunciados en este artículo.

Artículo 17.- Efectos del empleo de una firma electrónica. La aplicación de la firma electrónica a un mensaje de datos implica para las partes la presunción de:

a) que el mensaje de datos proviene del firmante;

b) que el firmante aprueba el contenido del mensaje de datos.

LEY N° 4017

Artículo 18.- Validez jurídica de la firma electrónica. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

Artículo 19.- De la revocación de una firma electrónica. La asignación de una firma electrónica a su titular quedará sin efecto y la misma perderá todo valor como firma en los siguientes casos:

1) Por extinción del plazo de vigencia de la misma.

2) A solicitud del titular de la firma.

3) Por fallecimiento del titular o disolución de la persona jurídica que represente, en su caso.

4) Por resolución judicial ejecutoriada, o

5) Por incumplimiento de las obligaciones del usuario establecidas en la presente Ley.

Sección II
De la Firma Digital

Artículo 20.- Validez jurídica de la firma digital. 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 21.- 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 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; y,

d) a los actos personalísimos en general.

Artículo 22.- Requisitos de validez de la firma digital. 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) haber sido debidamente verificada la relación entre el firmante y la firma digital, por la referencia a los datos indicados en el certificado digital, según el procedimiento de verificación correspondiente**.** Se exigirá la presencia física del solicitante del certificado con documento de identidad vigente y válido en la República del Paraguay;

c) que dicho certificado haya sido emitido por una entidad prestadora de servicios de certificación autorizada por la presente Ley;

d) que los datos de creación de la firma hayan estado, en el momento de la firma, bajo el control del firmante;

e) que sea posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma;

f) que sea posible detectar cualquier alteración de la información contenida en el mensaje de datos al cual está asociada, hecha después del momento de la firma;

g) el solicitante es el responsable respecto de la clave privada, cuya clave pública correspondiente se consigna en el certificado y todos los usos que a la misma se le dieran;

h) el solicitante deberá manifestar su total conocimiento y aceptación de la Declaración de Prácticas de Certificación y/o Política de Certificación correspondiente al certificado solicitado.

Artículo 23.- Efectos del empleo de una firma digital. La aplicación de la firma digital a un mensaje de datos implica para las partes la presunción de:

a) que el mensaje de datos proviene del remitente;

b) que el contenido del mensaje de datos no ha sido adulterado desde el momento de la firma y el firmante aprueba el contenido del mensaje de datos.

Para que la presunción expresada en el parágrafo anterior sea efectiva, la firma digital aplicada al mensaje de datos debe poder ser verificada con el certificado digital respectivo expedido por la prestadora de servicios de firma digital.

Los efectos enumerados en el presente artículo continuarán vigentes por tiempo indefinido para el mensaje de datos al que fuera aplicada la firma digital, aun cuando con posterioridad a la aplicación de la misma, ésta fuera revocada por cualquiera de los motivos indicados en la presente Ley.

Artículo 24.- De la revocación de una firma digital. La asignación de una firma digital a su titular quedará sin efecto y la misma perderá todo valor como firma digital en los siguientes casos:

1) Por extinción del plazo de vigencia de la firma digital, el cual no podrá exceder de dos años, contados desde la fecha de adjudicación de la misma a su titular por parte del prestador de servicios de firmas digitales respectivo.

2) Por revocación realizada por el prestador de servicios de certificación, la que tendrá lugar en las siguientes circunstancias:

a) a solicitud del titular de la firma;

b) por fallecimiento del titular o disolución de la persona jurídica que represente, en su caso;

c) por resolución judicial ejecutoriada, o

d) por incumplimiento de las obligaciones del usuario establecidas en la presente Ley.

La revocación de un certificado en las circunstancias del inciso d) del numeral 2) de este artículo, será comunicada previamente al prestador de servicios de certificación que hubiera emitido la misma, indicando la causa. En cualquier caso, la revocación no privará de valor a las firmas digitales antes del momento exacto que sea verificada por el prestador.

En caso de que el prestador de servicios de certificación que originalmente haya adjudicado la firma digital a ser revocada ya no existiera o su funcionamiento se encontrase suspendido, el titular deberá comunicar la revocación de su firma digital al prestador de servicios de firma digital que haya sido designado responsable de la verificación de las firmas emitidas por aquélla.

LEY N° 4017

Igualmente, cuando ocurriere una suspensión por causas técnicas, se aplicará lo dispuesto en el párrafo anterior.

Sección III
De los Prestadores de Servicios de Certificación

Artículo 25.- Del prestador de servicios de certificación. Podrán ser prestadores de servicios de certificación, las personas jurídicas que fueran habilitadas por la autoridad normativa indicada en la presente Ley, en base a las disposiciones de la presente Ley, así como a las disposiciones del decreto reglamentario correspondiente.

Artículo 26.- Del procedimiento de habilitación de prestadores de servicios de certificación. La autoridad normativa autorizará el funcionamiento de prestadores de servicios de certificación que hubiesen solicitado la habilitación requerida por esta Ley, siempre y cuando las mismas cumplan con todos los requisitos básicos individualizados en ella.

Una vez habilitado un prestador de servicios de certificación, el mismo deberá autoasignarse una firma digital, debiendo entregar la clave verificadora de la misma a la autoridad normativa, quien tendrá habilitado al efecto un registro de prestadores de servicios de certificación habilitados en la República del Paraguay, y a la cual podrá recurrirse para verificar la firma digital del prestador.

Artículo 27.- De la resolución ficta de habilitación de prestadores de servicios de certificación. Cuando la autoridad normativa considere que el solicitante de la habilitación para prestar servicios de certificación no cumple con los requisitos mínimos establecidos, deberá demostrarlo así en un procedimiento sumario que deberá completarse en un plazo máximo de cincuenta días hábiles, contados a partir de la fecha de presentación de la solicitud de habilitación respectiva.

En caso de que vencido el plazo no pudiera demostrarse el incumplimiento de los requisitos básicos establecidos, se producirá resolución ficta concediendo la habilitación solicitada y debiendo expedirse inmediatamente la documentación que acredite la habilitación del prestador.

Artículo 28.- Requisitos básicos que deben cumplir los prestadores de servicios de certificación para ser habilitados. Los proveedores de servicios de certificación deberán:

a) garantizar la utilización de un servicio rápido y seguro de guía de usuarios y de un servicio de revocación seguro e inmediato;

b) garantizar que pueda determinarse con precisión la fecha y la hora en que se expidió o revocó un certificado;

c) comprobar debidamente, de conformidad con el derecho nacional, la identidad y, si procede, cualesquiera atributos específicos de la persona a la que se expide un certificado reconocido;

d) emplear personal que tenga los conocimientos especializados, la experiencia y las cualificaciones necesarias correspondientes a los servicios prestados, en particular: competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma electrónica y familiaridad con los procedimientos de seguridad adecuados; deben poner asimismo en práctica los procedimientos administrativos y de gestión adecuados y conformes a normas reconocidas;

e) utilizar sistemas y productos fiables que se requiera para prestar servicios de certificación y que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procedimientos con que trabajan;

f) tomar medidas contra la falsificación de certificados y, en caso de que el proveedor de servicios de certificación genere datos de creación de firma, garantizar la confidencialidad durante el proceso de generación de dichos datos;

g) 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 y perjuicios, pudiendo emplearse para el efecto fianzas, avales, seguros o cualquier otro medio;

h) registrar toda la información pertinente relativa a un certificado reconocido durante un período de tiempo adecuado, en particular para aportar pruebas de certificación en procedimientos judiciales. Esta actividad de registro podrá realizarse por medios electrónicos;

i) no almacenar ni copiar los datos de creación de firma de la persona a la que el proveedor de servicios de certificación ha prestado servicios de asignación de firmas electrónicas;

j) utilizar sistemas fiables para almacenar certificados de forma verificable, de modo que:

- sólo personas autorizadas puedan hacer anotaciones y modificaciones;

- pueda comprobarse la autenticidad de la información;

- los certificados estén a disposición del público para su consulta sólo en los casos en los que se haya obtenido el consentimiento del titular del certificado; y

- el agente pueda detectar todos los cambios técnicos que pongan en entredicho los requisitos de seguridad mencionados.

k) demostrar la honestidad de sus representantes legales, administradores y funcionarios, a través de certificaciones de antecedentes policiales y judiciales.

Artículo 29.- Requisitos de validez de los certificados digitales. Los certificados digitales para ser válidos deberán:

a) ser emitidos por una entidad prestadora de servicios de certificación habilitada por la presente Ley; y,

b) responder a formatos estándares tecnológicos, preestablecidos reconocidos internacionalmente, fijados por la presente Ley y la reglamentación respectiva, y contener, como mínimo, los datos que permitan:

1. identificar indubitablemente a su titular y la entidad que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única;

2. ser susceptible de verificación respecto de su vigencia o revocación;

3. establecer claramente la información incluida en el certificado que haya podido ser verificada;

4. contemplar la información necesaria para la verificación de la firma;

LEY N° 4017

5. identificar la política de certificación bajo la cual fue emitida, en especial si la misma implica limitación en los fines en que ha de utilizarse o de la de responsabilidad que asume el prestador con relación al certificado emitido;

6. la firma digital del prestador de servicios de certificación.

Artículo 30.- Políticas de Certificación. El certificado de firma digital podrá establecer límites en cuanto a sus posibles usos, siempre y cuando los límites sean reconocibles por terceros. La Autoridad de aplicación deberá aprobar la Política de Certificación, que será empleada por las empresas prestadoras de los servicios de certificación.

Artículo 31.- De las prestadoras de servicios de certificación aprobadas por leyes anteriores. Las entidades prestadoras de servicios de certificación, cuyo funcionamiento hubiera sido autorizado con anterioridad a la presente Ley, deberán adecuar su funcionamiento a las disposiciones de ésta en un plazo perentorio máximo de seis meses y de no hacerlo así, su habilitación será revocada automáticamente, siendo a cargo exclusivo de las mismas las responsabilidades emergentes de su funcionamiento sin la habilitación pertinente.

La firma digital empleada en base a las disposiciones de la presente Ley será suficiente para su empleo ante cualquier dependencia estatal o privada, aun cuando por ley anterior estuviere establecido el empleo de una firma expedida por prestadoras de servicios de certificación determinados.

Artículo 32.- Obligaciones del prestador de servicios de certificación. El prestador de servicios de certificación deberá:

a) adjudicar una firma digital a quien lo solicite sin distinciones ni privilegios de ninguna clase, siempre y cuando el solicitante presente los recaudos establecidos para el efecto;

b) actuar con diligencia razonable para cerciorarse de que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del certificado o que estén consignadas en él sean exactas y cabales;

c) proporcionar medios de acceso razonablemente fácil que permitan a la parte que confía en el certificado determinar mediante éste:

i) la identidad del prestador de servicios de certificación;

ii) que el firmante nombrado en el certificado haya tenido bajo su control los datos de creación de la firma en el momento en que se aplicó ésta al mensaje de datos;

iii) que los datos de creación de la firma hayan sido válidos en la fecha que se expidió el certificado o antes de ella.

d) proporcionar medios de acceso razonablemente fácil que, según proceda, permitan a la parte que confía en el certificado determinar mediante éste o de otra manera:

i) el método utilizado para identificar al firmante;

ii) cualquier limitación en los fines o el valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado;

LEY N° 4017

iii) si los datos de creación de la firma son válidos y no están en entredicho;

iv) cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el prestador de servicios de certificación;

v) si existe un medio para que el firmante dé aviso de que los datos de creación de la firma están en entredicho;

vi) si se ofrece un servicio de revocación oportuna del certificado.

e) además deberá informar a quien solicita la adjudicación de una firma digital con carácter previo a su emisión las condiciones precisas de utilización de la firma digital, sus características y efectos, forma que garantiza su posible responsabilidad patrimonial. Esa información deberá estar libremente accesible en lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;

f) 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;

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

h) operar utilizando un sistema técnicamente confiable;

i) notificar al solicitante las medidas que está obligado a adoptar y las obligaciones que asume por el solo hecho de ser titular de una firma digital;

j) recabar únicamente aquellos datos personales del titular de la firma digital que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional;

k) mantener la confidencialidad de toda información que reciba y que no figure en el certificado digital;

l) poner a disposición del solicitante de una firma digital, toda la información relativa a su tramitación;

m) mantener la documentación respaldatoria de las firmas digitales y los certificados digitales emitidos, por diez años a partir de su fecha de vencimiento o revocación;

n) publicar en Internet o cualquier otra red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de firmas digitales vigentes y revocadas, 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 considere pertinente;

ñ) registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas;

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;

LEY N° 4017

p) 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;

q) llevar un registro de las claves públicas de las firmas digitales existentes, a los efectos de confirmar la veracidad de las mismas cuando éstos son empleados;

r) velar por la vigencia y, en su caso, cancelación oportuna de las firmas digitales cuando existan razones válidas para ello;

s) actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de firmas, así como de cualquier otra información obrante en su poder relacionada a las firmas electrónicas que administre o certifique;

t) dar aviso sin dilación indebida por lo menos en dos medios masivos de comunicación si:

i) sabe que los datos de creación de su firma digital o cualquier otra información relacionada a la misma ha quedado en entredicho; o

ii) las circunstancias de que tiene conocimiento dan lugar a un riesgo considerable de que datos de creación de su firma digital o cualquier otra información relacionada a la misma ha quedado en entredicho.

Artículo 33.- Responsabilidades de los prestadores de servicios de certificación. Los prestadores de servicios de certificación autorizados en base a la presente Ley serán responsables por los daños y perjuicios causados a toda persona física o jurídica que confíe razonablemente en el certificado digital por él emitido, en lo que respecta a:

a) la inclusión de todos los campos y datos requeridos por la ley y a la exactitud de los mismos, al momento de su emisión;

b) que al momento de la emisión de un certificado reconocido por el prestador de servicios de certificación autorizado, la firma en él identificada obedezca a los datos de creación de las firmas correspondientes a los datos de verificación incluidos en el certificado reconocido por el prestador, con el objeto de asegurar la cadena de confianza;

c) los errores u omisiones que presenten los certificados digitales que emitan; y,

d) el registro, en tiempo y forma, de la revocación de los certificados reconocidos que haya emitido, cuando así correspondiere.

Corresponde al prestador de servicios de certificación autorizado demostrar que no actuó ni con culpa ni con dolo.

Los prestadores no serán responsables de los daños y perjuicios causados por el uso que exceda de los límites de las Políticas de Certificación indicados en el certificado, ni de aquéllos que tengan su origen en el uso indebido o fraudulento de un certificado de firma digital.

Tampoco responderá por eventuales inexactitudes en el certificado reconocido que resulten de la información verificada facilitada por el titular, siempre que el prestador de servicios de certificación acreditado pueda demostrar que ha cumplido todas las medidas previstas en sus políticas y procedimientos de certificación.

A los efectos de salvaguardar los intereses de las partes que utilizan los servicios de certificación, el prestador de servicios de certificación deberá contar con un medio de garantía suficiente para cubrir las responsabilidades inherentes a su gestión, entre los que se podría citar: pólizas de seguros, cauciones bancarias o financieras o en fin cualquier sistema que el Reglamento de la presente Ley establezca para el efecto.

Artículo 34.- Protección de datos personales. Los prestadores de servicios de certificación sólo podrán recolectar los datos personales directamente de la persona a quien esos datos se refieran, después de haber obtenido su consentimiento expreso y sólo en la medida en que los mismos sean necesarios para la emisión y mantenimiento del certificado. Los datos no podrán ser obtenidos o utilizados para otro fin, sin el consentimiento expreso del titular de los datos.

Artículo 35.- De los aranceles. Los aranceles por la prestación de servicios de certificación serán fijados por la autoridad normativa, quien podrá establecer los montos máximos a ser cobrados por los mismos. Podrá la misma permitir que los aranceles sean fijados libremente por los prestadores siempre que a su criterio el mercado estuviera en condiciones de regularlos en un marco de libre competencia.

Artículo 36.- Reconocimiento de certificados extranjeros. Los certificados digitales emitidos por certificadores extranjeros podrán ser reconocidos en los mismos términos y condiciones exigidos en la presente Ley y sus normas reglamentarias cuando:

a) reúnan las condiciones que establece la presente Ley y la reglamentación correspondiente;

b) tales certificados provengan de proveedores extranjeros que sean reconocidos o aprobados por la autoridad normativa, facultándose a ésta a reglamentar el procedimiento para este reconocimiento o aprobación.

TÍTULO CUARTO

Del Expediente Electrónico y del Trámite Administrativo

Artículo 37.- Expediente electrónico. Se entiende por “expediente electrónico” la serie ordenada de documentos públicos registrados por vía informática, tendientes a la formación de la voluntad administrativa en un asunto determinado.

En la tramitación de expedientes administrativos, podrán utilizarse expedientes electrónicos total o parcialmente, de acuerdo con las siguientes reglas:

1) El expediente electrónico tendrá la misma validez jurídica y probatoria que el expediente tradicional.

2) La documentación emergente de la transmisión a distancia, por medios electrónicos, entre dependencias oficiales, constituirá, de por sí, documentación auténtica y hará plena fe a todos sus efectos en cuanto a la existencia del original trasmitido.

LEY N° 4017

3) La sustanciación de actuaciones en la Administración Pública, así como los actos administrativos que se dicten en las mismas, podrán realizarse por medios informáticos.

Cuando dichos trámites o actos, revestidos de carácter oficial, hayan sido redactados o extendidos por funcionarios competentes, según las formas requeridas, dentro del límite de sus atribuciones, y que aseguren su inalterabilidad por medio de la firma digital reconocida en la presente Ley tendrán el mismo valor probatorio y jurídico que se le asigna cuando son realizados por escrito en papel.

4) Cuando la sustanciación de las actuaciones administrativas se realice por medios informáticos, las firmas autógrafas que la misma requiera podrán ser sustituidas por firmas digitales.

5) Todas las normas sobre procedimiento administrativo serán de aplicación a los expedientes tramitados en forma electrónica, en la medida en que no sean incompatibles con la naturaleza del medio empleado.

6) Toda petición o recurso administrativo que se presente ante la Administración podrá realizarse por medio de documentos electrónicos. A tales efectos, los mismos deberán ajustarse a los formatos o parámetros técnicos establecidos por la autoridad normativa.

En caso de incumplimiento de dichas especificaciones, tales documentos se tendrán por no recibidos.

7) Toda vez que se presente un documento mediante transferencia electrónica, la Administración deberá expedir una constancia de su recepción. La constancia o acuse de recibo de un documento electrónico será prueba suficiente de su presentación. Su contenido será la fecha, lugar y firma digital del receptor.

8) La Administración admitirá la presentación de documentos registrados en papel para su utilización en un expediente electrónico. En tales casos, podrá optar entre la digitalización de dichos documentos para su incorporación al expediente electrónico, o la formación de una pieza separada, o una combinación de ambas, fijando como meta deseable la digitalización total de los documentos.

En caso de proceder a la digitalización del documento registrado en papel, se certificará la copia mediante la firma digital del funcionario encargado del proceso, así como la fecha y lugar de recepción.

9) Autorízase la reproducción y almacenamiento por medios informáticos de los expedientes y demás documentos registrados sobre papel, que fueran fruto de la aplicación de la presente Ley.

10) Podrán reproducirse sobre papel los expedientes electrónicos cuando sea del caso su sustanciación por ese medio, ya sea dentro o fuera de la repartición administrativa de que se trate, o para proceder a su archivo sobre papel. El funcionario responsable de dicha reproducción certificará su autenticidad.

11) Tratándose de expedientes totalmente digitalizados, el expediente original en papel deberá radicarse en un archivo centralizado. En caso de la tramitación de un expediente parcialmente digitalizado, la pieza separada que contenga los documentos registrados en papel, se radicará en un archivo a determinar por la repartición respectiva. En ambos casos, el lugar dispuesto propenderá a facilitar la consulta, sin obstaculizar el trámite del expediente.

12) Los plazos para la sustanciación de los expedientes electrónicos, se computarán a partir del día siguiente de su recepción efectiva por el funcionario designado.

Se entiende por “recepción efectiva” la fecha de ingreso del documento al subsistema de información al cual tiene acceso el funcionario designado a tales efectos.

13) Los sistemas de información de expedientes electrónicos deberán prever y controlar las demoras en cada etapa del trámite. A su vez, deberán permitir al superior jerárquico modificar el trámite para sortear los obstáculos detectados, minimizando demoras.

14) Los órganos administrativos que utilicen expedientes electrónicos, adoptarán procedimientos y tecnologías de respaldo o duplicación, a fin de asegurar su inalterabilidad y seguridad, según los estándares técnicos establecidos por la Autoridad Normativa.

15) Los documentos que hayan sido digitalizados en su totalidad, a través de los medios técnicos incluidos en el artículo anterior, se conservarán de acuerdo con lo dispuesto en la presente Ley. Los originales de valor histórico, cultural o de otro valor intrínseco, no podrán ser destruidos; por lo que luego de almacenados serán enviados para su guarda a la repartición pública que corresponda, en aplicación de las normas vigentes sobre conservación del patrimonio histórico y cultural del Estado.

16) La divulgación de la clave o contraseña personal de cualquier funcionario autorizado a documentar su actuación mediante firmas digitales, constituirá falta gravísima, aun cuando la clave o contraseña no llegase a ser utilizada.

17) Cuando los documentos electrónicos que a continuación se detallan, sean registrados electrónicamente, deberán identificarse mediante la firma digital de su autor:

a) los recursos administrativos, así como toda petición que se formule a la Administración;

b) los actos administrativos definitivos;

c) los actos administrativos de certificación o destinados a hacer fe pública; y,

d) los dictámenes o asesoramientos previos a una resolución definitiva.

TÍTULO QUINTO
De la Autoridad de Aplicación

Artículo 38.- Autoridad de Aplicación. La Autoridad de Aplicación de la presente Ley será el Instituto Nacional de Tecnología y Normalización.

Artículo 39.- Funciones. El Instituto Nacional de Tecnología y Normalización sin perjuicio de las funciones específicas del mismo, en su carácter de Autoridad de Aplicación de la presente Ley tendrá las siguientes atribuciones:

a) dictar las normas reglamentarias y de aplicación de la presente Ley;

b) establecer los estándares tecnológicos y operativos de la implementación de la presente Ley;

c) autorizar, conforme a la reglamentación expedida por el Poder Ejecutivo, la operación de entidades de certificación en el territorio nacional;

d) velar por el adecuado funcionamiento y la eficiente prestación del servicio por parte de las entidades de certificación y el cabal cumplimiento de las disposiciones legales y reglamentarias de la actividad;

LEY N° 4017

e) efectuar las auditorías de que trata la presente Ley;

f) determinar los efectos de la revocación de los certificados de los prestadores de servicios de certificación;

g) 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;

h) determinar las pautas de auditoría, incluyendo los dictámenes tipo que deban emitirse como conclusión de las revisiones;

i) requerir en cualquier momento a las entidades de certificación para que suministren información relacionada con los certificados, las firmas digitales emitidas y los documentos en soporte informático que custodien o administren;

j) imponer sanciones a las entidades de certificación por el incumplimiento o cumplimiento parcial de las obligaciones derivadas de la prestación del servicio;

k) otorgar o revocar las licencias a los prestadores del servicio de certificación habilitados y supervisar su actividad, según las exigencias establecidas por la reglamentación;

l) homologar los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la reglamentación; y,

m) aplicar las sanciones previstas en la reglamentación.

Artículo 40.- 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) 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; y,

d) supervisar la ejecución del plan de cese de actividades de los prestadores de servicio de certificación habilitados que discontinúan sus funciones.

Artículo 41.- Recursos. Los recursos que perciba la Autoridad Acreditadora por parte de los prestadores acreditados de servicios de certificación, constituirán ingresos propios de dicha entidad y se incorporarán a su presupuesto.

LEY N° 4017

Artículo 42.- Sistema de Auditorías. Los prestadores de servicios de certificación deben ser auditados periódicamente, de acuerdo con el 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 reglamentaciones vigentes.

TÍTULO SEXTO
De las Disposiciones Finales y Transitorias

Artículo 43.- Los datos de creación de firma digital son los datos únicos que el firmante utiliza para crear la firma digital, están contenidos en la clave privada, que es generada por un proceso matemático, que contiene datos únicos que el firmante utiliza para crear la firma digital. Su conocimiento y control es exclusivo del firmante. Si el firmante decidiera compartirla, se imputará como suyo todo aquello que fuera realizado mediante el uso de la misma.

Artículo 44.- 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 45.- **Reglamento de la ley.** El Poder Ejecutivo reglamentará la presente Ley, en un plazo de noventa días, contados desde su publicación.

Artículo 46.- Derogación. Quedan derogadas todas las disposiciones legales que se opongan a la presente Ley.

Artículo 47.- Comuníquese al Poder Ejecutivo.

Aprobado el Proyecto de Ley por la Honorable Cámara de Diputados, a los ocho días del mes de abril del año dos mil diez, y por la Honorable Cámara de Senadores, a los tres días del mes de junio del año dos mil diez, quedando sancionado el mismo, de conformidad con lo dispuesto en el Artículo 207, numeral 2 de la Constitución Nacional. Objetado totalmente por Decreto del Poder Ejecutivo N° 4.711 del 15 de julio de 2010. Rechazada la objeción total por la H. Cámara de Diputados el nueve de setiembre de 2010 y por la H. Cámara de Senadores, el once de noviembre de 2010, de conformidad con lo establecido en el Artículo 209 de la Constitución Nacional.

Víctor Alcides Bogado González
Presidente
H. Cámara de Diputados

Oscar González Daher
Presidente
H. Cámara de Senadores

Jorge Ramón Ávalos Mariño
Secretario Parlamentario

María Digna Roa Rojas
Secretaria Parlamentaria

Asunción, 23 de diciembre de 2010.

Téngase por Ley de la República, publíquese e insértese en el Registro Oficial.

El Presidente de la República

Fernando Lugo Méndez

Francisco José Rivas Almada
Ministro de Industria y Comercio