Proyecto De Ley nro:559/2010

Extracto:

ADHIERE LA PROVINCIA DEL CHACO A LA LEY 25506 DENOMINADA "LEY DE FIRMA DIGITAL"
Fecha de Presentacion:30/03/10 10:32 Estado: En Trámite-Comisiones
Presentado por:LEGISLATIVO

Autores:

// VP 1:Raffin,Oscar Mateo

Texto(Ultima version):

LA CÁMARA DE DIPUTADOS DE LA PROVINCIA DEL CHACO
SANCIONA CON FUERZA DE LEY

Título Primero
Capítulo Único: Disposiciones Generales

Artículo 1º. Adhesión .Adhiérase la Provincia de Chaco a la Ley 25.506, denominada "Ley de Firma Digital", en las condiciones y términos establecidos en la presente Ley.
Artículo 2º. Concepto. Sin perjuicio de las disposiciones establecidas por la Ley 25.506, y a los fines de la aplicación de las normas contenidas en la presente, entiéndase por Firma Electrónica al conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medios de identificación del firmante. Asimismo, se entenderá por firma digital a la que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
Artículo 3º. Ámbito de aplicación. Las disposiciones establecidas en la presente ley son de aplicación en el ámbito de la Administración Pública Provincial, centralizada y descentralizada, y Poderes Legislativo y Judicial de la Provincia del Chaco, sin perjuicio de las potestades reglamentarias de cada uno.
Artículo 4º. Autoridad de aplicación. Será autoridad de aplicación de la presente ley la Subsecretaría de Coordinación y Gestión Pública, dependiente de la Secretaría General de la Gobernación.
Artículo 5º. Implementación y coordinación. La Autoridad de Aplicación, a través del ProFyM (Programa de Fortalecimiento y Modernización del Estado) llevará a cabo la ejecución de la Firma Digital a través de una implementación gradual y coordinada con los demás Poderes y Jurisdicciones del Estado Provincial, en un marco compatible con las normas nacionales.

Título Segundo
Disposiciones Relativas a la Implementación de la Firma Digital
Capítulo Primero: Sobre Estándares Tecnológicos y de Seguridad

Artículo 6º. Establecimiento de estándares tecnológicos y de seguridad. La Autoridad de Aplicación establecerá los estándares tecnológicos y de seguridad correspondientes, y la modalidad de obtención de los certificados digitales, los procedimientos de firma, verificación, certificación y auditoria, a los fines de la aplicación de las disposiciones contenidas en la presente Ley.
Artículo 7º. Especificaciones de estándares y programas. Los estándares tecnológicos y de seguridad aplicables, los procedimientos de firma, verificación, certificación y auditoría deberán guardar relación con los utilizados en virtud de las disposiciones contenidas en la Ley Nº 25.506 y las disposiciones reconocidas internacionalmente que regulan la materia.

Capítulo Segundo: Del Organismo Certificador y la Autoridad de Registro

Artículo 8º. Organismo Certificador. Cada uno de los poderes del Estado mencionados en el Artículo 3º de la presente norma, podrán designar la Autoridad de Certificación responsable de realizar las certificaciones correspondientes.
Artículo 9º. Autoridad de Registro. Atento las disposiciones contenidas en el Artículo 3º de la presente, la Administración Pública Provincial y los Poderes Legislativo y Judicial podrán disponer de una Autoridad de Registro, con los alcances establecidos en la Ley 25.506, o la que en el futuro la reemplace a los fines de la aplicación de las disposiciones contenidas en la presente Ley.

Proyecto De Ley nro:559/2010

Artículo 10º. Reconocimiento Autoridad de Registro. La Autoridad de Aplicación podrá reconocer certificados de particulares emitidos por certificadores de otras jurisdicciones para la realización de trámites ante la Administración Pública Provincial, Poder Legislativo, Judicial y Municipios adheridos a la presente norma, siempre que los mismos respondan a los estándares establecidos en el artículo 6º de la Presente Ley.
Artículo 11º. Convenios. A los efectos de lo previsto en el Artículo 7º el Poder Ejecutivo Provincial podrá celebrar convenios con otras jurisdicciones para el reconocimiento recíproco de certificados emitidos por certificadores de las mismas.
Los certificados de firmas digitales emitidos por entidades provinciales y extranjeras tendrán la misma validez y eficacia jurídica siempre que los mismos sean reconocidos por la autoridad administrativa competente.
Artículo 12º. Reconocimiento de Firma Digital. A partir de la entrada en vigencia de la presente ley, en aquellos casos en que se establezca el requisito de firma hológrafa del funcionario o autoridad que lo emite, debe entenderse como equivalente el uso de la firma digital, conforme a los términos y bajo las condiciones habilitantes dispuestas por la presente ley y las reglamentaciones que se dicten.

Capítulo Tercero: De la Comisión Asesora

Artículo 13º. Comisión Asesora. Créase en el ámbito del Poder Legislativo Provincial, la Comisión Asesora de la Autoridad de Aplicación para el establecimiento e implementación de la Firma Digital.
Artículo 14º. Integración. La Comisión Asesora estará integrada por siete (7) miembros, y se constituirá de la siguiente manera: Un (1) representante del Poder Ejecutivo Provincial, dos (2) representantes del Poder Legislativo ?un (1) representante del partido mayoritario, y uno (1) de la primera minoría- , un (1) representante del Poder Judicial, un (1) representante de la Universidad Tecnológica Nacional ?Facultad Regional Resistencia-, un (1) representante de la Universidad Nacional del Chaco Austral, y un (1) representante por los Colegios y Consejos de Profesionales que acrediten experiencia profesional en la materia, los que durarán 4 años en sus funciones.
Artículo 15º. Funciones. Son funciones de la Comisión Asesora:
Asistir a la Autoridad de Aplicación en el diseño, implementación y seguimiento de las políticas de Firma Digital, y a los organismos en temas de su competencia, en lineamientos estratégicos y propuestas de normas reglamentarias.
Fomentar la mejora continua en los procesos de implementación de la Firma Digital, promoviendo su utilización en el territorio provincial, y observando que se brinden servicios al ciudadano con calidad, transparencia y accesibilidad a la gestión de gobierno.
Cooperar en la realización de estudios e investigaciones que contribuyan a la mejora y sostenimiento de un Estado eficiente.
Diseñar y conducir planes que aseguren la capacitación estratégica y formación de los recursos humanos en los mecanismos e implementación de la Firma Digital.
Asesorar en temas de su incumbencia a los poderes, municipios o jurisdicciones que lo soliciten.
Otros temas que le sean requeridos por la Autoridad de Aplicación.
Artículo 16º. Fomento de la Firma Digital. El Poder Ejecutivo Provincial, llevará a cabo acciones que promuevan el uso masivo de la Firma Digital en los diferentes organismos y jurisdicciones. Dichas acciones de promoción contarán con el referéndum de la Comisión Asesora creada en el artículo 15º de la presente Ley.

Capítulo Cuarto: Convenios, multas y sanciones

Artículo 17º. Convenios de cooperación y asistencia. El Poder Ejecutivo Provincial, a fin de fomentar y facilitar el uso de la Firma Digital, podrá celebrar convenios de cooperación y asistencia con organismos internacionales, con los demás poderes del estado provincial, entidades de carácter público, y municipios que adhieran a lo establecido por la presente ley.
Artículo 18º. Multas y Sanciones. Se faculta al Poder Ejecutivo Provincial para establecer en la reglamentación un sistema de multas y sanciones ante el incumplimiento de lo dispuesto por la presente ley.
La recaudación que derive de las mismas será utilizada para financiar el fomento de la Firma Digital y el funcionamiento de la Comisión Asesora.

Capítulo Quinto: Disposiciones Finales

Proyecto De Ley nro:559/2010

Artículo 19º. Presupuesto. Cada año se establecerá en la Ley General de Presupuesto la partida presupuestaria necesaria a los fines de la implementación de las prescripciones establecidas en la presente Ley.
Artículo 20º. Reglamentación. El Poder Ejecutivo provincial reglamentará la presente Ley en un plazo no mayor a los ciento ochenta (180) días de su publicación en el Boletín Oficial.
Artículo 21º. Adhesión. Invítese a los Municipios a adherir a la presente Ley.
Artículo 22º. Regístrese y comuníquese al Poder Ejecutivo.

FUNDAMENTOS
CONSIDERACIONES GENERALES

La provincia del Chaco en el marco de la Modernización del Estado no puede permanecer ajena a los avances tecnológicos y al empleo de los nuevos medios que provee el mercado, especialmente cuando contribuye a aumentar la productividad de los organismos (horas/hombre), a optimizar el manejo de la información y reducir los costos de almacenamiento y de traslado de papel.
El impacto que en los últimos años han generado las Tecnologías de Información (TICs) en el mundo moderno ha redefinido las formas y los modos de las relaciones personales e institucionales tanto en el ámbito público como privado. En este caso particular, la utilización de estos novedosos procedimientos tecnológicos permitirá a las diferentes esferas del Estado realizar prácticas más eficiente, eficaces y transparentes.
La tecnología existente en nuestro país en general y en nuestra provincia en particular permite el empleo de "Firma Digital" con la seguridad con que deben contar los documentos digitales, así como el intercambio de información de este tipo.
El mecanismo de la firma electrónica permite probar inequívocamente que una persona firmó un documento digital y que dicho documento no fue alterado desde el momento de su firma, siempre que su implementación se ajuste a los procedimientos y estándares preestablecidos.
La puesta en marcha de un sistema de estas características impone un seguimiento y etapas de evaluación de su impacto en las acciones comprendidas.
Conceptualmente la "Firma Digital" es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, permitiendo que estos gocen de una característica que únicamente era propia de los documentos en papel, es decir, es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje. El principal beneficio es despapelizar la administración pública provincial equiparando la firma de documentos electrónicos con los rubricados en forma manuscrita. La despapelización constituye un objetivo insoslayable en tanto que genera un considerable ahorro de recursos de todo tipo y provoca una relación más estrecha entre la Administración Pública y el ciudadano.
Técnicamente, la firma digital consiste en la utilización de un método de encriptación llamado asimétrico o de clave pública. Este método consiste en establecer un par de claves asociadas a un sujeto, una pública, conocida por todos los sujetos intervinientes en el sector, y otra privada, sólo conocida por el sujeto en cuestión. De esta forma cuando se quiera establecer una comunicación segura con otra parte basta con encriptar el mensaje con la clave pública del sujeto para que a su recepción sólo el sujeto que posee la clave privada pueda leerlo.
La definición de firma digital por sí sola podría conducirnos a suponer que a partir del desarrollo tecnológico, una persona o un grupo de personas pergeñaron un sistema para reemplazar la firma holográfica por un artilugio científico informático, si bien esto es en parte cierto, es sólo el principio de un proceso que reconoce a la "Firma Digital" como la conclusión lógica de la aplicación de las más modernas técnicas de la informática para la simplificación de operaciones comerciales o de cualquier otro tipo, que se inscriben en uno de los tantos aspectos que surgen de la globalización y que deben contar con una indubitable identificación de los integrantes.
Otro aspecto relevante, es el que conforma el universo de la Administración Pública ya que no existe área de los actos humanos que insuma más trámites y confección de formularios que el de las actividades del Estado en general, de esto se desprende que cualquier medida que apunte a lograr la eliminación de papeles, firmas, sellos, más papeles, más firmas y más sellos redundará no sólo en una economía de recursos sino en una agilización antes impensable, esto sin obviar que el campo de la corrupción se ve totalmente acotado.

Proyecto De Ley nro:559/2010

Entre los beneficios que permite la aplicación de la Firma Digital se destacan: la significativa contribución al proceso de "despapelización", equiparando la firma de documentos electrónicos con los rubricados en forma manuscrita; la garantía de autoría e integridad de los documentos digitales; la validez legal a la documentación electrónica, y la introducción de estándares de seguridad en las transacciones electrónicas.
Al tiempo que se aprovechan los beneficios de la tecnología de Firma Digital para mejorar la gestión del Estado, la difusión de su uso fomenta su adopción en otros sectores tanto de la administración pública como en el sector privado, (ejemplo: el bancario, la salud, el comercio nacional e internacional). Por lo que se hace necesaria la existencia de autoridades certificantes que convaliden la Firma Digital.
La firma digital traerá la posibilidad de hacer trámites públicos de toda índole a través de Internet, ya que hoy día el Estado cuenta con múltiples portales de Internet los que permiten hacer gestiones desde su propia casa u oficina. Ello permitirá impulsar con más profundidad y decisión el Gobierno electrónico al servicio del ciudadano.
Otra ventaja de la misma es su portabilidad, es decir, la firma digital puede ser realizada en diferentes puntos dentro del territorio provincial de forma simultánea y sin necesidad de testigos.
Además, tiende a aumentar la transparencia de los procesos de licitación del Estado hechos por la vía electrónica. Ello ayudará a la creación de nuevos mercados, generará redes productivas más ágiles entre diversas empresas e introducirá mayor eficiencia en sectores público y privado, produciendo significativos avances en materias de productividad.

ANTECEDENTES INTERNACIONALES Y NACIONALES

La enumeración de los siguientes organismos, instituciones internacionales y países que oportunamente se han pronunciado sobre la "Firma Digital" es de importancia:
En primer lugar debemos citar a la Comisión de las Naciones Unidas para el Derecho Comercial Internacional (UNCITRAL) que aprobó una Ley-Modelo sobre Comercio Electrónico y comenzó a trabajar en la preparación de normas uniformes en materia de firma digital, cuyas directivas han sido tomadas como base por la mayoría de los países latinoamericanos que legislaron en la materia, por su ductilidad para adaptarse a sus necesidades. Fue aprobada en la 85a. Sesión Plenaria de la Asamblea General de las Naciones Unidas, celebrada el 16 de diciembre de 1996, aprobada la Resolución No. 51/162,
A continuación surgió la Directiva 1999/93/CE del Parlamento Europeo y del Consejo del 13/12/99 por la que se estableció un marco comunitario para la firma electrónica.
En cuanto a países, España fue uno de los países que se pronunció al respecto, contando hoy en día con una legislación muy avanzada, sumándose Francia, Portugal, Finlandia, Panamá, Colombia, México, Costa Rica, Venezuela, Brasil, República Dominicana, Guatemala y Chile.
A esta lista hay que sumar a Alemania, Pakistán, Nueva Zelanda, República Dominicana, República de Corea, India, Ecuador, Taiwán, Australia, Canadá, Japón, Marruecos, Reino Unido y Estados Unidos.
En el ámbito del MERCOSUR hay dos Resoluciones: Nº 34/06 - Directrices para la celebración de acuerdos de reconocimiento mutuo de firmas electrónicas avanzadas en el ámbito del MERCOSUR y Nº 37/06 - Reconocimiento de la eficacia jurídica del documento electrónico, la firma electrónica y firma electrónica avanzada en el ámbito del MERCOSUR.
Ahora sí podemos abordar una somera síntesis de cómo se llega a la "Firma Digital" de nuestro país.
Entre los primeros antecedentes que reconoce nuestra legislación se encuentra el decreto 427/98, hoy derogado, por el cual se aprueba la infraestructura de Firma Digital para el Sector Público Nacional.
En éste, se trabajaba sobre los antecedentes que aportan legislaciones como la española que ha desarrollado ampliamente la "Firma Digital".
Es pertinente puntualizar que este decreto se generó en el ámbito de la Administración Pública y para los actos de su incumbencia, es decir, se tomó esto como el punto de partida de una metodología que debería concluir con una despapelización de la administración pública nacional.
En el año 2001, finalmente, se aprobó la ley Nº 25506 de Firma Digital, vigente en la actualidad y reglamentada por el Decreto Nacional 2628/2002. En dicha norma se establecen los principios rectores para la implementación de la Firma Digital y se invita a las provincias a adherir a los mismos, acto que se está llevando a cabo a través del presente proyecto.

ANTECEDENTES DE LEGISLACIÓN PROVINCIAL y MUNICIPAL

Proyecto De Ley nro:559/2010

Desde el año 2003 las provincias argentinas comenzaron a adherirse a la Ley Nacional. Actualmente las adheridas son: La Pampa, Tucumán, Mendoza, Tierra del Fuego, San Luis, Formosa, Jujuy, Río Negro, Chubut, Santa Fe, Buenos Aires, Córdoba, Neuquén, Misiones, Ciudad de Buenos Aires, Corrientes y Salta.
También regulan sobre este tema los municipios de Allen y Rosario.

COROLARIO
La necesidad de adhesión a la Ley 25.506 es consecuencia directa de representar, al menos, la primera parte de la citada norma, en lo que se refiere a la equiparación funcional normativa al instrumento digital electrónico o documento digital firmado electrónicamente, lo que es sin duda alguna materia referida a la delegación de facultades legislativas efectuada al gobierno federal por parte de las provincias, y guarda congruencia con las disposiciones del artículo 75 inciso 12 de nuestra Carta Magna.
Sin embargo, consideramos que no constituye materia delegada por las provincias los aspectos vinculados al procedimiento administrativo o judicial. En este sentido, que la firma digital sea efectuada sobre la base de certificados emitidos por certificadores estatales o en libre competencia, sin lugar a dudas es un procedimiento administrativo, así como la normativa vinculada a la fijación jurisdiccional de los conflictos y definición de autoridades certificadoras o de registro, según las disposiciones contenidas en el artículo 121º de la Constitución Nacional.
Estas consideraciones fundamentan la necesidad de dotar a la Provincia de Chaco de una herramienta normativa que permita adaptar las previsiones contenidas en la Ley 25.506, con las particularidades que deben adoptarse atento su vigencia en el ámbito provincial.
Las nuevas tecnologías constituyen aportes significativos para un avance decisivo en pos de profundizar el desarrollo de nuevos canales de comunicación y vinculación entre gobierno, administración pública y ciudadanía, nuestra provincia en consecuencia no debería estar al margen de esta importante cuestión. Es por ello que solicito la aprobación del presente proyecto de ley.

Antecedentes:

Antecedentes (PROV.) - Informacion Parlamentaria
1) PROYECTOS Nº 2554/04, 1924/05 Y 186/07.-
Antecedentes (PROV.) - Informacion Parlamentaria
2) PROYECTOS Nº 1260/07, 2124/07 Y 494/10.-
Antecedentes - Biblioteca Legislativa
1) FO-BL- REF 4

SERVICIO DE REFERENCIA

PROYECTO: Ley Nº 559/2010 AUTOR: Raffín, O. FECHA: 30/03/2010

SÍNTESIS: Adhesión de la Provincia del Chaco a la ley 25506 denominada "ley de Firma Digital"

LEGISLACIÓN PROVINCIAL

BUENOS AIRES
Ley 13666 Firma Digital. Ley de Firma Digital. Adhesión. Implementación. Organismo Certificador. Alcance. Convenios. (Información obtenida de Abeledo Perrot Online).-

BUENOS AIRES (CIUDAD)
Ley 2751 Firma Digital. Ley de Firma Digital. Adhesión. (Información obtenida de Abeledo Perrot Online).-

CHUBUT
Ley 5366 Firma Digital. Ley de Firma Digital. Adhesión. (Información obtenida de Abeledo Perrot Online).-

CÓRDOBA

Proyecto De Ley nro:559/2010

Ley 9401 Firma Digital. Ley de Firma Digital. Adhesión. (Información obtenida de Abeledo Perrot Online).-

CORRIENTES
Ley 5878 Firma Digital. Administración Pública. Ley Nacional de Firma Digital. Adhesión. Sector Público. Utilización. Autorización. (Información obtenida de Abeledo Perrot Online).-

FORMOSA
Ley 1454- Firma digital -- Adhesión de la Provincia a la ley nacional 25.506. (Información obtenida de La Ley Online).-

JUJUY
Ley 5425 - Ley de firma digital -- Adhesión de la Provincia a la ley nacional 25.506. (Información obtenida de La Ley Online).-

LA PAMPA
Ley 2073 - Firma digital -- Facultad al Poder Ejecutivo a instrumentar los recaudos necesarios para la operatividad de la ley nacional 25.506 en la Provincia. (Información obtenida de La Ley Online).-

MENDOZA
Ley 7234 - Firma digital -- Adhesión de la Provincia a la ley nacional 25.506. (Información obtenida de La Ley Online).-

MISIONES
Ley 4449 - Firma Digital. Ley de Firma Digital. Adhesión. (Información obtenida de Abeledo Perrot Online).-

NEUQUÉN
Ley 2578 Firma Digital. Ley de Firma Digital. Adhesión. (Información obtenida de Abeledo Perrot Online).-

RÍO NEGRO
Ley 3997 Firma Digital. Firma Digital y Firma Electrónica. Régimen. Objeto. Exclusiones. (Información obtenida de Abeledo Perrot Online).-

SAN LUIS
Ley V-591-2007 (591-2007) Firma Digital. Ley de Firma Digital. Adhesión. Implementación. Autoidad de Aplicación. Alcance. (Información obtenida de Abeledo Perrot Online).-

TIERRA DEL FUEGO, ANTÁRTIDA E ISLAS DEL ATLÁNTICO SUR
Ley 633 - Ley de firma digital -- Adhesión de la provincia a la ley nacional 25.506. (Información obtenida de La Ley Online).-

TUCUMÁN
Ley 7291 - Sumario: Firma digital -- Adhesión de la Provincia a la ley nacional 25.506. (Información obtenida de La Ley Online).-

LEGISLACIÓN COMPARADA
COSTA RICA
Decreto Legislativo N.º 8454- Ley de Certificados, Firmas Digitales y Documentos Electrónicos. (Información obtenida de http://asamblea.racsa.co.cr/ley/leyes/8000/L-8454.doc).-

ESPAÑA
Ley 59/2003 de 19 de diciembre, Firma electrónica. (Información obtenida de http://www.boe.es/aeboe/consultas/bases_datos/act.php?c=3&item=2003/23399).-
Antecedentes - Biblioteca Legislativa
   2) BUENOS AIRES

Proyecto De Ley nro:559/2010

LEY 13666
FIRMA DIGITAL
Ley de Firma Digital. Adhesión. Implementación. Organismo Certificador. Alcance. Convenios

sanc. 12/04/2007; promul. 02/05/2007; publ. 15/05/2007

El Senado y Cámara de Diputados de la provincia de Buenos Aires, sancionan con fuerza de ley:

Art. 1. La Provincia de Buenos Aires adhiere a la ley nacional 25506, Ley de Firma Digital en los términos del art. 50 Ver Texto de dicho cuerpo legal, en sus caps. I a IV, V en su art. 26 Ver Texto , VII, IX y Anexo, en las condiciones y términos dispuestos en la presente ley.

Art. 2. Las disposiciones de la presente ley serán de aplicación en el Poder Ejecutivo, Legislativo y Judicial, los Municipios, la Administración Centralizada y Descentralizada, los Organismos de la Constitución, Entes Autárquicos y todo otro Ente en que el Estado provincial o sus Organismos Descentralizados tengan participación suficiente para la formación de sus decisiones.

TÍTULO II (*):
DE LOS ESTÁNDARES TECNOLÓGICOS Y DE SEGURIDAD
(*) Sic B.O.
Art. 3. Para la implementación de las disposiciones de la ley 25506 Ver Texto sobre la digitalización de los trámites y procedimientos de la Administración Pública Provincial, la Autoridad de Aplicación establecerá los estándares tecnológicos y de seguridad aplicables, los procedimientos de firma, verificación, certificación y auditoría, de acuerdo a lo establecido en el art. 4 Ver Texto .

Art. 4. Especificaciones de estándares y programas. Los estándares tecnológicos y de seguridad aplicables, los procedimientos de firma, verificación, certificación y auditoría deberán ser consecuentes con los utilizados por el Gobierno Nacional y las regulaciones internacionales.

TÍTULO III:
DEL ORGANISMO CERTIFICADOR
Art. 5. El Poder Ejecutivo Provincial, designará el (o los) Organismos de la Administración Pública que actuarán como certificador para el ámbito de aplicación descrito en el art. 2 Ver Texto . El Organismo Certificador previa autorización de la Autoridad de Aplicación, podrá inscribirse como certificador licenciado en los términos de la ley nacional 25506 Ver Texto y decreto reglamentario nacional 2628/2002 Ver Texto . Para el cumplimiento de las responsabilidades a su cargo, el Organismo Certificador deberá delegar en Autoridades de Registro las funciones de validación de identidad y otros datos de los suscriptores de certificados y de registros, de las presentaciones y trámites que le sean formuladas.

Art. 6. Conforme a lo normado en el art. 2 Ver Texto y a los efectos de lo previsto en el último párrafo del art. 5 Ver Texto , cada Poder establecerá en el ámbito de su competencia una Autoridad de Registro, con las características que determine, y con los alcances que para la Autoridad de Registro se estipulan en la ley 25506 Ver Texto , su decreto reglamentario 2628/2002 Ver Texto y lo dispuesto por el Poder Ejecutivo Provincial a tal fin.

TÍTULO IV:
DEL ALCANCE DE LA CERTIFICACIÓN Y CONVENIOS
Art. 7. Las certificaciones para agentes de la Administración Pública Provincial y Municipal, destinados a la gestión interna de los Organismos, y la Certificación de particulares para cumplimiento de trámites ante la Administración Pública Provincial y Municipal, con la correspondiente emisión de la clave pública, serán emitidas por el Organismo Provincial de acuerdo al procedimiento que se establezca en orden a lo expresado en el artículo anterior. Sin perjuicio de ello, la Autoridad de Aplicación podrá reconocer certificados de particulares emitidos por certificadores de otras jurisdicciones para la realización de trámites ante la Administración Pública Provincial y Municipal.

Art. 8. A los efectos de lo previsto en el último párrafo del art. 7 Ver Texto la Autoridad de Aplicación

Proyecto De Ley nro:559/2010

podrá firmar convenios con otras jurisdicciones para el reconocimiento recíproco de certificados emitidos por certificadores de las mismas.

Art. 9. Luego del reconocimiento recíproco de certificados entre jurisdicciones, los Organismos comprendidos en el art. 2 Ver Texto deberán aceptar los certificados emitidos por las autoridades certificantes reconocidas por la Autoridad de Aplicación de la Provincia, sujeto a las condiciones de validez establecidas en el art. 9 Ver Texto de la ley nacional 25506 y a las que establezca el decreto reglamentario provincial.

Art. 10. A los fines de instalar en forma efectiva y progresiva el expediente digital, autorízase al Poder Ejecutivo a dictar un reglamento para tal fin, que contemple excepciones al régimen previsto en los caps. VII y VIII del decreto ley 7647/1970 Ver Texto .

Art. 11. En todos los casos donde la Ley de Procedimientos Administrativo establezca que los actos administrativos deban manifestarse por escrito deben contener la firma (ológrafa) de la autoridad que lo emite, debe entenderse que los documentos digitales firmados mediante Firma Digital conforme a los términos y bajo las condiciones habilitantes dispuestas por la presente ley y las reglamentaciones vigentes, cumplirá con los requisitos de escritura y firma antes especificados.

Art. 12. El Poder Ejecutivo determinará el Organismo que cumplirá la función de Autoridad de Aplicación de la presente ley.

Art. 13. Comuníquese, etc.

Passaglia - Giannettasio - Chaves - Rodríguez

NORMAS CITADAS: LN 25506: LA 2001-D-4722 - DN 2628/2002: LA 2002-D-4965.
Antecedentes - Biblioteca Legislativa
3) BUENOS AIRES (CIUDAD)

LEY 2751
FIRMA DIGITAL
Ley de Firma Digital. Adhesión

sanc. 12/06/2008; promul. 10/07/2008; publ. 15/07/2008

La Legislatura de la Ciudad Autónoma de Buenos Aires sanciona con fuerza de ley:

Art. 1. Adhiérese a la ley nacional 25506 (B.O. 14/12/2001) de Firma Digital conforme lo establece su art. 50 Ver Texto .

Art. 2. El Poder Ejecutivo de la Ciudad Autónoma de Buenos Aires debe dictar las normas reglamentarias y los actos administrativos tendientes a la implementación de la ley nacional 25506 Ver Texto y la creación de la Infraestructura de Firma Digital en el ámbito de la Ciudad de Buenos Aires.

Art. 3. La Jefatura de Gabinete de Ministros del Gobierno de la Ciudad Autónoma de Buenos Aires es la Autoridad de Aplicación de la presente ley.

Art. 4. Comuníquese, etc.

Santilli - Pérez
AR_LA002
Antecedentes - Biblioteca Legislativa
4) CHUBUT

LEY 5366
FIRMA DIGITAL

Proyecto De Ley nro:559/2010

Ley de Firma Digital. Adhesión

sanc. 05/07/2005; promul. 12/07/2005; publ. 18/07/2005

Art. 1. Adherir a la ley 25506 Ver Texto -de Firma Digital- sancionada por el Congreso de la Nación.

Art. 2. Autorízase al empleo de la firma digital, en todas las dependencias de los tres Poderes del Estado provincial.

Art. 3. El Estado provincial 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.

Art. 4. Ley general. Comuníquese al Poder Ejecutivo.

Vargas - Martoccia
Antecedentes - Biblioteca Legislativa
5) CÓRDOBA

LEY 9401
FIRMA DIGITAL
Ley de Firma Digital. Adhesión

sanc. 04/07/2007; promul. 13/07/2007; publ. 19/07/2007

La Legislatura de la Provincia de Córdoba sanciona con fuerza de ley:

Art. 1. Adhiérese la Provincia de Córdoba a la ley nacional 25506 "Ley de Firma Digital", en los términos del art. 50 Ver Texto de dicho cuerpo legal.

Art. 2. El Poder Ejecutivo determinará la Autoridad de Aplicación de la presente ley dentro de la Administración Pública Provincial, la que tendrá a su cargo establecer los estándares tecnológicos y de seguridad correspondientes y la modalidad de obtención de los certificados digitales.

Art. 3. Autorízase al Poder Ejecutivo Provincial a suscribir con los organismos correspondientes del Poder Ejecutivo Nacional los convenios y demás documentación necesaria a los fines de la implementación de la firma digital en el ámbito de la Provincia de Córdoba.

Art. 4. Comuníquese al Poder Ejecutivo Provincial.

Arias - Fortuna
Antecedentes - Biblioteca Legislativa
6) CORRIENTES

LEY 5878
FIRMA DIGITAL
ADMINISTRACIÓN PÚBLICA
Ley Nacional de Firma Digital. Adhesión. Sector Público. Utilización. Autorización

sanc. 06/05/2009; promul. 01/06/2009; publ. 05/06/2009

El Honorable Senado y la Honorable Cámara de Diputados de la provincia de corrientes, sancionan con fuerza de ley:

Art. 1. Adhiérese la Provincia de Corrientes, a la ley nacional 25506 Ver Texto , de Firma Digital.

Proyecto De Ley nro:559/2010

Art. 2. Autorizase el empleo de la Firma Digital, en todas las dependencias del Poder Ejecutivo Provincial.

Art. 3. El Poder Ejecutivo Provincial 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 cinco (5) 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 decretos, resoluciones y decisiones administrativas en general, emanados de las jurisdicciones y entidades comprendidas en el art. 2 Ver Texto de la presente ley.

Art. 4. El Poder Ejecutivo deberá reglamentar la presente ley dentro de los ciento ochenta (180) días de su publicación en el Boletín Oficial de la Provincia.

Art. 5. Comuníquese al Poder Ejecutivo.- Dada en la Sala de Sesiones de la Honorable Legislatura de la Provincia de Corrientes, a los seis días del mes de mayo de dos mil nueve.

Pruyas - Mathó - Giorasi - Karsten
AR_LA002
Antecedentes - Biblioteca Legislativa
7) FORMOSA

LEY 1454
Firma digital -- Adhesión de la Provincia a la ley nacional 25.506.

Fecha de Sanción: 26/08/2004

Fecha de Promulgación: 10/09/2004

Publicado en: Boletín Oficial 23/09/2004 - ADLA 2004 - E, 6122

Art. 1° - Adhiérese la Provincia de Formosa a la Ley Nacional 25.506 de firma digital.

Art. 2° - Autorízase el empleo de la Firma Digital en todas las dependencias del Poder Ejecutivo Provincial.

Art. 3° - Se promoverá el uso masivo de la Firma Digital de tal forma que se posibilite el trámite de los expedientes por vías simultáneas búsquedas automáticas de la información, seguimiento y control por parte del interesado propendiendo a la progresiva despapelización.

Art. 4° - El Poder Ejecutivo provincial deberá reglamentar la presente ley determinando la autoridad de aplicación y sus funciones.

Art. 5° - Se faculta al Poder Ejecutivo Provincial a designar el ente licenciante que ejercerá el contralor de la expedición de licencia a los certificadores digitales en el ámbito provincial.

Art. 6° - Comuníquese, etc.

Antecedentes - Biblioteca Legislativa
8) JUJUY

LEY 5425

Sumario: Ley de firma digital -- Adhesión de la Provincia a la ley nacional 25.506.

Proyecto De Ley nro:559/2010

Fecha de Sanción: 19/08/2004

Fecha de Promulgación: 07/09/2004

Publicado en: Boletín Oficial 22/09/2004 - ADLA 2005 - A, 1070

Art. 1º - Adhiérase la Provincia de Jujuy a las disposiciones de la Ley Nacional Nº 25.506 "De Firma Digital".

Art. 2º - Comuníquese, etc.

Antecedentes - Biblioteca Legislativa
9) LA PAMPA

LEY 2073

Sumario: Firma digital -- Facultad al Poder Ejecutivo a instrumentar los recaudos necesarios para la operatividad de la ley nacional 25.506 en la Provincia.
Fecha de Sanción: 09/10/2003

Fecha de Promulgación: 21/10/2003

Publicado en: Boletín Oficial 31/10/2003 - ADLA 2003 - E, 5723

Art. 1° - Facúltase al Poder Ejecutivo a instrumentar los recaudos que sean necesarios a los efectos de estabelcer la operatividad en la Provincia de La Pampa de la ley nacional 25.506 "Ley de Firma Digital".

Art. 2° - Comuníquese, etc.

Antecedentes - Biblioteca Legislativa
10) MENDOZA

LEY 7234

Sumario: Firma digital -- Adhesión de la Provincia a la ley nacional 25.506.

Fecha de Sanción: 29/06/2004

Fecha de Promulgación: 16/07/2004

Publicado en: Boletín Oficial 04/08/2004 - ADLA 2004 - D, 5068

Art. 1° - La Provincia de Mendoza adhiere a la Ley 25.506 - de Firma Digital- sancionada por el Honorable Congreso de la Nación.

Art. 2° - Autorízase el empleo de la Firma Digital, en todas las dependencias del Poder Ejecutivo Provincial.

Art. 3° - El Poder Ejecutivo Provincial 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 cinco (5) 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 decretos, resoluciones y decisiones administrativas en general, emanados de las jurisdicciones y entidades comprendidas en el Art. 2° de la presente ley.

Proyecto De Ley nro:559/2010

Art. 4° - El Poder Ejecutivo deberá reglamentar esta ley en un plazo no mayor a ciento ochenta (180) días de su publicación en el Boletín Oficial de la Provincia.

Art. 5° - Comuníquese, etc.

Antecedentes - Biblioteca Legislativa
11) MISIONES

LEY 4449
FIRMA DIGITAL
Ley de Firma Digital. Adhesión

sanc. 04/09/2008; promul. 19/09/2008; publ. 22/09/2008

La Cámara de Representantes de la Provincia de Misiones sanciona con fuerza de ley:

Art. 1. Adhiérese la Provincia de Misiones a la ley nacional 25506 Ver Texto -Ley de Firma Digital-.

Art. 2. La presente adhesión se efectúa con expresa reserva de jurisdicción, legislación, ejecución y control de las competencias que le corresponden a la provincia de Misiones y a los municipios que la conforman.

Art. 3. El Poder Ejecutivo determinará en la reglamentación la autoridad de aplicación de la presente Ley.

Art. 4. Invítase a los municipios a adherir a la presente ley.

Art. 5. Comuníquese al Poder Ejecutivo.

Rovira - Britto A/C
AR_LA002
Antecedentes - Biblioteca Legislativa
12) NEUQUÉN

LEY 2578
FIRMA DIGITAL
Ley de Firma Digital. Adhesión

sanc. 24/04/2008; promul. 09/05/2008; publ. 23/05/2008

La Legislatura de la Provincia del Neuquén sanciona con fuerza de ley:

Art. 1. Adhiérase a la ley nacional 25506 Ver Texto , de Firma Digital, sus modificatorias y normas reglamentarias que en su consecuencia se dicten.

Art. 2. La presente adhesión se efectúa con expresa reserva de jurisdicción, legislación, ejecución y control de las competencias que le correspondan a la Provincia del Neuquén y a los municipios que la integran.

Art. 3. Facúltase al Poder Ejecutivo provincial para determinar la autoridad de aplicación y reglamentar la presente, debiendo hacerlo en un plazo no mayor a los ciento ochenta (180) días desde la publicación en el Boletín Oficial de la Provincia.

Art. 4. Las disposiciones de la presente ley serán de aplicación en el ámbito del sector privado como así

Proyecto De Ley nro:559/2010

también en toda la jurisdicción del sector público provincial, el cual comprende la Administración centralizada y descentralizada, los entes autárquicos y todo otro ente en que el Estado provincial o sus organismos descentralizados tengan participación suficiente para la formación de sus decisiones.

Art. 5. Invítase a los municipios de la Provincia del Neuquén a efectuar similares adhesiones en el ámbito de sus respectivas jurisdicciones.

Art. 6. Autorízase a emplear la firma digital o la firma electrónica en losactos internos de la Administración Pública provincial y en aquellos actos que excediendo la órbita interna se celebren con instituciones, organismos o cualquier otro tipo de entes públicos o privados.

Art. 7. La Administración Pública en general, y la autoridad de aplicación en particular, deberán promover el uso de la firma digital.

Art. 8. Resérvase el derecho de aplicar cualquier tipo de gravamen que se estime conveniente sobre el empleo de la firma digital, en tanto no se oponga a lo establecido por la Constitución nacional Ver Texto , pudiendo ser éste de origen temporal o permanente.

Art. 9. A los efectos de la aplicación de esta ley, el Gobierno reconocerá como certificador licenciado a aquellos que contando con la aprobación nacional se avengan a encuadrarse en la presente ley, sus modificatorias y reglamentaciones.

Art. 10. Los certificadores licenciados que se desempeñen fuera de la órbita de la Administración Pública lo harán en términos de libre competencia, debiendo incluirse dentro de la reglamentación de la presente la delimitación de cupos, áreas geográficas o cualquier otro tipo de segmentación que asegure que los eventuales usuarios estarán debidamente protegidos por la legislación en materia de defensa del consumidor.

Art. 11. La autoridad de aplicación establecerá un sistema de registro, métodos y mecanismos para la evaluación y constatación de la confiabilidad, integridad, confidencialidad y disponibilidad de los esquemas utilizados por los registrados para la realización de identificaciones fehacientes dentro del marco de la infraestructura de firma digital.

Art. 12. Resérvase el derecho de adoptar todo cambio tecnológico que no oponiéndose a la ley nacional ni a los estándares internacionales, tienda a optimizar, adecuar y ampliar el uso de la firma digital.

Art. 13. La autoridad de aplicación, sin perjuicio de lo que indiquen las leyes tanto penales como civiles, establecerá un sistema de multas y sanciones para quienes incumplan con los métodos y mecanismos dispuestos por la presente, la ley 25506 Ver Texto , sus modificatorias y normas reglamentarias.

Art. 14. La autoridad de aplicación constatará el cumplimiento de la ley nacional 25326 Ver Texto , de Hábeas Data.Art. 15.- La presente ley, sus modificaciones y reglamentaciones no podrán interpretarse o aplicarse en un sentido que genere algún tipo de discriminación que afecte tanto a personas de la tercera edad, de bajos recursos o aquellas que puedan padecer algún tipo de capacidades diferentes, debiendo la autoridad de aplicación tomar los recaudos pertinentes.

Art. 16. Comuníquese al Poder Ejecutivo.

González - Zingoni
AR_LA002
Antecedentes - Biblioteca Legislativa
13) RÍO NEGRO

LEY 3997 (*)
FIRMA DIGITAL
Firma Digital y Firma Electrónica. Régimen. Objeto. Exclusiones

Proyecto De Ley nro:559/2010

sanc. 29/09/2005; promul. 12/10/2005; publ. 20/10/2005

(*) Esta norma ha sido consolidada por ley 4270 Ver Texto (sanc. 29/11/2007; promul. 21/12/2007; publ. 10/01/2008).

La Legislatura de la provincia de Río Negro sanciona con fuerza de ley:

Art. 1. La provincia de Río Negro, interpretando el art. 50 Ver Texto de la ley nacional 25506, adhiere a la misma en general invocando para ello lo previsto en el inc. 2 del art. 12 Ver Texto de la Constitución provincial.

Art. 2. Se faculta al gobernador para que nombre a la autoridad de aplicación de la presente ley.

Art. 3. El Poder Ejecutivo deberá reglamentar en un plazo no mayor a los ciento ochenta (180) días de promulgada la presente, la respectiva reglamentación. Dichos plazos correrán desde la publicación en el Boletín Oficial de la provincia.

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

Art. 5. Se crea en el ámbito de la provincia de Río Negro la Comisión Asesora Multidisciplinaria para la puesta en marcha y seguimiento de la aplicación de la presente ley.

Art. 6. La Comisión Asesora estará integrada por ocho (8) miembros de los cuales dos (2) serán legisladores, dos (2) representantes del Poder Ejecutivo, uno (1) designado por la Subsecretaría de Ciencia y Tecnología, dos (2) del Poder Judicial y dos (2) serán expertos en informática, especialmente en claves públicas y privadas y sistemas de encriptación asimétrica, designados por el Poder Ejecutivo y que no tendrán ningún tipo de vínculo con el Gobierno. Todos los integrantes de esta Comisión se ajustarán a lo siguiente:
a) La Comisión Asesora tendrá ese carácter y deliberará y se pronunciará reportando a la autoridad de aplicación.
b) La Comisión Asesora se dictará su propio reglamento de responsabilidades y funciones, el que no se podrá apartar de lo que la reglamentación de la ley dicte como así también las instrucciones de la autoridad de aplicación.
c) A solicitud de simple mayoría de sus miembros podrá pedir a la autoridad de aplicación incrementar el número de integrantes o conseguir el auxilio de profesionales que, a juicio de la comisión, sea necesario para dilucidar cuestiones de su competencia.
d) Las designaciones y remociones deberán ser todas aprobadas por la Legislatura de la provincia de Río Negro, incluyendo a los representantes de ese cuerpo gubernamental.
e) La duración en sus funciones será de dos (2) años y podrán continuar en sus cargos mientras la autoridad de aplicación así lo estime conveniente.
f) Todos los cargos en la Comisión Asesora serán ad honorem y los reemplazos que se estimen realizar se ajustarán a las directivas de la autoridad de aplicación y al reglamento que la comisión se dicte.
g) Se exceptúa de lo prescripto en el inciso anterior a los expertos en informática. Será facultad de la autoridad de aplicación la modalidad de contratación de los mismos.
h) La Comisión Asesora, a iniciativa propia o de terceros, propondrá a la autoridad de aplicación normas en el plano jurídico, en el de la puesta en marcha en el ámbito de la Administración Pública, en el de las contrataciones por parte del Gobierno, en el de los sistemas de interacción entre reparticiones nacionales y de la provincia, en la estandarización y la adecuación a cambios fruto de la experiencia y en la implementación en la órbita de las actividades de los particulares.
i) La comisión trabajará en forma permanente y de acuerdo a su reglamento, no obstante la misma tendrá la obligación de producir informes periódicos a la autoridad de aplicación, siendo también responsabilidad de su área la difusión de sus acciones ante quien lo reclame.

Art. 7. Se autoriza a emplear la firma digital o en su defecto la firma electrónica en los actos internos de

Proyecto De Ley nro:559/2010

la Administración Pública provincial y en aquellos actos que excediendo la órbita interna se celebren con instituciones, organismos o cualquier otro tipo de institución con los que exista convenio de reciprocidad o que ya tengan sancionada una norma legal de adhesión a la ley 25506 Ver Texto . También se regirá por este artículo el intercambio de información institucional.

Art. 8. Una vez puesta en marcha la presente ley, la Administración Pública en general y la autoridad de aplicación en particular, llevarán adelante toda clase de medidas que propugnen la aplicación de la firma digital orientándose a la despapelización.

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

Art. 10. A los efectos de la aplicación de esta ley, el Gobierno reconocerá como certificador licenciado a aquéllos que contando con la aprobación nacional (art. 17 Ver Texto del cap. III de la ley 25506) se avengan a encuadrarse en la presente ley.

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

Art. 12. La autoridad de aplicación, con el concurso de la Comisión Asesora para la puesta en marcha y seguimiento de la firma digital, sin perjuicio, de lo establecido en la ley 25506 Ver Texto , establecerá un sistema de registro, métodos y mecanismos para la evaluación y constatación de la confiabilidad, integridad, confidencialidad y disponibilidad de los esquemas utilizados por los registrados para la realización de identificaciones fehacientes dentro del marco de la infraestructura de firma digital.

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

Art. 14. La autoridad de aplicación, sin perjuicio de lo que indiquen las leyes tanto penales como civiles, establecerá un sistema de multas y sanciones para quienes incumplan con los métodos y mecanismos dispuestos por la autoridad de aplicación.
En este sentido, la autoridad de aplicación se subrogará el derecho de informar a la autoridad de aplicación nacional el resultado de los controles realizados.

Art. 15. Dado que la aplicación de la presente ley tiene directas implicancias sobre la identificación de las personas, la autoridad de aplicación constatará el cumplimiento de la ley nacional 25326 Ver Texto (Protección de datos personales) ya que la misma se encuadra en lo prescripto por el art. 20 Ver Texto de la Constitución de la provincia. Por ello, será su obligación la de informar a la Dirección Nacional de Protección de Datos Personales, los incumplimientos constatados que pudieran derivar en perjuicios de índole particular.

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

Art. 17. Comuníquese al Poder Ejecutivo y archívese.

De Rege - Medina

Proyecto De Ley nro:559/2010

NORMAS CITADAS:Normas Citadas: Const. Prov.: LA 1988-B-2907 - LN 25326: LA 2000-D-4363 - LN 25506: LA 2001-D-4722.
AR_LA002
Antecedentes - Biblioteca Legislativa
14) SAN LUIS
LEY V-591-2007 591-2007
FIRMA DIGITAL
Ley de Firma Digital. Adhesión. Implementación. Autoidad de Aplicación. Alcance

sanc. 28/11/2007; promul. 19/12/2007; publ. 21/12/2007

El Senado y la Cámara de Diputados de la Provincia de San Luis sancionan con fuerza de ley:

ADHESIÓN A LA LEY NACIONAL 25506 -FIRMA DIGITAL
Art. 1. La Provincia de San Luis, adhiere a la ley nacional 25506 Ver Texto Firma Digital- sancionada por el Honorable Congreso de la Nación, instrumentando los recaudos necesarios para establecer dentro de su jurisdicción la operatividad de los actos y mecanismos previstos en el cap. I a IV de la Ley de referencia.

Art. 2. Las disposiciones de la presente ley serán de aplicación en el ámbito del sector privado así como en toda la jurisdicción del sector público provincial, el cual comprende los Municipios, la Administración Centralizada y Descentralizada, los Organismos de la Constitución, los Entes Autárquicos y todo otro Ente en que el Estado Provincial o sus organismos descentralizados tengan participación suficiente para la formación de sus decisiones. Su aplicación incluye al Poder Ejecutivo, al Poder Legislativo y al Poder Judicial.

Art. 3. Se autoriza a emplear la firma digital o en su defecto la firma electrónica en los actos internos de la Administración Pública Provincial y en aquellos actos que excediendo la órbita interna se celebren con instituciones, organismos o cualquier otro tipo de institución con los que exista convenio de reciprocidad o que ya tengan sancionada una norma legal de adhesión a la ley nacional 25506 Ver Texto . También se regirá por este Artículo el intercambio de información institucional.

Art. 4. El Poder Ejecutivo Provincial promoverá el uso masivo de la firma digital en el ámbito del sector público de tal modo que facilite la tramitación de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a la progresiva despapelización.

Art. 5. Se faculta al Poder Ejecutivo para que establezca la Autoridad de Aplicación de la presente ley.

Art. 6. La Autoridad de Aplicación que se designe en virtud de la reglamentación de la presente ley estará facultada para requerir asesoría técnica y jurídica especializada mediante la solicitud de dictámenes que carecerán de valor vinculante.

Art. 7. Se faculta al Poder Ejecutivo a designar al Ente Licenciante que ejercerá el contralor de la expedición de licencias a los Certificadores Licenciados en el ámbito provincial.

Art. 8. A los efectos de la aplicación de la presente ley, el gobierno reconocerá como Certificador Licenciado a aquéllos que contando con la aprobación nacional se avengan a encuadrarse en la normativa que regula la infraestructura de firma digital de la Provincia de San Luis.

Art. 9. La Provincia de San Luis se reserva el derecho de aplicar cualquier tipo de gravamen que estime conveniente al empleo de firma digital en tanto no se oponga a lo establecido por el Gobierno Nacional, pudiendo ser éste de origen temporal o permanente.

Art. 10. La radicación de Certificadores Licenciados que se desempeñen fuera de la órbita de la administración pública lo harán en términos de libre competencia, reservándose el Gobierno Provincial la delimitación de cupos, áreas geográficas o cualquier otro tipo de segmentación que aseguren que los eventuales usuarios estarán debidamente protegidos por la legislación en materia de defensa del consumidor.

Proyecto De Ley nro:559/2010

Art. 11. La Autoridad de Aplicación, sin perjuicio de lo establecido en la ley nacional 25506 Ver Texto , establecerá un sistema de registro, métodos y mecanismos para la evaluación y constatación de la confiabilidad, integridad, confidencialidad y disponibilidad de los esquemas utilizados por los registrados para la realización de identificaciones fehacientes dentro del marco de la infraestructura de firma digital.

Art. 12. Atento a lo establecido en el artículo anterior, la Provincia de San Luis, a través de la Autoridad de Aplicación, se reserva el derecho de adoptar todo cambio tecnológico que, sin oponerse a la ley nacional ni a los estándares internacionales, tienda a optimizar, adecuar y ampliar el uso de la firma digital.

Art. 13. La Autoridad de Aplicación establecerá un sistema de multas y sanciones para quienes incumplan con los métodos y mecanismos dispuestos por la misma.

Art. 14. La Autoridad de Aplicación bregará por el fiel respeto de los principios relativos a la protección de los datos personales en un todo de acuerdo con lo normado por la ley nacional 25326 Ver Texto .

Art. 15. El Poder Ejecutivo deberá reglamentar la presente ley en un plazo no mayor de ciento ochenta (180) días de su publicación en el Boletín Oficial.

Art. 16. Regístrese, etc.

Álvarez - Sosa - Vallejo - Pereyra
Antecedentes - Biblioteca Legislativa
15) TIERRA DEL FUEGO

LEY 633

Sumario: Ley de firma digital -- Adhesión de la provincia a la ley nacional 25.506.

Fecha de Sanción: 06/07/2004

Fecha de Promulgación: 28/07/2004

Publicado en: Boletín Oficial 04/08/2004 - ADLA 2004 - D, 5325

Art. 1° - Adhiérase la Provincia de Tierra del Fuego, Antártida e Islas del Atlántico Sur a la Ley nacional 25.506 sobre firma digital.

Art. 2° - Comuníquese, etc.

Antecedentes - Biblioteca Legislativa
16) COSTA RICA

DECRETO LEGISLATIVO N.º 8454

LA ASAMBLEA LEGISLATIVA DE LA
REPÚBLICA DE COSTA RICA

PLENARIO

Proyecto De Ley nro:559/2010

LEY DE CERTIFICADOS, FIRMAS DIGITALES Y
DOCUMENTOS ELECTRÓNICOS

DECRETO LEGISLATIVO N.º 8454

EXPEDIENTE N.º 14.276

SAN JOSÉ - COSTA RICA

8454

ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA

DECRETA:

LEY DE CERTIFICADOS, FIRMAS DIGITALES Y
DOCUMENTOS ELECTRÓNICOS

CAPÍTULO I

DISPOSICIONES GENERALES

ARTÍCULO 1.- Ámbito de aplicación

Esta Ley se aplicará a toda clase de transacciones y actos jurídicos, públicos o privados, salvo disposición legal en contrario, o que la naturaleza o los requisitos particulares del acto o negocio concretos resulten incompatibles.

El Estado y todas las entidades públicas quedan expresamente facultados para utilizar los certificados, las firmas digitales y los documentos electrónicos, dentro de sus respectivos ámbitos de competencia.

ARTÍCULO 2.- Principios

En materia de certificados, firmas digitales y documentos electrónicos, la implementación, interpretación y aplicación de esta Ley deberán observar los siguientes principios:

a) Regulación legal mínima y desregulación de trámites.
b) Autonomía de la voluntad de los particulares para reglar sus relaciones.
c) Utilización, con las limitaciones legales, de reglamentos autónomos por la Administración Pública para desarrollar la organización y el servicio, interno o externo.
d) Igualdad de tratamiento para las tecnologías de generación, proceso o almacenamiento involucradas.

CAPÍTULO II

DOCUMENTOS

ARTÍCULO 3.- Reconocimiento de la equivalencia funcional

Proyecto De Ley nro:559/2010

Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático, se tendrá por jurídicamente equivalente a los documentos que se otorguen, residan o transmitan por medios físicos.

En cualquier norma del ordenamiento jurídico en la que se haga referencia a un documento o comunicación, se entenderán de igual manera tanto los electrónicos como los físicos. No obstante, el empleo del soporte electrónico para un documento determinado no dispensa, en ningún caso, el cumplimiento de los requisitos y las formalidades que la ley exija para cada acto o negocio jurídico en particular.

ARTÍCULO 4.- Calificación jurídica y fuerza probatoria

Los documentos electrónicos se calificarán como públicos o privados, y se les reconocerá fuerza probatoria en las mismas condiciones que a los documentos físicos.

ARTÍCULO 5.- En particular y excepciones

En particular y sin que conlleve la exclusión de otros actos, contratos o negocios jurídicos, la utilización de documentos electrónicos es válida para lo siguiente:

a) La formación, formalización y ejecución de los contratos.
b) El señalamiento para notificaciones conforme a la Ley de notificaciones, citaciones y otras comunicaciones judiciales.
c) La tramitación, gestión y conservación de expedientes judiciales y administrativos; asimismo, la recepción, práctica y conservación de prueba, incluida la recibida por archivos y medios electrónicos. De igual manera, los órganos jurisdiccionales que requieran la actualización de certificaciones y, en general, de otras piezas, podrán proceder sobre simples impresiones de los documentos en línea efectuadas por el despacho o aceptar las impresiones de dichos documentos en línea, aportadas por la parte interesada y certificadas notarialmente.
d) La emisión de certificaciones, constancias y otros documentos.
e) La presentación, tramitación e inscripción de documentos en el Registro Nacional.
f) La gestión, conservación y utilización, en general, de protocolos notariales, incluso la manifestación del consentimiento y la firma de las partes.

No se podrán consignar en documentos electrónicos:

a) Los actos o negocios en los que, por mandato legal, la fijación física resulte consustancial.
b) Las disposiciones por causa de muerte.
c) Los actos y convenios relativos al Derecho de familia.
d) Los actos personalísimos en general.

ARTÍCULO 6.- Gestión y conservación de documentos electrónicos

Cuando legalmente se requiera que un documento sea conservado para futura referencia, se podrá optar por hacerlo en soporte electrónico, siempre que se apliquen las medidas de seguridad necesarias para garantizar su inalterabilidad, se posibilite su acceso o consulta posterior y se preserve, además, la información relativa a su origen y otras características básicas.

La transición o migración a soporte electrónico, cuando se trate de registros, archivos o respaldos que por ley deban ser conservados, deberá contar, previamente, con la autorización de la autoridad competente.

En lo relativo al Estado y sus instituciones, se aplicará la Ley del Sistema Nacional de Archivos, N.° 7202, de 24 de octubre de 1990. La Dirección General del Archivo Nacional dictará las regulaciones necesarias para asegurar la gestión debida y conservación de los documentos, mensajes o archivos electrónicos.

ARTÍCULO 7.- Satisfacción de los requisitos fiscales

Proyecto De Ley nro:559/2010

Cuando la emisión de un acto o la celebración de un negocio jurídico en soporte electrónico conlleve el pago de requisitos fiscales, el obligado al pago deberá conservar el comprobante respectivo y exhibirlo cuando una autoridad competente lo requiera.

CAPÍTULO III

FIRMAS DIGITALES

ARTÍCULO 8.- Alcance del concepto

Entiéndese por firma digital cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico.
Una firma digital se considerará certificada cuando sea emitida al amparo de un certificado digital vigente, expedido por un certificador registrado.

ARTÍCULO 9.- Valor equivalente

Los documentos y las comunicaciones suscritos mediante firma digital, tendrán el mismo valor y la eficacia probatoria de su equivalente firmado en manuscrito. En cualquier norma jurídica que se exija la presencia de una firma, se reconocerá de igual manera tanto la digital como la manuscrita.

Los documentos públicos electrónicos deberán llevar la firma digital certificada.

ARTÍCULO 10.- Presunción de autoría y responsabilidad

Todo documento, mensaje electrónico o archivo digital asociado a una firma digital certificada se presumirá, salvo prueba en contrario, de la autoría y responsabilidad del titular del correspondiente certificado digital, vigente en el momento de su emisión.

No obstante, esta presunción no dispensa el cumplimiento de las formalidades adicionales de autenticación, certificación o registro que, desde el punto de vista jurídico, exija la ley para un acto o negocio determinado.

CAPÍTULO IV

CERTIFICACIÓN DIGITAL

Sección I

Los certificados

ARTÍCULO 11.- Alcance

Entiéndese por certificado digital el mecanismo electrónico o digital mediante el que se pueda garantizar, confirmar o validar técnicamente:

a) La vinculación jurídica entre un documento, una firma digital y una persona.
b) La integridad, autenticidad y no alteración en general del documento, así como la firma digital asociada.
c) La autenticación o certificación del documento y la firma digital asociada, únicamente en el supuesto del ejercicio de potestades públicas certificadoras.
d) Las demás que establezca esta Ley y su Reglamento.

ARTÍCULO 12.- Mecanismos

Proyecto De Ley nro:559/2010

Con las limitaciones de este capítulo, el Estado, las instituciones públicas y las empresas públicas y privadas, las personas jurídicas y los particulares, en general, en sus diversas relaciones, estarán facultados para establecer los mecanismos de certificación o validación que convengan a sus intereses.

Para tales efectos podrán:

a) Utilizar mecanismos de certificación o validación máquina a máquina, persona a persona, programa a programa y sus interrelaciones, incluso sistemas de llave pública y llave privada, firma digital y otros mecanismos digitales que ofrezcan una óptima seguridad.
b) Establecer mecanismos de adscripción voluntaria para la emisión, la percepción y el intercambio de documentos electrónicos y firmas asociadas, en función de las competencias, los intereses y el giro comercial.
c) De consuno, instituir mecanismos de certificación para la emisión, la recepción y el intercambio de documentos electrónicos y firmas asociadas, para relaciones jurídicas concretas.
d) Instaurar, en el caso de dependencias públicas, sistemas de certificación por intermedio de particulares, quienes deberán cumplir los trámites de la Ley de contratación administrativa.
e) Fungir como un certificador respecto de sus despachos y funcionarios, o de otras dependencias públicas, en el caso del Estado y las demás instituciones públicas.
f) Ofrecer, en el caso de las empresas públicas cuyo giro lo admita, servicios comerciales de certificación en condiciones de igualdad con las empresas de carácter privado.
g) Implantar mecanismos de certificación para la tramitación, gestión y conservación de expedientes judiciales y administrativos.

ARTÍCULO 13.- Homologación de certificados extranjeros

Se conferirá pleno valor y eficacia jurídica a un certificado digital emitido en el extranjero, en cualesquiera de los siguientes casos:

a) Cuando esté respaldado por un certificador registrado en el país, en virtud de existir una relación de corresponsalía en los términos del artículo 20 de esta Ley.
b) Cuando cumpla todos los requisitos enunciados en el artículo 19 de esta Ley y exista un acuerdo recíproco en este sentido entre Costa Rica y el país de origen del certificador extranjero.

ARTÍCULO 14.- Suspensión de certificados digitales

Se podrá suspender un certificado digital en los siguientes casos:

a) Por petición del propio usuario a favor de quien se expidió.
b) Como medida cautelar, cuando el certificador que lo emitió tenga sospechas fundadas de que el propio usuario haya comprometido su confiabilidad, desatendido los lineamientos de seguridad establecidos, suplido información falsa al certificador u omitido cualquier otra información relevante, para obtener o renovar el certificado. En este caso, la suspensión podrá ser recurrida ante la Dirección de Certificadores de Firma Digital regulada en la siguiente sección, con aplicación de lo dispuesto en el artículo 148 de la Ley General de la Administración Pública.
c) Si contra el usuario se ha dictado auto de apertura a juicio, por delitos en cuya comisión se haya utilizado la firma digital.
d) Por orden judicial o de la Dirección de Certificadores de Firma Digital. En este último caso, cuando esta lo determine o cuando el Ente Costarricense de Acreditación (ECA) acredite que el usuario incumple las obligaciones que le imponen esta Ley y su Reglamento.
e) Por no cancelar oportunamente el costo del servicio.

ARTÍCULO 15.- Revocación de certificados digitales

El certificado digital será revocado en los siguientes supuestos:

Proyecto De Ley nro:559/2010

a) A petición del usuario, en favor de quien se expidió.
b) Cuando se confirme que el usuario ha comprometido su confiabilidad, desatendido los lineamientos de seguridad establecidos, suplido información falsa al certificador u omitido otra información relevante, con el propósito de obtener o renovar el certificado.
c) Por fallecimiento, ausencia legalmente declarada, interdicción o insolvencia del usuario persona física, o por cese de actividades, quiebra o liquidación, en el caso de las personas jurídicas.
d) Por orden de la autoridad judicial o cuando recaiga condena firme contra el usuario, por delitos en cuya comisión se haya utilizado la firma digital.

ARTÍCULO 16.- Revocación por el cese de actividades del certificador

El cese de actividades del certificador implicará la revocatoria de todos los certificados que haya expedido, salvo que anteriormente hayan sido traspasados a otro certificador, previo consentimiento del usuario.

ARTÍCULO 17.- Conservación de efectos

La suspensión o revocación de un certificado digital no producirá, por sí sola, la invalidez de los actos o negocios realizados con anterioridad al amparo de dicho certificado.

Sección II

Certificadores

ARTÍCULO 18.- Definición y reconocimiento jurídico

Se entenderá como certificador la persona jurídica pública o privada, nacional o extranjera, que emite certificados digitales y está debidamente autorizada según esta Ley o su Reglamento; asimismo, que haya rendido la debida garantía de fidelidad. El monto de la garantía será fijado por la Dirección de Certificadores de Firma Digital y podrá ser hipoteca, fianza o póliza de fidelidad de un ente asegurador, o bien, un depósito en efectivo.

Sin perjuicio de lo dispuesto en los artículos 3, 9 y 19 de esta Ley, los certificados digitales expedidos por certificadores registrados ante la Dirección de Certificadores de Firma Digital, solo tendrán pleno efecto legal frente a terceros, así como respecto del Estado y sus instituciones.

ARTÍCULO 19.- Requisitos, trámites y funciones

La Dirección de Certificadores de Firma Digital será la encargada de establecer, vía reglamento, todos los requisitos, el trámite y las funciones de las personas que soliciten su registro ante esta Dirección; para ello, el ECA, a solicitud del Ministerio de Ciencia y Tecnología, deberá fijar los requerimientos técnicos para el estudio, de acuerdo con la Ley N.º 8279, de 2 de mayo de 2002, y las prácticas y los estándares internacionales.

ARTÍCULO 20.- Corresponsalía

Los certificadores registrados podrán concertar relaciones de corresponsalía con entidades similares del extranjero, para efectos de homologar los certificados digitales expedidos por estas entidades o que estas hagan lo propio en el exterior con los emitidos por los certificadores registrados.

Se deberá informar a la Dirección de Certificadores de Firma Digital, acerca del establecimiento de relaciones de esta clase, de previo a ofrecer ese servicio al público.

ARTÍCULO 21.- Auditorías

Proyecto De Ley nro:559/2010

Todo certificador registrado estará sujeto a los procedimientos de evaluación y auditoría que acuerde efectuar la Dirección de Certificadores de Firma Digital o el ECA.

ARTÍCULO 22.- Cesación voluntaria de funciones

Los certificadores registrados de carácter privado podrán cesar en sus funciones, siempre y cuando avisen, a los usuarios, con un mes de anticipación como mínimo, y con dos meses a la Dirección de Certificadores de Firma Digital.

Sección III

Administración del Sistema de Certificación

ARTÍCULO 23.- Dirección

La Dirección de Certificadores de Firma Digital, perteneciente al Ministerio de Ciencia y Tecnología, será el órgano administrador y supervisor del Sistema de Certificación.

ARTÍCULO 24.- Funciones

La Dirección de Certificadores de Firma Digital tendrá las siguientes funciones:

a) Recibir, tramitar y resolver las solicitudes de inscripción de los certificadores.
b) Llevar un registro de los certificadores y certificados digitales.
c) Suspender o revocar la inscripción de los certificadores y de certificados, así como ejercer el régimen disciplinario en los casos y en la forma previstos en esta Ley y su Reglamento.
d) Expedir claves y certificados a favor de los certificadores registrados, y mantener el correspondiente repositorio de acceso público, con las características técnicas que indique el Reglamento.
e) Fiscalizar el funcionamiento de los certificadores registrados, para asegurar su confiabilidad, eficiencia y el cabal cumplimiento de la normativa aplicable, imponiendo, en caso necesario, las sanciones previstas en esta Ley. La supervisión podrá ser ejercida por medio del ECA, en el ámbito de su competencia.
f) Mantener una página electrónica en la red Internet, a fin de divulgar, permanentemente, información relativa a las actividades de la Dirección de Certificadores de Firma Digital y el registro correspondiente de certificadores.
g) Señalar las medidas que estime necesarias para proteger los derechos, los intereses y la confidencialidad de los usuarios, así como la continuidad y eficiencia del servicio, y velar por la ejecución de tales disposiciones.
h) Dictar el Reglamento respectivo para el registro de certificadores.
i) Las demás funciones que esta Ley o su Reglamento le señalen.

ARTÍCULO 25.- Jefatura

El superior administrativo de la Dirección de Certificadores de Firma Digital será el director, quien será nombrado por el ministro de Ciencia y Tecnología y será un funcionario de confianza, de conformidad con el inciso g) del artículo 4, del Estatuto de Servicio Civil. El director deberá declarar sus bienes oportunamente, de acuerdo con la Ley contra el enriquecimiento ilícito de los servidores públicos.

CAPÍTULO V

SANCIONES

ARTÍCULO 26.- Sanciones a certificadores

Previa oportunidad de defensa, la Dirección de Certificadores de Firma Digital podrá imponerles, a los certificadores, las siguientes sanciones:

Proyecto De Ley nro:559/2010

a) Amonestación.
b) Multa hasta por el equivalente a cien salarios base; para la denominación salario base se considerará lo indicado en el artículo 2 de la Ley N.º 7337, de 5 de mayo de 1993.
c) Suspensión hasta por un año.
d) Revocatoria de la inscripción.

El certificador a quien se le haya revocado su inscripción, no podrá volver a registrarse durante los siguientes cinco años, ya sea como tal o por medio de otra persona jurídica en la que figuren las mismas personas como representantes legales, propietarias o dueñas de más de un veinticinco por ciento (25%) del capital.

ARTÍCULO 27.- Amonestación

Se aplicará la amonestación, a los certificadores, en los siguientes casos:

a) Por la emisión de certificados digitales que no incluyan la totalidad de los datos requeridos por esta Ley o su Reglamento, cuando la infracción no requiera una sanción mayor.
b) Por no suministrar a tiempo los datos requeridos por la Dirección de Certificadores de Firma Digital, en ejercicio de sus funciones.
c) Por cualquier otra infracción a la presente Ley que no tenga prevista una sanción mayor.

ARTÍCULO 28.- Multa

Se aplicará la multa, a los certificadores, en los siguientes casos:

a) Cuando se emita un certificado y no se observen las políticas de seguridad o de certificación previamente divulgadas, de modo que cause perjuicio a los usuarios o a terceros.
b) Cuando no se suspenda o revoque, oportunamente, un certificado, estando obligados a hacerlo.
c) Por cualquier impedimento u obstrucción a las inspecciones o auditorías por parte de la Dirección de Certificadores de Firma Digital o del ECA.
d) Por el incumplimiento de los lineamientos técnicos o de seguridad impartidos por la Dirección de Certificadores de Firma Digital.
e) Por la reincidencia en la comisión de infracciones, que hayan dado lugar a la sanción de amonestación, dentro de los dos años siguientes.

ARTÍCULO 29.- Suspensión

Se suspenderá al certificador que:

a) No renueve oportunamente la caución que respalde su funcionamiento o la rinda en forma indebida.
b) Reincida en cualesquiera de las infracciones que le hayan merecido una sanción de multa, dentro de los siguientes dos años.

ARTÍCULO 30.- Revocatoria de la inscripción

Se podrá revocar la inscripción de un certificador cuando:

a) Se compruebe la expedición de certificados falsos.
b) Se compruebe que el certificador suministró información o presentó documentos falsos, con el fin de obtener el registro.
c) Reincida en cualesquiera de las infracciones que le hayan merecido una sanción de suspensión, dentro de los cinco años siguientes.

ARTÍCULO 31.- Procedimiento

Todas las sanciones serán impuestas mediante el procedimiento administrativo ordinario, previsto en la Ley

Proyecto De Ley nro:559/2010

General de la Administración Pública, salvo en el caso de amonestación, en que podrá aplicarse el procedimiento sumario.

ARTÍCULO 32.- Publicidad

Excepto el caso de amonestación, todas las sanciones administrativas impuestas serán publicadas por medio de reseña o transcripción íntegra en La Gaceta, sin perjuicio de que, en atención al caso concreto, se disponga, además, publicarlas en uno o más medios de circulación o difusión nacional.

Asimismo, la Dirección de Certificadores de Firma Digital dispondrá la publicación electrónica en su página de información en Internet.

CAPÍTULO VI

DISPOSICIONES FINALES Y TRANSITORIAS

ARTÍCULO 33.- Reglamentación

El Poder Ejecutivo reglamentará esta Ley dentro de los seis meses siguientes a su publicación.

Además, para el trámite eficiente de sus asuntos, cada dependencia pública podrá adoptar las medidas particulares de aplicación de esta Ley de acuerdo con sus necesidades.

TRANSITORIO ÚNICO.-

Los rubros presupuestarios requeridos para que la Dirección de Certificadores de Firma Digital entre en funcionamiento, deberán ser incluidos por el Ministerio de Hacienda, a propuesta del Ministerio de Ciencia y Tecnología, en el primer presupuesto remitido a la Asamblea Legislativa, después de promulgada esta Ley.

Rige a partir de su publicación.

Asamblea Legislativa.- San José, a los veintitrés días del mes de agosto de dos mil cinco.

COMUNÍCASE AL PODER EJECUTIVO

Gerardo González Esquivel
PRESIDENTE

Daysi Serrano Vargas — PRIMERA SECRETARIA
Luis Paulino Rodríguez Mena — SEGUNDO SECRETARIO

daa.-

Dado en la Presidencia de la República.- San José, a los treinta días del mes de agosto del dos mil cinco.

Proyecto De Ley nro:559/2010

Ejecútese y publíquese

ABEL PACHECO DE LA ESPRIELLA

Fernando Gutiérrez Ortiz
MINISTRO DE CIENCIA Y TECNOLOGÍA

Sanción: 30-08-2005
Publicación: 13-10-2005 Gaceta: 197

http://asamblea.racsa.co.cr/ley/leyes/8000/L-8454.doc

Antecedentes - Biblioteca Legislativa
17) ESPAÑA

LEY 59/2003, de 19 de diciembre, de firma electrónica

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

EXPOSICIÓN DE MOTIVOS

I
El Real Decreto Ley 14/1999, de 17 de septiembre, sobre firma electrónica, fue aprobado con el objetivo de fomentar la rápida incorporación de las nuevas tecnologías de seguridad de las comunicaciones electrónicas en la actividad de las empresas, los ciudadanos y las Administraciones públicas. De este modo, se coadyuvaba a potenciar el crecimiento y la competitividad de la economía española mediante el rápido establecimiento de un marco jurídico para la utilización de una herramienta que aporta confianza en la realización de transacciones electrónicas en redes abiertas como es el caso de Internet. El citado real decreto ley incorporó al ordenamiento público español la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, incluso antes de su promulgación y publicación en el Diario Oficial de las Comunidades Europeas.

Tras su ratificación por el Congreso de los Diputados, se acordó la tramitación del Real Decreto Ley 14/1999 como proyecto de ley, con el fin de someterlo a una más amplia consulta pública y al posterior debate parlamentario para perfeccionar su texto. No obstante, esta iniciativa decayó al expirar el mandato de las Cámaras en marzo de 2000. Esta ley, por tanto, es el resultado del compromiso asumido en la VI Legislatura, actualizando a la vez el marco establecido en el Real Decreto Ley 14/1999 mediante la incorporación de las modificaciones que aconseja la experiencia acumulada desde su entrada en vigor tanto en nuestro país como en el ámbito internacional.

Proyecto De Ley nro:559/2010

II

El desarrollo de la sociedad de la información y la difusión de los efectos positivos que de ella se derivan exige la generalización de la confianza de la ciudadanía en las comunicaciones telemáticas. No obstante, los datos más recientes señalan que aún existe desconfianza por parte de los intervinientes en las transacciones telemáticas y, en general, en las comunicaciones que las nuevas tecnologías permiten a la hora de transmitir información, constituyendo esta falta de confianza un freno para el desarrollo de la sociedad de la información, en particular, la Administración y el comercio electrónicos.

Como respuesta a esta necesidad de conferir seguridad a las comunicaciones por internet surge, entre otros, la firma electrónica. La firma electrónica constituye un instrumento capaz de permitir una comprobación de la procedencia y de la integridad de los mensajes intercambiados a través de redes de telecomunicaciones, ofreciendo las bases para evitar el repudio, si se adoptan las medidas oportunas basándose en fechas electrónicas.

Los sujetos que hacen posible el empleo de la firma electrónica son los denominados prestadores de servicios de certificación. Para ello expiden certificados electrónicos, que son documentos electrónicos que relacionan las herramientas de firma electrónica en poder de cada usuario con su identidad personal, dándole así a conocer en el ámbito telemático como firmante.

La ley obliga a los prestadores de servicios de certificación a efectuar una tutela y gestión permanente de los certificados electrónicos que expiden. Los detalles de esta gestión deben recogerse en la llamada declaración de prácticas de certificación, donde se especifican las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados electrónicos. Además, estos prestadores están obligados a mantener accesible un servicio de consulta sobre el estado de vigencia de los certificados en el que debe indicarse de manera actualizada si éstos están vigentes o si su vigencia ha sido suspendida o extinguida.

Asimismo, debe destacarse que la ley define una clase particular de certificados electrónicos denominados certificados reconocidos, que son los certificados electrónicos que se han expedido cumpliendo requisitos cualificados en lo que se refiere a su contenido, a los procedimientos de comprobación de la identidad del firmante y a la fiabilidad y garantías de la actividad de certificación electrónica.

Los certificados reconocidos constituyen una pieza fundamental de la llamada firma electrónica reconocida, que se define siguiendo las pautas impuestas en la Directiva 1999/93/CE como la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. A la firma electrónica reconocida le otorga la ley la equivalencia funcional con la firma manuscrita respecto de los datos consignados en forma electrónica.

Por otra parte, la ley contiene las garantías que deben ser cumplidas por los dispositivos de creación de firma para que puedan ser considerados como dispositivos seguros y conformar así una firma electrónica reconocida.

La certificación técnica de los dispositivos seguros de creación de firma electrónica se basa en el marco establecido por la Ley 21/1992, de 16 de julio, de Industria y en sus disposiciones de desarrollo. Para esta certificación se utilizarán las normas técnicas publicadas a tales efectos en el "Diario Oficial de las Comunidades Europeas" o, excepcionalmente, las aprobadas por el Ministerio de Ciencia y Tecnología.

Adicionalmente, la ley establece un marco de obligaciones aplicables a los prestadores de servicios de certificación, en función de si éstos emiten certificados reconocidos o no, y determina su régimen de responsabilidad, teniendo en cuenta los deberes de diligencia que incumben a los firmantes y a los terceros destinatarios de documentos firmados electrónicamente.

III

Esta ley se promulga para reforzar el marco jurídico existente incorporando a su texto algunas novedades

Proyecto De Ley nro:559/2010

respecto del Real Decreto Ley 14/1999 que contribuirán a dinamizar el mercado de la prestación de servicios de certificación.

Así, se revisa la terminología, se modifica la sistemática y se simplifica el texto facilitando su comprensión y dotándolo de una estructura más acorde con nuestra técnica legislativa.

Una de las novedades que la ley ofrece respecto del Real Decreto Ley 14/1999, es la denominación como firma electrónica reconocida de la firma electrónica que se equipara funcionalmente a la firma manuscrita. Se trata simplemente de la creación de un concepto nuevo demandado por el sector, sin que ello implique modificación alguna de los requisitos sustantivos que tanto la Directiva 1999/93/CE como el propio Real Decreto Ley 14/1999 venían exigiendo. Con ello se aclara que no basta con la firma electrónica avanzada para la equiparación con la firma manuscrita ; es preciso que la firma electrónica avanzada esté basada en un certificado reconocido y haya sido creada por un dispositivo seguro de creación.

Asimismo, es de destacar de manera particular, la eliminación del registro de prestadores de servicios de certificación, que ha dado paso al establecimiento de un mero servicio de difusión de información sobre los prestadores que operan en el mercado, las certificaciones de calidad y las características de los productos y servicios con que cuentan para el desarrollo de su actividad.

Por otra parte, la ley modifica el concepto de certificación de prestadores de servicios de certificación para otorgarle mayor grado de libertad y dar un mayor protagonismo a la participación del sector privado en los sistemas de certificación y eliminando las presunciones legales asociadas a la misma, adaptándose de manera más precisa a lo establecido en la directiva. Así, se favorece la autorregulación de la industria, de manera que sea ésta quien diseñe y gestione, de acuerdo con sus propias necesidades, sistemas voluntarios de acreditación destinados a mejorar los niveles técnicos y de calidad en la prestación de servicios de certificación.

El nuevo régimen nace desde el convencimiento de que los sellos de calidad son un instrumento eficaz para convencer a los usuarios de las ventajas de los productos y servicios de certificación electrónica, resultando imprescindible facilitar y agilizar la obtención de estos símbolos externos para quienes los ofrecen al público.

Si bien se recogen fielmente en la ley los conceptos de "acreditación" de prestadores de servicios de certificación y de "conformidad" de los dispositivos seguros de creación de firma electrónica contenidos en la directiva, la terminología se ha adaptado a la más comúnmente empleada y conocida recogida en la Ley 21/1992, de 16 de julio, de Industria.

Otra modificación relevante es que la ley clarifica la obligación de constitución de una garantía económica por parte de los prestadores de servicios de certificación que emitan certificados reconocidos, estableciendo una cuantía mínima única de tres millones de euros, flexibilizando además la combinación de los diferentes instrumentos para constituir la garantía.

Por otra parte, dado que la prestación de servicios de certificación no está sujeta a autorización previa, resulta importante destacar que la ley refuerza las capacidades de inspección y control del Ministerio de Ciencia y Tecnología, señalando que este departamento podrá ser asistido de entidades independientes y técnicamente cualificadas para efectuar las labores de supervisión y control sobre los prestadores de servicios de certificación.

También ha de destacarse la regulación que la ley contiene respecto del documento nacional de identidad electrónico, que se erige en un certificado electrónico reconocido llamado a generalizar el uso de instrumentos seguros de comunicación electrónica capaces de conferir la misma integridad y autenticidad que la que actualmente rodea las comunicaciones a través de medios físicos. La ley se limita a fijar el marco normativo básico del nuevo DNI electrónico poniendo de manifiesto sus dos notas más características -acredita la identidad de su titular en cualquier procedimiento administrativo y permite la firma electrónica de documentos- remitiéndose a la normativa específica en cuanto a las particularidades de su régimen jurídico.

Proyecto De Ley nro:559/2010

Asimismo, otra novedad es el establecimiento en la ley del régimen aplicable a la actuación de personas jurídicas como firmantes, a efectos de integrar a estas entidades en el tráfico telemático. Se va así más allá del Real Decreto Ley de 1999, que sólo permitía a las personas jurídicas ser titulares de certificados electrónicos en el ámbito de la gestión de los tributos.

Precisamente, la enorme expansión que han tenido estos certificados en dicho ámbito en los últimos años, sin que ello haya representado aumento alguno de la litigiosidad ni de inseguridad jurídica en las transacciones, aconsejan la generalización de la titularidad de certificados por personas morales.

En todo caso, los certificados electrónicos de personas jurídicas no alteran la legislación civil y mercantil en cuanto a la figura del representante orgánico o voluntario y no sustituyen a los certificados electrónicos que se expidan a personas físicas en los que se reflejen dichas relaciones de representación.

Como resortes de seguridad jurídica, la ley exige, por un lado, una especial legitimación para que las personas físicas soliciten la expedición de certificados ; por otro lado, obliga a los solicitantes a responsabilizarse de la custodia de los datos de creación de firma electrónica asociados a dichos certificados, todo ello sin perjuicio de que puedan ser utilizados por otras personas físicas vinculadas a la entidad. Por último, de cara a terceros, limita el uso de estos certificados a los actos que integren la relación entre la persona jurídica y las Administraciones públicas y a las cosas o servicios que constituyen el giro o tráfico ordinario de la entidad, sin perjuicio de los posibles límites cuantitativos o cualitativos que puedan añadirse. Se trata de conjugar el dinamismo que debe presidir el uso de estos certificados en el tráfico con las necesarias dosis de prudencia y seguridad para evitar que puedan nacer obligaciones incontrolables frente a terceros debido a un uso inadecuado de los datos de creación de firma. El equilibrio entre uno y otro principio se ha establecido sobre las cosas y servicios que constituyen el giro o tráfico ordinario de la empresa de modo paralelo a cómo nuestro más que centenario Código de Comercio regula la vinculación frente a terceros de los actos de comercio realizados por el factor del establecimiento.

Con la expresión "giro o tráfico ordinario" de una entidad se actualiza a un vocabulario más acorde con nuestros días lo que en la legislación mercantil española se denomina "establecimiento fabril o mercantil". Con ello se comprenden las transacciones efectuadas mediata o inmediatamente para la realización del núcleo de actividad de la entidad y las actividades de gestión o administrativas necesarias para el desarrollo de la misma, como la contratación de suministros tangibles e intangibles o de servicios auxiliares. Por último, debe recalcarse que, aunque el "giro o tráfico ordinario" sea un término acuñado por el derecho mercantil, la regulación sobre los certificados de personas jurídicas no sólo se aplica a las sociedades mercantiles, sino a cualquier tipo de persona jurídica que quiera hacer uso de la firma electrónica en su actividad.

Adicionalmente, se añade un régimen especial para la expedición de certificados electrónicos a entidades sin personalidad jurídica a las que se refiere el artículo 33 de la Ley General Tributaria, a los solos efectos de su utilización en el ámbito tributario, en los términos que establezca el Ministerio de Hacienda.

Por otra parte, siguiendo la pauta marcada por la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, se incluye dentro de la modalidad de prueba documental el soporte en el que figuran los datos firmados electrónicamente, dando mayor seguridad jurídica al empleo de la firma electrónica al someterla a las reglas de eficacia en juicio de la prueba documental.

Además, debe resaltarse que otro aspecto novedoso de la ley es el acogimiento explícito que se efectúa de las relaciones de representación que pueden subyacer en el empleo de la firma electrónica. No cabe duda que el instituto de la representación está ampliamente generalizado en el tráfico económico, de ahí la conveniencia de dotar de seguridad jurídica la imputación a la esfera jurídica del representado las declaraciones que se cursan por el representante a través de la firma electrónica.

Para ello, se establece como novedad que en la expedición de certificados reconocidos que admitan entre sus atributos relaciones de representación, ésta debe estar amparada en un documento público que acredite fehacientemente dicha relación de representación así como la suficiencia e idoneidad de los poderes conferidos al representante. Asimismo, se prevén mecanismos para asegurar el mantenimiento de las facultades de representación durante toda la vigencia del certificado reconocido.

Proyecto De Ley nro:559/2010

Por último, debe destacarse que la ley permite que los prestadores de servicios de certificación podrán, con el objetivo de mejorar la confianza en sus servicios, establecer mecanismos de coordinación con los datos que preceptivamente deban obrar en los Registros públicos, en particular, mediante conexiones telemáticas, a los efectos de verificar los datos que figuran en los certificados en el momento de la expedición de éstos.

Dichos mecanismos de coordinación también podrán contemplar la notificación telemática por parte de los registros a los prestadores de servicios de certificación de las variaciones registrales posteriores.

IV

La ley consta de 36 artículos agrupados en seis títulos, 10 disposiciones adicionales, dos disposiciones transitorias, una disposición derogatoria y tres disposiciones finales.

El título I contiene los principios generales que delimitan los ámbitos subjetivo y objetivo de aplicación de la ley, los efectos de la firma electrónica y el régimen de empleo ante las Administraciones públicas y de acceso a la actividad de prestación de servicios de certificación.

El régimen aplicable a los certificados electrónicos se contiene en el título II, que dedica su primer capítulo a determinar quiénes pueden ser sus titulares y a regular las vicisitudes que afectan a su vigencia. El capítulo II regula los certificados reconocidos y el tercero el documento nacional de identidad electrónico.

El título III regula la actividad de prestación de servicios de certificación estableciendo las obligaciones a que están sujetos los prestadores -distinguiendo con nitidez las que solamente afectan a los que expiden certificados reconocidos-, y el régimen de responsabilidad aplicable.

El título IV establece los requisitos que deben reunir los dispositivos de verificación y creación de firma electrónica y el procedimiento que ha de seguirse para obtener sellos de calidad en la actividad de prestación de servicios de certificación.

Los títulos V y VI dedican su contenido, respectivamente, a fijar los regímenes de supervisión y sanción de los prestadores de servicios de certificación.

Por último, cierran el texto las disposiciones adicionales -que aluden a los regímenes especiales que resultan de aplicación preferente-, las disposiciones transitorias -que incorporan seguridad jurídica a la actividad desplegada al amparo de la normativa anterior-, la disposición derogatoria y las disposiciones finales relativas al fundamento constitucional, la habilitación para el desarrollo reglamentario y la entrada en vigor.

Esta disposición ha sido sometida al procedimiento de información en materia de normas y reglamentaciones técnicas previsto en la Directiva 98/34/CE, del Parlamento Europeo y del Consejo, de 22 de junio de 1998, por la que se establece un procedimiento de información en materia de normas y reglamentaciones técnicas, modificada por la Directiva 98/48/CE, del Parlamento Europeo y del Consejo, de 20 de julio de 1998, y en el Real Decreto 1337/1999, de 31 de julio, por el que se regula la remisión de información en materia de normas y reglamentaciones técnicas y reglamentos relativos a los servicios de la sociedad de la información.

[Bloque 2]
TÍTULO I

Disposiciones generales

[Bloque 3]
Artículo 1. Objeto.

1. Esta ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

Proyecto De Ley nro:559/2010

2. Las disposiciones contenidas en esta ley no alteran las normas relativas a la celebración, formalización, validez y eficacia de los contratos y cualesquiera otros actos jurídicos ni las relativas a los documentos en que unos y otros consten.

[Bloque 4]
Artículo 2. Prestadores de servicios de certificación sujetos a la ley.

1. Esta ley se aplicará a los prestadores de servicios de certificación establecidos en España y a los servicios de certificación que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.

2. Se denomina prestador de servicios de certificación la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

3. Se entenderá que un prestador de servicios de certificación está establecido en España cuando su residencia o domicilio social se halle en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios. En otro caso, se atenderá al lugar en que se realice dicha gestión o dirección.

4. Se considerará que un prestador opera mediante un establecimiento permanente situado en territorio español cuando disponga en él, de forma continuada o habitual, de instalaciones o lugares de trabajo en los que realice toda o parte de su actividad.

5. Se presumirá que un prestador de servicios de certificación está establecido en España cuando dicho prestador o alguna de sus sucursales se haya inscrito en el Registro Mercantil o en otro registro público español en el que fuera necesaria la inscripción para la adquisición de personalidad jurídica.

La mera utilización de medios tecnológicos situados en España para la prestación o el acceso al servicio no implicará, por sí sola, el establecimiento del prestador en España.

[Bloque 5]
Artículo 3. Firma electrónica, y documentos firmados electrónicamente.

1. La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

2. La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

3. Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

4. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

5. Se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Sin perjuicio de lo dispuesto en el párrafo anterior, para que un documento electrónico tenga la naturaleza de documento público o de documento administrativo deberá cumplirse, respectivamente, con lo dispuesto en las letras a) o b) del apartado siguiente y, en su caso, en la normativa específica aplicable.

6. El documento electrónico será soporte de:

Proyecto De Ley nro:559/2010

a) Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.

b) Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.

c) Documentos privados.

7. Los documentos a que se refiere el apartado anterior tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable.

8. El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio. Si se impugnare la autenticidad de la firma electrónica reconocida con la que se hayan firmado los datos incorporados al documento electrónico se procederá a comprobar que se trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados, así como que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica.

La carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento electrónico firmado con firma electrónica reconocida. Si dichas comprobaciones obtienen un resultado positivo, se presumirá la autenticidad de la firma electrónica reconocida con la que se haya firmado dicho documento electrónico siendo las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 120 a 600 euros.

Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil.

9. No se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica.

10. A los efectos de lo dispuesto en este artículo, cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellas.

Se modifican los apartados 5 y 8 por los arts. 5.1 y 5.2 de la Ley 56/2007, de 28 de diciembre. Ref. BOE-A-2007-22440

  Última actualización, publicada el 29/12/2007, en vigor a partir del 30/12/2007.
Texto original, publicado el 20/12/2003, en vigor a partir del 20/03/2004.

[Bloque 6]
Artículo 4. Empleo de la firma electrónica en el ámbito de las Administraciones públicas.

1. Esta ley se aplicará al uso de la firma electrónica en el seno de las Administraciones públicas, sus organismos públicos y las entidades dependientes o vinculadas a las mismas y en las relaciones que mantengan aquéllas y éstos entre sí o con los particulares.

Las Administraciones públicas, con el objeto de salvaguardar las garantías de cada procedimiento, podrán establecer condiciones adicionales a la utilización de la firma electrónica en los procedimientos. Dichas condiciones podrán incluir, entre otras, la imposición de fechas electrónicas sobre los documentos electrónicos integrados en un expediente administrativo. Se entiende por fecha electrónica el conjunto de

Proyecto De Ley nro:559/2010

datos en forma electrónica utilizados como medio para constatar el momento en que se ha efectuado una actuación sobre otros datos electrónicos a los que están asociados.

2. Las condiciones adicionales a las que se refiere el apartado anterior sólo podrán hacer referencia a las características específicas de la aplicación de que se trate y deberán garantizar el cumplimiento de lo previsto en el artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Estas condiciones serán objetivas, proporcionadas, transparentes y no discriminatorias y no deberán obstaculizar la prestación de servicios de certificación al ciudadano cuando intervengan distintas Administraciones públicas nacionales o del Espacio Económico Europeo.

3. Las normas que establezcan condiciones generales adicionales para el uso de la firma electrónica ante la Administración General del Estado, sus organismos públicos y las entidades dependientes o vinculadas a las mismas se dictarán a propuesta conjunta de los Ministerios de Administraciones Públicas y de Ciencia y Tecnología y previo informe del Consejo Superior de Informática y para el impulso de la Administración Electrónica.

4. La utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa nacional se regirá por su normativa específica.

[Bloque 7]
Artículo 5. Régimen de prestación de los servicios de certificación.

1. La prestación de servicios de certificación no está sujeta a autorización previa y se realizará en régimen de libre competencia. No podrán establecerse restricciones para los servicios de certificación que procedan de otro Estado miembro del Espacio Económico Europeo.

2. Los órganos de defensa de la competencia velarán por el mantenimiento de condiciones de competencia efectiva en la prestación de servicios de certificación al público mediante el ejercicio de las funciones que tengan legalmente atribuidas.

3. La prestación al público de servicios de certificación por las Administraciones públicas, sus organismos públicos o las entidades dependientes o vinculadas a las mismas se realizará con arreglo a los principios de objetividad, transparencia y no discriminación.

[Bloque 8]
TÍTULO II

Certificados electrónicos

[Bloque 9]
CAPÍTULO I

Disposiciones generales

[Bloque 10]
Artículo 6. Concepto de certificado electrónico y de firmante.

1. Un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

2. El firmante es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.

[Bloque 11]
Artículo 7. Certificados electrónicos de personas jurídicas.

Proyecto De Ley nro:559/2010

1. Podrán solicitar certificados electrónicos de personas jurídicas sus administradores, representantes legales y voluntarios con poder bastante a estos efectos.

Los certificados electrónicos de personas jurídicas no podrán afectar al régimen de representación orgánica o voluntaria regulado por la legislación civil o mercantil aplicable a cada persona jurídica.

2. La custodia de los datos de creación de firma asociados a cada certificado electrónico de persona jurídica será responsabilidad de la persona física solicitante, cuya identificación se incluirá en el certificado electrónico.

3. Los datos de creación de firma sólo podrán ser utilizados cuando se admita en las relaciones que mantenga la persona jurídica con las Administraciones públicas o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario.

Asimismo, la persona jurídica podrá imponer límites adicionales, por razón de la cuantía o de la materia, para el uso de dichos datos que, en todo caso, deberán figurar en el certificado electrónico.

4. Se entenderán hechos por la persona jurídica los actos o contratos en los que su firma se hubiera empleado dentro de los límites previstos en el apartado anterior.

Si la firma se utiliza transgrediendo los límites mencionados, la persona jurídica quedará vinculada frente a terceros sólo si los asume como propios o se hubiesen celebrado en su interés. En caso contrario, los efectos de dichos actos recaerán sobre la persona física responsable de la custodia de los datos de creación de firma, quien podrá repetir, en su caso, contra quien los hubiera utilizado.

5. Lo dispuesto en este artículo no será de aplicación a los certificados que sirvan para verificar la firma electrónica del prestador de servicios de certificación con la que firme los certificados electrónicos que expida.

6. Lo dispuesto en este artículo no será de aplicación a los certificados que se expidan a favor de las Administraciones públicas, que estarán sujetos a su normativa específica.

[Bloque 12]
Artículo 8. Extinción de la vigencia de los certificados electrónicos.

1. Son causas de extinción de la vigencia de un certificado electrónico:

a) Expiración del período de validez que figura en el certificado.

b) Revocación formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.

c) Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por un tercero.

d) Resolución judicial o administrativa que lo ordene.

e) Fallecimiento o extinción de la personalidad jurídica del firmante ; fallecimiento, o extinción de la personalidad jurídica del representado ; incapacidad sobrevenida, total o parcial, del firmante o de su representado ; terminación de la representación ; disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica.

f) Cese en la actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos por aquél sean transferidos a otro prestador de servicios de certificación.

Proyecto De Ley nro:559/2010

g) Alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.

h) Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

2. El período de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma.

En el caso de los certificados reconocidos este período no podrá ser superior a cuatro años.

3. La extinción de la vigencia de un certificado electrónico surtirá efectos frente a terceros, en los supuestos de expiración de su período de validez, desde que se produzca esta circunstancia y, en los demás casos, desde que la indicación de dicha extinción se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación.

[Bloque 13]
Artículo 9. Suspensión de la vigencia de los certificados electrónicos.

1. Los prestadores de servicios de certificación suspenderán la vigencia de los certificados electrónicos expedidos si concurre alguna de las siguientes causas:

a) Solicitud del firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.

b) Resolución judicial o administrativa que lo ordene.

c) La existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los certificados contempladas en los párrafos c) y g) del artículo 8.1.

d) Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

2. La suspensión de la vigencia de un certificado electrónico surtirá efectos desde que se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación.

[Bloque 14]
Artículo 10. Disposiciones comunes a la extinción y suspensión de la vigencia de certificados electrónicos.

1. El prestador de servicios de certificación hará constar inmediatamente, de manera clara e indubitada, la extinción o suspensión de la vigencia de los certificados electrónicos en el servicio de consulta sobre la vigencia de los certificados en cuanto tenga conocimiento fundado de cualquiera de los hechos determinantes de la extinción o suspensión de su vigencia.

2. El prestador de servicios de certificación informará al firmante acerca de esta circunstancia de manera previa o simultánea a la extinción o suspensión de la vigencia del certificado electrónico, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto. En los casos de suspensión, indicará, además, su duración máxima, extinguiéndose la vigencia del certificado si transcurrido dicho plazo no se hubiera levantado la suspensión.

3. La extinción o suspensión de la vigencia de un certificado electrónico no tendrá efectos retroactivos.

4. La extinción o suspensión de la vigencia de un certificado electrónico se mantendrá accesible en el servicio de consulta sobre la vigencia de los certificados al menos hasta la fecha en que hubiera finalizado su período inicial de validez.

Proyecto De Ley nro:559/2010

[Bloque 15]
CAPÍTULO II

Certificados reconocidos

[Bloque 16]
Artículo 11. Concepto y contenido de los certificados reconocidos.

1. Son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.

2. Los certificados reconocidos incluirán, al menos, los siguientes datos:

a) La indicación de que se expiden como tales.

b) El código identificativo único del certificado.

c) La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.

d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.

e) La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.

f) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.

g) El comienzo y el fin del período de validez del certificado.

h) Los límites de uso del certificado, si se establecen.

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

3. Los certificados reconocidos podrán asimismo contener cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo en función del fin propio del certificado y siempre que aquél lo solicite.

4. Si los certificados reconocidos admiten una relación de representación incluirán una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales, de conformidad con el apartado 2 del artículo 13.

[Bloque 17]
Artículo 12. Obligaciones previas a la expedición de certificados reconocidos.

Antes de la expedición de un certificado reconocido, los prestadores de servicios de certificación deberán cumplir las siguientes obligaciones:

a) Comprobar la identidad y circunstancias personales de los solicitantes de certificados con arreglo a lo dispuesto en el artículo siguiente.

b) Verificar que la información contenida en el certificado es exacta y que incluye toda la información prescrita para un certificado reconocido.

Proyecto De Ley nro:559/2010

c) Asegurarse de que el firmante está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.

d) Garantizar la complementariedad de los datos de creación y verificación de firma, siempre que ambos sean generados por el prestador de servicios de certificación.

[Bloque 18]
Artículo 13. Comprobación de la identidad y otras circunstancias personales de los solicitantes de un certificado reconocido.

1. La identificación de la persona física que solicite un certificado reconocido exigirá su personación ante los encargados de verificarla y se acreditará mediante el documento nacional de identidad, pasaporte u otros medios admitidos en derecho. Podrá prescindirse de la personación si su firma en la solicitud de expedición de un certificado reconocido ha sido legitimada en presencia notarial.

El régimen de personación en la solicitud de certificados que se expidan previa identificación del solicitante ante las Administraciones públicas se regirá por lo establecido en la normativa administrativa.

2. En el caso de certificados reconocidos de personas jurídicas, los prestadores de servicios de certificación comprobarán, además, los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y d4e apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

3. Si los certificados reconocidos reflejan una relación de representación voluntaria, los prestadores de servicios de certificación comprobarán los datos relativos a la personalidad jurídica del representado y a la extensión y vigencia de las facultades del representante mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los mencionados datos, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

Si los certificados reconocidos admiten otros supuestos de representación, los prestadores de servicios de certificación deberán exigir la acreditación de las circunstancias en las que se fundamenten, en la misma forma prevista anteriormente.

Cuando el certificado reconocido contenga otras circunstancias personales o atributos del solicitante, como su condición de titular de un cargo público, su pertenencia a un colegio profesional o su titulación, éstas deberán comprobarse mediante los documentos oficiales que las acrediten, de conformidad con su normativa específica.

4. Lo dispuesto en los apartados anteriores podrá no ser exigible en los siguientes casos:

a) Cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya al prestador de servicios de certificación en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubieran empleado los medios señalados en este artículo y el período de tiempo transcurrido desde la identificación es menor de cinco años.

b) Cuando para solicitar un certificado se utilice otro vigente para cuya expedición se hubiera identificado al firmante en la forma prescrita en este artículo y le conste al prestador de servicios de certificación que el período de tiempo transcurrido desde la identificación es menor de cinco años.

5. Los prestadores de servicios de certificación podrán realizar las actuaciones de comprobación previstas en

Proyecto De Ley nro:559/2010

este artículo por sí o por medio de otras personas físicas o jurídicas, públicas o privadas, siendo responsable, en todo caso, el prestador de servicios de certificación.

Se modifican los apartados 2 y 3 por el art. 5.3 de la Ley 56/2007, de 28 de diciembre. Ref. BOE-A-2007-22440

Última actualización, publicada el 29/12/2007, en vigor a partir del 30/12/2007.
Texto original, publicado el 20/12/2003, en vigor a partir del 20/03/2004.

[Bloque 19]
Artículo 14. Equivalencia internacional de certificados reconocidos.

Los certificados electrónicos que los prestadores de servicios de certificación establecidos en un Estado que no sea miembro del Espacio Económico Europeo expidan al público como certificados reconocidos de acuerdo con la legislación aplicable en dicho Estado se considerarán equivalentes a los expedidos por los establecidos en España, siempre que se cumpla alguna de las siguientes condiciones:

a) Que el prestador de servicios de certificación reúna los requisitos establecidos en la normativa comunitaria sobre firma electrónica para la expedición de certificados reconocidos y haya sido certificado conforme a un sistema voluntario de certificación establecido en un Estado miembro del Espacio Económico Europeo.

b) Que el certificado esté garantizado por un prestador de servicios de certificación establecido en el Espacio Económico Europeo que cumpla los requisitos establecidos en la normativa comunitaria sobre firma electrónica para la expedición de certificados reconocidos.

c) Que el certificado o el prestador de servicios de certificación estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad Europea y terceros países u organizaciones internacionales.

[Bloque 20]
CAPÍTULO III

El documento nacional de identidad electrónico

[Bloque 21]
Artículo 15. Documento nacional de identidad electrónico.

1. El documento nacional de identidad electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos.

2. Todas la personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del documento nacional de identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos.

[Bloque 22]
Artículo 16. Requisitos y características del documento nacional de identidad electrónico.

1. Los órganos competentes del Ministerio del Interior para la expedición del documento nacional de identidad electrónico cumplirán las obligaciones que la presente Ley impone a los prestadores de servicios de certificación que expidan certificados reconocidos con excepción de la relativa a la constitución de la garantía a la que se refiere el apartado 2 del artículo 20.

2. La Administración General del Estado empleará, en la medida de lo posible, sistemas que garanticen la compatibilidad de los instrumentos de firma electrónica incluidos en el documento nacional de identidad electrónico con los distintos dispositivos y productos de firma electrónica generalmente aceptados.

Proyecto De Ley nro:559/2010

[Bloque 23]
TÍTULO III

Prestación de servicios de certificación

[Bloque 24]
CAPÍTULO I

Obligaciones

[Bloque 25]
Artículo 17. Protección de los datos personales.

1. El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y los órganos administrativos para el ejercicio de las funciones atribuidas por esta ley se sujetará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en sus normas de desarrollo.

2. Para la expedición de certificados electrónicos al público, los prestadores de servicios de certificación únicamente podrán recabar datos personales directamente de los firmantes o previo consentimiento expreso de éstos.

Los datos requeridos serán exclusivamente los necesarios para la expedición y el mantenimiento del certificado electrónico y la prestación de otros servicios en relación con la firma electrónica, no pudiendo tratarse con fines distintos sin el consentimiento expreso del firmante.

3. Los prestadores de servicios de certificación que consignen un seudónimo en el certificado electrónico a solicitud del firmante deberán constatar su verdadera identidad y conservar la documentación que la acredite.

Dichos prestadores de servicios de certificación estarán obligados a revelar la identidad de los firmantes cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica de Protección de Datos de Carácter Personal en que así se requiera.

4. En cualquier caso, los prestadores de servicios de certificación no incluirán en los certificados electrónicos que expidan, los datos a los que se hace referencia en el artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

[Bloque 26]
Artículo 18. Obligaciones de los prestadores de servicios de certificación que expidan certificados electrónicos.

Los prestadores de servicios de certificación que expidan certificados electrónicos deberán cumplir las siguientes obligaciones:

a) No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios.

b) Proporcionar al solicitante antes de la expedición del certificado la siguiente información mínima, que deberá transmitirse de forma gratuita, por escrito o por vía electrónica:

1.º Las obligaciones del firmante, la forma en que han de custodiarse los datos de creación de firma, el procedimiento que haya de seguirse para comunicar la pérdida o posible utilización indebida de dichos datos y determinados dispositivos de creación y de verificación de firma electrónica que sean compatibles con los datos de firma y con el certificado expedido.

2.º Los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del

Proyecto De Ley nro:559/2010

tiempo.

3.º El método utilizado por el prestador para comprobar la identidad del firmante u otros datos que figuren en el certificado.

4.º Las condiciones precisas de utilización del certificado, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial.

5.º Las certificaciones que haya obtenido, en su caso, el prestador de servicios de certificación y los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir por el ejercicio de su actividad.

6.º Las demás informaciones contenidas en la declaración de prácticas de certificación.

La información citada anteriormente que sea relevante para terceros afectados por los certificados deberá estar disponible a instancia de éstos.

c) Mantener un directorio actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida. La integridad del directorio se protegerá mediante la utilización de los mecanismos de seguridad adecuados.

d) Garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados rápido y seguro.

[Bloque 27]
Artículo 19. Declaración de prácticas de certificación.

1. Todos los prestadores de servicios de certificación formularán una declaración de prácticas de certificación en la que detallarán, en el marco de esta ley y de sus disposiciones de desarrollo, las obligaciones que se comprometen a cumplir en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los certificados y, en su caso la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata sobre la vigencia de los poderes indicados en los certificados y que deban figurar preceptivamente inscritos en dichos registros.

2. La declaración de prácticas de certificación de cada prestador estará disponible al público de manera fácilmente accesible, al menos por vía electrónica y de forma gratuita.

3. La declaración de prácticas de certificación tendrá la consideración de documento de seguridad a los efectos previstos en la legislación en materia de protección de datos de carácter personal y deberá contener todos los requisitos exigidos para dicho documento en la mencionada legislación.

[Bloque 28]
Artículo 20. Obligaciones de los prestadores de servicios de certificación que expidan certificados reconocidos.

1. Además de las obligaciones establecidas en este capítulo, los prestadores de servicios de certificación que expidan certificados reconocidos deberán cumplir las siguientes obligaciones:

a) Demostrar la fiabilidad necesaria para prestar servicios de certificación.

b) Garantizar que pueda determinarse con precisión la fecha y la hora en las que se expidió un certificado o se extinguió o suspendió su vigencia.

Proyecto De Ley nro:559/2010

c) Emplear personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y de gestión adecuados en el ámbito de la firma electrónica.

d) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.

e) Tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación y su entrega por un procedimiento seguro al firmante.

f) Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.

g) Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.

2. Los prestadores de servicios de certificación que expidan certificados reconocidos deberán constituir un seguro de responsabilidad civil por importe de al menos 3.000.000 de euros para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados que expidan.

La citada garantía podrá ser sustituida total o parcialmente por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea al menos de 3.000.000 de euros.

Las cuantías y los medios de aseguramiento y garantía establecidos en los dos párrafos anteriores podrán ser modificados mediante real decreto.

[Bloque 29]
Artículo 21. Cese de la actividad de un prestador de servicios de certificación.

1. El prestador de servicios de certificación que vaya a cesar en su actividad deberá comunicarlo a los firmantes que utilicen los certificados electrónicos que haya expedido así como a los solicitantes de certificados expedidos a favor de personas jurídicas ; y podrá transferir, con su consentimiento expreso, la gestión de los que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador de servicios de certificación que los asuma o, en caso contrario, extinguir su vigencia.

La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad e informará, en su caso, sobre las características del prestador al que se propone la transferencia de la gestión de los certificados.

2. El prestador de servicios de certificación que expida certificados electrónicos al público deberá comunicar al Ministerio de Ciencia y Tecnología, con la antelación indicada en el anterior apartado, el cese de su actividad y el destino que vaya a dar a los certificados, especificando, en su caso, si va a transferir la gestión y a quién o si extinguirá su vigencia.

Igualmente, comunicará cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, la apertura de cualquier proceso concursal que se siga contra él.

3. Los prestadores de servicios de certificación remitirán al Ministerio de Ciencia y Tecnología con carácter previo al cese definitivo de su actividad la información relativa a los certificados electrónicos cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a efectos de lo previsto en el

Proyecto De Ley nro:559/2010

artículo 20.1.f). Este ministerio mantendrá accesible al público un servicio de consulta específico donde figure una indicación sobre los citados certificados durante un período que considere suficiente en función de las consultas efectuadas al mismo.

[Bloque 30]
CAPÍTULO II

Responsabilidad

[Bloque 31]
Artículo 22. Responsabilidad de los prestadores de servicios de certificación.

1. Los prestadores de servicios de certificación responderán por los daños y perjuicios que causen a cualquier persona en el ejercicio de su actividad cuando incumplan las obligaciones que les impone esta ley.

La responsabilidad del prestador de servicios de certificación regulada en esta ley será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, si bien corresponderá al prestador de servicios de certificación demostrar que actuó con la diligencia profesional que le es exigible.

2. Si el prestador de servicios de certificación no cumpliera las obligaciones señaladas en los párrafos b) al d) del artículo 12 al garantizar un certificado electrónico expedido por un prestador de servicios de certificación establecido en un Estado no perteneciente al Espacio Económico Europeo, será responsable por los daños y perjuicios causados por el uso de dicho certificado.

3. De manera particular, el prestador de servicios de certificación responderá de los perjuicios que se causen al firmante o a terceros de buena fe por la falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados de la extinción o suspensión de la vigencia del certificado electrónico.

4. Los prestadores de servicios de certificación asumirán toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de certificación.

5. La regulación contenida en esta ley sobre la responsabilidad del prestador de servicios de certificación se entiende sin perjuicio de lo establecido en la legislación sobre cláusulas abusivas en contratos celebrados con consumidores.

[Bloque 32]
Artículo 23. Limitaciones de responsabilidad de los prestadores de servicios de certificación.

1. El prestador de servicios de certificación no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe, si el firmante incurre en alguno de los siguientes supuestos:

a) No haber proporcionado al prestador de servicios de certificación información veraz, completa y exacta sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o para la extinción o suspensión de su vigencia, cuando su inexactitud no haya podido ser detectada por el prestador de servicios de certificación.

b) La falta de comunicación sin demora al prestador de servicios de certificación de cualquier modificación de las circunstancias reflejadas en el certificado electrónico.

c) Negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.

d) No solicitar la suspensión o revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma.

Proyecto De Ley nro:559/2010

e) Utilizar los datos de creación de firma cuando haya expirado el período de validez del certificado electrónico o el prestador de servicios de certificación le notifique la extinción o suspensión de su vigencia.

f) Superar los límites que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al firmante por el prestador de servicios de certificación.

2. En el caso de los certificados electrónicos que recojan un poder de representación del firmante, tanto éste como la persona o entidad representada, cuando ésta tenga conocimiento de la existencia del certificado, están obligados a solicitar la revocación o suspensión de la vigencia del certificado en los términos previstos en esta ley.

3. Cuando el firmante sea una persona jurídica, el solicitante del certificado electrónico asumirá las obligaciones indicadas en el apartado 1.

4. El prestador de servicios de certificación tampoco será responsable por los daños y perjuicios ocasionados al firmante o a terceros de buena fe si el destinatario de los documentos firmados electrónicamente actúa de forma negligente. Se entenderá, en particular, que el destinatario actúa de forma negligente en los siguientes casos:

a) Cuando no compruebe y tenga en cuenta las restricciones que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él.

b) Cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado electrónico publicada en el servicio de consulta sobre la vigencia de los certificados o cuando no verifique la firma electrónica.

5. El prestador de servicios de certificación no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe por la inexactitud de los datos que consten en el certificado electrónico si éstos le han sido acreditados mediante documento público, inscrito en un registro público si así resulta exigible. En caso de que dichos datos deban figurar inscritos en un registro público, el prestador de servicios de certificación podrá, en su caso, comprobarlos en el citado registro antes de la expedición del certificado, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

6. La exención de responsabilidad frente a terceros obliga al prestador de servicios de certificación a probar que actuó en todo caso con la debida diligencia.

Se modifica el apartado 5 por el art. 5.4 de la Ley 56/2007, de 28 de diciembre. Ref. BOE-A-2007-22440

Última actualización, publicada el 29/12/2007, en vigor a partir del 30/12/2007.
Texto original, publicado el 20/12/2003, en vigor a partir del 20/03/2004.

[Bloque 33]
TÍTULO IV

Dispositivos de firma electrónica y sistemas de certificación de prestadores de servicios de certificación y de dispositivos de firma electrónica

[Bloque 34]
CAPÍTULO I

Dispositivos de firma electrónica

[Bloque 35]
Artículo 24. Dispositivos de creación de firma electrónica.

Proyecto De Ley nro:559/2010

1. Los datos de creación de firma son los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.

2. Un dispositivo de creación de firma es un programa o sistema informático que sirve para aplicar los datos de creación de firma.

3. Un dispositivo seguro de creación de firma es un dispositivo de creación de firma que ofrece, al menos, las siguientes garantías:

a) Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.

b) Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.

c) Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.

d) Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma.

[Bloque 36]
Artículo 25. Dispositivos de verificación de firma electrónica.

1. Los datos de verificación de firma son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

2. Un dispositivo de verificación de firma es un programa o sistema informático que sirve para aplicar los datos de verificación de firma.

3. Los dispositivos de verificación de firma electrónica garantizarán, siempre que sea técnicamente posible, que el proceso de verificación de una firma electrónica satisfaga, al menos, los siguientes requisitos:

a) Que los datos utilizados para verificar la firma correspondan a los datos mostrados a la persona que verifica la firma.

b) Que la firma se verifique de forma fiable y el resultado de esa verificación se presente correctamente.

c) Que la persona que verifica la firma electrónica pueda, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.

d) Que se muestren correctamente tanto la identidad del firmante o, en su caso, conste claramente la utilización de un seudónimo, como el resultado de la verificación.

e) Que se verifiquen de forma fiable la autenticidad y la validez del certificado electrónico correspondiente.

f) Que pueda detectarse cualquier cambio relativo a su seguridad.

4. Asimismo, los datos referentes a la verificación de la firma, tales como el momento en que ésta se produce o una constatación de la validez del certificado electrónico en ese momento, podrán ser almacenados por la persona que verifica la firma electrónica o por terceros de confianza.

[Bloque 37]
CAPÍTULO II

Proyecto De Ley nro:559/2010

Certificación de prestadores de servicios de certificación y de dispositivos de creación de firma electrónica

[Bloque 38]
Artículo 26. Certificación de prestadores de servicios de certificación.

1. La certificación de un prestador de servicios de certificación es el procedimiento voluntario por el que una entidad cualificada pública o privada emite una declaración a favor de un prestador de servicios de certificación, que implica un reconocimiento del cumplimiento de requisitos específicos en la prestación de los servicios que se ofrecen al público.

2. La certificación de un prestador de servicios de certificación podrá ser solicitada por éste y podrá llevarse a cabo, entre otras, por entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo con lo dispuesto en la Ley 21/1992, de 16 de julio, de Industria, y en sus disposiciones de desarrollo.

3. En los procedimientos de certificación podrán utilizarse normas técnicas u otros criterios de certificación adecuados. En caso de utilizarse normas técnicas, se emplearán preferentemente aquellas que gocen de amplio reconocimiento aprobadas por organismos de normalización europeos y, en su defecto, otras normas internacionales o españolas.

4. La certificación de un prestador de servicios de certificación no será necesaria para reconocer eficacia jurídica a una firma electrónica.

[Bloque 39]
Artículo 27. Certificación de dispositivos seguros de creación de firma electrónica.

1. La certificación de dispositivos seguros de creación de firma electrónica es el procedimiento por el que se comprueba que un dispositivo cumple los requisitos establecidos en esta ley para su consideración como dispositivo seguro de creación de firma.

2. La certificación podrá ser solicitada por los fabricantes o importadores de dispositivos de creación de firma y se llevará a cabo por las entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo con lo dispuesto en la Ley 21/1992, de 16 de julio, de Industria y en sus disposiciones de desarrollo.

3. En los procedimientos de certificación se utilizarán las normas técnicas cuyos números de referencia hayan sido publicados en el "Diario Oficial de la Unión Europea" y, excepcionalmente, las aprobadas por el Ministerio de Ciencia y Tecnología que se publicarán en la dirección de Internet de este Ministerio.

4. Los certificados de conformidad de los dispositivos seguros de creación de firma serán modificados o, en su caso, revocados cuando se dejen de cumplir las condiciones establecidas para su obtención.

Los organismos de certificación asegurarán la difusión de las decisiones de revocación de certificados de dispositivos de creación de firma.

[Bloque 40]
Artículo 28. Reconocimiento de la conformidad con la normativa aplicable a los productos de firma electrónica.

1. Se presumirá que los productos de firma electrónica aludidos en el párrafo d) del apartado 1 del artículo 20 y en el apartado 3 del artículo 24 son conformes con los requisitos previstos en dichos artículos si se ajustan a las normas técnicas correspondientes cuyos números de referencia hayan sido publicados en el "Diario Oficial de la Unión Europea".

2. Se reconocerá eficacia a los certificados de conformidad sobre dispositivos seguros de creación de firma que hayan sido otorgados por los organismos designados para ello en cualquier Estado miembro del Espacio Económico Europeo.

Proyecto De Ley nro:559/2010

[Bloque 41]
TÍTULO V

Supervisión y control

[Bloque 42]
Artículo 29. Supervisión y control.

1. El Ministerio de Ciencia y Tecnología controlará el cumplimiento por los prestadores de servicios de certificación que expidan al público certificados electrónicos de las obligaciones establecidas en esta ley y en sus disposiciones de desarrollo. Asimismo, supervisará el funcionamiento del sistema y de los organismos de certificación de dispositivos seguros de creación de firma electrónica.

2. El Ministerio de Ciencia y Tecnología realizará las actuaciones inspectoras que sean precisas para el ejercicio de su función de control.

Los funcionarios adscritos al Ministerio de Ciencia y Tecnología que realicen la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

3. El Ministerio de Ciencia y Tecnología podrá acordar las medidas apropiadas para el cumplimiento de esta ley y sus disposiciones de desarrollo.

4. El Ministerio de Ciencia y Tecnología podrá recurrir a entidades independientes y técnicamente cualificadas para que le asistan en las labores de supervisión y control sobre los prestadores de servicios de certificación que le asigna esta ley.

[Bloque 43]
Artículo 30. Deber de información y colaboración.

1. Los prestadores de servicios de certificación, la entidad independiente de acreditación y los organismos de certificación tienen la obligación de facilitar al Ministerio de Ciencia y Tecnología toda la información y colaboración precisas para el ejercicio de sus funciones.

En particular, deberán permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la inspección de que se trate, siendo de aplicación, en su caso, lo dispuesto en el artículo 8.5 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa. En sus inspecciones podrán ir acompañados de expertos o peritos en las materias sobre las que versen aquéllas.

2. Los prestadores de servicios de certificación deberán comunicar al Ministerio de Ciencia y Tecnología el inicio de su actividad, sus datos de identificación, incluyendo la identificación fiscal y registral, en su caso, los datos que permitan establecer comunicación con el prestador, incluidos el nombre de dominio de internet, los datos de atención al público, las características de los servicios que vayan a prestar, las certificaciones obtenidas para sus servicios y las certificaciones de los dispositivos que utilicen. Esta información deberá ser convenientemente actualizada por los prestadores y será objeto de publicación en la dirección de internet del citado ministerio con la finalidad de otorgarle la máxima difusión y conocimiento.

3. Cuando, como consecuencia de una actuación inspectora, se tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, se dará cuenta de los mismos a los órganos u organismos competentes para su supervisión y sanción.

[Bloque 44]
TÍTULO VI

Infracciones y sanciones

Proyecto De Ley nro:559/2010

[Bloque 45]
Artículo 31. Infracciones.

1. Las infracciones de los preceptos de esta ley se clasifican en muy graves, graves y leves.

2. Son infracciones muy graves:

a) El incumplimiento de alguna de las obligaciones establecidas en los artículos 18 y 20 en la expedición de certificados reconocidos, siempre que se hayan causado daños graves a los usuarios o la seguridad de los servicios de certificación se haya visto gravemente afectada.

Lo dispuesto en este apartado no será de aplicación respecto al incumplimiento de la obligación de constitución de la garantía económica prevista en el apartado 2 del artículo 20.

b) La expedición de certificados reconocidos sin realizar todas las comprobaciones previas señaladas en el artículo 12, cuando ello afecte a la mayoría de los certificados reconocidos expedidos en los tres años anteriores al inicio del procedimiento sancionador o desde el inicio de la actividad del prestador si este período es menor.

3. Son infracciones graves:

a) El incumplimiento de alguna de las obligaciones establecidas en los artículos 18 y 20 en la expedición de certificados reconocidos, excepto de la obligación de constitución de la garantía prevista en el apartado 2 del artículo 20, cuando no constituya infracción muy grave.

b) La falta de constitución por los prestadores que expidan certificados reconocidos de la garantía económica contemplada en el apartado 2 del artículo 20.

c) La expedición de certificados reconocidos sin realizar todas las comprobaciones previas indicadas en el artículo 12, en los casos en que no constituya infracción muy grave.

d) El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de las obligaciones señaladas en el artículo 18, si se hubieran causado daños graves a los usuarios o la seguridad de los servicios de certificación se hubiera visto gravemente afectada.

e) El incumplimiento por los prestadores de servicios de certificación de las obligaciones establecidas en el artículo 21 respecto al cese de actividad de los mismos o la producción de circunstancias que impidan la continuación de su actividad, cuando las mismas no sean sancionables de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

f) La resistencia, obstrucción, excusa o negativa injustificada a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta ley y la falta o deficiente presentación de la información solicitada por parte del Ministerio de Ciencia y Tecnología en su función de inspección y control.

g) El incumplimiento de las resoluciones dictadas por el Ministerio de Ciencia y Tecnología para asegurar que el prestador de servicios de certificación se ajuste a esta ley.

4. Constituyen infracciones leves:

El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de las obligaciones establecidas en el artículo 18; y el incumplimiento por los prestadores de servicios de certificación de las restantes obligaciones establecidas en esta Ley, cuando no constituya infracción grave o muy grave, con excepción de las obligaciones contenidas en el apartado 2 del artículo 30.

Se modifica el apartado 4 por el art. 5.5 de la Ley 56/2007, de 28 de diciembre. Ref. BOE-A-2007-22440

Proyecto De Ley nro:559/2010

Última actualización, publicada el 29/12/2007, en vigor a partir del 30/12/2007.
Texto original, publicado el 20/12/2003, en vigor a partir del 20/03/2004.

[Bloque 46]
Artículo 32. Sanciones.

1. Por la comisión de infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

a) Por la comisión de infracciones muy graves, se impondrá al infractor multa de 150.001 a 600.000 euros.

La comisión de dos o más infracciones muy graves en el plazo de tres años, podrá dar lugar, en función de los criterios de graduación del artículo siguiente, a la sanción de prohibición de actuación en España durante un plazo máximo de dos años.

b) Por la comisión de infracciones graves, se impondrá al infractor multa de 30.001 a 150.000 euros.

c) Por la comisión de infracciones leves, se impondrá al infractor una multa por importe de hasta 30.000 euros.

2. Las infracciones graves y muy graves podrán llevar aparejada, a costa del sancionado, la publicación de la resolución sancionadora en el "Boletín Oficial del Estado" y en dos periódicos de difusión nacional o en la página de inicio del sitio de internet del prestador y, en su caso, en el sitio de internet del Ministerio de Ciencia y Tecnología, una vez que aquélla tenga carácter firme.

Para la imposición de esta sanción, se considerará la repercusión social de la infracción cometida, el número de usuarios afectados y la gravedad del ilícito.

[Bloque 47]
Artículo 33. Graduación de la cuantía de las sanciones.

La cuantía de las multas que se impongan, dentro de los límites indicados, se graduará teniendo en cuenta lo siguiente:

a) La existencia de intencionalidad o reiteración.

b) La reincidencia, por comisión de infracciones de la misma naturaleza, sancionadas mediante resolución firme.

c) La naturaleza y cuantía de los perjuicios causados.

d) Plazo de tiempo durante el que se haya venido cometiendo la infracción e) El beneficio que haya reportado al infractor la comisión de la infracción.

f) Volumen de la facturación a que afecte la infracción cometida.

[Bloque 48]
Artículo 34. Medidas provisionales.

1. En los procedimientos sancionadores por infracciones graves o muy graves el Ministerio de Ciencia y Tecnología podrá adoptar, con arreglo a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y sus normas de desarrollo, las medidas de carácter provisional que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte, el buen fin del procedimiento, evitar el mantenimiento de los efectos de la infracción y las exigencias de los intereses generales.

Proyecto De Ley nro:559/2010

En particular, podrán acordarse las siguientes:

a) Suspensión temporal de la actividad del prestador de servicios de certificación y, en su caso, cierre provisional de sus establecimientos.

b) Precinto, depósito o incautación de registros, soportes y archivos informáticos y de documentos en general, así como de aparatos y equipos informáticos de todo tipo.

c) Advertencia al público de la existencia de posibles conductas infractoras y de la incoación del expediente sancionador de que se trate, así como de las medidas adoptadas para el cese de dichas conductas.

En la adopción y cumplimiento de las medidas de restricción a que alude este apartado se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y a la protección de los datos personales, cuando éstos pudieran resultar afectados.

2. En los supuestos de daños de excepcional gravedad en la seguridad de los sistemas empleados por el prestador de servicios de certificación que menoscaben seriamente la confianza de los usuarios en los servicios ofrecidos, el Ministerio de Ciencia y Tecnología podrá acordar la suspensión o pérdida de vigencia de los certificados afectados, incluso con carácter definitivo.

3. En todo caso, se respetará el principio de proporcionalidad de la medida a adoptar con los objetivos que se pretendan alcanzar en cada supuesto.

4. En casos de urgencia y para la inmediata protección de los intereses implicados, las medidas provisionales previstas en este artículo podrán ser acordadas antes de la iniciación del expediente sancionador.

Las medidas deberán ser confirmadas, modificadas o levantadas en el acuerdo de iniciación del procedimiento, que deberá efectuarse dentro de los 15 días siguientes a su adopción, el cual podrá ser objeto del recurso que proceda.

En todo caso, dichas medidas quedarán sin efecto si no se inicia el procedimiento sancionador en dicho plazo o cuando el acuerdo de iniciación no contenga un pronunciamiento expreso acerca de las mismas.

[Bloque 49]
Artículo 35. Multa coercitiva.

El órgano administrativo competente para resolver el procedimiento sancionador podrá imponer multas coercitivas por importe que no exceda de 6.000 euros por cada día que transcurra sin cumplir las medidas provisionales que hubieran sido acordadas.

[Bloque 50]
Artículo 36. Competencia y procedimiento sancionador.

1. La imposición de sanciones por el incumplimiento de lo previsto en esta ley corresponderá, en el caso de infracciones muy graves, al Ministro de Ciencia y Tecnología y en el de infracciones graves y leves, al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

No obstante, el incumplimiento de las obligaciones establecidas en el artículo 17 será sancionado por la Agencia de Protección de Datos con arreglo a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. La potestad sancionadora regulada en esta Ley se ejercerá de conformidad con lo establecido al respecto en la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y en sus normas de desarrollo.

[Bloque 51]

Proyecto De Ley nro:559/2010

Disposición adicional primera. Fe pública y uso de firma electrónica.

1. Lo dispuesto en esta ley no sustituye ni modifica las normas que regulan las funciones que corresponden a los funcionarios que tengan legalmente la facultad de dar fe en documentos en lo que se refiere al ámbito de sus competencias siempre que actúen con los requisitos exigidos en la ley.

2. En el ámbito de la documentación electrónica, corresponderá a las entidades prestadoras de servicios de certificación acreditar la existencia de los servicios prestados en el ejercicio de su actividad de certificación electrónica, a solicitud del usuario, o de una autoridad judicial o administrativa.

[Bloque 52]
Disposición adicional segunda. Ejercicio de la potestad sancionadora sobre la entidad de acreditación y los organismos de certificación de dispositivos de creación de firma electrónica.

1. En el ámbito de la certificación de dispositivos de creación de firma, corresponderá al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Ciencia y Tecnología la imposición de sanciones por la comisión, por los organismos de certificación de dispositivos seguros de creación de firma electrónica o por la entidad que los acredite, de las infracciones graves previstas en los párrafos e), f) y g) del apartado segundo del artículo 31 de la Ley 21/1992, de 16 de julio, de Industria, y de las infracciones leves indicadas en el párrafo a) del apartado 3 del artículo 31 de la citada ley que cometan en el ejercicio de actividades relacionadas con la certificación de firma electrónica.

2. Cuando dichas infracciones merezcan la calificación de infracciones muy graves, serán sancionadas por el Ministro de Ciencia y Tecnología.

[Bloque 53]
Disposición adicional tercera. Expedición de certificados electrónicos a entidades sin personalidad jurídica para el cumplimiento de obligaciones tributarias.

Podrán expedirse certificados electrónicos a las entidades sin personalidad jurídica a que se refiere el artículo 33 de la Ley General Tributaria a los solos efectos de su utilización en el ámbito tributario, en los términos que establezca el Ministro de Hacienda.

[Bloque 54]
Disposición adicional cuarta. Prestación de servicios por la Fabrica Nacional de Moneda y Timbre-Real Casa de la Moneda.

Lo dispuesto en esta ley se entiende sin perjuicio de lo establecido en el artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social.

[Bloque 55]
Disposición adicional quinta. Modificación del artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social.

Se añaden apartado doce al artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, con la siguiente redacción.

"Doce. En el ejercicio de las funciones que le atribuye el presente artículo, la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda estará exenta de la constitución de la garantía a la que se refiere el apartado 2 del artículo 20 de la Ley 59/2003, de Firma Electrónica."

[Bloque 56]
Disposición adicional sexta. Régimen jurídico del documento nacional de identidad electrónico.

1. Sin perjuicio de la aplicación de la normativa vigente en materia del documento nacional de identidad en todo aquello que se adecue a sus características particulares, el documento nacional de identidad electrónico

Proyecto De Ley nro:559/2010

se regirá por su normativa específica.

2. El Ministerio de Ciencia y Tecnología podrá dirigirse al Ministerio del Interior para que por parte de éste se adopten las medidas necesarias para asegurar el cumplimiento de las obligaciones que le incumban como prestador de servicios de certificación en relación con el documento nacional de identidad electrónico.

[Bloque 57]
Disposición adicional séptima. Emisión de facturas por vía electrónica.

Lo dispuesto en esta ley se entiende sin perjuicio de las exigencias derivadas de las normas tributarias en materia de emisión de facturas por vía electrónica.

[Bloque 58]
Disposición adicional octava. Modificaciones de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Uno. Adición de un nuevo apartado 3 al artículo 10 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Se añade un apartado 3 con el siguiente texto:

"3. Cuando se haya atribuido un rango de numeración telefónica a servicios de tarificación adicional en el que se permita el acceso a servicios de la sociedad de la información y se requiera su utilización por parte del prestador de servicios, esta utilización y la descarga de programas informáticos que efectúen funciones de marcación, deberán realizarse con el consentimiento previo, informado y expreso del usuario.

A tal efecto, el prestador del servicio deberá proporcionar al menos la siguiente información:

a) Las características del servicio que se va a proporcionar.

b) Las funciones que efectuarán los programas informáticos que se descarguen, incluyendo el número telefónico que se marcará.

c) El procedimiento para dar fin a la conexión de tarificación adicional, incluyendo una explicación del momento concreto en que se producirá dicho fin, y d) El procedimiento necesario para restablecer el número de conexión previo a la conexión de tarificación adicional.

La información anterior deberá estar disponible de manera claramente visible e identificable.

Lo dispuesto en este apartado se entiende sin perjuicio de lo establecido en la normativa de telecomunicaciones, en especial, en relación con los requisitos aplicables para el acceso por parte de los usuarios a los rangos de numeración telefónica, en su caso, atribuidos a los servicios de tarificación adicional."

Dos. Los apartados 2, 3 y 4 del artículo 38 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico se redactan en los siguientes términos:

"2. Son infracciones muy graves:

a) El incumplimiento de las órdenes dictadas en virtud del artículo 8 en aquellos supuestos en que hayan sido dictadas por un órgano administrativo.

b) El incumplimiento de la obligación de suspender la transmisión, el alojamiento de datos, el acceso a la red o la prestación de cualquier otro servicio equivalente de intermediación, cuando un órgano administrativo competente lo ordene, en virtud de lo dispuesto en el artículo 11.

Proyecto De Ley nro:559/2010

c) El incumplimiento significativo de la obligación de retener los datos de tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información, prevista en el artículo 12.

d) La utilización de los datos retenidos, en cumplimiento del artículo 12, para fines distintos de los señalados en él.

3. Son infracciones graves:

a) El incumplimiento de la obligación de retener los datos de tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información, prevista en el artículo 12, salvo que deba ser considerado como infracción muy grave.

b) El incumplimiento significativo de lo establecido en los párrafos a) y f) del artículo 10.1.

c) El envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente o el envío, en el plazo de un año, de más de tres comunicaciones comerciales por los medios aludidos a un mismo destinatario, cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21.

d) El incumplimiento significativo de la obligación del prestador de servicios establecida en el apartado 1 del artículo 22, en relación con los procedimientos para revocar el consentimiento prestado por los destinatarios.

e) No poner a disposición del destinatario del servicio las condiciones generales a que, en su caso, se sujete el contrato, en la forma prevista en el artículo 27.

f) El incumplimiento habitual de la obligación de confirmar la recepción de una aceptación, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor.

g) La resistencia, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta ley.

h) El incumplimiento significativo de lo establecido en el apartado 3 del artículo 10.

i) El incumplimiento significativo de las obligaciones de información o de establecimiento de un procedimiento de rechazo del tratamiento de datos, establecidas en el apartado 2 del artículo 22.

4. Son infracciones leves:

a) La falta de comunicación al registro público en que estén inscritos, de acuerdo con lo establecido en el artículo 9, del nombre o nombres de dominio o direcciones de Internet que empleen para la prestación de servicios de la sociedad de la información.

b) No informar en la forma prescrita por el artículo 10.1 sobre los aspectos señalados en los párrafos b), c), d), e) y g) del mismo, o en los párrafos a) y f) cuando no constituya infracción grave.

c) El incumplimiento de lo previsto en el artículo 20 para las comunicaciones comerciales, ofertas promocionales y concursos.

d) El envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21 y no constituya infracción grave.

e) No facilitar la información a que se refiere el artículo 27.1, cuando las partes no hayan pactado su exclusión o el destinatario sea un consumidor.

Proyecto De Ley nro:559/2010

f) El incumplimiento de la obligación de confirmar la recepción de una petición en los términos establecidos en el artículo 28, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor, salvo que constituya infracción grave.

g) El incumplimiento de las obligaciones de información o de establecimiento de un procedimiento de rechazo del tratamiento de datos, establecidas en el apartado 2 del artículo 22, cuando no constituya una infracción grave.

h) El incumplimiento de la obligación del prestador de servicios establecida en el apartado 1 del artículo 22, en relación con los procedimientos para revocar el consentimiento prestado por los destinatarios cuando no constituya infracción grave.

i) El incumplimiento de lo establecido en el apartado 3 del artículo 10, cuando no constituya infracción grave."

Tres. Modificación del artículo 43, apartado 1, segundo párrafo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

El segundo párrafo del apartado 1 del artículo 43 queda redactado como sigue:

"No obstante lo anterior, la imposición de sanciones por incumplimiento de las resoluciones dictadas por los órganos competentes en función de la materia o entidad de que se trate a que se refieren los párrafos a) y b) del artículo 38.2 de esta ley corresponderá al órgano que dictó la resolución incumplida. Igualmente, corresponderá a la Agencia de Protección de Datos la imposición de sanciones por la comisión de las infracciones tipificadas en los artículos 38.3 c), d) e i) y 38.4 d), g) y h) de esta ley."

Cuatro. Modificación del artículo 43, apartado 2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

El apartado 2 del artículo 43 queda redactado como sigue:

"2. La potestad sancionadora regulada en esta ley se ejercerá de conformidad con lo establecido al respecto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y en sus normas de desarrollo. No obstante, el plazo máximo de duración del procedimiento simplificado será de tres meses."

[Bloque 59]
Disposición adicional novena. Garantía de accesibilidad para las personas con discapacidad y de la tercera edad.

Los servicios, procesos, procedimientos y dispositivos de firma electrónica deberán ser plenamente accesibles a las personas con discapacidad y de la tercera edad, las cuales no podrán ser en ningún caso discriminadas en el ejercicio de los derechos y facultades reconocidos en esta ley por causas basadas en razones de discapacidad o edad avanzada.

[Bloque 60]
Disposición adicional décima. Modificación de la Ley de Enjuiciamiento Civil.

Se añade un apartado tres al artículo 326 de la Ley de Enjuiciamiento Civil con el siguiente tenor:

"Cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá con arreglo a lo establecido en el artículo 3 de la Ley de Firma Electrónica."

[Bloque 61]
Disposición adicional undécima. Resolución de conflictos.

Proyecto De Ley nro:559/2010

Los usuarios y prestadores de servicios de certificación podrán someter los conflictos que se susciten en sus relaciones al arbitraje.

Cuando el usuario tenga la condición de consumidor o usuario, en los términos establecidos por la legislación de protección de los consumidores, el prestador y el usuario podrán someter sus conflictos al arbitraje de consumo, mediante la adhesión de aquéllos al Sistema Arbitral de Consumo competente.

Se añade por el art. 5.6 de la Ley 56/2007, de 28 de diciembre. Ref. BOE-A-2007-22440

[Esta "Disposición adicional undécima" ha sido añadida por la actualización publicada el 29/12/2007, en vigor a partir del 30/12/2007]

[Bloque 62]
Disposición transitoria primera. Validez de los certificados electrónicos expedidos previamente a la entrada en vigor de esta ley.

Los certificados electrónicos que hayan sido expedidos por prestadores de servicios de certificación en el marco del Real Decreto Ley 14/1999, de 17 de septiembre, sobre firma electrónica, mantendrán su validez.

[Bloque 63]
Disposición transitoria segunda. Prestadores de servicios de certificación establecidos en España antes de la entrada en vigor de esta ley.

Los prestadores de servicios de certificación establecidos en España antes de la entrada en vigor de esta ley deberán comunicar al Ministerio de Ciencia y Tecnología su actividad y las características de los servicios que presten en el plazo de un mes desde la referida entrada en vigor. Esta información será objeto de publicación en la dirección de internet del citado ministerio con la finalidad de otorgarle la máxima difusión y conocimiento.

[Bloque 64]
Disposición derogatoria única. Derogación normativa.

Queda derogado el Real Decreto Ley 14/1999, de 17 de septiembre, sobre firma electrónica y cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta ley.

[Bloque 65]
Disposición final primera. Fundamento constitucional.

Esta ley se dicta al amparo del artículo 149.1.8.ª, 18.ª, 21.ª y 29.ª de la Constitución.

[Bloque 66]
Disposición final segunda. Desarrollo reglamentario.

1. El Gobierno adaptará la regulación reglamentaria del documento nacional de identidad a las previsiones de esta ley.

2. Así mismo, se habilita al Gobierno para dictar las demás disposiciones reglamentarias que sean precisas para el desarrollo y aplicación de esta ley.

[Bloque 67]
Disposición final tercera. Entrada en vigor.

La presente ley entrará en vigor a los tres meses de su publicación en el "Boletín Oficial del Estado".

[Bloque 68]

Proyecto De Ley nro:559/2010

Por tanto, Mando a todos los españoles, particulares y autoridades, que guarden y hagan guardar esta ley.

Madrid, 19 de diciembre de 2003.

JUAN CARLOS R.

El Presidente del Gobierno,

JOSÉ MARÍA AZNAR LÓPEZ

http://www.boe.es/aeboe/consultas/bases_datos/act.php?c=3&item=2003/23399
Antecedentes (NAC.) - Informacion Parlamentaria
2) LEY 25.506
LEY DE FIRMA DIGITAL
BUENOS AIRES, 14 DE NOVIEMBRE DE 2001
BOLETIN OFICIAL, 14 DE DICIEMBRE DE 2001
- LEY VIGENTE -

REGLAMENTACION

Reglamentado por: DECRETO NACIONAL 2.628/2002 ((B.O. 20/12/2002))

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

OBSERVACIONES GENERALES

CANTIDAD DE ARTICULOS QUE COMPONEN LA NORMA 53

TEMA

LEY DE FIRMA DIGITAL-FIRMA DIGITAL-DOCUMENTO ELECTRONICO-FIRMA ELECTRONICACERTIFICADO DIGITAL

CAPITULO I
Consideraciones generales (artículos 1 al 12)
Objeto

ARTICULO 1 - 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.

Firma Digital.

ARTICULO 2 - 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.

Del requerimiento de firma.

ARTICULO 3 - 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

Proyecto De Ley nro:559/2010

o prescribe consecuencias para su ausencia.

Exclusiones.

ARTICULO 4 - 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.

Firma electrónica.

ARTICULO 5 - 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.

Documento digital.

ARTICULO 6 - 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.

Presunción de autoría.

ARTICULO 7 - Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma.

Presunción de integridad.

ARTICULO 8 - 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.

Validez.

ARTICULO 9 - Una firma digital es válida si cumple con los siguientes requisitos: a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante; b) Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente; c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado.

Remitente. Presunción.

ARTICULO 10. - 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.

Original.

ARTICULO 11. - 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.

Conservación.

Proyecto De Ley nro:559/2010

ARTICULO 12. - La exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción.

CAPITULO II
De los certificados digitales (artículos 13 al 16)
Certificado digital.

ARTICULO 13. - Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.

Requisitos de validez de los certificados digitales.

ARTICULO 14. - 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.

Período de vigencia del certificado digital.

ARTICULO 15. -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.

Reconocimiento de certificados extranjeros.

ARTICULO 16. - Los certificados digitales emitidos por certificadores extranjeros podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley y sus normas reglamentarias cuando: a) Reúnan las condiciones que establece la presente ley y la reglamentación correspondiente para los certificados emitidos por certificadores nacionales y se encuentre vigente un acuerdo de reciprocidad firmado por la República Argentina y el país de origen del certificador extranjero, o b) Tales certificados sean reconocidos por un certificador licenciado en el país, que garantice su validez y vigencia conforme a la presente ley. A fin de tener efectos, este reconocimiento deberá ser validado por la autoridad de aplicación.

CAPITULO III
Del certificador licenciado (artículos 17 al 23)
Del certificador licenciado.

ARTICULO 17. - 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.

Proyecto De Ley nro:559/2010

Certificados por profesión.

ARTICULO 18. - 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.

Funciones.

ARTICULO 19. - 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.

Licencia.

ARTICULO 20. - 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.

Obligaciones.

ARTICULO 21. - 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 nin guna 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

Proyecto De Ley nro:559/2010

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.

Cese del certificador.

ARTICULO 22. - 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.

Desconocimiento de la validez de un certificado digital.

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

CAPITULO IV
Del titular de un certificado digital (artículos 24 al 25)

Derechos del titular de un certificado digital.

ARTICULO 24. - 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

Proyecto De Ley nro:559/2010

intermedio del certificador licenciado.

Obligaciones del titular del certificado digital.

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

CAPITULO V
De la organización institucional (artículos 26 al 28)
Infraestructura de Firma Digital.

ARTICULO 26. - Los certificados digitales regulados por esta ley deben ser emitidos o reconocidos, según lo establecido por el artículo 16, por un certificador licenciado.

Sistema de Auditoría.

ARTICULO 27. - 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.

Comisión Asesora para la Infraestructura de Firma
Digital.

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

CAPITULO VI
De la autoridad de aplicación (artículos 29 al 32)
Autoridad de Aplicación.

ARTICULO 29. - La autoridad de aplicación de la presente ley será la Jefatura de Gabinete de Ministros.

Funciones.

ARTICULO 30. - 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.

Obligaciones.

Proyecto De Ley nro:559/2010

ARTICULO 31. - 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.

Arancelamiento.

ATICULO 32. - La autoridad de aplicación podrá cobrar un arancel de licenciamiento para cubrir su costo operativo y el de las auditorías realizadas por sí o por terceros contratados a tal efecto.

CAPITULO VII
Del sistema de auditoría (artículos 33 al 34)
Sujetos a auditar.

ARTICULO 33.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.

Requisitos de habilitación.

ARTICULO 34. - Podrán ser terceros habilitados para efectuar las auditorías las Universidades y organismos científicos y/o tecnológicos nacionales o provinciales, los Colegios y Consejos profesionales que acrediten experiencia profesional acorde en la materia.

CAPITULO VIII
De la Comisión Asesora para la Infraestructura de
Firma Digital (artículos 35 al 36)
Integración y funcionamiento.

ARTICULO 35.- 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.

Funciones.

ARTICULO 36. - 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

Proyecto De Ley nro:559/2010

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

CAPITULO IX
Responsabilidad (artículos 37 al 39)
Convenio de partes.

ARTICULO 37. - 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.

Responsabilidad de los certificadores licenciados
ante terceros.

ARTICULO 38. - 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.

Limitaciones de responsabilidad.

ARTICULO 39. - Los certificadores licenciados no son responsables en los siguientes casos: a) Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstos en la ley; b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización; c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el certificador pueda demostrar que ha tomado todas las medidas razonables.

CAPITULO X
Sanciones (artículos 40 al 46)
Procedimiento.

ARTICULO 40. - 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.

Referencias Normativas: Ley 19.549

Sanciones.

ARTICULO 41. - El incumplimiento de las obligaciones establecidas en la presente ley para los certificadores licenciados dará lugar a la aplicación de las siguientes sanciones: a) Apercibimiento; b) Multa de pesos diez mil ($ 10.000) a pesos quinientos mil ($ 500.000); c) Caducidad de la licencia. Su gradación según reincidencia y/u oportunidad serán establecidas por la reglamentación. El pago de la sanción que aplique el ente licenciante no relevará al certificador licenciado de eventuales reclamos por daños y perjuicios causados a terceros y/o bienes de propiedad de éstos, como consecuencia de la ejecución del contrato que celebren y/o por el incumplimiento de las obligaciones asumidas conforme al mismo y/ o la prestación del servicio.

Apercibimiento.

Proyecto De Ley nro:559/2010

ARTICULO 42. - 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.

Multa.

ARTICULO 43. - 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 par te 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.

Caducidad.

ARTICULO 44. - 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.

Recurribilidad.

ARTICULO 45. - 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.

Jurisdicción.

ARTICULO 46. - 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 Contenciosoadministrativo Federal.

CAPITULO XI
Disposiciones Complementarias (artículos 47 al 53)
Utilización por el Estado Nacional.

ARTICULO 47. - El Estado nacional utilizará las tecnologías y previsiones de la presente ley en su ámbito interno y en relación con los administrados de acuerdo con las condiciones que se fijen reglamentariamente en cada uno de sus poderes.

Implementación.

ARTICULO 48. - 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

Proyecto De Ley nro:559/2010

emanados de las jurisdicciones y entidades comprendidas en el artículo 8 de la Ley 24.156.

Referencias Normativas: LEY 24.156 Art.8

Reglamentación.

ARTICULO 49. - 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.

Invitación.

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

Equiparación a los efectos del derecho penal.

ARTICULO 51. - NOTA DE REDACCION (MODIFICA CODIGO PENAL)

Modifica a: Ley 11.179 - TEXTO ORDENADO POR DECRETO 3992/84 Art.78 Bis (INCORPORA ARTICULO)

Autorización al Poder Ejecutivo.

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

ARTICULO 53. Comuníquese al Poder Ejecutivo.

FIRMANTES

PASCUAL-MENEM-Aramburu-Oyarzún

ANEXO

Información: conocimiento adquirido acerca de algo o alguien. Procedimiento de verificación: proceso utilizado para determinar la validez de una firma digital. Dicho proceso debe considerar al menos: a) que dicha firma digital ha sido creada durante el período de validez del certificado digital del firmante; b) que dicha firma digital ha sido creada utilizando los datos de creación de firma digital correspondientes a los datos de verificación de firma digital indicados en el certificado del firmante; c) la verificación de la autenticidad y la validez de los certificados involucrados. Datos de creación de firma digital: datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear su firma digital. Datos de verificación de firma digital: datos únicos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma digital, la integridad del documento digital y la identidad del firmante. Dispositivo de creación de firma digital: dispositivo de hardware o software técnicamente confiable que permite firmar digitalmente. Dispositivo de verificación de firma digital: dispositivo de hardware o software técnicamente confiable que permite verificar la integridad del documento digital y la identidad del firmante. Políticas de certificación: reglas en las que se establecen los criterios de emisión y utilización de los certificados digitales. Técnicamente confiable: cualidad del conjunto de equipos de computación, software, protocolos de comunicación y de seguridad y procedimientos administrativos relacionados que cumplan los siguientes requisitos: 1. Resguardar contra la posibilidad de intrusión y/o uso no autorizado; 2. Asegurar la disponibilidad, confiabilidad, confidencialidad y correcto funcionamiento; 3.

Proyecto De Ley nro:559/2010

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.

Antecedentes (NAC.) - Informacion Parlamentaria
3) DECRETO NACIONAL 2.628/2002
DECRETO REGLAMENTARIO DE LA LEY 25506 SOBRE FIRMA DIGITAL
BUENOS AIRES, 19 DE DICIEMBRE DE 2002
BOLETIN OFICIAL, 20 DE DICIEMBRE DE 2002
- VIGENTE DE ALCANCE GENERAL -

GENERALIDADES
Sintesis:

SE REGLAMENTA LA LEY 25506 SOBRE FIRMA DIGITAL.

Reglamenta a: LEY 25.506

Observaciones Generales:

CANTIDAD DE ARTICULOS QUE COMPONEN LA NORMA: 46

TEMA

DECRETO REGLAMENTARIO-FIRMA DIGITAL-DOCUMENTO ELECTRONICO-FIRMA ELECTRONICACERTIFICADO DIGITAL

VISTO

la Ley Nº 25.506, el Decreto Nº 427 del 16 de abril de 1998, el Decreto Nº 78 del 10 de enero de 2002, el Decreto Nº 333 del 19 de febrero de 1985 y sus modificatorios y la Resolución Nº 194 del 27 de noviembre de 1998 de la ex SECRETARIA DE LA FUNCION PUBLICA, y

CONSIDERANDO

Que la sanción de la Ley Nº 25.506 de firma digital representa un avance significativo para la inserción, de nuestro país en la sociedad de la información y en la economía digital, brindando una oportunidad para el desarrollo del sector productivo vinculado a las nuevas tecnologías. Que otros países ya han normado sobre la materia, con positiva repercusión tanto en el ámbito privado como público. Que con la sanción de la citada Ley Nº 25.506, de firma digital se reconoce el empleo de la firma, digital y de la firma electrónica y su eficacia jurídica en las condiciones que la misma ley establece. Que dicho reconocimiento constituye un elemento esencial para otorgar seguridad a las transacciones electrónicas, promoviendo el comercio electrónico seguro, de modo de permitir la identificación en forma fehaciente de las personas que realicen transacciones electrónicas. Que asimismo, la sanción de la Ley Nº 25.506 otorga un decisivo impulso para la progresiva despapelización del Estado, contribuyendo a mejorar su gestión, facilitar el acceso de la comunidad a la información pública y posibilitar la realización de trámites por Internet en forma segura. Que la reglamentación de la Ley Nº 25.506 permitirá establecer una Infraestructura de Firma Digital que ofrezca autenticación, y garantía de integridad para los

Proyecto De Ley nro:559/2010

documentos digitales o electrónicos y constituir la base tecnológica que permita otorgarles validez jurídica. Que debe regularse el funcionamiento de los certificadores licenciados de manera de garantizar la adecuada prestación de los servicios de certificación. Que resulta necesario crear un Ente Administrador de Firma Digital, encargado de otorgar las licencias a los certificadores, supervisar su actividad y dictar las normas tendientes a asegurar el régimen de libre competencia en el mercado de los prestadores y protección de los usuarios de Firma Digital. Que la citada Ley contempla la creación de una Comisión Asesora para la Infraestructura de Firma Digital, conformada por un equipo multidisciplinario de especialistas en la materia, con el fin de asesorar y recomendar a la Autoridad de Aplicación estándares tecnológicos, y otros aspectos que hacen al funcionamiento de la mencionada Infraestructura, por lo cual deben establecerse las bases para su formación y adecuado funcionamiento. Que el Decreto Nº 427 del 16 de abril de 1998 ha sido una de las normas pioneras a nivel nacional e internacional en reconocer la validez jurídica de la firma digital, para lo cual creó una Infraestructura de Firma Digital para el Sector Público Nacional bajo la dependencia de la JEFATURA DE GABINETE DE MINISTROS. Que esta experiencia ha sido un antecedente fundamental para la incorporación de la tecnología en la gestión pública, constituyendo una fuente de consulta para distintas jurisdicciones nacionales y provinciales. Que dado que la Ley Nº 25.506 establece una Infraestructura de Firma Digital de alcance federal, a fin de optimizar el aprovechamiento de los recursos y las experiencias desarrolladas, resulta conveniente subsumir la mencionada Infraestructura del Sector Público Nacional dentro de la creada a nivel federal por la Ley citada. Que a tal fin, corresponde derogar el Decreto Nº 427/98, por el cual se reconoce el empleo de la firma digital en el ámbito de la Administración Pública Nacional, ya que la Ley Nº 25.506 cubre los objetivos y el alcance del mencionado Decreto. Que ha tomado intervención el servicio jurídico competente. Que la presente medida se dicta en virtud lo dispuesto por el artículo 49 de la Ley Nº 25.506, y por el artículo 99, inciso 2, de la Constitución de la Nación Argentina. Por ello,

EL PRESIDENTE DE LA NACION ARGENTINA DECRETA:

CAPITULO I CONSIDERACIONES GENERALES (artículos 1 al 3)
Objeto

*Artículo 1º - La presente reglamentación regula el empleo de la firma electrónica y de la firma digital y su eficacia jurídica. En los casos contemplados por los artículos 3º, 4º y 5º de la Ley Nº 25.506 podrán utilizarse los siguientes sistemas de comprobación de autoría e integridad: a) Firma electrónica, b) Firma electrónica basada en certificados digitales emitidos porcertificadores no licenciados en el marco de la presente reglamentación. c) Firma digital basada en certificados digitales emitidos por certificadores licenciados en el marco de la presente reglamentación, d) Firma digital basada en certificados digitales emitidos por certificadores extranjeros que hayan sido reconocidos en los siguientes casos: 1. En virtud de la existencia de acuerdos de reciprocidad entre la República Argentina y el país de origen del certificador extranjero. 2. Por un certificador licenciado en el país en el marco de la presente reglamentación y validado por la Autoridad de Aplicación.

Modificado por: DECRETO NACIONAL 724/2006 Art.5 (Inc. b) sustituido (B.O. 13-06-2006).)

Validez de los certificados, digitales emitidos por certificadores no licenciados

Art. 2 - . Los certificados digitales emitidos por certificadores no licenciados serán válidos para producir los efectos jurídicos que la ley otorga a la firma electrónica.

Certificados digitales emitidos por certificadores licenciados.

Art. 3º - Los certificados digitales contemplados, en el artículo 13 de la Ley Nº 25.506 son aquellos cuya utilización permite disponer de una firma digital amparada por las presunciones de autoría e integridad establecidas en los artículos 7º y 8º de la ley citada.

CAPITULO II DE LA AUTORIDAD DE APLICACION (artículos 4 al 6)

Proyecto De Ley nro:559/2010

Normas técnicas.

Art. 4º - Facúltase a la JEFATURA DE GABINETE DE MINISTROS, a determinar las normas y los procedimientos técnicos para la generación, comunicación, archivo y conservación del documento digital o electrónico, según lo previsto en los artículos 11 y 12 de la Ley Nº 25.506.

Conservación.

Art. 5º - El cumplimiento de la exigencia legal de conservar documentos, registros o datos, conforme a la legislación vigente a la materia, podrá quedar satisfecha con la conservación de los correspondientes, documentos digitales firmados digitalmente. Los documentos, registros o datos electrónicos, deberán ser almacenados por los intervinientes o por terceros confiables aceptados por los intervinientes, durante los plazos establecidos en las normas específicas. Se podrán obtener copias autenticadas a partir de los originales en formato digital firmado digitalmente. La certificación de autenticidad se hará de conformidad a los procedimientos legales, vigentes para el acto de que se trate, identificando el soporte que procede la copia.

Regulación.

Art. 6º - Facúltase a la JEFATURA DE GABINETE DE MINISTROS a establecer: a) Los estándares tecnológicos y de seguridad aplicables en consonancia con estándares internacionales. b) Los procedimientos de firma y verificación en consonancia con los estándares tecnológicos definidos conforme el inciso precedente. c) Las condiciones mínimas de emisión de certificados digitales. d) Los casos en los cuales deben revocarse los certificados digitales e) Los datos considerados públicos contenidos en los certificados digitales. f) Los mecanismos que garantizarán la validez y autoría de las listas de certificados revocados. g) La información que los certificadores licenciados deberán publicar por internet. h) La información que los certificadores licenciados deberán publicar en el Boletín Oficial. i) Los procedimientos mínimos de revocación de certificados digitales cualquiera que sea la fuente de emisión, y los procedimientos mínimos de conservación de la documentación de respaldo de la operatoria de los certificadores licenciados, en el caso que éstos cesen su actividad. j) El sistema de auditoría, incluyendo las modalidades de difusión de los informes de auditoría y los requisitos de habilitación para efectuar auditorías. k) Las condiciones y procedimientos para el otorgamiento y revocación de las licencias. l) Las normas y procedimientos para la homologación de los dispositivos de creación y verificación de firmas digitales. m) El reglamento de funcionamiento de la Comisión Asesora para la Infraestructura de Firma Digital. n) El procedimiento de instrucción sumarial y la gradación de sanciones previstas en la Ley Nº 25.506, en virtud de reincidencia y/u oportunidad. o) Los procedimientos aplicables para el reconocimiento de certificados extranjeros. p) Las condiciones de aplicación de la presente ley en el Sector Público Nacional, incluyendo la autorización para prestar servicios de certificación digital para las entidades y jurisdicciones de la Administración Pública Nacional. q) Los contenidos mínimos de las políticas de certificación de acuerdo con los estándares nacionales e internacionales y las condiciones mínimas que deberán cumplirse en el caso de cese de actividades de un certificador licenciado. r) Los niveles de licenciamiento. s) Reglamentar el uso y los alcances de los certificados de firma digital emitidos por los Registros Públicos de Contratos. t) Exigir las garantías y seguros necesarios para prestar el servicio previsto. u) Las condiciones de prestación de otros servicios en relación con la firma digital y otros temas cubiertos en la ley.

Nota de redacción. Ver: Resolución 435/2004 Art.1 (Jefatura de Gabinete de Ministros (B.O. 12-07-2004). Se aprueba el Reglamento de funcionamiento de la Comisión Asesora para la Infraestructura de Firma Digital.)

CAPITULO III
DE LA COMISION ASESORA PARA LA INFRAESTRUCTURA DE FIRMA DIGITAL (artículos 7 al 10)

Comisión Asesora para la Infraestructura de Firma Digital.

Art. 7º - En el ámbito de la JEFATURA DE GABINETE DE MINISTROS funcionará la Comisión Asesora para la

Proyecto De Ley nro:559/2010

Infraestructura de Firma Digital, que se constituirá de acuerdo a lo dispuesto por el artículo 35 de la Ley Nº 25.506.

Integración.

Art. 8º - La Comisión Asesora para la Infraestructura de Firma Digital estará integrada multidisciplinariamente por profesionales de carreras afines a la actividad, de reconocida trayectoria y experiencia, provenientes de organismos del Estado Nacional, Universidades, Cámaras, Colegios u otros entes representativos profesionales. Para integrar la Comisión Asesora para la Infraestructura de Firma Digital se deberán reunir los siguientes requisitos: a) Poseer título universitario, expedido por Universidad Nacional o privada reconocida por el Estado, correspondiente a carrera profesional de duración no inferior a CUATRO (4) años, con incumbencias relacionadas con la materia. b) Antecedentes académicos y/o profesionales o laborales en la materia.

Ejercicio de funciones.

Art. 9 - El ejercicio de las funciones como miembro de la Comisión Asesora para la Infraestructura de Firma Digital será ad honorem.

Consulta Pública.

Art. 10. - La Comisión Asesora para la Infraestructura de Firma Digital establecerá los mecanismos que permitan mantener un intercambio de información fluido con organismos públicos, Cámaras, usuarios y asociaciones de consumidores sobre los temas que se está tratando a los efectos de recibir aportes y opiniones. Para cumplir con este cometido podrá implementar consultas públicas presenciales, por escrito o mediante foros virtuales, abiertos e indiscriminados, o cualquier otro medio que la Comisión considere conveniente o necesario.

CAPITULO IV DEL ENTE ADMINISTRADOR DE FIRMA DIGITAL (artículos 11 al 17)
Ente Administrador de Firma Digital.

Art. 11. - Créase el Ente Administrador de Firma Digital dependiente de la JEFATURA DE GABINETE DE MINISTROS, como órgano técnico, administrativo encargado de otorgar las licencias a los certificadores y de supervisar su actividad, según las exigencias instituidas por el presente decreto y las normas reglamentarias, modificatorias o de aplicación que se dicten en el futuro y de dictar las normas tendientes a asegurar el régimen de libre competencia, equilibrio de participación en el mercado de los prestadores y protección de los usuarios.

Nota de redacción. Ver: DECRETO NACIONAL 1.028/2003 Art.1 ((B.O. 10-11-2003) SE DISUELVE EL ENTE ADMINISTRADOR DE FIRMA DIGITAL.)

Autoridades del Ente Administrador de Firma Digital

Art. 12. - . El Ente Administrador de Firma Digital será conducido por un Directorio integrado por TRES (3) miembros, designados por el JEFE DE GABINETE DE MINISTROS, previo concurso. Hasta tanto, sea realizado el concurso el JEFE DE GABINETE DE MINISTROS designará a los integrantes del Directorio, uno de los cuales ocupará el cargo de Presidente del Ente. El gerenciamiento del Ente estará a cargo del Coordinador Ejecutivo designado por el JEFE DE GABINETE DE MINISTROS.

Funciones del Ente Administrador.

Art. 13. - Son funciones del Ente Administrador: a) Otorgar las licencias habilitantes para acreditar a los certificadores en las condiciones que fijen el presente decreto y las normas reglamentarias, modificatorias o de aplicación que se dicten en el futuro. b) Fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los certificadores licenciados. c) Denegar las solicitudes de licencia a los prestadores de servicios de certificación que no cumplan

Proyecto De Ley nro:559/2010

con los requisitos establecidos para su licenciamiento. d) Revocar las licencias otorgadas a los Certificadores licenciados que dejen de cumplir con los requisitos establecidos para su licenciamiento. e) Aprobar las políticas de certificación, el manual de procedimiento, el plan de seguridad, de cese de actividades y el plan de contingencia, presentado por los certificadores solicitantes de la licencia o licenciados. f) Solicitar los informes de auditoría en los casos que correspondiere. g) Realizar inspecciones a los certificadores licenciados por sí o por terceros. h) Homologar los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la presente reglamentación. i) Disponer la instrucción sumarial, la aplicación de sanciones e inhabilitar en forma temporal o permanente a todo certificador o licenciado que no respetare o incumpliere los requerimientos y disposiciones de la Ley Nº 25.506, el presente decreto y las normas complementarias. j) 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, direcciones de internet y certificados digitales de los certificadores licenciados. 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, los domicilios, los números telefónicos, direcciones de internet y certificados digitales de los certificadores cuyas licencias han sido revocadas. I) 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, el domicilio, números telefónicos, direcciones de internet y certificados digitales del Ente Administrador. m) Administrar los recursos generados de acuerdo con lo dispuesto por el artículo 16 de la presente reglamentación, provenientes de las distintas fuentes de financiamiento. n) Fijar el concepto y los importes de todo tipo de aranceles y multas previstos en la Ley Nº 25.506 y en el artículo 16 de la presente reglamentación. o) Solicitar la ampliación o aclaración sobre la documentación presentada por el certificador. p) Dictar las normas tendientes a asegurar el régimen de libre competencia, equilibrio de parti- cipación en el mercado de los prestadores y protección de los usuarios.

Obligaciones del Ente Administrador.

Art. 14. - El Ente Administrador tiene idénticas obligaciones que los titulares, de certificados y que los Certificadores Licenciados, en su caso, y además debe: a) Permitir el acceso público permanente a la nómina actualizada de certificadores licenciados con los datos correspondientes. b) Supervisar la ejecución del plan de cese de actividades de los Certificadores licenciados que discontinúan sus funciones; c) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas. d) Supervisar la ejecución de planes de contingencia de los certificadores licenciados. e) Efectuar las tareas de control del cumplimiento de las recomendaciones formuladas por el Ente Administrador para determinar si se han tomado las acciones correctivas correspondientes. f) Recibir, evaluar y resolver los reclamos de los usuarios de certificados digitales relativos a la prestación del servicio por parte de certificadores licenciados.

Organización del Ente Administrador.

Art. 15. - Dentro del plazo de SESENTA (60) días corridos de la fecha de constitución del Directorio, el ENTE ADMINISTRADOR DE FIRMA DIGITAL elevará para su consideración al JEFE DE GABINETE DE MINISTROS la propuesta de su estructura organizativa y de su reglamento de funcionamiento.

Recursos del Ente Administrador.

Art. 16. - El Ente Administrador podrá arancelar los servicios que preste para cubrir total o parcialmente sus costos. Los recursos propios del Ente Administrador se integrarán con: a) Los importes provenientes de los aranceles que se abonen por la provisión de los siguientes servicios: 1.- Servicios de certificación digital, 2.- Servicios de certificación digital de fecha y hora, 3.- Servicios de almacenamiento seguro de documentos electrónicos, 4.- Servicios prestados por autoridades de registro, 5. - Servicios prestados por terceras partes confiables, 6. - Servicios de certificación de documentos electrónicos firmados digitalmente 7.- Otros servicios o actividades relacionados a la firma digital. b) Los importes provenientes de los aranceles de homologación de dispositivos de creación y verificación de firmas digitales. c) Los importes provenientes de los aranceles de certificación de sistemas que utilizan

Proyecto De Ley nro:559/2010

firma digital. d) Los importes provenientes de los aranceles de administración del sistema de auditoría y las auditorías que el organismo realice por sí o por terceros. e) Los subsidios, herencias, legados, donaciones o transferencias bajo cualquier título que reciba. f) El producido de multas. g) Los importes que se le asignen en el cálculo de recursos de la respectiva ley de presupuesto para la administración nacional. h) Los demás fondos, bienes, o recursos que puedan serle asignados en virtud de las leyes y reglamentaciones aplicables.

Financiamiento del Ente Administrador.

Art. 17. - Instrúyese a la JEFATURA DE GABINETE DE MINISTROS para que proceda a incluir en su presupuesto los fondos necesarios para que el Ente Administrador pueda cumplir adecuadamente sus funciones. Transitoriamente, desde la entrada en vigencia de la presente reglamentación y hasta que se incluyan las partidas necesarias en el Presupuesto Nacional los costos de financiamiento del Ente Administrador serán afrontados con el crédito presupuestario correspondiente a la JEFATURA DE GABINETE DE MINISTROS.

CAPITULO V DEL SISTEMA DE AUDITORIA (artículos 18 al 21)
Precalificación de entidades de auditoría.

Art. 18. - La JEFATURA DE GABINETE DE MINISTROS convocará a concurso público para la precalificación de entidades de auditoría entre las universidades y organismos científicos y/o tecnológicos nacionales o provinciales, los Colegios y Consejos profesionales, que acrediten experiencia profesional acorde en la materia, interesadas en prestar el servicio de auditoría de entidades prestadoras de servicios de certificación digital. A tal fin, elaborará un Pliego Estándar de Precalificación de Entidades de Auditoría, y determinará la periodicidad de la convocatoria.

Informe de auditoría.

Art. 19. - El informe de auditoría evaluará los sistemas utilizados por el certificador de acuerdo con los requerimientos de la Ley Nº 25.506, el presente decreto y las normas complementarias.

Conflicto de intereses.

Art. 20. - Para garantizar la objetividad e imparcialidad de la actividad de auditoría no podrán desempeñarse en la prestación de servicios de auditoría aquellas entidades o personas vinculadas con prestadores de servicios de certificación, lo que será establecido en el Pliego Estándar de Precalificación de Entidades de Auditoría previsto en el artículo 18 del presente decreto.

Deber de confidencialidad.

Art. 21. - Las entidades auditantes y las personas que efectúen las auditorías deben mantener la confidencialidad sobre la información considerada amparada bajo normas de confidencialidad por el Certificado Licenciado.

CAPITULO VI DE LOS ESTANDARES TECNOLOGICOS (artículo 22)
Aplicación provisoria de los estándares vigentes.

Art. 22. - Hasta tanto la JEFATURA DE GABINETE DE MINISTROS apruebe los Estándares Tecnológicos de Infraestructura de Firma Digital en consonancia con estándares tecnológicos internacionales, mantendrán su vigencia los establecidos en la Resolución Nº 194/98 de la ex Secretaría de la Función Publica.

CAPITULO VII DE LA REVOCACION DE CERTIFICADOS DIGITALES (artículo 23)
Revocación de certificados.

Art. 23. - Se deberán revocar los certificados digitales emitidos en los siguientes casos: a) A solicitud del titular determina que un certificado digital fue emitido en base a una información falsa que en el

Proyecto De Ley nro:559/2010

momento de la emisión hubiera sido objeto de verificación. c) Si se determina que los procedimientos de emisión y/o verificación han dejado de ser seguros. d) Por condiciones especiales definidas en las Políticas de Certificación. e) Por Resolución Judicial o de la Autoridad de Aplicación debidamente fundada. f) Por fallecimiento del titular. g) Por declaración judicial de ausencia con presunción de fallecimiento del titular. h) Por declaración judicial de incapacidad del titular. i) Si se determina que la información contenida en el certificado ha dejado de ser válida. j) Por el cese de la relación de representación respecto de una persona.

CAPITULO VIII DE LOS CERTIFICADORES LICENCIADOS (artículos 24 al 34)
Obtención de la licencia.

Art. 24. - Para obtener una licencia, los proveedores de servicios de certificación deberán particularizar las actividades para las cuales requieren la licencia y acreditar por los medios que este determine ante el Ente Administrador de Firma Digital: a) Documentación que demuestre: 1.- En el caso de personas jurídicas, su personería. 2.- En el caso de registro público de contratos, tal condición 3.- En el caso de organización pública, la autorización de su máxima autoridad para iniciar el proceso de licenciamiento y la correspondiente aprobación de la JEFATURA DE GABINETE DE MINISTROS, de acuerdo con lo dispuesto en el artículo 41 de la presente reglamentación. b) El cumplimiento de las condiciones establecidas en la ley; este decreto y las normas complementarias. c) Las políticas de certificación para las cuales solicita licencia que respaldan la emisión de sus certificados, Manual de Procedimientos, Plan de Seguridad, Plan de Cese de Actividades y Plan de Contingencia satisfactorias de acuerdo con las normas reglamentarias. d) Toda aquella información o requerimiento, que demande la Autoridad de Aplicación.

Efectos del licenciamiento.

Art. 25. - El otorgamiento de la licencia no implica que el Ente Administrador de la Infraestructura de Firma Digital, la JEFATURA DE GABINETE DE MINISTROS, las entidades auditantes o cualquier organismo del Estado garantice la provisión de los servicios de certificación o los productos provistos por el Certificador Licenciado.

Duración de la licencia.

Art. 26. - Las licencias tendrán un plazo de duración de CINCO (5) años y podrán ser renovadas. Los certificadores licenciados deberán efectuar anualmente una declaración jurada en la cual conste el cumplimiento de las normas establecidas en la Ley Nº 25.506, en el presente decreto y en las normas complementarias. Los certificadores licenciados serán sometidos a auditorías anuales.

Causales de caducidad de la licencia.

Art. 27. - El Ente Administrador podrá disponer de oficio, y en forma preventiva la caducidad de la licencia en los siguientes casos: a) Falta de presentación de la declaración jurada anual. b) Falsedad de los datos contenidos en la declaración jurada anual. c) Dictamen desfavorable de auditoría basado en causales graves. d) Informe de la inspección dispuesta por el Ente Administrador desfavorable basado, en causales graves. e) Cuando el certificador licenciado no permita la realización de auditorías o inspecciones dispuestas por el Ente Administrador.

Reconocimiento de certificados extranjeros.

Art. 28. - De acuerdo a lo establecido en el artículo 6º de la presente reglamentación, facúltase a la JEFATURA DE GABINETE DE MINISTROS a elaborar y firmar acuerdos de reciprocidad con gobiernos de países extranjeros, a fin de otorgar validez, en sus respectivos territorios, a los certificados digitales emitidos por certificadores de ambos países, en tanto se verifique el cumplimiento de las condiciones establecidas por la Ley Nº 25.506 y su reglamentación para los certificados emitidos por certificadores nacionales. Los certificadores licenciados no podrán reconocer certificaciones emitidas por certificadores extranjeros correspondientes a personas con domicilio o residencia en la República

Proyecto De Ley nro:559/2010

Argentina. El Ente Administrador de Firma Digital establecerá las relaciones que los certificadores licenciados deberán guardar entre los certificados emitidos en la República Argentina y los certificados reconocidos de certificadores extranjeros.

Políticas de Certificación.

Art. 29. - La JEFATURA DE GABINETE DE MINISTROS definirá el contenido, mínimo de las políticas de certificación de acuerdo con los estándares nacionales e internacionales vigentes, las que deberán contener al menos la siguiente información: a) Identificación del certificador licenciado. b) Política de administración de los certificados y detalles de los servicios arancelados. c) Obligaciones de la entidad y de los suscriptores de los certificados. d) Tratamiento de la información suministrada por los suscriptores, y resguardo de la confidencialidad en su caso. e) Garantías que ofrece para el cumplimiento de las obligaciones que se deriven de sus actividades.

Seguros.

*Art. 30. - (Nota de Redacción) Derogado por art. 1 del Dec. 724/2006.

Modificado por: DECRETO NACIONAL 724/2006 Art.1 (Artículo derogado (B.O. 13-06-2006).)

Responsabilidad de los certificadores licenciados.

Art. 31. - En ningún caso, la responsabilidad que pueda emanar de una certificación efectuada por un certificador licenciado, público o privado, comprometerá la responsabilidad pecuniaria del Estado en su calidad de Ente Administrador de la Infraestructura de Firma Digital.

Recursos de los certificadores licenciados

Art. 32. - Para el desarrollo adecuado de las actividades de certificación, el certificador deberá acreditar que cuenta con un equipo de profesionales, infraestructura física tecnológica y recursos financieros, como así también procedimientos y sistemas de seguridad que permitan: a) Generar en un ambiente seguro las firmas digitales propias y todos los servicios para los cuales solicite licencia. b) Cumplir con lo previsto en sus políticas y procedimientos de certificación. c) Garantizar la confiabilidad de los sistemas de acuerdo con los estándares aprobados por la Autoridad de Aplicación. d) Expedir certificados que cumplan con: 1.- Lo previsto en los artículos 13 y 14 de la Ley Nº 25.506. 2.- Los estándares tecnológicos aprobados por la JEFATURA DE GABINETE DE MINISTROS. e) Garantizar la existencia de sistemas de seguridad física y lógica que cumplimenten las normativas vigentes. f) Proteger el manejo de la clave privada de la entidad mediante un procedimiento de seguridad que impida el acceso a la misma a personal no autorizado. g) Proteger el acceso y el uso de la clave privada mediante procedimientos que exijan la participación de más de una persona. h) Registrar las transacciones realizadas, a fin de identificar el autor y el momento de cada una de las operaciones. i) Utilizar con exclusividad los sistemas que cumplan las funciones de certificación con ese propósito, sin que se les asigne ninguna otra función. j) Proteger a todos los sistemas utilizados directa o indirectamente en la función de certificación con procedimientos de autenticación y seguridad de alto nivel de protección, que deban ser actualizados de acuerdo a los avances tecnológicos para garantizar la correcta prestación de los servicios de certificación. k) Garantizar la continuidad de las operaciones mediante un Plan de Contingencia actualizado y aprobado. I) Disponer de los recursos financieros adecuados al tipo de actividad de certificación que desarrolla, acorde con los niveles de responsabilidad derivados de la misma.

Servicios de Terceros

Art. 33. - . En los casos en que el certificador licenciado requiera o utilice los servicios de infraestructura tecnológicos prestados por un tercero, deberá prever dentro de su Plan de Contingencia los procedimientos a seguir en caso de interrupción de estos servicios, de modo tal que permita continuar prestando sus servicios de certificación sin ningún perjuicio para los suscriptores.

Proyecto De Ley nro:559/2010

Los contratos entre el certificador licenciado y los proveedores de servicios o infraestructura deberán garantizar la ejecución de los procedimientos contemplados en el Plan de Cese de actividades aprobado por el Ente Licenciante. El certificador licenciado o en proceso de licenciamiento deberá facilitar al Ente Licenciante toda aquella información obrante en los contratos vinculada a la prestación de servicios de certificación y a la implementación del Plan de Cese de actividades y el Plan de Contingencia. La contratación de servicios o infraestructura no exime al prestador de la presentación de los informes de auditoría, los cuales deberán incluir los sistemas y seguridades del prestador contratado.

Obligaciones del certificador licenciado.

Art. 34. - Además de lo previsto en el artículo 21 de la Ley Nº 25.506, los certificadores licenciados deberán: a) Comprobar por sí o por medio de una Autoridad de Registro que actúe en nombre y por cuenta suya, la identidad y cualquier otro dato de los solicitantes considerado relevante para los procedimientos de verificación de identidad previos a la emisión del certificado digital, según la Política de Certificación bajo la cual se solicita. b) Mantener a disposición permanente del público las Políticas de Certificación y el Manual de Procedimientos correspondiente. c) Cumplir cabalmente con las políticas de certificación acordadas con el titular y con su Manual de Procedimientos. d) Garantizar la prestación establecida según los niveles definidos en el acuerdo de servicios pactados con sus usuarios, relativo a los servicios para los cuales solicitó el licenciamiento. e) Informar al solicitante de un certificado digital, en un lenguaje claro y accesible, en idioma nacional, respecto de las características del certificado solicitado, las limitaciones a la responsabilidad, si las hubiere, los precios de los servicios de certificación, uso, administración y otros asociados, incluyendo cargos adicionales y formas de pago, los niveles de servicio al proveer, las obligaciones que el suscriptor asume como usuario del servicio de certificación, su domicilio en la República Argentina y los medios a los que el suscriptor puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema o presentar sus reclamos. f) Disponer de un servicio de atención a titulares y terceros, que permita evacuar las consultas y la pronta solicitud de revocación de certificados. g) Garantizar el acceso permanente, eficiente y gratuito de los titulares y terceros al repositorio de certificados revocados. h) Mantener actualizados los repositorios de certificados revocados por el período establecido por el Ente Administrador. i) Abstenerse de generar, exigir, tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada del suscriptor. j) Informar al Ente Administrador de modo inmediato la ocurrencia de cualquier evento que comprometa la correcta prestación del servicio. k) Respetar el derecho del titular del certificado digital a no recibir publicidad de ningún tipo por su intermedio, salvo consentimiento expreso de éste. l) Publicar en el Boletín Oficial durante UN (1) día, el certificado de clave pública correspondiente a la política para la cual obtuvo licenciamiento; m) Cumplir las normas y recaudos establecidos para la protección de datos personales. n) En los casos de revocación de certificados contemplados en el apartado 3 del inciso e) del artículo 19 de la Ley Nº25.506, deberá sustituir en forma gratuita aquel certificado digital que ha dejado de ser seguro por otro que sí cumpla con estos requisitos. El Ente Administrador deberá establecer el proceso de reemplazo de certificados en estos casos. En los casos en los que un certificado digital haya dejado de ser seguro por razones atribuibles a su titular, el certificador licenciado no estará obligado a sustituir el certificado digital. o) Enviar periódicamente al Ente Administrador, informes de estado de operaciones con carácter de declaración jurada. p) Contar con personal idóneo y confiable, con antecedentes profesionales acordes a la función desempeñada. q) Responder a los pedidos de informes por parte de un tercero respecto de la validez y alcance de un certificado digital emitido por él.

*Art. 34 bis - Aceptación por parte de terceros usuarios de documentoselectrónicos firmados digitalmente. Los terceros usuarios que sean personas jurídicas que implementen aplicacionesque requieran firma digital, tienen la facultad de definir las características yrequerimientos que deben cumplir las Políticas de Certificación, a los efectos deaceptar documentos electrónicos firmados digitalmente utilizando certificadosdigitales amparados por dichas Políticas. Dichas características y requerimientosdeben ser manifestados previamente en forma clara y transparente a los titularesde certificados que pretendan operar con ellos.

Proyecto De Ley nro:559/2010

Modificado por: DECRETO NACIONAL 724/2006 Art.4 (Artículo incorporado (B.O. 13-06-2006).)

CAPITULO IX DE LAS AUTORIDADES DE REGISTRO (artículos 35 al 36)
Funciones de las Autoridades de Registro.

Art. 35. - Los Certificadores Licenciados podrán delegar en Autoridades de Registro las funciones de validación de identidad y otros datos de los suscriptoresde certificados y de registro de las presentaciones y trámites que les sean formuladas, bajo la responsabilidad del Certificador Licenciado, cumpliendo las normas y procedimientos establecidos por la presente reglamentación. Una autoridad de Registro es una entidad responsable de las siguientes funciones: a) La recepción de las solicitudes de emisión de certificados. b) La validación de la identidad y autenticación de los datos de los titulares de certificados. c) La validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador Licenciado. d) La remisión de las solicitudes aprobadas al Certificador Licenciado con la que se encuentre operativamente vinculada. e) La recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento al Certificador Licenciado con el que se vinculen. f) La identificación y autenticación de los solicitantes de revocación de certificados. g) El archivo y la conservación de toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el certificador licenciado. h) El cumplimiento de las normas y recaudos establecidos para la protección de datos personales. i) El cumplimiento de las disposiciones que establezca la Política de Certificación y el Manual de Procedimientos del Certificador Licenciado con el que se encuentre vinculada, en la parte que resulte aplicable.

Responsabilidad del certificador licenciado respecto de
la Autoridad de Registro.

Art. 36. - Una Autoridad de Registro puede constituirse como una única unidad o con varias unidades dependientes jerárquicamente entre sí, pudiendo, delegar su operatoria en otras autoridades de registro, siempre que medie la aprobación del Certificador Licenciado. El Certificador, Licenciado es responsable con los alcances establecidos en la Ley Nº 25.506, aún en el caso de que delegue parte de su operatoria en Autoridades de Registro, sin perjuicio del derecho del certificador de reclamar a la Autoridad de Registro las indemnizaciones por los daños y perjuicios que aquél sufriera como consecuencia de los actos y/u omisiones de ésta.

CAPITULO X DISPOSICIONES PARA LA ADMINISTRACION PUBLICA NACIONAL (artículos 37 al 46)
Despapelización del Estado.

Art. 37. - Sin perjuicio de la aplicación directa de la ley en lo relativo a la validez jurídica de la firma electrónica, de la firma digital y de los documentos digitales, la implementación de las disposiciones de la ley y del presente decreto para la digitalización de procedimientos y trámites internos de la Administración Pública Nacional, de las Administraciones Públicas Provinciales, y de los Poderes Legislativos y Judiciales del orden nacional y provincial, así como los vinculados a la relación de las mencionadas jurisdicciones y entidades con los administrados, se hará de acuerdo a lo que fijen reglamentariamente cada uno de los Poderes y Administraciones.

Aplicaciones en organismos de la Administración Pública
Nacional.

*Art. 38. - Las entidades y jurisdicciones pertenecientes a la AdministraciónPública Nacional podrán ser certificadores licenciados y emitir certificados paraagentes y funcionarios públicos y particulares, tanto sean personas físicas comojurídicas. Dichos certificados deberán ser provistos en forma gratuita. En aquellas aplicaciones en las que la Administración Pública Nacional interactúecon la comunidad, solamente se admitirá la recepción de documentos digitalesfirmados digitalmente utilizando certificados emitidos por certificadoreslicenciados o certificados extranjeros reconocidos en los términos del artículo 16de Ley 25.506.

Modificado por: DECRETO NACIONAL 724/2006 Art.2 (Artículo sustituido (B.O. 13-06-2006).)

Proyecto De Ley nro:559/2010

Autoridades de Registro pertenecientes a la Administración Pública Nacional.

Art. 39. - En las entidades y jurisdicciones pertenecientes a la Administración Pública Nacional, las áreas de recursos humanos cumplirán las funciones de Autoridades de Registro para los agentes y funcionarios de su jurisdicción. En el caso, y si las aplicaciones de que se trate lo requieren, la máxima autoridad del organismo podrá asignar, adicionalmente, a otra unidad las funciones de Autoridad de Registro.

Agentes y funcionarios.

Art. 40. - La Autoridad de Aplicación podrá requerir para el cumplimiento de lo establecido en la presente reglamentación la adscripción de agentes y funcionarios pertenecientes a las entidades y jurisdicciones comprendidas en el artículo 8º de la Ley Nº 24.156 y sus modificatorias.

Utilización por las entidades y jurisdicciones de la Administración Pública Nacional

Art. 41. -. La JEFATURA DE GABINETE DE MINISTROS, establecerá las normas de aplicación de la presente reglamentación en la Administración Pública Nacional, que deberán contemplar: a) Las acciones tendientes a promover el uso masivo de la firma digital con el fin de posibilitar el trámite de los expedientes en forma simultánea, búsquedas automáticas de información, seguimiento y control por parte de los interesados. b) Las acciones tendientes a implementar la progresiva despapelización del Estado, a fin de contar en un plazo de CINCO (5) años con la totalidad de la documentación administrativa en formato digital. c) La interoperabilidad entre aplicaciones. d) La autorización para solicitar el licenciamiento como certificador ante el Ente Administrador de la Infraestructura de Firma Digital para las entidades y jurisdicciones de la Administración Pública Nacional. e) La participación del Cuerpo de Administradores Gubernamentales a los fines de difundir el uso de la firma digital y facilitar los procesos de despapelización.

Presentación de documentos electrónicos.

Art. 42. - Los organismos de la Administración Pública Nacional deberán establecer mecanismos que garanticen la opción de remisión, recepción, mantenimiento y publicación de información electrónica, siempre que esto sea aplicable, tanto para la gestión de documentos entre organismos como para con los ciudadanos.

Normas para la elaboración y redacción de la documentación administrativa.

Art. 43. - Lo dispuesto en la presente reglamentación constituye una alternativa a lo establecido por el Decreto Nº 333/85 y sus modificatorios.

Glosario.

Art. 44. - Apruébase el glosario que obra como Anexo I del presente Decreto.

Derogación.

Art. 45. - Derógase el Decreto Nº 427/98.

Deroga a: DECRETO NACIONAL 427/1998

Art.46. - Comuníquese, publíquese,dése a la Dirección Nacional del Registro Oficial y archívese.

Proyecto De Ley nro:559/2010

FIRMANTES

DUHALDE-Atanasof-Alvarez

ANEXO I
GLOSARIO

CANTIDAD DE ARTICULOS QUE COMPONEN LA NORMA 1

1.- Firma Electrónica: Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizados por el signatario como su medio de identificación, que carezca de algunos de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez (artículo 5º, Ley Nº 25.506). 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 (artículo 2º, Ley Nº 25.506). 3.- Documento Digital o Electrónico: Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte: utilizado para su fijación, almacenamiento archivo. Un documento digital también satisface el requerimiento de escritura (artículo 6º, Ley Nº 25.506). 4.- Certificado Digital: Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular (artículo 13, Ley Nº 25.506). 5.- Certificador Licenciado: Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante. La actividad de los certificadores licenciados no pertenecientes al sector público se prestará en régimen de competencia. El arancel de los servicios prestados por los certificadores licenciados será establecido libremente por éstos (artículo 17, Ley Nº 25.506). 6.- Política de Certificación: Conjunto de criterios que indican la aplicabilidad de un certificado a un grupo de usuarios en particular o a un conjunto de aplicaciones con similares requerimientos de seguridad. En inglés Certification Policy (CP). 7.- Manual de Procedimientos: Conjunto de prácticas utilizadas por el certificador licenciado en la remisión y administración de los certificados. En inglés Certification Practice Statement (CPS). 8.- Plan de Seguridad: Conjunto de políticas, prácticas y procedimientos destinados a la protección; de los recursos del certificador licenciado. 9.- Plan de Cese de Actividades: conjunto de actividades a desarrollar por el certificador licenciado en caso de finalizar la prestación de sus servicios. 10.- Plan de Contingencias: Conjunto de procedimientos a seguir por el certificador licenciado ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones. 11.- Lista de certificados revocados: Lista de certificados que han sido dejados sin efecto en forma permanente por el Certificador Licenciado, la cual ha sido firmada digitalmente y publicada por el mismo. En inglés Certificate Revocation List (CRL). 12.- Certificación digital de fecha y hora: Indicación de la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella. 13.- Terceras partes confiables: Entidades independientes que otorgan seguridad y confiabilidad al manejo de la información. 14.- Proveedor de servicios de certificación digital: Entidad que provee el servicio de emisión y administración de certificados digitales. 15.- Homologación de dispositivos de creación y verificación de firmas digitales: Proceso de comprobación efectuado para establecer la adecuación de los dispositivos a requerimientos mínimos establecidos. 16.- Certificación de sistemas que utilizan firma digital: Proceso de comprobación efectuado para establecer la adecuación de un sistema o aplicación a requerimientos mínimos establecidos. 17.- Suscriptor o Titular de certificado digital: Persona a cuyo nombre se emite un certificado y posee una clave privada que se corresponde con la clave pública contenida en el mismo. 18. TERCERO USUARIO: persona física o jurídica que recibe un documento firmadodigitalmente y que genera una consulta para verificar la

Proyecto De Ley nro:559/2010

validez del certificadodigital correspondiente.

Modificado por: DECRETO NACIONAL 724/2006 Art.3 (Definición incorporada (B.O. 13-06-2006).)
Antecedentes (NAC.) - Informacion Parlamentaria
4) D.427/1998- DEROGADO DE ALCANCE GENERAL -
INFRAESTRUCTURA DE FIRMA DIGITAL PARA EL SECTOR PUBLICO NACIONAL.
BUENOS AIRES, 16 DE ABRIL DE 1998
BOLETIN OFICIAL, 21 DE ABRIL DE 1998
- DEROGADO DE ALCANCE GENERAL -

EFECTO PASIVO

Nota de redacción. Ver: Decisión Administrativa Nacional 102/2000 Art.1 (ART. 1 (B.O. 25-1-2001)) Derogado por: DECRETO NACIONAL 2.628/2002 Art.45 (B.O. 20-12-2002)

GENERALIDADES
Sintesis:

SE ESTABLECE EL REGIMEN AL QUE SE AJUSTARA EL EMPLEO DE LA FIRMA DIGITAL EN LA INSTRUMENTACION DE LOS ACTOS INTERNOS DEL SECTOR PUBLICO NACIONAL, QUE NO PRODUZCAN EFECTOS JURIDICOS INDIVIDUALES EN FORMA DIRECTA, QUE TENDRA LOS MISMOS EFECTOS DE LA FIRMA OLOGRAFA.

Derogado por: DECRETO NACIONAL 2.628/2002 Art.45 (B.O. 20-12-2002)

NOTICIAS ACCESORIAS

OBSERVACION: SE PRORROGA POR 2 AÑOS A PARTIR DEL 31 DE DICIEMBRE DE 2000, EL PLAZO ESTABLECIDO EN EL ART. 1 DEL PRESENTE. B.O. 25-1-2001 OBSERVACION: DECRETO DEROGADO POR ART. 45 DEL DECRETO 2.628/2002. B.O. 20-12-2002

TEMA

ADMINISTRACION PUBLICA NACIONAL-ACTO ADMINISTRATIVO-DOCUMENTO ELECTRONICO-FIRMA DIGITAL-SECRETARIA DE LA FUNCION PUBLICA-JEFE DE GABINETE

VISTO

los Decretos Nros. 660 del 24 de junio de 1996 y 998 del 30 de agosto de 1996, la Resolución N. 45 del 17 de marzo de 1997 de la SECRETARIA DE LA FUNCION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS, y

Referencias Normativas: Resolución 45/1997 (SECRETARIA DE LA FUNCION PUBLICA)Decreto Nacional 660/96Decreto Nacional 998/96

CONSIDERANDO

Que la necesidad de optimizar la actividad de la Administración Pública Nacional adecuando sus sistemas de registración de datos, tendiendo a eliminar el uso del papel y automatizando sus circuitos administrativos, amerita la introducción de tecnología de última generación, entre las cuales se destacan aquellas relativas al uso de la firma digital, susceptible de la misma o superior garantía de confianza que la firma ológrafa. Que la Resolución N. 45 del 17 de marzo de 1997 de la SECRETARIA DE LA FUNCION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS ha constituido un hito importante en tal dirección, al autorizar su empleo en todo el ámbito del Sector Público Nacional. Que se considera necesario estimular la difusión de las citadas tecnologías a través del dictado de una norma de jerarquía superior, que promueva la extensión del uso de la firma digital a todo el ámbito del Sector Público Nacional. Que la tecnología aquí propuesta ya ha sido incorporada en la legislación de otros países, con positiva

Proyecto De Ley nro:559/2010

repercusión tanto en el ámbito privado como público. Que el mecanismo de la firma digital cumple con la condición de no repudio, por la cual resulta posible probar inequívocamente que una persona firmó efectivamente un documento digital y que dicho documento no fue alterado desde el momento de su firma, siempre que su implementación se ajuste a los procedimientos aquí descriptos. Que es indispensable establecer una Infraestructura de Firma Digital para el Sector Público Nacional con el fin de crear las condiciones de un uso confiable del documento suscripto digitalmente. Que la presente normativa fue concebida con el propósito de crear una alternativa válida a la firma ológrafa para el Sector Público Nacional. Que resulta conveniente, en virtud del grado de especialidad alcanzado con la puesta en práctica de la reglamentación del Artículo 49 de la Ley N. 11.672 (t.o. 1997), que las funciones del Organo Auditante recaigan en la CONTADURIA GENERAL DE LA NACION, dependiente de la SUBSECRETARIA DE PRESUPUESTO de la SECRETARIA DE HACIENDA del MINISTERIO DE ECONOMIA Y OBRAS Y SERVICIOS PUBLICOS. Que las disposiciones de la presente normativa complementan las disposiciones del Decreto N. 333 del 19 de febrero de 1985 y sus modificatorios. Que dada su índole, se ha considerado conveniente y necesario que la autorización del empleo de la tecnología de la firma digital en el ámbito del Sector Público Nacional se sujete a un término de vigencia, que permita evaluar, a partir de su efectiva utilización, tanto su funcionamiento en las diferentes jurisdicciones cuanto el grado de confiabilidad y seguridad del sistema. Que en mérito a tales circunstancias se prevé expresamente en la presente normativa la elaboración, por la Autoridad de Aplicación, de un informe acerca de los resultados del empleo de la firma digital a fin de que, sobre la base de las conclusiones emergentes, la JEFATURA DE GABINETE DE MINISTROS proponga al PODER EJECUTIVO NACIONAL las medidas tendientes a fijar un régimen definitivo en la materia. Que asimismo y con idéntico fundamento, se delega en la JEFATURA DE GABINETE DE MINISTROS la facultad de prorrogar, por una única vez, el plazo del Artículo 1 del presente Decreto. Que la presente medida se dicta en uso de las facultades conferidas por el Artículo 99 inciso 1 de la CONSTITUCION NACIONAL. Por ello,

EL PRESIDENTE DE LA NACION ARGENTINA DECRETA:

Referencias Normativas: Resolución 45/1997 (SECRETARIA DE LA FUNCION PUBLICA)Ley 11.672 - TEXTO ORDENADO POR DECRETO 1486/97 Art.49DECRETO NACIONAL 333/1985

*Art. 1: Autorízase por el plazo de DOS (2) años, a contar del dictado de los manuales de procedimiento y de los estándares aludidos en el artículo 6 del presente Decreto, el empleo de la firma digital en la instrumentación de los actos internos del Sector Público Nacional, que no produzcan efectos jurídicos individuales en forma directa, en las condiciones definidas en la Infraestructura de Firma Digital para el Sector Público Nacional que como Anexo I integra el presente Decreto. En el régimen del presente Decreto la firma digital tendrá los mismos efectos de la firma ológrafa, siempre que se hayan cumplido los recaudos establecidos en el Anexo I y dentro del ámbito de aplicación definido en el artículo 3.

Art. 2: Los términos de este reglamento tendrán los alcances definidos en el Glosario que como Anexo II integra el presente Decreto.

Art. 3: Las disposiciones del presente Decreto serán de aplicación en todo el ámbito del Sector Público Nacional, dentro del cual se comprende la administración centralizada y la descentralizada, los entes autárquicos, las empresas del Estado, Sociedades del Estado, Sociedades Anónimas con participación estatal mayoritaria, los bancos y entidades financieras oficiales y todo otro ente, cualquiera que sea su denominación o naturaleza jurídica, en que el Estado Nacional o sus organismos descentralizados tengan participación suficiente para la formación de sus decisiones.

Art. 4: Los organismos del Sector Público Nacional deberán arbitrar los medios que resulten adecuados para extender el empleo de la tecnología de la firma digital, en función de los recursos con los que cuenten y en el más corto plazo posible.

Proyecto De Ley nro:559/2010

Art. 5: La correspondencia entre una clave pública, elemento del par de claves que permite verificar una firma digital, y el agente titular de la misma, será acreditada mediante un certificado de clave pública emitido por una Autoridad Certificante Licenciada. Los requisitos y condiciones para la vigencia y validez de los certificados de clave pública (emisión, aceptación, revocación, expiración y demás contingencias del procedimiento), así como las condiciones bajo las cuales deben operar las Autoridades Certificantes Licenciadas integrantes de la Infraestructura de Firma Digital para el Sector Público Nacional, quedan establecidas en el citado Anexo I.

Art. 6: Dispónese que la Secretaría de la Función Pública, dependiente de la Jefatura de Gabinete de Ministros, sea la Autoridad de Aplicación del presente Decreto, estando facultada, además, para dictar los manuales de procedimiento de las Autoridades Certificantes Licenciadas y de los Organismos Auditante y Licenciante, y los estándares tecnológicos aplicables a las claves, los que deberán ser definidos en un plazo no mayor de CIENTO OCHENTA (180) DIAS corridos, y cuyos contenidos deberán reflejar el último estado del arte. Los organismos del Sector Público Nacional deberán informar a la Autoridad de Aplicación, con la periodicidad que ésta establezca, las aplicaciones que concreten de la tecnología autorizada por el presente Decreto.

Art. 7: Dispónese que el presente Decreto establece una alternativa a las estipulaciones pertinentes del Decreto N. 333 del 19 de febrero de 1985 y sus modificatorios, respecto de los actos alcanzados por el artículo 1.

Referencias Normativas: DECRETO NACIONAL 333/1985

Art. 8: La Secretaría de la Función Pública de la Jefatura de Gabinete de Ministros cumplirá las funciones de Organismo Licenciante con los alcances definidos en el Anexo I del presente Decreto.

Art. 9: La Contaduría General de la Nación, dependiente de la Subsecretaría de Presupuesto de la Secretaría de Hacienda del Ministerio de Economía y Obras y Servicios Públicos, cumplirá las funciones de Organismo Auditante en los términos de lo establecido en el Anexo I del presente Decreto.

Art. 10: CIENTO OCHENTA (180) días corridos antes de la finalización del plazo establecido en el artículo 1, la Autoridad de Aplicación definida en el artículo 6 del presente Decreto deberá elaborar y remitir a la Jefatura de Gabinete de Ministros un informe acerca de los resultados que la aplicación del sistema autorizado hubiere tenido en las respectivas jurisdicciones. La Jefatura de Gabinete de Ministros examinará dicho informe y propondrá al Poder Ejecutivo el régimen definitivo a adoptar en la materia.

Art. 11: Delégase en la Jefatura de Gabinete de Ministros la facultad de prorrogar, por una única vez, el plazo establecido en el Artículo 1 del presente Decreto.

Art. 12: Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese.

FIRMANTES

MENEM-RODRIGUEZ-GRANILLO OCAMPO

INFRAESTRUCTURA DE FIRMA DIGITAL PARA EL SECTOR PUBLICO NACIONAL

Proyecto De Ley nro:559/2010

ORGANISMO LICENCIANTE Funciones: 1. Otorga las licencias habilitantes para acreditar a las autoridades certificantes y emite los correspondientes CERTIFICADOS DE CLAVE PUBLICA, que permiten VERIFICAR LAS FIRMAS DIGITALES de los CERTIFICADOS que éstas emitan; 2. Deniega las solicitudes de licencias a las autoridades certificantes que no cumplan con los requisitos establecidos para su autorización; 3. Revoca las licencias otorgadas a las AUTORIDADES CERTIFICANTES LICENCIADAS que dejan de cumplir con los requisitos establecidos para su autorización; 4. Verifica que las AUTORIDADES CERTIFICANTES LICENCIADAS utilicen sistemas TECNICAMENTE CONFIABLES; 5. Considera para su aprobación el manual de procedimientos, el plan de seguridad y el de cese de actividades presentados por las autoridades certificantes; 6. Acuerda con el ORGANISMO AUDITANTE el plan de auditoría para las AUTORIDADES CERTIFICANTES LICENCIADAS 7. Dispone la realización de auditorías de oficio; 8. Resuelve los conflictos individuales que se susciten entre el SUSCRIPTOR de un CERTIFICADO y la AUTORIDAD CERTIFICANTE LICENCIADA emisora del mismo; 9. Resuelve todas aquellas contingencias respecto a la Infraestructura de FIRMA DIGITAL. Obligaciones: En su calidad de SUSCRIPTOR de CERTIFICADO y de autoridad certificante, el ORGANISMO LICENCIANTE tiene idénticas obligaciones que las AUTORIDADES CERTIFICANTES LICENCIADAS, y además debe: 1. Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a la CLAVE PRIVADA de cualquier SUSCRIPTOR de los CERTIFICADOS que emita; 2. Mantener el control de su propia CLAVE PRIVADA e impedir su divulgación; 3. Revocar su propio CERTIFICADO DE CLAVE PUBLICA frente al compromiso de su CLAVE PRIVADA; 4. Permitir el acceso público permanente a los CERTIFICADOS DE CLAVE PUBLICA que ha emitido en favor de las AUTORIDADES CERTIFICANTES LICENCIADAS, y a la LISTA DE CERTIFICADOS REVOCADOS, por medio de conexiones de telecomunicaciones públicamente accesibles. Esto también se aplica a la información sobre direcciones y números telefónicos de las AUTORIDADES CERTIFICANTES LICENCIADAS; 5. Permitir el ingreso de los funcionarios autorizados del ORGANISMO AUDITANTE a su local operativo, poner a su disposición toda la información necesaria, y proveer la asistencia del caso; 6. Publicar su propio CERTIFICADO DE CLAVE PUBLICA en el Boletín Oficial, y en DOS (2) diarios de difusión nacional, durante TRES (3) días consecutivos a partir del día de su emisión; 7. Revocar los CERTIFICADOS emitidos en favor de las AUTORIDADES CERTIFICANTES LICENCIADAS incursas en causales de revocación de licencia, o que han cesado sus actividades; 8. Revocar los CERTIFICADOS emitidos en favor de las AUTORIDADES CERTIFICANTES LICENCIADAS, cuando las CLAVES PUBLICAS que en ellos figuran dejan de ser TECNICAMENTE CONFIABLES; 9. Supervisar la ejecución del plan de cese de actividades de las AUTORIDADES CERTIFICANTES LICENCIADAS que discotinúan sus funciones; 10. Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas. ORGANISMO AUDITANTE Funciones: 1. Audita periódicamente al ORGANISMO LICENCIANTE y a las AUTORIDADES CERTIFICANTES LICENCIADAS; 2. Audita a las autoridades certificantes previo a la obtención de sus licencias; 3. Acuerda con el ORGANISMO LICENCIANTE el plan de auditoría para las AUTORIDADES CERTIFICANTES LICENCIADAS; 4. Audita a las AUTORIDADES CERTIFICANTES LICENCIADAS a solicitud del ORGANISMO LICENCIANTE; 5. Efectúa las revisiones de cumplimiento de las recomendaciones formuladas en las auditorías. Obligaciones: El ORGANISMO AUDITANTE debe: 1. Utilizar técnicas de auditoría apropiadas en sus evaluaciones; 2. Evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad, y disponibilidad de los datos, como así también el cumplimiento con las especificaciones del manual de procedimientos y el plan de seguridad aprobados por el ORGANISMO LICENCIANTE. 3. Verificar que se utilicen sistemas TECNICAMENTE CONFIABLES; 4. Emitir informes de auditoría con los hallazgos, conclusiones y recomendaciones en cada caso; 5. Realizar revisiones de seguimiento de las auditorías, para determinar si el organismo auditado ha tomado las acciones correctivas que surjan de las recomendaciones; 6. Emitir informes con las conclusiones de las revisiones de seguimiento de auditorías; 7. Intervenir en los simulacros de planes de contingencia; 8. Dar copia de todos los informes de auditoría por él emitidos al ORGANISMO LICENCIANTE. AUTORIDAD CERTIFICANTE LICENCIADA Funciones: 1. Emite CERTIFICADOS DE CLAVE PUBLICA; Para emitir CERTIFICADOS DE CLAVE PUBLICA, la AUTORIDAD CERTIFICANTE LICENCIADA debe: a) recibir del agente requirente una solicitud de EMISION DE CERTIFICADO DE CLAVE PUBLICA, la cual deberá estar firmada digitalmente con la correspondiente CLAVE PRIVADA; b) verificar fehacientemente la información identificatoria del solicitante, la cual deberá estar siempre incluida en el CERTIFICADO, y toda otra información que según lo dispuesto en el manual de procedimientos de la AUTORIDAD CERTIFICANTE LICENCIADA, deba ser objeto de verificación, lo cual deberá realizarse de acuerdo a lo dispuesto en el citado

Proyecto De Ley nro:559/2010

manual; c) numerar correlativamente los certificados EMITIDOS; d) Mantener copia de todos los CERTIFICADOS emitidos, consignando su fecha de emisión. La AUTORIDAD CERTIFICANTE LICENCIADA puede, opcionalmente, incluir en un CERTIFICADO información no verificada, debiendo indicar claramente tal cualidad. 2. Revoca CERTIFICADOS DE CLAVE PUBLICA; La AUTORIDAD CERTIFICANTE LICENCIADA revocará los CERTIFICADOS DE CLAVE PUBLICA por ella emitidos: a) por solicitud de su SUSCRIPTOR; o b) por solicitud de un TERCERO; o c) si llegara a determinar que un CERTIFICADO fue emitido en base a una información falsa, que en el momento de la EMISION hubiera sido objeto de verificación; o d) si llegara a determinar que las CLAVES PUBLICAS contenidas en los CERTIFICADOS dejan de ser TECNICAMENTE CONFIABLES; o e) si cesa en sus actividades y no transfiere los CERTIFICADOS emitidos por ella a otra AUTORIDAD CERTIFICANTE LICENCIADA; La solicitud de REVOCACION DE UN CERTIFICADO debe hacerse en forma personal o por medio de un DOCUMENTO DIGITAL FIRMADO. Si la revocación es solicitada por el SUSCRIPTOR, ésta deberá concretarse de inmediato. Si la revocación es solicitada por un TERCERO, tendrá lugar dentro de los plazos mínimos necesarios para realizar las verificaciones del caso. La revocación debe indicar el momento desde el cual se aplica y no puede ser retroactiva o a futuro. El CERTIFICADO revocado deberá incluirse inmediatamente en la LISTA DE CERTIFICADOS REVOCADOS, y la lista debe estar firmada por la AUTORIDAD CERTIFICANTE LICENCIADA. Dicha lista debe hacerse pública en forma permanente, por medio de conexiones de telecomunicaciones públicamente accesibles. La AUTORIDAD CERTIFICANTE LICENCIADA debe emitir una constancia de la revocación para el solicitante. 3. Provee, opcionalmente, el servicio de SELLADO DIGITAL DE FECHA Y HORA. Obligaciones: Adicionalmente a sus obligaciones emergentes como SUSCRIPTORA de su CERTIFICADO emitido por el ORGANISMO LICENCIANTE, la AUTORIDAD CERTIFICANTE LICENCIADA debe: 1. Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a la CLAVE PRIVADA del SUSCRIPTOR; 2. Mantener el control de su CLAVE PRIVADA e impedir su divulgación; 3. Solicitar inmediatamente la REVOCACION DE SU CERTIFICADO, cuando tuviera sospechas fundadas de que su CLAVE PRIVADA ha sido comprometida; 4. Solicitar al ORGANISMO LICENCIANTE la revocación de su CERTIFICADO cuando la CLAVE PUBLICA en él contenida deje de ser TECNICAMENTE CONFIABLE; 5. Informar inmediatamente al ORGANISMO LICENCIANTE sobre cualquier cambio en los datos contenidos en su CERTIFICADO, o sobre cualquier hecho significativo que pueda afectar la información contenida en el mismo; 6. Operar utilizando un sistema TECNICAMENTE CONFIABLE; 7. Notificar al solicitante sobre las medidas necesarias que éste está obligado a adoptar para crear FIRMAS DIGITALES seguras y para su VERIFICACION confiable; y de las obligaciones que éste asume por el solo hecho de ser SUSCRIPTOR de un CERTIFICADO DE CLAVE PUBLICA; 8. Recabar únicamente aquellos datos personales del SUSCRIPTOR del CERTIFICADO que sean necesarios y de utilidad para la emisión del mismo, quedando el solicitante en libertad de proveer información adicional. Toda información así recabada, pero que no figure en el CERTIFICADO, será de trato confidencial por parte de la AUTORIDAD CERTIFICANTE LICENCIADA; 9. Poner a disposición del SUSCRIPTOR de un CERTIFICADO emitido por ésta AUTORIDAD CERTIFICANTE LICENCIADA, toda la información relativa a la tramitación del CERTIFICADO; 10. Mantener la documentación respaldatoria de los CERTIFICADOS emitidos por DIEZ (10) años a partir de su fecha de vencimiento o revocación; 11. Permitir el acceso público permanente a los CERTIFICADOS que ha emitido, y a la LISTA DE CERTIFICADOS REVOCADOS, por medio de conexiones de telecomunicaciones públicamente accesibles; 12. Publicar su dirección y sus números telefónicos; 13. Permitir el ingreso de los funcionarios autorizados del ORGANISMO LICENCIANTE o del ORGANISMO AUDITANTE a su local operativo, poner a su disposición toda la información necesaria, y proveer la asistencia del caso; 14. Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas. Cese de Actividades: Los CERTIFICADOS emitidos por una AUTORIDAD CERTIFICANTE LICENCIADA que cesa en sus funciones se revocarán a partir del día y la hora en que cesa su actividad, a menos que sean transferidos a otra AUTORIDAD CERTIFICANTE LICENCIADA. La AUTORIDAD CERTIFICANTE LICENCIADA notificará mediante la publicación por TRES (3) días consecutivos en el Boletín Oficial, la fecha y hora de cese de sus actividades, que no podrá ser anterior a los NOVENTA (90) días corridos contados desde la fecha de la última publicación. La notificación también deberá hacerse individualmente al ORGANISMO LICENCIANTE. Cuando se hayan emitido CERTIFICADOS a personas ajenas al Sector Público Nacional, la AUTORIDAD CERTIFICANTE LICENCIADA publicará durante TRES (3) días consecutivos en uno o más diarios de difusión nacional, el cese de sus actividades. La AUTORIDAD CERTIFICANTE LICENCIADA podrá disponer de medios adicionales de comunicación del cese de sus actividades a los SUSCRIPTORES de CERTIFICADOS que son ajenos al Sector Público Nacional. Si los CERTIFICADOS son transferidos a otra AUTORIDAD CERTIFICANTE LICENCIADA, toda la documentación pertinente también deberá ser transferida a ella. Requisitos para obtener la licencia de autoridad certificante: La autoridad certificante que

Proyecto De Ley nro:559/2010

desee obtener una licencia deberá: 1. Presentar una solicitud; 2. Contar con un dictamen favorable emitido por el ORGANISMO AUDITANTE; 3. Someter a aprobación del ORGANISMO 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; 4. Emplear para el ejercicio de las actividades de certificación, personal técnicamente idóneo y que no se encuentre incurso en los supuestos de inhabilitación para desempeñar funciones dentro del Sector Público Nacional; 5. Presentar toda otra información relevante al proceso de otorgamiento de licencias que sea exigida por el ORGANISMO LICENCIANTE. SUSCRIPTOR DE CERTIFICADO DE CLAVE PUBLICA Obligaciones del SUSCRIPTOR: El SUSCRIPTOR de un CERTIFICADO DE CLAVE PUBLICA debe: 1. Proveer todos los datos requeridos por la AUTORIDAD CERTIFICANTE LICENCIADA bajo declaración jurada; 2. Mantener el control de su CLAVE PRIVADA e impedir su divulgación; 3. Informar inmediatamente a la AUTORIDAD CERTIFICANTE LICENCIADA, sobre cualquier circunstancia que pueda haber comprometido su CLAVE PRIVADA; 4. Informar inmediatamente a la AUTORIDAD CERTIFICANTE LICENCIADA cuando cambie alguno de los datos contenidos en el CERTIFICADO que hubieran sido objeto de verificación. CERTIFICADOS DE CLAVE PUBLICA Contenido del CERTIFICADO DE CLAVE PUBLICA: El CERTIFICADO DE CLAVE PUBLICA contendrá, como mínimo, los siguientes datos: 1. Nombre del SUSCRIPTOR del CERTIFICADO; 2. Tipo y número de documento del SUSCRIPTOR del CERTIFICADO, o número de licencia, en el caso de CERTIFICADOS emitidos para AUTORIDADES CERTIFICANTES LICENCIADAS; 3. CLAVE PUBLICA utilizada por el SUSCRIPTOR; 4. Nombre del algoritmo que debe utilizarse con la CLAVE PUBLICA en él contenida; 5. Número de serie del CERTIFICADO; 6. PERIODO DE VIGENCIA del CERTIFICADO; 7. Nombre de la AUTORIDAD CERTIFICANTE LICENCIADA emisora del CERTIFICADO; 8. FIRMA DIGITAL de la AUTORIDAD CERTIFICANTE LICENCIADA que emite el CERTIFICADO, identificando los algoritmos utilizados. 9. Todo otro dato relevante para la utilización del CERTIFICADO, se explicitará en el manual de procedimientos de la AUTORIDAD CERTIFICANTE LICENCIADA emisora. Condiciones de Validez del CERTIFICADO DE CLAVE PUBLICA: El CERTIFICADO DE CLAVE PUBLICA es válido únicamente si: 1. ha sido emitido por una AUTORIDAD CERTIFICANTE LICENCIADA; 2. no ha sido revocado; 3. no ha expirado.

GLOSARIO

AUTORIDAD CERTIFICANTE LICENCIADA: Organo administrativo que emite CERTIFICADOS DE CLAVE PUBLICA. CERTIFICADO o CERTIFICADO DE CLAVE PUBLICA: DOCUMENTO DIGITAL emitido y firmado digitalmente por una AUTORIDAD CERTIFICANTE LICENCIADA, que asocia una CLAVE PUBLICA con su SUSCRIPTOR durante el PERIODO DE VIGENCIA del CERTIFICADO, y que asimismo hace plena prueba dentro del Sector Público Nacional, de la veracidad de su contenido. CLAVE PRIVADA: En un CRIPTOSISTEMA ASIMETRICO, es aquella que se utiliza para firmar digitalmente CLAVE PUBLICA: En un CRIPTOSISTEMA ASIMETRICO, es aquella que se utiliza para verificar una FIRMA DIGITAL. COMPUTACIONALMENTE NO FACTIBLE: Dícese 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 en la actualidad. CORRESPONDER: Con referencia a un cierto PAR DE CLAVES, significa pertenecer a dicho par. CRIPTOSISTEMA ASIMETRICO: Algoritmo que utiliza un PAR DE CLAVES, una CLAVE PRIVADA para firmar digitalmente y su correspondiente CLAVE PUBLICA para verificar esa FIRMA DIGITAL. A efectos de este Decreto, se entiende que el CRIPTOSISTEMA ASIMETRICO deberá ser TECNICAMENTE CONFIABLE. DIGESTO SEGURO (Hash Result): La secuencia de bits de longitud fija producida por una FUNCION DE DIGESTO SEGURO luego de procesar un DOCUMENTO DIGITAL. DOCUMENTO DIGITAL: Representación digital de actos, hechos o datos jurídicamente relevantes. DOCUMENTO DIGITAL FIRMADO: DOCUMENTO DIGITAL al cual se le ha aplicado una FIRMA DIGITAL EMISION DE UN CERTIFICADO: La creación de un CERTIFICADO por parte de una AUTORIDAD CERTIFICANTE LICENCIADA. ORGANISMO AUDITANTE: Organo administrativo encargado de auditar la actividad del ORGANISMO LICENCIANTE y de las AUTORIDADES CERTIFICANTES LICENCIADAS. ORGANISMO LICENCIANTE: Organo administrativo encargado de otorgar las licencias a las autoridades certificantes y de supervisar la actividad de las AUTORIDADES CERTIFICANTES LICENCIADAS. FIRMA DIGITAL: Resultado de una transformación de un DOCUMENTO DIGITAL empleando un CRIPTOGRAMA ASIMETRICO y un DIGESTO SEGURO, de forma tal que una persona que posea el DOCUMENTO DIGITAL inicial y la CLAVE PUBLICA del firmante pueda determinar con certeza: 1. Si la transformación se llevó a cabo utilizando la CLAVE PRIVADA que corresponde a la CLAVE PUBLICA del firmante; 2. Si el DOCUMENTO DIGITAL ha sido modificado desde que se efectuó la transformación. La conjunción de los dos requisitos anteriores garantiza su NO REPUDIO y su INTEGRIDAD. FUNCION DE DIGESTO SEGURO: Es una función matemática que

Proyecto De Ley nro:559/2010

transforma un DOCUMENTO DIGITAL en una secuencia de bits de longitud fija, llamada DIGESTO SEGURO, de forma tal que: 1. Se obtiene la misma secuencia de bits de longitud fija cada vez que se calcula esta función respecto del mismo DOCUMENTO DIGITAL; 2. Es COMPUTACIONALMENTE NO FACTIBLE inferir o reconstituir un DOCUMENTO DIGITAL a partir de su DIGESTO SEGURO; 3. Es COMPUTACIONALMENTE NO FACTIBLE encontrar dos DOCUMENTOS DIGITALES diferentes que produzcan el mismo DIGESTO SEGURO. INTEGRIDAD: Condición de no alteración de un DOCUMENTO DIGITAL. LISTA DE CERTIFICADOS REVOCADOS: Es la lista publicada por la AUTORIDAD CERTIFICANTE LICENCIADA, de los CERTIFICADOS DE CLAVE PUBLICA por ella emitidos cuya vigencia ha cesado antes de su fecha de vencimiento, por acto revocatorio. NO REPUDIO: Cualidad de la FIRMA DIGITAL, por la cual su autor no puede desconocer un DOCUMENTO DIGITAL que él ha firmado digitalmente. PAR DE CLAVES: CLAVE PRIVADA y su correspondiente CLAVE PUBLICA en un CRIPTOSISTEMA ASIMETRICO, tal que la CLAVE PUBLICA puede verificar una FIRMA DIGITAL creada por la CLAVE PRIVADA. PERIODO DE VIGENCIA (de un CERTIFICADO): Período durante el cual el SUSCRIPTOR puede firmar DOCUMENTOS DIGITALES utilizando la CLAVE PRIVADA correspondiente a la CLAVE PUBLICA contenida en el CERTIFICADO, de modo tal que la FIRMA DIGITAL no sea repudiable. El PERIODO DE VIGENCIA de un CERTIFICADO comienza en la fecha y hora en que fue emitido por la AUTORIDAD CERTIFICANTE LICENCIADA, o en una fecha y hora posterior si así lo especifica el CERTIFICADO, y termina en la fecha y hora de su vencimiento o revocación. REVOCACION DE UN CERTIFICADO: Acción de dejar sin efecto en forma permanente un CERTIFICADO a partir de una fecha cierta, incluyéndolo en la LISTA DE CERTIFICADOS REVOCADOS. SELLADO DIGITAL DE FECHA Y HORA: Acción mediante la cual la AUTORIDAD CERTIFICANTE LICENCIADA adiciona la fecha, hora, minutos y segundos (como mínimo) de su intervención, a un DOCUMENTO DIGITAL o a su DIGESTO SEGURO. La información resultante del proceso antes descripto es firmada digitalmente por la AUTORIDAD CERTIFICANTE LICENCIADA. SISTEMA CONFIABLE: Equipos de computación, software y procedimientos relacionados que: 1. Sean razonablemente confiables para resguardar contra la posibilidad de intrusión o de uso indebido; 2. Brinden un grado razonable de disponibilidad, confiabilidad, confidencialidad y correcto funcionamiento; 3. Sean razonablemente aptos para el desempeño de sus funciones específicas; 4. Cumplan con los requisitos de seguridad generalmente aceptados. SUSCRIPTOR: Persona: 1. A cuyo nombre se emite un CERTIFICADO, y 2. Que es titular de la CLAVE PRIVADA correspondiente a la CLAVE PUBLICA incluida en dicho CERTIFICADO. TECNICAMENTE CONFIABLE: Dícese de los SISTEMAS CONFIABLES que cumplen con los estándares tecnológicos que al efecto dicte la Secretaría de la Función Pública de la Jefatura de Gabinete de Ministros. TERCERO: Todo aquél que ostenta un derecho subjetivo o interés legítimo. VERIFICACION DE UNA FIRMA DIGITAL: En relación a un DOCUMENTO DIGITAL, su FIRMA DIGITAL, el correspondiente CERTIFICADO DE CLAVE PUBLICA y la LISTA DE CERTIFICADOS REVOCADOS, es la determinación fehaciente de que: 1. El DOCUMENTO DIGITAL fue firmado digitalmente con la CLAVE PRIVADA correspondiente a la CLAVE PUBLICA incluida en el CERTIFICADO; 2. El DOCUMENTO DIGITAL no fue alterado desde que fue firmado digitalmente. Para aquel documento cuya naturaleza pudiera exigir la necesidad de certificación de fecha cierta, o bien ésta fuere conveniente dado sus efectos, deberá determinarse adicionalmente que el mismo fue firmado digitalmente durante el PERIODO DE VIGENCIA del correspondiente CERTIFICADO.
Antecedentes (NAC.) - Informacion Parlamentaria
5) RESOLUCIÓN 51/162 DE LA ASAMBLEA GENERAL DE 16 DE DICIEMBRE DE 1996
LEY MODELO
DE LA CNUDMI
SOBRE COMERCIO ELECTRÓNICO

1996

con la adición del Artículo 5 bis en la forma aprobada en 1998

NACIONES UNIDAS

ÍNDICE

Proyecto De Ley nro:559/2010

GUÍA PARA LA INCORPORACIÓN AL DERECHO INTERNO DE LA LEY MODELO
DE LA CNUDMI SOBRE COMERCIO ELECTRÓNICO párrs. 1-150

Resolución aprobada por la Asamblea General

[sobre la base del informe de la Sexta Comisión (A/51/628)]
51/162. Ley Modelo sobre Comercio Electrónico aprobada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional

La Asamblea General,

Recordando su resolución 2205 (XXI), de 17 de diciembre de 1966, por la que estableció la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional con el mandato de fomentar la armonización y la unificación progresivas del derecho mercantil internacional y de tener presente, a ese respecto, el interés de todos los pueblos, en particular el de los países en desarrollo, en el progreso amplio del comercio internacional,

Observando que un número creciente de transacciones comerciales internacionales se realizan por medio del intercambio electrónico de datos y por otros medios de comunicación, habitualmente conocidos como "comercio electrónico", en los que se usan métodos de comunicación y almacenamiento de información sustitutivos de los que utilizan papel,

Proyecto De Ley nro:559/2010

Recordando la recomendación relativa al valor jurídico de los registros computadorizados aprobada por la Comisión en su 18. período de sesiones, celebrado en 1985, y el inciso b) del párrafo 5 de la resolución 40/71 de la Asamblea General, de 11 de diciembre de 1985, en la que la Asamblea pidió a los gobiernos y a las organizaciones internacionales que, cuando así convenga, adopten medidas acordes con las recomendaciones de la Comisión a fin de garantizar la seguridad jurídica en el contexto de la utilización más amplia posible del procesamiento automático de datos en el comercio internacional,

Convencida de que la elaboración de una ley modelo que facilite el uso del comercio electrónico y sea aceptable para Estados que tengan sistemas jurídicos, sociales y económicos diferentes podría contribuir de manera significativa al establecimiento de relaciones económicas internacionales armoniosas,

Observando que la Ley Modelo sobre Comercio Electrónico fue aprobada por la Comisión en su 29. período de sesiones después de examinar las observaciones de los gobiernos y de las organizaciones interesadas,

Estimando que la aprobación de la Ley Modelo sobre Comercio Electrónico por la Comisión ayudará de manera significativa a todos los Estados a fortalecer la legislación que rige el uso de métodos de comunicación y almacenamiento de información sustitutivos de los que utilizan papel y a preparar tal legislación en los casos en que carezcan de ella,

1. Expresa su agradecimiento a la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional por haber terminado y aprobado la Ley Modelo sobre Comercio Electrónico que figura como anexo de la presente resolución y por haber preparado la Guía para la Promulgación de la Ley Modelo;

2. Recomienda que todos los Estados consideren de manera favorable la Ley Modelo cuando promulguen o revisen sus leyes, habida cuenta de la necesidad de que el derecho aplicable a los métodos de comunicación y almacenamiento de información sustitutivos de los que utilizan papel sea uniforme;

3. Recomienda también que no se escatimen esfuerzos para velar por que la Ley Modelo y la Guía sean ampliamente conocidas y estén a disposición de todos.

85a. sesión plenaria
16 de diciembre de 1996

LEY MODELO DE LA CNUDMI SOBRE COMERCIO ELECTRÓNICO

[Original: árabe, chino, español, francés, inglés, ruso]

PRIMERA PARTE

Comercio electrónico en general

Capítulo I

Disposiciones generales

Artículo 1

Ámbito de aplicación*

La presente Ley** será aplicable a todo tipo de información en forma de mensaje de datos utilizada en el contexto*** de actividades comerciales****.

_____

Proyecto De Ley nro:559/2010

* La Comisión sugiere el siguiente texto para los Estados que deseen limitar el ámbito de aplicación de la presente Ley a los mensajes de datos internacionales:

La presente Ley será aplicable a todo mensaje de datos que sea conforme a la definición del párrafo 1) del artículo 2 y que se refiera al comercio internacional.

** La presente ley no deroga ninguna norma jurídica destinada a la protección del consumidor.

*** La Comisión sugiere el siguiente texto para los Estados que deseen ampliar el ámbito de aplicación de la presente Ley:

La presente Ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en las situaciones siguientes: [...].

**** El término "comercial" deberá ser interpretado ampliamente de forma que abarque las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; de facturaje ("factoring"); de arrendamiento de bienes de equipo con opción de compra ("leasing"); de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; de inversión; de financiación; de banca; de seguros; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera.

Artículo 2

Definiciones

Para los fines de la presente Ley:

a) Por "mensaje de datos" se entenderá la información generada, enviada, recibida o 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;

b) Por "intercambio electrónico de datos (EDI)" se entenderá la transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto;

c) Por "iniciador" de un mensaje de datos se entenderá toda persona que, a tenor del mensaje, haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar o generar ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de intermediario con respecto a él;

d) Por "destinatario" de un mensaje de datos se entenderá la persona designada por el iniciador para recibir el mensaje, pero que no esté actuando a título de intermediario con respecto a él;

e) Por "intermediario", en relación con un determinado mensaje de datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él;

f) Por "sistema de información" se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

Artículo 3

Interpretación

1) En la interpretación de la presente Ley habrán de tenerse en cuenta su origen internacional y la necesidad

Proyecto De Ley nro:559/2010

de promover la uniformidad de su aplicación y la observancia de la buena fe.

2) Las cuestiones relativas a materias que se rijan por la presente Ley y que no estén expresamente resueltas en ella serán dirimidas de conformidad con los principios generales en que ella se inspira.

Artículo 4

Modificación mediante acuerdo

1) Salvo que se disponga otra cosa, en las relaciones entre las partes que generan envían, reciben, archivan o procesan de alguna otra forma mensajes de datos, las disposiciones del capítulo III podrán ser modificadas mediante acuerdo.

2) Lo dispuesto en el párrafo 1) no afectará a ningún derecho de que gocen las partes para modificar de común acuerdo alguna norma jurídica a la que se haga referencia en el capítulo II.

Capítulo II

Aplicación de los requisitos jurídicos a los mensajes de datos

Artículo 5

Reconocimiento jurídico de los mensajes de datos

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.

Artículo 5 bis

Incorporación por remisión

(En la forma aprobada por la Comisión en su 31.º período de sesiones, en junio de 1998)

No 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 6

Escrito

1) Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos si la información que éste contiene es accesible para su ulterior consulta.

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no conste por escrito.

3) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 7

Firma

1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje

Proyecto De Ley nro:559/2010

de datos:

a) Si se utiliza 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) Si ese método es tan fiable como sea 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.

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no exista una firma.

3) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 8

Original

1) Cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos:

a) Si existe alguna garantía fidedigna de que se ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma;

b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar.

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no sea presentada o conservada en su forma original.

3) Para los fines del inciso a) del párrafo 1):

a) La integridad de la información será evaluada conforme al criterio de que haya permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de su comunicación, archivo o presentación; y

b) El grado de fiabilidad requerido será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias del caso.

4) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 9

Admisibilidad y fuerza probatoria de los mensajes de datos

1) En todo trámite legal, no se dará aplicación a regla alguna de la prueba que sea óbice para la admisión como prueba de un mensaje de datos:

a) Por la sola razón de que se trate de un mensaje de datos; o

b) Por razón de no haber sido presentado en su forma original, de ser ese mensaje la mejor prueba que quepa razonablemente esperar de la persona que la presenta.

2) Toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria. Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la fiabilidad de la forma en la que se

Proyecto De Ley nro:559/2010

haya generado, archivado o comunicado el mensaje, la fiabilidad de la forma en la que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

Artículo 10

Conservación de los mensajes de datos

1) Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho mediante la conservación de los mensajes de datos, siempre que se cumplan las condiciones siguientes:

a) Que la información que contengan sea accesible para su ulterior consulta; y

b) Que el mensaje de datos sea conservado con el formato en 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

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

2) La obligación de conservar ciertos documentos, registros o informaciones conforme a lo dispuesto en el párrafo 1) no será aplicable a aquellos datos que tengan por única finalidad facilitar el envío o recepción del mensaje.

3) Toda persona podrá recurrir a los servicios de un tercero para observar el requisito mencionado en el párrafo 1), siempre que se cumplan las condiciones enunciadas en los incisos a), b) y c) del párrafo 1).

Capítulo III

Comunicación de los mensajes de datos

Artículo 11

Formación y validez de los contratos

1) En la formación de un contrato, de no convenir las partes otra cosa, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación un mensaje de datos.

2) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 12

Reconocimiento por las partes de los mensajes de datos

1) En las relaciones entre el iniciador y el destinatario de un mensaje de datos, no se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de mensaje de datos.

2) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 13

Atribución de los mensajes de datos

1) Un mensaje de datos proviene del iniciador si ha sido enviado por el propio iniciador.

Proyecto De Ley nro:559/2010

2) En las relaciones entre el iniciador y el destinatario, se entenderá que un mensaje de datos proviene del iniciador si ha sido enviado:

a) Por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje; o

b) Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.

3) En las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que un mensaje de datos proviene del iniciador, y a actuar en consecuencia, cuando:

a) Para comprobar que el mensaje provenía del iniciador, el destinatario haya aplicado adecuadamente un procedimiento aceptado previamente por el iniciador con ese fin; o

b) El mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio.

4) El párrafo 3) no se aplicará:

a) A partir del momento en que el destinatario haya sido informado por el iniciador de que el mensaje de datos no provenía del iniciador y haya dispuesto de un plazo razonable para actuar en consecuencia; o

b) En los casos previstos en el inciso b) del párrafo 3), desde el momento en que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el mensaje de datos no provenía del iniciador.

5) Siempre que un mensaje de datos provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá actuar en consecuencia. El destinatario no gozará de este derecho si sabía, o hubiera sabido de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la transmisión había dado lugar a algún error en el mensaje de datos recibido.

6) El destinatario tendrá derecho a considerar que cada mensaje de datos recibido es un mensaje de datos separado y a actuar en consecuencia, salvo en la medida en que duplique otro mensaje de datos, y que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el mensaje de datos era un duplicado.

Artículo 14

Acuse de recibo

1) Los párrafos 2) a 4) del presente artículo serán aplicables cuando, al enviar o antes de enviar un mensaje de datos, el iniciador solicite o acuerde con el destinatario que se acuse recibo del mensaje de datos.

2) Cuando el iniciador 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 basten para indicar al iniciador que se ha recibido el mensaje de datos.

3) Cuando el iniciador haya indicado que los efectos del mensaje de datos estarán condicionados a la recepción

Proyecto De Ley nro:559/2010

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.

4) Cuando el iniciador 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 iniciador:

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.

5) Cuando el iniciador 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.

6) 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.

7) 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 15

Tiempo y lugar del envío y la recepción de un mensaje de datos

1) De no convenir otra cosa el iniciador 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 iniciador o de la persona que envió el mensaje de datos en nombre del iniciador.

2) De no convenir otra cosa el iniciador 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 al entrar el mensaje de datos en un sistema de información del destinatario.

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 iniciador y el destinatario, el mensaje de datos se tendrá por expedido en el lugar donde el iniciador tenga su establecimiento y por recibido en el lugar donde el destinatario tenga el suyo. Para los fines del presente párrafo:

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

Proyecto De Ley nro:559/2010

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

5) Lo dispuesto en el presente artículo no será aplicable a: [...].

SEGUNDA PARTE

Comercio electrónico en materias específicas

Capítulo I

Transporte de mercancías

Artículo 16

Actos relacionados con los contratos de transporte de mercancías

Sin perjuicio de lo dispuesto en la parte I de la presente Ley, el presente capítulo será aplicable a cualquiera de los siguientes actos que guarde relación con un contrato de transporte de mercancías, o con su cumplimiento, sin que la lista sea exhaustiva:

a)

i) indicación de las marcas, el número, la cantidad o el peso de las mercancías;

ii) declaración de la índole o el valor de las mercancías;

iii) emisión de un recibo por las mercancías;

iv) confirmación de haberse completado la carga de las mercancías;

b)

i) notificación a alguna persona de las cláusulas y condiciones del contrato;

ii) comunicación de instrucciones al portador;

c)

i) reclamación de la entrega de las mercancías;

ii) autorización para proceder a la entrega de las mercancías;

iii) notificación de la pérdida de las mercancías o de los daños que hayan sufrido;

d)cualquier otra notificación o declaración relativas al cumplimiento del contrato;

e) promesa de hacer entrega de las mercancías a la persona designada o a una persona autorizada para reclamar esa entrega;

f) concesión, adquisición, renuncia, restitución, transferencia o negociación de algún derecho sobre mercancías;

g) adquisición o transferencia de derechos y obligaciones con arreglo al contrato.

Proyecto De Ley nro:559/2010

Artículo 17

Documentos de transporte

1) Con sujeción a lo dispuesto en el párrafo 3), en los casos en que la ley requiera que alguno de los actos enunciados en el artículo 16 se lleve a cabo por escrito o mediante un documento que conste de papel, ese requisito quedará satisfecho cuando el acto se lleve a cabo por medio de uno o más mensajes de datos.

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no se lleve a cabo el acto por escrito o mediante un documento.

3) Cuando se conceda algún derecho a una persona determinada y a ninguna otra, o ésta adquiera alguna obligación, y la ley requiera que, para que ese acto surta efecto, el derecho o la obligación hayan de transferirse a esa persona mediante el envío, o la utilización, de un documento, ese requisito quedará satisfecho si el derecho o la obligación se transfiere mediante la utilización de uno o más mensajes de datos, siempre que se emplee un método fiable para garantizar la singularidad de ese mensaje o esos mensajes de datos.

4) Para los fines del párrafo 3), el nivel de fiabilidad requerido será determinado a la luz de los fines para los que se transfirió el derecho o la obligación y de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

5) Cuando se utilicen uno o más mensajes de datos para llevar a cabo alguno de los actos enunciados en los incisos f) y g) del artículo 16, no será válido ningún documento utilizado para llevar a cabo cualquiera de esos actos, a menos que se haya puesto fin al uso de mensajes de datos para sustituirlo por el de documentos. Todo documento que se emita en esas circunstancias deberá contener una declaración a tal efecto. La sustitución de mensajes de datos por documentos no afectará a los derechos ni a las obligaciones de las partes.

6) Cuando se aplique obligatoriamente una norma jurídica a un contrato de transporte de mercancías que esté consignado, o del que se haya dejado constancia, en un documento, esa norma no dejará de aplicarse a un contrato de transporte de mercancías del que se haya dejado constancia en uno o más mensajes de datos por razón de que el contrato conste en ese mensaje o esos mensajes de datos en lugar de constar en un documento.

7) Lo dispuesto en el presente artículo no será aplicable a: [...].

Antecedentes (NAC.) - Informacion Parlamentaria

6) MERCOSUR/GMC EXT./RES. Nº 34/06

DIRECTRICES PARA LA CELEBRACIÓN DE ACUERDOS DE RECONOCIMIENTO MUTUO DE FIRMAS ELECTRÓNICAS AVANZADAS EN EL ÁMBITO DEL MERCOSUR

VISTO: El Tratado de Asunción, el Protocolo de Ouro Preto, la Decisión Nº 59/00 del Consejo del Mercado Común y las Resoluciones Nº 24/03 y 22/04 del Grupo Mercado Común.

CONSIDERANDO:

Que en la necesidad de fortalecer la confianza mutua y alcanzar el reconocimiento de firmas electrónicas avanzadas, los Estados Partes podrán celebrar Acuerdos de Reconocimiento Mutuo a través de sus respectivos órganos competentes.

Que es preciso establecer criterios comunes y procedimientos transparentes para la implementación de Acuerdos de Reconocimiento Mutuo entre los Estados Partes.

EL GRUPO MERCADO COMÚN

RESUELVE:

Art. 1 - Aprobar las Directrices para la Celebración de Acuerdos de Reconocimiento Mutuo de firmas electrónicas avanzadas en el ámbito del MERCOSUR, en los términos de la presente Resolución.

Art. 2 - Definiciones

A efectos de la presente Resolución, se entenderá por:

Proyecto De Ley nro:559/2010

1) "Datos de creación de firma": los datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica;
2) "Dispositivo de creación de firma": un programa informático configurado o un aparato informático configurado que sirve para aplicar los datos de creación de firma electrónica;
3) "Datos de verificación de firma": los datos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica;
Art. 3 - El seguimiento de las Directrices será realizado por el SGT Nº 13, cuyas funciones incluirán las siguientes: intercambiar información, proponer pautas, estándares y procedimientos operativos, analizar los avances nacionales en la materia, estudiar la adecuación de las normas nacionales a los lineamientos establecidos en la presente Resolución, analizar la aplicabilidad de criterios de homologación y los supuestos aplicables a la certificación digital.
El SGT Nº 13 promoverá el desarrollo de estudios para la implementación de un sistema de control común entre los Estados Partes con vistas a la aproximación de sus respectivas infraestructuras y armonización de procedimientos.
Art. 4 - Los Estados Partes, en la elaboración de acuerdos de reconocimiento mutuo de firmas electrónicas avanzadas que celebren entre sí, deberán observar las siguientes Directrices:
I. Estándares generales de interoperabilidad
Se adoptarán los siguientes estándares internacionales de interoperabilidad:
a) el estándar ITU X.509 v3 o ISO/IEC 9594 para los certificados digitales;
b) el estándar ITU X.509 v2 para la lista de certificados digitales revocados;
c) las recomendaciones de IETF RFC 2560 para la verificación en línea del estado del certificado digital;
d) las recomendaciones de IETF RFC 2527 o RFC 3647 para los contenidos de las políticas de certificación y las prácticas de certificación.
El SGT Nº 13 propondrá al GMC la actualización de los estándares técnicos y operativos que consideren convenientes teniendo en cuenta el estado del arte en la materia.
II. Criterios de seguridad física y lógica de los prestadores de servicios de certificación.
Se deberá prever la evaluación y armonización de los aspectos relacionados con el ambiente operativo, en especial aquellos relacionados con:
a) el control de los accesos a servicios y perfiles;
b) la separación de las tareas y atribuciones relacionadas con cada perfil;
c) los mecanismos de seguridad aplicados a los datos e informaciones sensibles;
d) los mecanismos de generación y almacenamiento de los registros de auditoría;
e) los mecanismos internos de seguridad que garanticen la integridad de los datos y los procesos críticos;
f) los aspectos referidos a la seguridad física y lógica de las instalaciones;
g) los mecanismos tendientes a garantizar la continuidad del funcionamiento de los sistemas críticos.
h) el módulo criptográfico utilizado para el almacenamiento de la clave privada de conformidad con el estándar FIPS 140-1 nivel 3, o equivalente según la evaluación que se realizará en el SGT Nº 13
III. Criterios de auditoría y control de los prestadores de servicios de certificación
Se requerirá la existencia de un sistema de acreditación y control de prestadores de servicios de certificación que contemple:
a) la realización de auditorías sobre los prestadores de servicios de certificación que verifiquen todos los aspectos relacionados con el ciclo de vida de los certificados reconocidos y de sus claves criptográficas.
b) los mecanismos de sanción para aquellos prestadores de servicios de certificación que no cumplan con los criterios acordados.
Se dispondrá la evaluación y armonización de los aspectos relacionados con el sistema de control de prestadores de servicios de certificación acreditados, en especial aquellos relacionados con:
2
a) el alcance y la periodicidad de las auditorías, las cuales deben contemplar como mínimo la revisión de las políticas y prácticas de certificación, de seguridad, del ambiente de seguridad física y lógica, la evaluación de tecnología utilizada, los controles sobre la administración de los servicios, la selección y administración del personal y los contratos de tercerización.
b) la identificación de los eventos a ser registrados, la información mínima de cada uno de ellos y los procedimientos para garantizar la integridad y veracidad de los mismos.
c) la documentación respaldatoria del ciclo de vida de los certificados reconocidos.
IV. Criterios para la emisión de certificados reconocidos
Se contemplará la evaluación y armonización del contenido de los certificados reconocidos, con los siguientes

Proyecto De Ley nro:559/2010

requisitos mínimos:
a) la identificación del proveedor de servicios de certificación que lo expide y del Estado del MERCOSUR donde está establecido
b) los datos de identificación del titular del certificado reconocido: nombre y apellido en caso de ser persona física, o la denominación en caso de ser persona jurídica
c) los datos de verificación de firma que correspondan a los datos de creación de firma bajo control del titular del certificado reconocido
d) el periodo de validez del certificado reconocido
e) el número de serie del certificado reconocido
f) la firma electrónica avanzada del proveedor de servicios de certificación que expide el certificado reconocido
g) la indicación del sitio de Internet en el que se encuentra la política de certificación bajo la cual se emitió el certificado reconocido.
h) la indicación del sitio de Internet que permita acceder a la lista de certificados revocados o al servicio de verificación en linea de su estado.
La evaluación y armonización comprenderán también los mecanismos de seguridad utilizados para la protección de los dispositivos de creación de firma.
V. Recomendación para la verificación segura de firma electrónica avanzada
Durante el proceso de verificación de firma deberá garantizarse con suficiente certeza que:
a) los datos utilizados para verificar la firma corresponden a los datos mostrados al verificador;
b) la firma se verifica de forma fiable y el resultado de esa verificación figura correctamente;
c) se puede identificar de forma fiable el documento electrónico firmado;
d) se verifican de forma fiable la autenticidad y la validez de los certificados digitales al momento de la firma del documento electrónico;
e) figuran correctamente el resultado de la verificación y la identidad del firmante;
f) puede detectarse cualquier cambio pertinente relativo a la integridad del documento electrónico firmado.
3
VI. Otras características de los prestadores de servicios de certificación
Se deberá incluir la evaluación y armonización de otros aspectos relacionados con la prestación del servicio de certificación, como:
a) los procedimientos de verificación de identidad de quien solicite un certificado reconocido.
b) los criterios de confidencialidad de la información suministrada a los prestadores de servicios de certificación
c) la información mínima a ser publicada por el prestador de servicios de certificación
d) las fuentes de hora confiables utilizadas por los prestadores de servicios de certificación en su operatoria, en sus sistemas y registros de auditoría.
Art. 4 - Esta Resolución no necesita ser incorporada al ordenamiento jurídico de los Estados Partes, por reglamentar aspectos de la organización o del funcionamiento del MERCOSUR.
XXXI GMC EXT. Córdoba, 18/VII/06
4
Antecedentes (NAC.) - Informacion Parlamentaria
7) MERCOSUR/GMC EXT./RES. Nº 37/06
RECONOCIMIENTO DE LA EFICACIA JURÍDICA DEL
DOCUMENTO ELECTRÓNICO, LA FIRMA ELECTRÓNICA Y LA FIRMA ELECTRÓNICA AVANZADA EN EL ÁMBITO DEL MERCOSUR
VISTO: El Tratado de Asunción, el Protocolo de Ouro Preto, el Protocolo de Olivos, las Decisiones N° 04/91 y 59/00 del Consejo del Mercado Común y la Resolución Nº 24/03 del Grupo Mercado Común.
CONSIDERANDO:
Que el desarrollo continuo de las tecnologías de la información y comunicación están al servicio de la consolidación y del desarrollo de una sociedad de la información inclusiva, que promueva el mejor aprovechamiento socio-económico de los bienes inmateriales.
Que el desarrollo de las relaciones sociales y el estrechamiento de los lazos entre los ciudadanos y las administraciones de los Estados Partes, y de éstos entre sí, dependen de medidas que garanticen la seguridad y la confianza en los documentos electrónicos.
Que para la seguridad y confianza en los documentos electrónicos se requieren firmas electrónicas y servicios conexos.
Que las firmas electrónicas avanzadas, basadas en un certificado reconocido, permiten lograr un mayor nivel de

Proyecto De Ley nro:559/2010

seguridad.
Que debido a la asimetría en los marcos jurídicos nacionales sobre la materia, es necesario adoptar normas comunes, de acuerdo a los estándares internacionales a fin de promover un entendimiento tecnológico entre las respectivas estructuras legales y técnicas de los Estados Partes.
Que el desarrollo de la firma electrónica avanzada en los Estados Partes no restringirá las actividades relacionadas a la emisión de certificados digitales vinculados a firmas electrónicas, que tendrán sus efectos jurídicos limitados a la autonomía de la voluntad de las partes que confían en dichas tecnologías o no se oponen a su utilización.
EL GRUPO MERCADO COMÚN
RESUELVE:
Art. 1- Ámbito de aplicación
La presente Resolución tiene por finalidad reconocer, en las condiciones previstas en la presente norma, la eficacia jurídica de los documentos electrónicos, de la firma electrónica y de la firma electrónica avanzada en el ámbito del MERCOSUR, contribuyendo a su utilización.
La presente normativa no regula otros aspectos relacionados con la celebración y validez de los actos jurídicos cuando existan requisitos de forma establecidos en las legislaciones nacionales, ni afecta a las normas y límites contenidos en las legislaciones nacionales que rigen el uso de documentos.
1
La presente normativa no habilita la libre circulación de servicios de certificación digital en el ámbito del MERCOSUR. En lo atinente a la prestación de servicios de certificación digital, los Estados Partes observarán las disciplinas establecidas en el Protocolo de Montevideo sobre Comercio de Servicios del MERCOSUR y en sus listas de compromisos específicos.
Art. 2- Principios
Los Estados Partes observarán los siguientes principios:
1. Autonomía operativa y coordinación permanente entre las Infraestructuras nacionales;
2. Interoperabilidad basada en estándares internacionales;
3. Intercambio de información y documentación digital entre los Estados Partes en condiciones técnicas seguras, con validez legal y valor probatorio;
4. Transparencia en la gestión de la certificación digital;
5. Tratamiento neutro en las leyes nacionales con relación a las diversas tecnologías utilizadas en las actividades previstas en la presente Resolución, de modo de permitir la adaptación al ritmo del desarrollo tecnológico inherente a esas actividades (neutralidad tecnológica);
6. Interpretación funcional de los términos y conceptos, a fin de asegurar que no sean negados efectos jurídicos a un proceso o tecnología utilizado por un Estado Parte, por el sólo hecho de que se le atribuye una nomenclatura distinta a la prevista en la presente Resolución.
Art. 3. Definiciones
A efectos de la presente Resolución, se entenderá por:
1) "Firma electrónica": los datos en forma electrónica anexos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados por el firmante como medio de identificación;
2) "Firma electrónica avanzada": la firma electrónica que cumple los requisitos siguientes:
a) requerir información de exclusivo conocimiento del firmante, permitiendo su identificación unívoca;
b) ser creada por medios que el firmante pueda mantener bajo su exclusivo control;
c) ser susceptible de verificación por terceros;
d) estar vinculada a estos datos de tal modo que cualquier alteración subsiguiente en los mismos sea detectable; y
e) haber sido creada utilizando un dispositivo de creación de firma técnicamente seguro y confiable y estar basada en un certificado reconocido y válido al momento de la firma.
3) Firma digital: utilizada indistintamente con firma electrónica avanzada a los efectos de la presente Resolución.
4) Firmante: la persona física o jurídica que utiliza legalmente un dispositivo para la creación de firma electrónica;
5) Documento electrónico: representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo.
2
6) Documento digital: utilizada indistintamente con documento electrónico a los efectos de la presente Resolución.

Proyecto De Ley nro:559/2010

7) Certificado digital: documento electrónico firmado digitalmente que vincula unos datos de verificación de firma con su titular y confirma su identidad.
8) Certificado reconocido: certificado digital emitido por un prestador de servicios acreditado que cumple con los requisitos establecidos por la legislación nacional.
9) Certificado avanzado: utilizada indistintamente con Certificado reconocido a los efectos de la presente Resolución.
10) Prestador de servicios de certificación: persona física o jurídica, conforme a la legislación nacional, que expide certificados o presta otros servicios en relación con la firma electrónica.
Art. 4. Efectos Legales de los Documentos Electrónicos y de las Firmas Electrónicas
Los Estados Partes reconocen que los documentos electrónicos satisfacen los requerimientos de escritura. En virtud de ello, en cualquiera de los Estados Partes los documentos electrónicos tendrán los mismos efectos jurídicos que los documentos escritos, salvo excepciones contempladas en las legislaciones nacionales.
Los Estados Partes reconocerán efectos jurídicos a la firma electrónica cuando la misma fuese admitida como válida por las partes que la utilizan o fuese aceptada por la persona a quien fuese opuesto el documento a ella vinculado.
Los Estados Partes asegurarán que no sean negados efectos probatorios a un documento electrónico por el sólo hecho de que éste no esté vinculado a una firma electrónica avanzada, si por algún medio inequívoco se pudiese demostrar su autenticidad e integridad.
Se respetará la libertad de las partes para concertar de común acuerdo las condiciones en que aceptarán las firmas electrónicas, conforme a su legislación nacional.
En caso de ser desconocida la firma electrónica por una de las partes, corresponde a la otra parte probar su validez.
Art. 5- Firma electrónica avanzada: Reconocimiento Mutuo
Con el objetivo de alcanzar el reconocimiento mutuo de las firmas electrónicas avanzadas y de los certificados digitales, los Estados Partes podrán celebrar, entre sí, acuerdos de reconocimiento mutuo. A tales efectos, el GMC aprobará las Directrices para la celebración de dichos acuerdos. Dichas Directrices reflejarán el estado de la materia al momento de su aprobación y podrán ser actualizadas a propuesta del SGT Nº 13, de manera de acompañar la evolución de las tecnologías a ellas relacionadas.
A través de los Acuerdos de Reconocimiento Mutuo se otorgará a las firmas electrónicas avanzadas, que cumplan con las condiciones dispuestas en ellos, el mismo valor jurídico y probatorio que el otorgado a las firmas manuscritas.
Los Estados Partes reconocerán la autenticidad e integridad de un documento electrónico firmado con una firma electrónica avanzada, admitiéndola como prueba documental en procesos judiciales, conforme lo que se disponga en los Acuerdos de Reconocimiento Mutuo.
3
Los Estados Partes indicarán, en el ámbito del SGT Nº 13, cuáles serán los organismos competentes habilitados para suscribir Acuerdos de Reconocimiento Mutuo.
Art. 6- Certificados Digitales Reconocidos
Los Acuerdos de Reconocimiento Mutuo establecerán las condiciones bajo las cuales los certificados digitales expedidos en un Estado Parte de ese Acuerdo tendrán la misma validez jurídica en los demás Estados Partes que suscriban el Acuerdo.
Dichas condiciones deberán contemplar, como mínimo, que los certificados digitales:
a) sean emitidos por un prestador de servicios de certificación bajo el sistema nacional de acreditación y control previsto en el artículo 7;
b) respondan a formatos estándares reconocidos internacionalmente, fijados por la autoridad de aplicación de cada Estado Parte;
c) respondan a los criterios mínimos establecidos en las Directrices mencionadas en el artículo 5; y
d) contengan como mínimo, los datos que permitan:
1. identificar indubitablemente a su titular y al prestador de servicios de certificación 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 digital;
4. contemplar la información necesaria para la verificación de la firma;
5. identificar la política de certificación bajo la cual fue emitido.
Art. 7- Prestación de Servicios de Certificación
Los Estados Partes no sujetarán a acreditación previa la prestación de servicios de certificación, excepto en

Proyecto De Ley nro:559/2010

aquellos vinculados a una firma electrónica avanzada, de conformidad con los términos de la presente Resolución.
Los Estados Partes asegurarán la creación de un sistema adecuado de acreditación y control de los prestadores de servicios de certificación que emitan certificados reconocidos que permitan la verificación de firmas electrónicas avanzadas, establecidos en sus respectivos territorios.
Los Estados Partes podrán supeditar el uso de la firma electrónica y la firma electrónica avanzada en el sector público a posibles prescripciones adicionales. Tales prescripciones serán objetivas, transparentes, proporcionadas y no discriminatorias, y sólo podrán hacer referencia a las características específicas de la aplicación de que se trate. Estas prescripciones no deberán obstaculizar los servicios transfronterizos.
4
Art. 8- Responsabilidades
Los Estados Partes asegurarán como mínimo que un prestador de servicios de certificación acreditado en los términos del artículo 7, sea responsable por los daños y perjuicios causados a cualquier 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 las respectivas Infraestructuras nacionales para el certificado reconocido y a la exactitud de los mismos, al momento de su emisión.
b) que al momento de emisión de un certificado reconocido por parte del prestador de servicios de certificación acreditado, la firma en él identificada obedece a los datos de creación de firma correspondientes a los datos de verificación incluidos en el certificado reconocido del prestador, con el objeto de asegurar la cadena de confianza.
c) los errores u omisiones que presenten los certificados reconocidos que emitan, o por la inobservancia de los procedimientos de certificación establecidos a partir de los Acuerdos de Reconocimiento Mutuo.
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 acreditado demostrar que no actuó ni con culpa ni con dolo.
Los Estados Partes asegurarán que el prestador de servicios de certificación acreditado en los términos del artículo 7, pueda indicar en un certificado reconocido de forma identificable por terceros, los límites de su utilización.
El prestador de servicios de certificación acreditado en los términos del artículo 7, no será responsable por los perjuicios resultantes de la utilización de un certificado reconocido por él emitido, que exceda el alcance definido en su Política de Certificación. 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.
Art. 9- Protección de Datos Personales
Los Estados Partes deberán prever que un prestador de servicios de certificación que emite certificados reconocidos destinados al público, sólo pueda recolectar los datos personales directamente de la persona a quien esos datos se refieren, 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.
Los Estados Partes garantizarán la confidencialidad de los demás datos personales requeridos para la emisión del certificado reconocido y que no figuren en él, en los términos dispuestos por el presente artículo.
5
Art. 10 - Incorporación
Los Estados Partes deberán incorporar la presente Resolución a sus ordenamientos jurídicos nacionales.
XXXI GMC EXT. Córdoba, 18/VII/06
6
Antecedentes (NAC.) - Informacion Parlamentaria
   8) ART. 75 INC. 12 DE CONST. NACIONAL

CONSTITUCION DE LA NACION ARGENTINA

Preámbulo

Nos los representantes del pueblo de la Nación Argentina, reunidos en Congreso General Constituyente por

Proyecto De Ley nro:559/2010

voluntad y elección de las provincias que la componen, en cumplimiento de pactos preexistentes, con el objeto de constituir la unión nacional, afianzar la justicia, consolidar la paz interior, proveer a la defensa común, promover el bienestar general, y asegurar los beneficios de la libertad, para nosotros, para nuestra posteridad, y para todos los hombres del mundo que quieran habitar en el suelo argentino: invocando la protección de Dios, fuente de toda razón y justicia: ordenamos, decretamos y establecemos esta Constitución para la Nación Argentina.

Capítulo Cuarto

Atribuciones del Congreso

Artículo 75- Corresponde al Congreso:

12. Dictar los Códigos Civil, Comercial, Penal, de Minería, y del Trabajo y Seguridad Social, en cuerpos unificados o separados, sin que tales códigos alteren las jurisdicciones locales, correspondiendo su aplicación a los tribunales federales o provinciales, según que las cosas o las personas cayeren bajo sus respectivas jurisdicciones; y especialmente leyes generales para toda la Nación sobre naturalización y nacionalidad, con sujeción al principio de nacionalidad natural y por opción en beneficio de la Argentina; así como sobre bancarrotas, sobre falsificación de la moneda corriente y documentos públicos del estado, y las que requiera el establecimiento del juicio por jurados.