FIRMA DIGITAL

Decreto 2628/2002

Reglamentación de la Ley N° 25.506. Consideraciones Generales. Autoridad de Aplicación. Comisión Asesora para la Infraestructura de Firma Digital. Ente Administrador de Firma Digital. Sistema de Auditoría. Estándares Tecnológicos. Revocación de Certificados Digitales. Certificadores Licenciados. Autoridades de Registro. Disposiciones para la Administración Pública Nacional

Bs. As., 19/12/2002

VISTO la Ley N° 25.506, el Decreto N° 427 del 16 de abril de 1998, el Decreto N° 78 del 10 de enero de 2002, el Decreto N° 333 del 19 de febrero de 1985 y sus modificatorios y la Resolución N° 194 del 27 de noviembre de 1998 de la ex SECRETARIA DE LA FUNCION PUBLICA, y

CONSIDERANDO:

Que la sanción de la Ley N° 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 N° 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 N° 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 N° 25.506 permitirá establecer una Infraestructura de Firma Digital que ofrezca autenticación, y garantía de integridad para los 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 N° 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 N° 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 N° 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 N° 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 N° 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

Artículo 1° — Objeto. 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 3°, 4° y 5° de la Ley N° 25.506 podrán utilizarse los siguientes sistemas de comprobación de autoría e integridad:

a) Firma electrónica,

b) Firma digital basada en certificados digitales emitidos por certificadores 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.

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

Art. 3° — Certificados digitales emitidos por certificadores licenciados. Los certificados digitales contemplados, en el artículo 13 de la Ley N° 25.506 son aquellos cuya utilización permite disponer de una firma digital amparada por las presunciones de autoría e integridad establecidas en los artículos 7° y 8° de la ley citada.

CAPITULO II

DE LA AUTORIDAD DE APLICACION

Art. 4° — Normas técnicas. 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 N° 25.506.

Art. 5° — Conservación. 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.

Art. 6° — Regulación. Facúltase a la JEFATURA DE GABINETE DE MINISTROS a establecer:

a) Los estándares tecnológicos y de seguridadaplicables 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 certificadosdigitales.

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 lagradación de sanciones previstas en la Ley N° 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.

CAPITULO III

DE LA COMISION ASESORA PARA LA INFRAESTRUCTURA DE FIRMA DIGITAL

Art. 7° — Comisión Asesora para la Infraestructura de Firma Digital. En el ámbito de la JEFATURA DE GABINETE DE MINISTROS funcionará la Comisión Asesora para la Infraestructura de Firma Digital, que se constituirá de acuerdo a lo dispuesto por el artículo 35 de la Ley N° 25.506.

Art. 8° — Integración. 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.

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

Art. 10. — Consulta Pública. 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 tratandoa 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

Art. 11. — Ente Administrador de Firma Digital. 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.

Art. 12. — Autoridades del Ente Administrador de Firma Digital. 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.

Art. 13. — Funciones del Ente Administrador.

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 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 N° 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 N° 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 participación en el mercado de los prestadores y protección de los usuarios.

Art. 14. — Obligaciones del Ente Administrador.

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.

Art. 15. — Organización del Ente Administrador. 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.

Art. 16. — Recursos del Ente Administrador. El Ente Administrador podrá arancelar los servicios que preste para cubrir total o parcialmente sus costos. Los recursos propios del Ente Administrador se integrarán con:

a) Los importes provenientes de los aranceles que se abonen por la provisión de los siguientes servicios:

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 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.

Art. 17. — Financiamiento del Ente Administrador. 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

Art. 18. — Precalificación de entidades de auditoría. 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.

Art. 19. — Informe de auditoría. El informe de auditoría evaluará los sistemas utilizados por el certificador de acuerdo con los requerimientos de la Ley N° 25.506, el presente decreto y las normas complementarias.

Art. 20. — Conflicto de intereses. 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.

Art. 21. — Deber de confidencialidad. 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

Art. 22. — Aplicación provisoria de los estándares vigentes. 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 N° 194/98 de la ex Secretaría de la Función Publica.

CAPITULO VII

DE LA REVOCACION DE CERTIFICADOS DIGITALES

Art. 23. — Revocación de certificados. Se deberán revocar los certificados digitales emitidos en los siguientes casos:

a) A solicitud del titular del certificado digital

b) Si se determina que un certificado digital fue emitido en base a una información falsa que en el 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

Art. 24. — Obtención de la licencia. 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.

Art. 25. — Efectos del licenciamiento. 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.

Art. 26. — Duración de la licencia. 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 N° 25.506, en el presente decreto y en las normas complementarias.

Los certificadores licenciados serán sometidos a auditorías anuales.

Art. 27. — Causales de caducidad de la licencia. 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.

Art. 28. — Reconocimiento de certificados extranjeros. De acuerdo a lo establecido en el artículo 6° 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 N° 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 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.

Art. 29. — Políticas de Certificación. 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.

Art. 30. — Seguros. El certificador licenciado debe contar con seguros vigentes acordes con las responsabilidades asumidas, que cumplan con los siguientes requisitos.

a) Ser expedidos por una entidad aseguradora autorizada para operar en la República Argentina.

b) Establecer la obligación de la entidad aseguradora de informar previamente al Ente Administrador de la Infraestructura de Firma Digital la terminación del contrato o las modificaciones que reduzcan el alcance o monto de la cobertura.

Los certificadores licenciados pertenecientes a entidades y jurisdicciones del sector público quedarán exentos de la obligación de constituir el seguro previsto en el presente artículo.

Art. 31. — Responsabilidad de los certificadores licenciados. 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.

Art. 32. — Recursos de los certificadores licenciados. 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 N° 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.

l) Disponer de los recursos financieros adecuados al tipo de actividad de certificación que desarrolla, acorde con los niveles de responsabilidad derivados de la misma.

Art. 33. — Servicios de Terceros. 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.

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.

Art. 34. — Obligaciones del certificador licenciado. Además de lo previsto en el artículo 21 de la Ley N° 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 N° 25.506, 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.

CAPITULO IX

DE LAS AUTORIDADES DE REGISTRO

Art. 35. — Funciones de las Autoridades de Registro. Los Certificadores Licenciados podrán delegar en Autoridades de Registro las funciones de validación de identidad y otros datos de los suscriptores de 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.

Art. 36. — Responsabilidad del certificador licenciado respecto de la Autoridad de Registro. 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 N° 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

Art. 37. — Despapelización del Estado. 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.

Art. 38. — Aplicaciones en organismos de la Administración Pública Nacional. Los organismos de la Administración Pública Nacional que para la tramitación de documentos digitales o la implementación de aplicaciones requieran firma digital, solamente aceptarán certificados digitales

emitidos por Certificadores, Licenciados, o certificados digitales emitidos por certificadores extranjeros reconocidos por acuerdos internacionales o por certificadores licenciados del país.

Las entidades y jurisdicciones pertenecientes al sector público podrán ser certificadores licenciados y emitir certificados para agentes y funcionarios públicos destinados a las aplicaciones de gestión interna de los organismos públicos a que éstos pertenecieran. Cuando razones de orden público o de interés social lo ameriten y cuenten con la autorización de la JEFATURA DE GABINETE DE MINISTROS podrán emitir certificados a particulares.

En aquellas aplicaciones en las que el Estado interactúe con la comunidad, se deberá admitir la recepción de documentos digitales firmados digitalmente utilizando certificados digitales emitidos por certificadores licenciados privados o públicos, indistintamente.

Art. 39. — Autoridades de Registro pertenecientes a la Administración Pública Nacional. 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.

Art. 40. — Agentes y funcionarios. 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 8° de la Ley N° 24.156 y sus modificatorias.

Art. 41. — Utilización por las entidades y jurisdicciones de la Administración Pública Nacional. 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.

Art. 42. — Presentación de documentos electrónicos. 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.

Art. 43. — Normas para la elaboración y redacción de la documentación administrativa. Lo dispuesto en la presente reglamentación constituye una alternativa a lo establecido por el Decreto N° 333/85 y sus modificatorios.

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

Art. 45. — Derogación. Derógase el Decreto N° 427/98.

Art. 46. — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — DUHALDE. — Alfredo N. Atanasof. — Juan J. Alvarez.

ANEXO I

GLOSARIO

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 5°, Ley N° 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 2°, Ley N° 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 6°, Ley N° 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 N° 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 N° 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.