

**LEY N° 25.506 DE FIRMA DIGITAL  
ANTEPROYECTO DE DECRETO REGLAMENTARIO DE LA FIRMA ELECTRONICA Y LA  
FIRMA DIGITAL**

BUENOS AIRES,

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, la Resolución N° 194 del 27 de noviembre de 1998 de la ex Secretaría de la Función Pública, 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.

Que asimismo, constituye una herramienta fundamental 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.

Que si bien la ley citada otorga un plazo al PODER EJECUTIVO NACIONAL de CIENTO OCHENTA (180) días para su reglamentación, corresponde proceder a su reglamentación parcial a fines de poner en funcionamiento la Infraestructura de Firma Digital.

Por ello,

EL PRESIDENTE DE LA NACIÓN ARGENTINA  
DECRETA:

**CAPITULO I  
CONSIDERACIONES GENERALES**

**ARTICULO 1°.- Objeto**

La presente reglamentación regula el reconocimiento del empleo de la firma electrónica y de la firma digital y su eficacia jurídica.

Para aquellos casos en que las leyes no establezcan la forma de los actos jurídicos y contratos, las partes podrán acordar el uso de mecanismos de comprobación de autoría e integridad tales como:

1. firma electrónica,
2. firma digital basada en certificados digitales emitidos por certificadores no licenciados en el marco de la presente reglamentación,
3. firma digital basada en certificados digitales emitidos por certificadores licenciados en el marco de la presente reglamentación,
4. firma digital basada en certificados digitales emitidos por certificadores extranjeros que hayan sido reconocidos en los siguientes casos:
  - a. en virtud de la existencia de acuerdos de reciprocidad entre la República Argentina y el país de origen del certificador extranjero
  - b. por un certificador licenciado en el país en el marco de la presente reglamentación y validado por la Autoridad de Aplicación.

#### **ARTICULO 2°.- Firma electrónica.**

Se considera válido a los fines de la manifestación de voluntad de una persona con respecto a un documento digital o electrónico, la efectuada a través de medios electrónicos que, aunque carezcan de alguno de los recaudos propios de la firma digital, sean

1. aceptados a tal fin por el destinatario, o
2. cuando dicha manifestación no ha sido repudiada por el receptor, o
3. cuando el emisor ha acreditado su titularidad por cualquier medio de prueba idóneo según las normas procesales de su domicilio.

#### **ARTICULO 3°.- Documento digital o electrónico**

A los efectos de esta reglamentación quedan comprendidos en el concepto de documento digital o electrónico aquellos instrumentos privados firmados, generados por medios electrónicos que pueden hacerse constar en cualquier soporte, siempre que su contenido pueda ser representado como texto inteligible, aunque para su lectura se requiera la intervención de medios técnicos.

#### **ARTICULO 4°.- 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.

#### **ARTICULO 5°.- Certificados digitales emitidos por certificadores licenciados**

Los certificados digitales contemplados en el artículo 14 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 APLICACIÓN**

#### **ARTICULO 6°.- Normas técnicas**

Facúltase a la JEFATURA DE GABINETE DE MINISTROS, a determinar las normas técnicas para la generación, comunicación, archivo y conservación del documento digital o electrónico, y los procedimientos previstos en los artículos 11 y 12 de la Ley N° 25.506.

#### **ARTICULO 7°.- Conservación**

El cumplimiento de la exigencia legal de conservar documentos, registros o datos, podrá quedar satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente. Los documentos, registros o datos electrónicos deberán ser almacenados por las partes intervinientes en cada transacción electrónica, o por una tercera parte confiable aceptada por las partes 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 del que procede la copia.

#### **ARTICULO 8°.- Regulación**

Facúltase a la JEFATURA DE GABINETE DE MINISTROS a establecer:

1. Las condiciones mínimas de emisión de certificados digitales
2. Los casos en los cuales deben revocarse los certificados digitales
3. Los datos considerados públicos contenidos en los certificados digitales.
4. Los mecanismos que garantizarán la validez y autoría de las listas de certificados revocados

5. La información que los certificadores licenciados deberán publicar por internet
6. La información que los certificadores licenciados deberán publicar en el Boletín Oficial
7. Los procedimientos mínimos de revocación de los 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 en su actividad.
8. El sistema de auditoría, incluyendo las modalidades de difusión de los informes de auditoría y los requisitos de habilitación para efectuar auditorías
9. Las condiciones para el otorgamiento y revocación de las licencias
10. Las normas y procedimientos para la homologación de los dispositivos de creación y verificación de firmas digitales.
11. El reglamento de funcionamiento de la Comisión Asesora para la Infraestructura de Firma Digital.
12. La gradación de sanciones previstas en la Ley N° 25.506, en virtud de reincidencia y/u oportunidad.
13. Los procedimientos aplicables para el reconocimiento de certificados extranjeros.
14. 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 Nacional.
15. Los contenidos mínimos de las políticas de certificación, de acuerdo con estándares nacionales e internacionales
16. Los niveles de licenciamiento.
17. Las condiciones de prestación de otros servicios en relación con la firma digital y otros temas cubiertos en la ley.

### **CAPITULO III DE LA ORGANIZACIÓN INSTITUCIONAL**

#### **ARTICULO 9°.- 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.

La Comisión Asesora para la Infraestructura de Firma Digital contará como mínimo con 2 (DOS) miembros propuestos por Cámaras, colegios y consejos profesionales, o entes representativos de la actividad. Las entidades mencionadas comunicarán a la JEFATURA DE GABINETE DE MINISTROS los nombres y antecedentes profesionales (curriculum vitae) de las personas propuestas para la integración de la Comisión Asesora para la Infraestructura de Firma Digital.

#### **ARTICULO 10°.- Integración**

Para integrar la Comisión Asesora para la Infraestructura de Firma Digital se deberán reunir los siguientes requisitos:

1. 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.
2. Antecedentes académicos y/o profesionales o laborales en la materia.

Una vez integrada la Comisión Asesora, ésta podrá conformar subcomisiones temáticas con representantes de las entidades anteriormente nominadas. Los informes producidos por las subcomisiones temáticas deberán contar con la aprobación del pleno de la Comisión Asesora para la Infraestructura de Firma Digital en forma previa a su remisión a la JEFATURA DE GABINETE DE MINISTROS.

#### **ARTICULO 11.- Ejercicio de funciones**

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

#### **ARTICULO 12.- Consulta pública**

La Comisión Asesora para la Infraestructura de Firma Digital establecerá los mecanismos que permitan mantener un intercambio de información fluido con las Cámaras, usuarios y asociaciones de consumidores sobre los temas que 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, que incluyan a usuarios de certificados digitales.

#### **ARTICULO 13.- Ente Licenciante de la Infraestructura de Firma Digital**

Créase el Ente Licenciante de la Infraestructura de Firma Digital, en el ámbito de la JEFATURA DE GABINETE DE MINISTROS, como órgano técnico - administrativo encargado de otorgar las licencias a los certificadores licenciados 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.

El Ente Licenciante podrá cobrar un arancel de licenciamiento para cubrir su costo operativo y de las auditorías realizadas por sí o por terceros contratados a tal efecto.

#### **ARTICULO 14.- Autoridades del Ente Licenciante**

El Ente Licenciante de la Infraestructura de Firma Digital será conducido por un Directorio integrado por UN (1) Presidente y CUATRO (4) Vocales, cuyo desempeño tendrá carácter ad-honorem.

La Presidencia del Directorio será ejercida por el titular a cargo de la JEFATURA DE GABINETE DE MINISTROS y los cargos de vocales serán desempeñados por el titular a cargo de la SUBSECRETARIA DE LA GESTION PUBLICA, por ....., por ....., por .....

El gerenciamiento del Ente Licenciante estará a cargo de UN (1) Director, designado por el JEFE DE GABINETE DE MINISTROS.

#### **ARTICULO 15.- Organización del Ente Licenciante**

Dentro de los SESENTA (60) días corridos de la fecha del presente Decreto, el ENTE LICENCIANTE DE LA INFRAESTRUCTURA DE FIRMA DIGITAL presentará la propuesta de su estructura organizativa, del plan de transferencia de la Infraestructura de Firma Digital para el Sector Público Nacional y de su reglamento de funcionamiento.

#### **ARTICULO 16.- Recursos del Ente Licenciante**

Los recursos propios del ENTE LICENCIANTE DE LA INFRAESTRUCTURA DE FIRMA DIGITAL se formarán con:

1. Los importes provenientes de los aranceles que abonen los proveedores de servicios de certificación digital, de certificación digital de fecha y hora, de almacenamiento seguro de documentos electrónicos, las autoridades de registro, otras terceras partes confiables, así como aquellas actividades relacionadas a la firma digital que pudieran surgir en el futuro.
2. Los importes provenientes de los aranceles de homologación de dispositivos de creación y verificación de firmas digitales.
3. Los importes provenientes de los aranceles de certificación de sistemas que utilizan firma digital.
4. Los importes provenientes de los aranceles de certificación de documentos electrónicos firmados digitalmente.
5. Los importes provenientes de los aranceles de administración del sistema de auditoría y las auditorías que el organismo realice por sí o por terceros.

6. Los subsidios, herencias, legados, donaciones o transferencias bajo cualquier título que reciba.
7. El producido de multas.
8. Los importes que se le asignen en el cálculo de recursos de la respectiva Ley de Presupuesto para la Administración Nacional.
9. Los demás fondos, bienes o recursos que puedan serle asignados en virtud de las leyes y reglamentaciones aplicables.

#### **ARTICULO 17.- Financiamiento del Ente Licenciante**

Instrúyese a la JEFATURA DE GABINETE DE MINISTROS para que proceda a prever presupuestariamente los ingresos provenientes de la percepción de los correspondientes aranceles de conformidad con lo dispuesto en el presente decreto, y su imputación específica para atender su costo operativo y el de las auditorías realizadas por sí o por terceros contratados a tal efecto.

Transitoriamente, desde la entrada en vigencia de la presente reglamentación y hasta el 31 de diciembre de 2002, el costo de la estructura será afrontado con el crédito presupuestario correspondiente a la JEFATURA DE GABINETE DE MINISTROS para el año 2002.

### **CAPITULO IV DEL SISTEMA DE AUDITORIA**

#### **ARTICULO 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.

#### **ARTICULO 19.- Informe de auditoría**

El informe de auditoría dictaminará que el certificador actúa o está en capacidad de actuar, de acuerdo con los requerimientos de la Ley N° 25.506, el presente decreto y las normas reglamentarias, modificatorias o de aplicación que se dicten en el futuro.

#### **ARTICULO 20.- Conflicto de interés**

No podrán presentarse a concurso público para la prestación de servicios de auditoría aquellas entidades o personas que participen en la prestación de servicios de certificación.

#### **ARTICULO 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 Certificador Licenciado.

### **CAPITULO V DE LOS ESTANDARES TECNOLOGICOS**

#### **ARTICULO 22.- Aplicación provisoria de los estándares vigentes**

Hasta tanto la JEFATURA DE GABINETE DE MINISTROS apruebe los estándares tecnológicos de la Infraestructura de Firma Digital en consonancia con estándares tecnológicos internacionales, adóptanse los establecidos en la Resolución N° 194/98 de la ex Secretaría de la Función Pública.

## **CAPITULO VI DE LOS CERTIFICADORES LICENCIADOS**

### **ARTICULO 23.- Duración de la licencia**

Las licencias tendrán un plazo de duración de UN (1) año que podrá ser renovado previo dictamen favorable de auditoría.

### **ARTICULO 24.- Obtención de 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 éste determine, ante el Ente Licenciante de la Infraestructura de Firma Digital:

1. Documentación que demuestre:
  - a. En el caso de personas jurídicas, su personería jurídica
  - b. En el caso de registro público de contratos, tal condición
  - c. 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 43 de la presente reglamentación.
2. Cumplimiento de las condiciones establecidas en la ley, esta reglamentación o las que posteriormente fijare la JEFATURA DE GABINETE DE MINISTROS.
3. Políticas de certificación para la cual 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 los requisitos establecidos por la JEFATURA DE GABINETE DE MINISTROS.
4. Constitución de las garantías previstas en el presente Decreto.
5. Dictamen de auditoría favorable.

### **ARTICULO 25.- Efectos de la licencia**

La obtención de una licencia por parte del Certificador Licenciado lo habilita:

1. A presentarse ante terceros acreditando el nivel de licenciamiento obtenido
2. A proveer aquellos servicios de certificación para los cuales obtuvo la licencia.

El otorgamiento de la licencia no implica que el Ente Licenciante 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.

### **ARTICULO 26.- Certificadores Licenciados pertenecientes al sector público**

Las entidades y jurisdicciones pertenecientes al sector público podrán ser certificadores licenciados y emitir certificados pudiendo cobrar un arancel para ello. Cuando razones de interés social lo ameriten el servicio no será arancelado.

La JEFATURA DE GABINETE DE MINISTROS establecerá los procedimientos para la aplicación del presente artículo.

### **ARTICULO 27.- Aclaraciones**

El Ente Licenciante de la Infraestructura de Firma Digital podrá solicitar ampliación o aclaración sobre la documentación presentada por el certificador.

### **ARTICULO 28.- Reconocimiento de certificados extranjeros**

De acuerdo a lo establecido en el artículo 8 de la presente reglamentación, facúltase a la JEFATURA DE GABINETE DE MINISTROS a elaborar y firmar acuerdos de reciprocidad con 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.

En los casos que no medie un acuerdo de reciprocidad, y un certificador licenciado en el país reconozca un certificado emitido por un certificador extranjero garantizando su validez y vigencia, la JEFATURA DE GABINETE DE MINISTROS establecerá los procedimientos de reconocimiento y validación de dicho certificado. En estos casos los certificadores licenciados que soliciten la validación del reconocimiento de los certificados de un certificador extranjero, deberán acreditar adicionalmente la entidad reconocida, los certificados reconocidos, la vigencia y los términos de reconocimiento.

#### **ARTICULO 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:

1. Identificación del certificador licenciado
2. Política de administración de los certificados y detalle de los servicios arancelados.
3. Obligaciones de la entidad y de los suscriptores de los certificados.
4. Tratamiento de la información suministrada por los suscriptores, y resguardo de la confidencialidad en su caso.
5. Garantías que ofrece para el cumplimiento de las obligaciones que se deriven de sus actividades
6. Límites de responsabilidad

#### **ARTICULO 30.- Garantías**

El certificador licenciado debe contar con seguros vigentes que cumplan con los siguientes requisitos:

1. Ser expedidos por una entidad aseguradora autorizada para operar en la República Argentina. En caso de no ser posible, por una entidad aseguradora del exterior que cuente con la autorización previa de la Superintendencia de Seguros de la Nación.
2. Establecer la obligación de la entidad aseguradora a informar previamente al Ente Licenciante 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 la garantía prevista en el presente artículo.

#### **ARTICULO 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 Licenciante de la Infraestructura de Firma Digital.

#### **ARTICULO 32.- Recursos de los certificadores**

Para el desarrollo adecuado de las actividades de certificación, el certificador deberá acreditar que cuenta con un equipo de profesionales, infraestructura física y tecnológica y recursos financieros, como así también procedimientos y sistemas de seguridad que permitan:

1. Generar en un ambiente seguro las firmas digitales propias y todos los servicios para los cuales solicite licencia.
2. Cumplir con lo previsto en sus políticas y procedimientos de certificación
3. Garantizar la confiabilidad de los sistemas de acuerdo con los estándares aprobados por la Autoridad de Aplicación.
4. Expedir certificados que cumplan con:
  - a) Lo previsto en los artículos 13 y 14 de la Ley N° 25.506.
  - b) Los estándares tecnológicos aprobados por la JEFATURA DE GABINETE DE MINISTROS.

5. Garantizar la existencia de sistemas de seguridad física y lógica en sus instalaciones que aseguren el acceso restringido a los equipos que manejan los sistemas de operación de la entidad certificadora.
6. 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.
7. Proteger el acceso y el uso de la clave privada mediante procedimientos que exijan la participación de más de una persona.
8. Registrar las transacciones realizadas, a fin de identificar al autor y el momento de cada una de las operaciones.
9. Utilizar con exclusividad los sistemas que cumplan las funciones de certificación con ese propósito, sin que se les asigne ninguna otra función.
10. 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.
11. Garantizar la continuidad de las operaciones mediante un Plan de Contingencia actualizado y probado.
12. Disponer de los recursos financieros adecuados al tipo de actividad de certificación que desarrolla, acorde con los niveles de responsabilidad derivados de la misma.

### **ARTICULO 33.- Servicios de terceros**

En los casos en que el certificador requiera o utilice los servicios o 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. Los contratos y sus modificaciones deben ser presentados al Ente Licenciante.

La contratación de servicios o infraestructura no exime al certificador de la presentación de los informes de auditoría, los cuales deberán incluir los sistemas y seguridades del prestador contratado.

### **ARTICULO 34.- Deberes del certificador licenciado**

Además de lo previsto en el artículo 21 de la Ley N° 25.506, los certificadores licenciados deberán:

1. 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.
2. Mantener a disposición permanente del público las Políticas de Certificación y el Manual de Procedimientos correspondientes.
3. Cumplir cabalmente con las políticas de certificación acordadas con el titular y con su Manual de Procedimientos.
4. Garantizar la prestación permanente e ininterrumpida de los servicios autorizados, salvo las interrupciones que autorice el Ente Licenciante.
5. Informar al solicitante de un certificado digital, en un lenguaje claro y accesible, en castellano, 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, 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



6. Disponer de una línea telefónica de atención permanente a titulares y terceros, que permita las consultas y la pronta solicitud de revocación de certificados.
7. Garantizar el acceso permanente, eficiente y gratuito de los titulares y terceros al repositorio de certificados revocados.
8. Mantener actualizados los repositorios de certificados emitidos y de certificados revocados.
9. Abstenerse de acceder, tomar conocimiento o almacenar la clave privada del suscriptor.
10. Informar al Ente Licenciante de modo inmediato la ocurrencia de cualquier evento que comprometa la correcta prestación del servicio.
11. Respetar el derecho del titular del certificado digital a no recibir publicidad de ningún tipo por su intermedio, salvo consentimiento expreso de éste.
12. Publicar en el Boletín Oficial durante UN (1) día, el certificado de clave pública correspondiente a la política para la cual obtuvo licenciamiento;
13. Cumplir las normas y recaudos establecidos para la protección de datos personales.
14. 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 a aquel certificado digital que ha dejado de ser seguro por otro que sí cumpla con estos requisitos.
15. El Ente Licenciante 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.

## **CAPITULO VII DEL ENTE LICENCIANTE DE LA INFRAESTRUCTURA DE FIRMA DIGITAL**

### **ARTICULO 35.- Funciones del Ente Licenciante:**

Son funciones del Ente Licenciante:

1. Otorgar las licencias habilitantes para acreditar a los certificadores licenciados en las condiciones que fije el presente decreto y las normas reglamentarias, modificatorias o de aplicación que se dicten en el futuro.
2. Fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los certificadores licenciados
3. Denegar las solicitudes de licencias a los prestadores de servicios de certificación que no cumplan con los requisitos establecidos para su licenciamiento.
4. Revocar las licencias otorgadas a los Certificadores licenciados que dejan de cumplir con los requisitos establecidos para su licenciamiento;
5. Aprobar las políticas de certificación, el manual de procedimientos, el plan de seguridad, de cese de actividades y el plan de contingencia, presentados por los certificadores solicitantes de la licencia o licenciados;
6. Solicitar los informes de auditoría para emitir la licencia o en los casos previstos por la Autoridad de Aplicación.
7. Realizar inspecciones a los certificadores licenciados, por sí o por terceros.
8. Homologar los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la presente reglamentación
9. Disponer la instrucción sumarial y la aplicación de sanciones a los certificadores licenciados por la violación de las disposiciones legales y reglamentarias.
10. 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 si correspondiere;
11. 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 certificado digital de los Certificadores cuyas licencias han sido revocadas.

12. Administrar los recursos generados de acuerdo con lo dispuesto por el artículo 16 de la presente reglamentación, provenientes de las distintas fuentes de financiamiento.
13. 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.

### **ARTICULO 36.- Obligaciones del Ente Licenciante**

El Ente Licenciante tiene idénticas obligaciones que los titulares de certificados y que los Certificadores Licenciados, en su caso, y además debe:

1. Permitir el acceso público permanente a la nómina de certificadores licenciados actualizada, los datos respecto de las mismas, y a los certificados de clave pública de los Certificadores Licenciados, por medio de conexiones de telecomunicaciones públicamente accesibles. Esto también se aplica a la información sobre nombre, direcciones y números telefónicos propios y de los Certificadores licenciados y todo otro dato relevante;
2. Supervisar la ejecución del plan de cese de actividades de los Certificadores licenciados que discontinúan sus funciones;
3. Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas.
4. Supervisar la ejecución de planes de contingencia de los certificadores licenciados.
5. Efectuar las tareas de control del cumplimiento de las recomendaciones formuladas en los dictámenes de auditoría de los Certificadores Licenciados, para determinar, en su caso, si el auditado ha tomado las acciones correctivas correspondientes.

## **CAPITULO VIII DE LAS AUTORIDADES DE REGISTRO**

### **ARTICULO 37.- 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:

1. La recepción de las solicitudes de emisión de certificados
2. La validación de la identidad y autenticación de los datos de los titulares de certificados
3. La validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador Licenciado
4. La remisión de las solicitudes aprobadas al Certificador Licenciado con la que se encuentre operativamente vinculada
5. La recepción y validación de las solicitudes de revocación de certificados, y su direccionamiento al Certificador Licenciado con el que se vinculen.
6. La identificación y autenticación de los solicitantes de revocación de certificados
7. 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
8. Cumplir las normas y recaudos establecidos para la protección de datos personales.
9. 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.

### **ARTICULO 38.- Responsabilidad del certificador licenciado respecto de la Autoridad de Registro**

Una Autoridad de Registro puede constituirse como una única unidad o como 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 que delegue parte de su operatoria en Autoridades de Registro.

## **CAPITULO IX DISPOSICIONES PARA EL ESTADO NACIONAL**

### **ARTICULO 39.- 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 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.

### **ARTICULO 40.- Aplicaciones en organismos públicos**

Los organismos públicos 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.

Para todas aquellas aplicaciones en las cuales se requiera que una entidad, agente o funcionario público utilice un certificado digital para firmar un documento digital, se utilizarán certificados digitales emitidos por certificadores licenciados públicos.

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

### **ARTICULO 41.- Autoridades de Registro pertenecientes a la Administración Nacional**

En las entidades y jurisdicciones pertenecientes a la Administración Nacional, las áreas de recursos humanos cumplirán las funciones de Autoridades de Registro para los agentes y funcionarios de su jurisdicción. En su 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.

### **ARTICULO 42.- 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.

### **ARTICULO 43.- Utilización por las entidades y jurisdicciones de la Administración Nacional**

La JEFATURA DE GABINETE DE MINISTROS establecerá las normas de aplicación de la presente reglamentación en la Administración Nacional, que deberán contemplar:

1. 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.

2. 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.
3. La interoperabilidad entre aplicaciones.
4. La autorización para solicitar el licenciamiento como certificador ante el Ente Licenciante de la Infraestructura de Firma Digital para las entidades y jurisdicciones de la Administración Nacional.
5. La participación del Cuerpo de Administradores Gubernamentales a los fines de difundir el uso de la firma digital y facilitar los procesos de despapelización.

#### **ARTICULO 44.- Presentación de documentos electrónicos**

Los organismos públicos 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.

#### **ARTICULO 45.- 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.

#### **ARTICULO 46.- Glosario**

Apruébase el glosario que obra como Anexo I de la presente reglamentación.

#### **ARTICULO 47.- Derogación**

Derógase el Decreto N° 427/98.

#### **ARTICULO 48.-**

Comuníquese, publíquese, dése a la Dirección del Registro Oficial y archívese.

## **ANEXO I GLOSARIO**

### **Firma Electrónica:**

Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez. (artículo 5º Ley N° 25.506)

### **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 N° 25.506)

### **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 o archivo. Un documento digital también satisface el requerimiento de escritura. (artículo 6º Ley N° 25.506)

### **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)

### **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)

### **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)

### **Manual de Procedimientos:**

Conjunto de prácticas utilizadas por el certificador licenciado en la emisión y administración de los certificados. En inglés Certification Practice Statement (CPS).

### **Plan de Seguridad:**

Conjunto de políticas, prácticas y procedimientos destinados a la protección de los recursos del certificador licenciado.

### **Plan de Cese de Actividades:**

Conjunto de actividades a desarrollar por el certificador licenciado en caso de finalizar la prestación de sus servicios.

**Plan de Contingencias:**

Conjunto de procedimientos a seguir por el certificador licenciado ante situaciones de ocurrencia no prevista que comprometan la continuidad de sus operaciones.

**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).

**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..

**Terceras partes confiables:**

Entidades independientes que otorgan seguridad y confiabilidad al manejo de la información.

**Proveedor de servicios de certificación digital:**

Entidad que provee el servicio de emisión y administración de certificados digitales.

**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.

**Certificación de sistemas que utilizan firma digital:**

Proceso de comprobación efectuado para establecer la adecuación de un sistema o aplicación a requerimientos mínimos establecidos.

**Suscriptor o Titular de certificado digital:**

Persona a cuyo nombre se emite un certificado y que posee una clave privada que se corresponde con la clave pública contenida en el mismo.