

Decreto 182/2019

FIRMA DIGITAL Reglamentación

Ciudad de Buenos Aires, 11/03/2019

VISTO: el Expediente Nº EX-2018-68180684-APN-SECMA#JGM, las Leyes Nº 25.506 y su modificatoria Nº 27.446, los Decretos Nros. 2628 del 19 de diciembre de 2002 y sus modificatorios, 283 del 14 de febrero de 2003, 561 del 6 de abril de 2016, 1063 del 4 de octubre de 2016, 892 del 1º de noviembre de 2017, 801 del 5 de septiembre de 2018 y 802 del 5 de septiembre de 2018, y

CONSIDERANDO:

Que la creación de un clima de confianza en el entorno digital es esencial para el desarrollo económico y social, por lo que resulta conveniente reforzar la confianza en las transacciones electrónicas en nuestro país, para lograr interacciones electrónicas seguras entre los ciudadanos, las empresas y la Administración Pública e incrementar, en consecuencia, la economía digital, la prestación de servicios en línea públicos y privados y el comercio electrónico.

Que la Ley Nº 25.506 y su modificatoria reconoció la eficacia jurídica del documento electrónico, la firma electrónica y la firma digital, complementando las normas de derecho civil y comercial relativas a la firma, al documento, a su condición de original y a la conservación documental, elementos esenciales para otorgar seguridad a las transacciones electrónicas, promoviendo el comercio electrónico seguro y la autenticación fehaciente de las personas que realizan dichas transacciones en entornos virtuales.

Que la citada Ley Nº 25.506 y su modificatoria instituyó la Infraestructura de Firma Digital con alcance federal, abarcando todo el territorio nacional, estableciendo las facultades y obligaciones de sus componentes: la Autoridad de Aplicación, el Ente Licenciante, el Ente Auditante, los certificadores licenciados y los titulares de certificados digitales.

Que, asimismo, la sanción de la Ley Nº 25.506 otorgó 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, en tal sentido, y siendo la materia administrativa de carácter local, la Ley Nº 25.506 y su modificatoria estableció en sus artículos 47 y 48 el uso obligatorio de la firma digital para las transacciones de la Administración Pública Nacional, e invitó a las provincias a adherir en cuanto a su uso.

Que los avances tecnológicos producidos desde el año 2001, año de sanción de la Ley Nº 25.506, así como la experiencia de implementación de la Infraestructura de Firma Digital, hizo necesario actualizar y adecuar su contenido.

Que, por ende, la Ley Nº 27.446, amplió el alcance de la mencionada Ley Nº 25.506, suprimiendo las exclusiones contempladas en el artículo 4º, y asignando a la SINDICATURA GENERAL DE LA NACIÓN el rol de Organismo Auditante de la Infraestructura de Firma Digital, entre otras modificaciones.

Que la Ley Nº 27.446 estableció que los documentos oficiales electrónicos firmados digitalmente, los expedientes electrónicos, las comunicaciones oficiales, las notificaciones electrónicas y el domicilio especial constituido electrónico de la Plataforma de Trámites a Distancia y de los Sistemas de Gestión Documental Electrónica que utiliza el Sector Público Nacional, las provincias, el Gobierno de la CIUDAD AUTÓNOMA DE BUENOS AIRES, municipios, Poderes Judiciales, entes públicos no estatales, Sociedades del Estado, entes tripartitos, entes binacionales, BANCO CENTRAL de la REPÚBLICA ARGENTINA, en procedimientos administrativos y procesos judiciales, tienen para el Sector Público Nacional idéntica eficacia y valor probatorio que sus equivalentes en soporte papel o cualquier otro soporte que se utilice a la fecha de entrada en vigencia de la presente medida, debido a su interoperabilidad que produce su reconocimiento automático en los Sistemas de Gestión Documental Electrónica, por lo que no se requerirá su legalización.

Que, en consecuencia, el Decreto Nº 2628/02 reglamentario de la Ley Nº 25.506, requiere ser actualizado en función de las modificaciones y disposiciones de la Ley Nº 27.446.

Que el Decreto Nº 283/03 autorizó con carácter transitorio y hasta tanto no estuviese implementada la Infraestructura de Firma Digital, a la entonces OFICINA NACIONAL DE TECNOLOGÍAS INFORMÁTICAS dependiente de la ex SUBSECRETARÍA DE LA GESTIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS a proveer certificados digitales en el ámbito de la Administración Pública Nacional.

Que el Decreto Nº 724/06 modificó el Decreto Nº 2628/02 reglamentario de la Ley Nº 25.506.

Que, por otra parte, el Decreto Nº 561/16 le asignó al entonces MINISTERIO DE MODERNIZACIÓN, en su carácter de Autoridad de Aplicación de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA, y a la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS distintas funciones contempladas en el Decreto Nº 2628/02 reglamentario de la Ley Nº 25.506 de Firma Digital.

Que el Decreto Nº 1063/16 modificó el Decreto Nº 2628/02 incluyendo disposiciones respecto de las autoridades de registro, aprobó el uso de la Plataforma de Trámites a Distancia (TAD) del Sistema de Gestión Documental Electrónica – GDE como sede virtual de la Administración Pública Nacional y estableció el uso de la firma digital en el Sistema de Gestión Documental Electrónica - GDE.

Que el Decreto Nº 892/17 creó la Plataforma de Firma Digital Remota, en el ámbito del entonces MINISTERIO DE MODERNIZACIÓN, por lo que corresponde incluir a la firma digital remota como una de las firmas digitales admitidas en el Sistema de Gestión Documental Electrónica – GDE, modificando en consecuencia el artículo 13 del Decreto Nº 1063/16.

Que, por lo expuesto, resulta necesario adecuar la reglamentación de la Ley Nº 25.506 y su modificatoria Nº 27.446, actualizando su contenido a la luz de los avances tecnológicos y de la experiencia de implementación de la Infraestructura de Firma Digital, derogando los Decretos Nros. 2628/02, 283/03 y 724/06, así como los artículos 8º, 9º y 10 del Decreto Nº 561/16.

Que por el Decreto Nº 801/18 se sustituyó el artículo 8º del Título II de la Ley de Ministerios (texto ordenado por Decreto Nº 438/92) y sus modificatorias, indicándose que cada Ministerio podrá proponer al PODER EJECUTIVO NACIONAL la creación, entre otras, de las Secretarías de Gobierno, cuyas funciones serán determinadas por decreto, suprimiéndose el artículo 23 octies.

Que, en este contexto, mediante el Decreto Nº 802/18 se creó, entre otros, el cargo de Secretario de Gobierno de Modernización, el cual actúa como Vicejefe de Gabinete atribuyéndole las competencias del entonces MINISTERIO DE MODERNIZACIÓN.

Que ha tomado intervención la DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS de la SUBSECRETARÍA DE COORDINACIÓN ADMINISTRATIVA de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS.

Que la presente medida se dicta en virtud de las previsiones contenidas en el artículo 99, incisos 1 y 2 de la CONSTITUCIÓN NACIONAL y el artículo 49 de la Ley Nº 25.506 y su modificatoria.

Por ello,

EL PRESIDENTE DE LA NACIÓN ARGENTINA

DECRETA:

ARTÍCULO 1º.- Apruébase la reglamentación de la Ley Nº 25.506 de Firma Digital, que como Anexo IF-2019-13755383-APN-SECMA#JGM, forma parte integrante del presente decreto.

ARTÍCULO 2º.- Interoperabilidad documental. La interoperabilidad documental prevista en el artículo 7º de la Ley Nº 27.446 se instrumentará mediante el módulo Interoperabilidad (IOP) del sistema de Gestión Documental Electrónica – GDE administrado por la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS.

ARTÍCULO 3º.- Poderes. Cuando una norma requiera la formalidad de escritura pública para otorgar poderes generales o particulares, para diligenciar actuaciones, interponer recursos administrativos, realizar trámites, formular peticiones o solicitar inscripciones, dicho requisito se considera satisfecho mediante el apoderamiento realizado por el interesado en la plataforma de Trámites a Distancia (TAD) del sistema de Gestión Documental Electrónica – GDE, salvo disposición legal en contrario.

ARTÍCULO 4º.- Sustitúyese el artículo 13 del Decreto Nº 1063 del 4 de octubre de 2016, por el siguiente:

“ARTÍCULO 13.- Firmas digitales del Sistema de Gestión Documental Electrónica (GDE). El Sistema de Gestión Documental Electrónica (GDE) permite la firma digital de los documentos electrónicos con las siguientes modalidades:

- a) Firma digital remota: se utiliza para para firmar digitalmente todo tipo de documento electrónico incluyendo actos administrativos.
- b) Firma digital con dispositivo criptográfico externo: se utiliza para firmar digitalmente todo tipo de documento electrónico incluyendo actos administrativos.
- c) Firma digital con certificado del sistema: se utiliza para firmar documentos electrónicos, excepto actos administrativos, como dictámenes, informes, comunicaciones oficiales, etc.

Estas firmas digitales gozan de plena validez en virtud de lo dispuesto en el artículo 9º de la Ley Nº 25.506 y su modificatoria, asegurando indubitadamente la autoría e integridad del documento electrónico firmado digitalmente.”

ARTÍCULO 5º.- Derogaciones. Deróganse los Decretos Nros. 2628/02, 283/03 y 724/06 y los artículos 8º, 9º y 10 del Decreto Nº 561/2016.

ARTÍCULO 6º.- Comuníquese, publíquese, dése a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese. MACRI - Marcos Peña

ANEXO

CAPÍTULO I CONSIDERACIONES GENERALES

ARTÍCULO 1º.- Objeto. La presente reglamentación regula el empleo del documento electrónico, de la firma electrónica y de la firma digital y su eficacia jurídica en el marco de la Infraestructura de Firma Digital establecida por la Ley Nº 25.506 y su modificatoria.

ARTÍCULO 2º.- Certificación de firmas. La firma digital de un documento electrónico satisface el requisito de certificación de firma establecido para la firma ológrafa.

ARTÍCULO 3º.- Conservación. La exigencia legal de conservar documentos, registros o datos, conforme a la legislación vigente en la materia, queda 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 prestadores de servicios de confianza aceptados por los intervinientes, durante los plazos establecidos en las normas específicas.

La conservación de documentos, registros o datos en formato electrónico deberá garantizar su integridad, accesibilidad y disponibilidad.

CAPÍTULO II DE LA INFRAESTRUCTURA DE FIRMA DIGITAL

ARTÍCULO 4º.- Componen la Infraestructura de Firma Digital:

1. La Autoridad Certificante Raíz de la REPÚBLICA ARGENTINA.
2. El Ente Licenciantes conformado por la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS y la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA dependiente de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS.
3. Los certificadores licenciados, incluyendo sus autoridades certificadoras y sus autoridades de registro, según los servicios que presten.
4. Las autoridades de sello de tiempo.
5. Los suscriptores de los certificados.
6. Los terceros usuarios.
7. Los certificadores reconocidos por la Autoridad de Aplicación.
8. El Organismo Auditante establecido en el artículo 34 de la Ley Nº 25.506 y su modificatoria.
9. Los prestadores de servicios de confianza.

ARTÍCULO 5º.- Autoridad Certificante Raíz. La Autoridad Certificante Raíz es la Autoridad Certificante administrada por la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS. Constituye la única instalación de su tipo y reviste la mayor jerarquía de la Infraestructura de Firma Digital establecida por la Ley Nº 25.506 y su modificatoria. Emite certificados digitales a las Autoridades Certificadoras de los certificadores licenciados, una vez aprobados los requisitos de licenciamiento.

ARTÍCULO 6º.- Sistema de Auditoría. El Organismo Auditante realizará las siguientes auditorías:

- 1) Auditoría de inicio: como requisito para el otorgamiento de la licencia.
- 2) Auditoría de renovación: como requisito para la renovación de la licencia.
- 3) Auditorías periódicas anuales: a solicitud del Ente Licenciante.
- 4) Auditorías extraordinarias: a solicitud del Ente Licenciante.

Las auditorías podrán recaer en los certificadores que solicitan licencia, en los certificadores licenciados y en las autoridades de registro. El Ente Licenciante determinará la periodicidad de las auditorías.

ARTÍCULO 7º.- Informe de auditoría. El informe de auditoría evaluará los sistemas utilizados por el certificador de acuerdo con los requerimientos de la Ley Nº 25.506 y su modificatoria, el presente Decreto y las normas complementarias. El Organismo Auditante, previa consulta con el Ente Licenciante, determinará los objetivos de control.

ARTÍCULO 8º.- Deber de confidencialidad. Las personas que integran las entidades que componen la Infraestructura de Firma Digital establecida por la Ley Nº 25.506 y su modificatoria, están obligadas a mantener la confidencialidad sobre la información que no sea pública. Dicha obligación subsistirá aun cuando se hayan desvinculado de la entidad o la entidad deje de ser parte de la Infraestructura de Firma Digital establecida por la Ley Nº 25.506 y su modificatoria.

ARTÍCULO 9º.- Certificados Digitales. Los Certificados Digitales contemplados en el artículo 13 de la Ley Nº 25.506 y su modificatoria son aquellos emitidos por un certificador licenciado y 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 Nº 25.506 y su modificatoria. Son personales e interoperables.

ARTÍCULO 10.- 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.

ARTÍCULO 11.- Revocación de certificados. Se deberán revocar los certificados digitales emitidos en los siguientes casos:

- 1) A solicitud del titular del certificado digital.
- 2) 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.
- 3) Si se determina que los procedimientos de emisión y/o verificación han dejado de ser seguros.
- 4) Por condiciones especiales definidas en las Políticas de Certificación.
- 5) Por Resolución Judicial o de la Autoridad de Aplicación debidamente fundada.
- 6) Por fallecimiento del titular.
- 7) Por declaración judicial de ausencia con presunción de fallecimiento del titular.
- 8) Por declaración judicial de incapacidad del titular.
- 9) Si se determina que la información contenida en el certificado ha dejado de ser válida.

ARTÍCULO 12.- 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 determine el Ente Licenciante:

- 1) Documentación que demuestre:
 - 1.1 En el caso de personas jurídicas, su personería.
 - 1.2 En el caso de registro público de contratos, tal condición.
 - 1.3 En el caso de organización pública, la autorización de su máxima autoridad para iniciar el proceso de licenciamiento.
- 2) El cumplimiento de las condiciones establecidas en la Ley, este decreto y las normas complementarias.
- 3) La política única de certificación que respalda la emisión de sus certificados, el Manual de Procedimientos, el Plan de Seguridad, el Plan de Cese de Actividades y el Plan de Contingencia satisfactorios, de acuerdo con las normas reglamentarias.
- 4) Los seguros de caución en caso de corresponder.
- 5) Toda aquella información o requerimiento que demande el Ente Licenciante.

ARTÍCULO 13.- Efectos del licenciamiento. El otorgamiento de la licencia no implica que el Ente Licenciante, el Organismo Auditante o cualquier organismo del Estado garanticen la provisión de los servicios de certificación o los productos provistos por el Certificador Licenciado.

ARTÍCULO 14.- Duración de la licencia. Las licencias tendrán un plazo de duración de CINCO (5) años y podrán ser renovadas, previa auditoría que acredite el cumplimiento de la normativa vigente y de las condiciones técnicas y de procedimientos comprometidas al momento del licenciamiento. 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 y su modificatoria, en el presente Decreto y en las normas complementarias, así como los procedimientos detallados en los documentos de licenciamiento.

Los certificadores licenciados serán sometidos a auditorías periódicas anuales de acuerdo a las pautas que determine el Ente Licenciante.

ARTÍCULO 15.- Causales de caducidad de la licencia. El Ente Licenciante podrá disponer de oficio, y en forma preventiva, la caducidad de la licencia en los siguientes casos:

- 1) Falta de presentación de la declaración jurada anual.
- 2) Falsedad de los datos contenidos en la declaración jurada anual.
- 3) Dictamen desfavorable de auditoría basado en causales graves.
- 4) Informe de la inspección dispuesta por el Ente Licenciante desfavorable basado en causales graves.
- 5) Cuando el certificador licenciado no permita la realización de auditorías o inspecciones dispuestas por el Ente Licenciante.

ARTÍCULO 16.- Reconocimiento de certificados extranjeros. Facúltase a la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de 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, su modificatoria y su reglamentación para los certificados emitidos por certificadores nacionales.

El Ente Licenciante establecerá los procedimientos y demás condiciones para el reconocimiento de certificados emitidos por certificadores de otros países.

ARTÍCULO 17.- Política Única de Certificación. La SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS establecerá la Política Única de Certificación de acuerdo con los estándares nacionales e internacionales vigentes, la que será de cumplimiento obligatorio para todos los certificadores licenciados que integran la Infraestructura de Firma Digital establecida por la Ley Nº 25.506 y su modificatoria.

La Política Única de Certificación deberá contener al menos la siguiente información:

- 1) Identificación del certificador licenciado.
- 2) Política de administración de los certificados y detalles 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.

ARTÍCULO 18.- 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 establecida por la Ley Nº 25.506 y su modificatoria.

ARTÍCULO 19.- 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:

- 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 el Ente Licenciante.
- 4) Expedir certificados que cumplan con:
 - 4.1 Lo previsto en los artículos 13 y 14 de la Ley Nº 25.506 y su modificatoria.
 - 4.2 Los estándares tecnológicos aprobados por el Ente Licenciante.
- 5) Garantizar la existencia de sistemas de seguridad física y lógica que cumplan con las normativas vigentes.
- 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) Registrar las transacciones realizadas, a fin de identificar el autor y el momento de cada una de las operaciones.
- 8) Utilizar con exclusividad los sistemas que cumplan las funciones de certificación con ese propósito, sin que se les asigne ninguna otra función.
- 9) 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.
- 10) Garantizar la continuidad de las operaciones mediante un Plan de Contingencia actualizado y aprobado.
- 11) Disponer de los recursos financieros adecuados al tipo de actividad de certificación que desarrolla, acorde con los niveles de responsabilidad derivados de la misma.

ARTÍCULO 20.- 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.

Serán objeto de auditoría e inspección también aquellos servicios o infraestructura contratados a terceros, incluyendo los sistemas y medidas de seguridad del prestador contratado.

ARTÍCULO 21.- Obligaciones del certificador licenciado. Además de lo previsto en el artículo 21 de la Ley Nº 25.506 y su modificatoria, los certificadores licenciados deberán:

1. Estar domiciliados en la REPÚBLICA ARGENTINA, considerándose que cumplen con este requisito, cuando el establecimiento en el cual desempeñan su actividad en forma permanente, habitual o continuada y sus infraestructuras se encuentren situados en el territorio argentino.
2. 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 Única de Certificación. La verificación de los datos de identidad debe hacerse de manera presencial, mediante los datos biométricos que determine la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA dependiente de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS.
3. Abstenerse de generar, exigir, tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada del suscriptor.
4. Mantener a disposición permanente del público su Política Única de Certificación y el Manual de Procedimientos correspondiente.
5. Cumplir cabalmente con la Política Única de Certificación acordada con el titular y con su Manual de Procedimientos.
6. 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.
7. 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 a 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.
8. Disponer de un servicio de atención a titulares y terceros, que permita evacuar las consultas y la pronta solicitud de revocación de certificados.
9. Garantizar el acceso permanente, eficiente y gratuito de los titulares y terceros al repositorio de certificados revocados.
10. Mantener actualizados los repositorios de certificados revocados por el período establecido por el Ente Licenciante.
11. Informar al Ente Licenciante de modo inmediato la ocurrencia de cualquier evento que comprometa la correcta prestación del servicio.
12. Respetar el derecho del titular del certificado digital a no recibir publicidad de ningún tipo por su intermedio, salvo consentimiento expreso de éste.
13. Publicar en el Boletín Oficial durante UN (1) día, su certificado de clave pública emitido por la Autoridad Certificante Raíz de la REPÚBLICA ARGENTINA, correspondiente a la Política Única de Certificación para la cual obtuvo licenciamiento.
14. Cumplir las normas y recaudos establecidos para la protección de datos personales.
15. En los casos de revocación de certificados contemplados en el apartado 3 del inciso e) del artículo 19 de la Ley Nº 25.506 y su modificatoria, deberá sustituir en forma gratuita aquel certificado digital que ha dejado de ser seguro por otro que sí cumpla con estos requisitos.

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.
16. Enviar periódicamente al Ente Licenciante informes de estado de operaciones con carácter de declaración jurada.
17. Contar con personal idóneo y confiable, con antecedentes profesionales acordes a la función desempeñada.
18. Responder a los pedidos de informes por parte de un tercero respecto de la validez y alcance de un certificado digital emitido por él.

CAPÍTULO III

DE LA AUTORIDAD DE APLICACIÓN Y DEL ENTE LICENCIANTE

ARTÍCULO 22- Funciones. La SECRETARA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS tendrá las siguientes funciones:

- 1) Establecer las condiciones y procedimientos para el otorgamiento y revocación de las licencias.

- 2) Fijar el procedimiento de instrucción sumarial y la gradación de sanciones previstas en la Ley Nº 25.506 y su modificatoria, en virtud de reincidencia y/u oportunidad.
- 3) 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.
- 4) Revocar las licencias otorgadas a los Certificadores Licenciados que dejen de cumplir con los requisitos establecidos para su licenciamiento.
- 5) Disponer la instrucción sumarial, la aplicación de sanciones e inhabilitar en forma temporal o permanente a todo Certificador Licenciado que no respetare o incumpliere los requerimientos y disposiciones de la Ley Nº 25.506 y su modificatoria, el presente Decreto y las normas complementarias.

ARTÍCULO 23.- Regulaciones técnicas. La SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS tendrá las siguientes funciones:

- 1) Establecer los estándares tecnológicos y de seguridad aplicables en consonancia con estándares internacionales.
- 2) Determinar los procedimientos de firma y verificación en consonancia con los estándares tecnológicos definidos conforme el inciso precedente.
- 3) Fijar las condiciones mínimas de emisión de certificados digitales.
- 4) Establecer los casos en los cuales deben revocarse los certificados digitales.
- 5) Determinar los datos considerados públicos contenidos en los certificados digitales.
- 6) Establecer los mecanismos que garantizarán la validez y autoría de las listas de certificados revocados.
- 7) Indicar la información que los certificadores licenciados deberán publicar por internet.
- 8) Indicar la información que los certificadores licenciados deberán publicar en el Boletín Oficial.
- 9) Determinar 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.
- 10) Fijar las modalidades de difusión de los informes de auditoría.
- 11) Establecer las normas y procedimientos para la homologación de los dispositivos de creación y verificación de firmas digitales.
- 12) Estipular los procedimientos aplicables para el reconocimiento de certificados extranjeros.
- 13) Determinar las condiciones de aplicación de la Ley Nº 25.506 y su modificatoria en el Sector Público Nacional.
- 14) Fijar 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.
- 15) Fijar los niveles de licenciamiento.
- 16) Exigir las garantías y seguros necesarios para prestar el servicio previsto.
- 17) Determinar las condiciones de prestación de otros servicios de confianza en relación con la firma digital y otros temas cubiertos en la Ley Nº 25.506 y su modificatoria.
- 18) Establecer la regulación exclusiva y excluyente del uso de la firma digital en sistemas y aplicaciones, así como su homologación.
- 19) Estipular la regulación de la hora oficial en entornos electrónicos.
- 20) 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 y su modificatoria.
- 21) Administrar la Autoridad Certificante Raíz de la REPÚBLICA ARGENTINA.
- 22) Fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los Certificadores Licenciados.
- 23) Denegar las solicitudes de licencia a los prestadores de servicios de certificación que no cumplan con los requisitos establecidos para su licenciamiento.
- 24) Aprobar las políticas de certificación, el manual de procedimiento, el plan de seguridad, el plan de cese de actividades y el plan de contingencia, presentados por los certificadores solicitantes de la licencia o licenciados.
- 25) Solicitar los informes de auditoría en los casos que correspondiere.
- 26) Realizar inspecciones a los Certificadores Licenciados por sí o por terceros.
- 27) Homologar los dispositivos de creación y verificación de firmas digitales así como las aplicaciones o sistemas informáticos que utilicen firmas digitales.
- 28) 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 datos de contacto y certificados digitales de:
 - 28.1 los Certificadores Licenciados,
 - 28.2 los Certificadores cuyas licencias han sido revocadas,
 - 28.3 la Autoridad Certificante Raíz de la REPÚBLICA ARGENTINA,
 - 28.4 el Ente Licenciante.
- 29) Fijar el concepto y los importes de todo tipo de aranceles, multas y montos de los seguros de caución previstos en la Ley Nº 25.506 y su modificatoria y en la presente reglamentación.
- 30) Solicitar la ampliación o aclaración sobre la documentación presentada por el certificador.
- 31) 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.

- 32) Recibir, evaluar y resolver los reclamos de los usuarios de certificados digitales relativos a la prestación del servicio por parte de certificadores licenciados.
- 33) Supervisar la ejecución del plan de cese de actividades de los Certificadores Licenciados que discontinúan sus funciones;
- 34) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas.
- 35) Supervisar la ejecución de planes de contingencia de los Certificadores Licenciados.
- 36) Efectuar las tareas de control del cumplimiento de las recomendaciones formuladas por la SINDICATURA GENERAL DE LA NACIÓN para determinar si se han tomado las acciones correctivas correspondientes.
- 37) Renovar las licencias a los Certificadores Licenciados, en el marco de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA.
- 38) Determinar los recursos tecnológicos que deberán disponer las Autoridades de Registro.

ARTÍCULO 24.- Obligaciones de la Autoridad Certificante Raíz de la REPÚBLICA ARGENTINA. En su calidad de titular de certificado digital, la Autoridad Certificante Raíz de la REPÚBLICA ARGENTINA tiene las mismas obligaciones que los titulares de certificados y que los Certificadores Licenciados. Debe permitir el acceso público permanente a la nómina actualizada de Certificadores Licenciados con los datos correspondientes.

ARTÍCULO 25.- Aranceles y multas. La SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS fijará los montos de:

- 1) Aranceles de licenciamiento, renovación de la licencia, presentación de nuevas versiones de las políticas, certificaciones y otros trámites de certificadores y prestadores de servicios de confianza.
- 2) Aranceles de auditorías, inspecciones y gastos conexos.
- 3) Aranceles que se abonen por la provisión de los siguientes servicios de certificadores del sector público:
 - 3.1. Servicios de certificación digital,
 - 3.2. Servicios de certificación digital de fecha y hora,
 - 3.3. Servicios de almacenamiento seguro de documentos electrónicos,
 - 3.4. Servicios prestados por autoridades de registro,
 - 3.5. Servicios prestados por terceras partes confiables,
 - 3.6. Servicios de certificación de documentos electrónicos firmados digitalmente,
 - 3.7. Otros servicios o actividades relacionados a la firma digital.
- 4) Aranceles de homologación de dispositivos de creación y verificación de firmas digitales.
- 5) Aranceles de homologación de aplicaciones o sistemas informáticos que utilizan firma digital.
- 6) Aranceles de uso de la Plataforma de Firma Digital Remota.
- 7) Aranceles aplicables a prestadores de servicios de confianza.
- 8) Montos mínimos de los seguros de caución.
- 9) Montos de multas.

ARTÍCULO 26.- Aranceles. Las entidades y jurisdicciones que integran el Sector Público están exentas del pago de aranceles de licenciamiento.

CAPÍTULO IV DE LAS AUTORIDADES DE REGISTRO

ARTÍCULO 27.- 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.

La presencia física del solicitante ante el Certificador Licenciado o sus autoridades de registro será condición ineludible para el cumplimiento de los trámites necesarios para la emisión del correspondiente certificado digital.

ARTÍCULO 28.- Funciones de las Autoridades de Registro. Las Autoridades de Registro son responsables 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) El cumplimiento de las normas y recaudos establecidos para la protección de datos personales.
- 9) El cumplimiento de las disposiciones que establezca la Política Única de Certificación y el Manual de Procedimientos del Certificador Licenciado con el que se encuentre vinculada, en la parte que resulte aplicable.

ARTÍCULO 29.- Roles en las Autoridades de Registro. Las Autoridades de Registro deberán contar con personal idóneo para el cumplimiento de los siguientes roles:

- 1) Responsable de la Autoridad de Registro: ejercerá el nexo formal de comunicación entre el Responsable de la Autoridad Certificante y la Autoridad de Registro.
- 2) Oficial de Registro: será el responsable de ejecutar la operatoria principal de la Autoridad de Registro y de cumplir con las obligaciones, funciones y recaudos de seguridad que el Certificador Licenciado le delega.
- 3) Responsable de Soporte Técnico de Firma Digital: brindará soporte técnico y capacitación sobre las disposiciones de la Política Única de Certificación del Certificador Licenciado.

ARTÍCULO 30.- Cooperación entre Autoridades de Registro. Las Autoridades de Registro vinculadas a un mismo Certificador Licenciado deben operar cooperativamente, de acuerdo con las pautas que determine la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS. La SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA podrá autorizar una excepción a solicitud fundada del Certificador Licenciado. Los titulares de certificados podrán solicitar la revocación de su certificado en cualquiera de las Autoridades de Registro del Certificador Licenciado emisor.

ARTÍCULO 31.- Modalidades de las Autoridades de Registro. Las Autoridades de Registro podrán operar en modalidad fija o móvil. Deberán constituir un domicilio y podrán establecer tantas sedes como sea necesario, en la medida que cumplan con los procedimientos y requisitos que fije la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS para su autorización.

ARTÍCULO 32.- Responsabilidad del Certificador Licenciado respecto de la Autoridad de Registro. El Certificador Licenciado es responsable con los alcances establecidos en la Ley Nº 25.506 y su modificatoria, 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.

ARTÍCULO 33.- Autoridades de Registro de Certificadores Licenciados del sector público. Los Certificadores Licenciados pertenecientes al sector público podrán constituir Autoridades de Registro en organizaciones del sector privado o entes públicos no estatales, previa autorización de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS. A los fines del presente artículo, las Autoridades de Registro del sector privado o de entes públicos no estatales, dependientes de certificadores licenciados del sector público, deberán constituir una garantía mediante un seguro de caución a fin de garantizar el cumplimiento de las obligaciones establecidas en la normativa vigente.

ARTÍCULO 34.- Obligados a constituir seguros de caución. Deberán constituir un seguro de caución a fin de garantizar el cumplimiento de sus obligaciones:

1. Los Certificadores Licenciados pertenecientes al sector privado,
2. Las Autoridades de Registro del sector privado que dependan de Certificadores Licenciados del sector público,
3. Las Autoridades de Registro de entes públicos no estatales que dependan de Certificadores Licenciados del sector público.

ARTÍCULO 35.- Seguros de caución. Las pólizas de seguro de caución deberán reunir los siguientes requisitos básicos:

- 1) Estar aprobadas por la SUPERINTENDENCIA DE SEGUROS DE LA NACIÓN, organismo descentralizado en el ámbito el MINISTERIO DE HACIENDA.
- 2) Ser extendidas a favor de:
 - 2.1 La JEFATURA DE GABINETE DE MINISTROS en los casos de Certificadores Licenciados,
 - 2.2 De la jurisdicción o entidad de la cual depende el Certificador Licenciado público en el caso de Autoridades de Registro del sector privado o de entes públicos no estatales.
- 2) Ser sustituidas, a solicitud del Ente Licenciente o del Certificador Licenciado, cuando la aseguradora originaria deje de cumplir los requisitos que se hubieren requerido.
- 3) Mantener la vigencia y actualización del seguro de caución mientras no se extingan las obligaciones cuyo cumplimiento se pretende cubrir.
- 4) La garantía exigida deberá ser acreditada por la Autoridad de Registro del sector privado o de entes públicos no estatales ante el Certificador Licenciado público correspondiente, como requisito previo al otorgamiento de la autorización de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS para operar como tal, en cualquier modalidad.
- 5) Los montos mínimos a integrarse en concepto de garantía o seguro de caución, serán fijados por la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS.

CAPÍTULO V
DE LOS PRESTADORES DE SERVICIOS DE CONFIANZA

ARTÍCULO 36.- Servicios de Confianza. Se entiende por Servicio de Confianza al servicio electrónico prestado por un tercero de confianza relativo a:

1. La conservación de archivos digitales.
2. La custodia de declaraciones de voluntad realizadas en formato electrónico, contratos electrónicos, y toda otra transacción que las partes decidan confiar a un tercero depositario.
3. La notificación fehaciente de documentos electrónicos.
4. El depósito de declaraciones de voluntad realizadas en formato electrónico.
5. La operación de cadenas de bloques para la conservación de documentos electrónicos, gestión de contratos inteligentes y otros servicios digitales.
6. Los servicios de autenticación electrónica.
7. Los servicios de identificación digital.
8. Otras prestaciones que determine el Ente Licenciante.

ARTÍCULO 37.- Prestadores de Servicios de Confianza. Podrán brindar servicios de confianza las personas humanas, jurídicas, consorcios, entes públicos, entes públicos no estatales, de acuerdo a los procedimientos, estándares y condiciones que determine la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS.
