ADMINISTRATIVAS
DECRETOS
MINISTERIO DEL PROGRESO

DECRETO Nº 428-MP-2008
San Luis, 4 de Marzo de 2008

VISTO:

El Expediente Nº 0000-2008-011380, por el cual tramita el proyecto de decreto reglamentario de la Ley Nº V-0591-2007 de firma digital, y;

CONSIDERANDO:

Que el acceso a la información, la despapelización, el gobierno electrónico y el desarrollo del comercio electrónico se han convertido en una política de Estado;

Que, en virtud de ello se ha generado y dado curso a la llamada “Autopista de la Información”;

Que, la implementación de tecnologías de la información y las comunicaciones, conllevan al logro de los objetivos perseguidos;

Que, el camino emprendido se encuadra en una orientación tendiente a la promoción del perfeccionamiento de la organización y el adecuado funcionamiento de la Administración Pública

Provincial así como en el fomento y desarrollo del comercio celebrado con el empleo de las nuevas tecnologías de la información y las comunicaciones;

Que, la despapelización constituye un objetivo insoslayable en tanto que genera un considerable ahorro de recursos de todo tipo y provoca una relación más estrecha entre la Administración Pública y el ciudadano;

Que la Administración Pública Provincial, el Poder Legislativo y el Poder Judicial no pueden permanecer ajenos a los avances tecnológicos y al empleo de los nuevos medios que el desarrollo tecnológico provee, especialmente cuando contribuye a aumentar la productividad, a optimizar el manejo de la información y a reducir los costos de almacenamiento y de traslado de papel;

Que la tecnología necesaria para otorgar seguridad a los documentos digitales, así como el intercambio de información digital, tanto en el ámbito público como en el privado, se encuentra actualmente disponible, habiendo alcanzado un suficiente grado de seguridad y confiabilidad;

Que, la implementación de tecnología de firma digital es, precisamente, el paso siguiente en la consecución del objetivo buscado;

Que la legislación nacional ya ha incorporado tecnología adecuada para estos objetivos y a nivel internacional el avance es sostenido;

Que la Ley Nacional Nº 25.506 ha asimilado el documento digital al documento en papel, reconociendo validez y eficacia jurídica a aquél;

Que deviene imprescindible brindar un marco normativo que favorezca el empleo y difusión de la transferencia electrónica de información y el uso de la firma digital en todos los organismos públicos, en el ámbito de los tres poderes de la Provincia y en el ámbito de los negocios privados;

Que el mecanismo de la firma digital permite probar inequívocamente que una persona firmó un documento digital y que dicho documento no fue alterado desde el momento de su firma, siempre que su implementación se ajuste a los procedimientos preestablecidos;

Que por lo expuesto deviene imprescindible establecer una infraestructura de clave pública con el fin de crear las condiciones de un uso confiable del documento suscripto digitalmente, permitir el proceso de archivo y despapelización y generar las condiciones para el desarrollo del comercio electrónico;

Por ello y en uso de sus atribuciones;

EL GOBERNADOR DE LA PROVINCIA
DECRETA:

CAPITULO I
OBJETO - ÁMBITO DE APLICACIÓN
ARTICULO 1º.- Esta reglamentación tiene por objeto regular el empleo de la firma digital a los efectos de su plena eficacia jurídica tanto en el ámbito público como en el privado.-

ARTICULO 2º.- Las disposiciones del presente Decreto, en virtud del alcance previsto por la Ley de Firma Digital de la Provincia Nº V-0591-2007, serán de aplicación en toda la jurisdicción del Sector Público Provincial. Este comprende a la administración centralizada y descentralizada, los organismos de la Constitución Provincial, los Entes Autárquicos, los bancos y entidades financieras oficiales y todo otro ente en que el Estado Provincial o sus organismos descentralizados tengan participación suficiente para la formación de sus decisiones. Asimismo, su aplicación, alcanza a los actos del Poder Legislativo y del Poder Judicial. El Sector Privado podrá utilizar la infraestructura de firma digital en las relaciones de las personas físicas y/o personas jurídicas entre sí y/o con el Estado Provincial y sus distintos Poderes.-

ARTICULO 3º.- En concordancia con lo dispuesto por la Ley Provincial de Firma Digital, autorizase el empleo de la firma digital en la instrumentación de actos internos y en la generación de archivos, registros, bases y bancos de datos del Sector Público Provincial. Su utilización deberá sujetarse a las condiciones definidas en la Infraestructura de Firma Digital para dicho Sector que se detalla en este mismo Decreto. A sus efectos, en los casos que resulten pertinentes, se requerirá la previa celebración de un convenio cuya implementación corresponderá a la Autoridad de Aplicación.

Asimismo, los organismos podrán utilizar la tecnología de firma digital para la transferencia de información con terceros. A esos efectos deberán respetar los parámetros y la compatibilidad con las normas que rigen su funcionamiento y celebrar un convenio de reciprocidad y garantía, cuyas pautas serán determinadas por la Autoridad de Aplicación.-

ARTICULO 4º.- Mediante documentos digitales firmados digitalmente se dará cumplimiento con la exigencia legal de conservar documentos, registros o datos, conforme a la legislación vigente en la materia. Los plazos de conservación de los documentos, registros o datos electrónicos, almacenados electrónicamente serán los que establezcan las normas pertinentes.-

ARTICULO 5º.- 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. La certificación será emitida por cada organismo de acuerdo a su normativa jurídica interna que deberá responder a los lineamientos determinados por la Autoridad de Aplicación.-

ARTICULO 6º.- Los organismos que componen el Sector Público Provincial podrán arbitrar, en coordinación con la autoridad de aplicación, los medios que resulten necesarios para extender el empleo de la tecnología de la firma digital a aquellos ámbitos que, no previstos en la normativa, resulten de interés para la comunidad.-

CAPITULO II
DEFINICIONES

ARTICULO 7º.- Se entiende por “firma digital” al resultado de una transformación de un documento digital empleando una criptografía asimétrica y un digesto seguro, de forma tal que una persona que posea el documento digital inicial y la clave pública del firmante pueda determinar con certeza lo siguiente: 1) si la transformación se llevó a cabo utilizando la clave privada que corresponde a la clave pública del firmante, lo que impide su repudio; 2) si el documento digital ha sido modificado desde que se efectuó la transformación, de manera tal de garantizar con esta comprobación la integridad del documento. Todo lo cual conlleva a garantizar las características de “no repudio” y la “integridad” del documento que son requisitos de la firma digital.-

ARTICULO 8º.- Por “criptografía asimétrica” se entiende al algoritmo que utiliza por un lado, una clave privada que es utilizada para firmar digitalmente y por otro su correspondiente clave pública para verificar esa firma digital. A efectos de este Decreto, se entiende que la criptografía asimétrica deberá ser técnicamente confiable.-

ARTICULO 9º.- La función de “digesto seguro” es una función matemática que transforma un documento digital en una secuencia de bits de longitud fija, llamada como tal, de forma que se obtiene la misma secuencia de bits de longitud fija cada vez que se calcula esta función respecto del mismo documento digital.-

ARTICULO 10º.- Por “Infraestructura de Firma Digital” se entiende al conjunto integrado por las leyes, decretos y normativa legal complementaria que regulen la firma digital, las obligaciones y deberes de todas aquellas instituciones, organismos y personas que formen parte del circuito de la firma digital tales como la Autoridad de Aplicación, el Ente Licenciante, los Certificadores Licenciados, las Autoridades de Registro, así como también, a los estándares tecnológicos, los procedimientos de seguridad, el hardware, el software, las redes, los bancos de datos y la infraestructura física de alojamiento, que permitan la utilización de la firma digital en condiciones de seguridad e integridad.-

CAPITULO III
DE LA AUTORIDAD DE APLICACIÓN

ARTICULO 11º.-La Universidad de La Punta será la Autoridad de Aplicación de la Ley Nº V-

0591-2007 y del presente decreto reglamentario. Como tal, se encuentra facultada para dictar los manuales de procedimiento del Ente Licenciante, de los Certificadores Licenciados y las normas de auditoría. Queda bajo su competencia la generación de la política de certificación. Asimismo fijará los estándares tecnológicos aplicables a las claves conteniendo el último estado del arte.
Se encuentra facultada para realizar todas las diligencias necesarias para adquirir, administrar y mantener la Infraestructura de Firma Digital de la Provincia lo que involucra el espacio físico que responda a las normas nacionales e internacionales, el hardware y el software de base, los dispositivos criptográficos y de seguridad, el diseño lógico y físico de la infraestructura y todo cuanto fuese necesario para la generación y mantenimiento de aquélla.
Llevará a cabo las auditorías de acuerdo a lo dispuesto en el Capítulo V y resolverá todas aquellas contingencias respecto a la Infraestructura de Firma Digital.-
ARTICULO 12º.- La Autoridad de Aplicación se encuentra facultada para emitir Certificados Digitales así como para utilizar en el ámbito público, aquellos certificados por ella generados.-
ARTICULO 13º.- La Autoridad de Aplicación podrá celebrar convenios con la Subsecretaría de la Gestión Pública de la Jefatura de Gabinete de Ministros de la Nación en su carácter de Autoridad de Aplicación de la ley nacional de firma digital. Esos convenios tendrán como objeto la asistencia y transferencia de tecnología, la constitución de la Universidad de La Punta en tanto Autoridad de Aplicación como una Autoridad de Registro de la Autoridad Certificante de la Oficina Nacional de Tecnología Información o bien como Certificador Licenciado de la Oficina mencionada, incorporar el uso de certificados digitales en la aplicación que sea seleccionada por la Universidad de La Punta y todo aquello que contribuya al mejor desarrollo de los objetivos que este decreto reglamenta.-
ARTICULO 14º.- La Autoridad de Aplicación en representación de la Provincia de San Luis suscribirá acuerdos de reciprocidad con otros Estados Provinciales o Extranjeros a fin de reconocer recíprocamente la validez de los certificados digitales emitidos por las respectivas autoridades certificantes. A tales fines deberá evaluar las condiciones jurídicas y tecnológicas de la infraestructura de firma digital de los Estados signatarios de manera de corroborar que dan cumplimiento con los estándares previstos.-
ARTICULO 15º.- La Universidad de La Punta en su condición de Autoridad de Aplicación deberá presentar el diseño de la estructura operativa que le permita cumplir con el mandato incorporado en el presente Decreto, la que deberá ser acompañada de su correspondiente presupuesto a fin de disponer de la pertinente partida presupuestaria.-

CAPITULO IV
SANCIONES
ARTICULO 16º.- La Autoridad de Aplicación evaluará el accionar de todos los partícipes de la Infraestructura de Firma Digital y recibirá las denuncias que contra cualquiera de ellos se presentasen. En su carácter de órgano de control aplicará sanciones de apercibimiento, suspensión, multa, clausura o cancelación para funcionar como tal a los Certificadores Licenciados o a las Autoridades de Registro. Las multas aplicables por la Autoridad de Aplicación van de un mínimo de una (1) Unidad de Multa y hasta un máximo de un mil (1000) Unidades de Multa. A los efectos del presente Decreto, la Unidad de Multa, será un importe equivalente a un (1) salario mínimo vital y móvil vigente a la fecha de comisión del hecho.-
ARTICULO 17º.- La cuantía de las sanciones se graduará atendiendo a: la naturaleza de los derechos afectados, los beneficios obtenidos, grado de intencionalidad, la reincidencia, los daños y perjuicios causados a las personas interesadas y a terceros, y cualquier otra circunstancia que sea relevante para determinar el grado de antijuricidad y de culpabilidad presentes en la concreta actuación infractora. Se considerará reincidente a quien habiendo sido sancionado por una infracción incurriera en otra de similar naturaleza dentro del término de Tres (3) años, a contar desde la aplicación de la sanción.-
ARTICULO 18º.- El producido de las multas a que se refiere el artículo 16 se aplicará al financiamiento de la Infraestructura de Firma Digital según la imputación que disponga la Autoridad de Aplicación.-
ARTICULO 19º.- El procedimiento se ajustará a las siguientes disposiciones: 1. La Autoridad de Aplicación iniciará actuaciones administrativas en caso de presuntas infracciones a las disposiciones de la Ley Provincial de Firma Digital, a este Decreto Reglamentario y/o a las demás normas reglamentarias, de oficio o por denuncia de quien invocare un interés particular, o asociaciones de consumidores o usuarios. 2. Se procederá a labrar acta en la que se dejará constancia del hecho denunciado o verificado y de la disposición presuntamente infringida. En la misma acta se dispondrá agregar la documentación acompañada y citar al presunto infractor para que, dentro del plazo de Cinco (5) días hábiles, presente su descargo por escrito o por vía telemática con firma digital. En su primera presentación, el presunto infractor deberá constituir domicilio y acreditar personería. 3. La constancia del acta labrada conforme a lo previsto en este artículo, así como las comprobaciones técnicas que se dispusieran, constituirán prueba suficiente de los hechos así comprobados, salvo en

los casos en que resultaren desvirtuados por otras pruebas. 4. Las pruebas se admitirán solamente en caso de existir hechos controvertidos y siempre que no resulten manifiestamente inconducentes. Contra la resolución que deniegue medidas de prueba sólo se concederá recurso de reconsideración. La prueba deberá producirse dentro del término de Diez (10) días hábiles, prorrogables cuando haya causas justificadas, teniéndose por desistidas aquellas no producidas dentro de dicho plazo por causa imputable al infractor. 5. Concluidas las diligencias sumariales, se dictará la resolución definitiva dentro del término de Veinte (20) días hábiles.-
ARTICULO 20º.-A los fines del cumplimiento de lo establecido en la Ley Provincial Nº V-0591-2007 y en el presente Decreto Reglamentario, se faculta expresamente a la Autoridad de Aplicación a fijar en la oportunidad que lo considere pertinente, el monto de los aranceles a abonarse por los diferentes servicios a prestar a fin de efectivizar la operatoria de la firma digital en el ámbito público y privado.-

CAPITULO V
DE LA AUDITORIA
ARTICULO 21º.- La Autoridad de Aplicación en cumplimiento de la manda dispuesta por el art. 11 de este Decreto Reglamentario auditará la actividad del Ente Licenciante y de los Certificadores Licenciados.-
ARTICULO 22º.- A los efectos mencionados en el artículo precedente estarán a su cargo las siguientes funciones: 1. Auditar periódicamente al Ente Licenciante y a los Certificadores Licenciados; 2. Auditar a quienes pretenden constituirse en Certificadores Licenciados con anticipación a la obtención de sus licencias; 3. Acordar con el Ente Licenciante el plan de auditorías para aquellas auditorías que estos realicen a los Certificadores Licenciados; 4. Auditar a los Certificadores Licenciados a solicitud del Ente Licenciante; 5. Efectuar las revisiones de cumplimiento de las recomendaciones formuladas en las auditorías.-
ARTICULO 23º.- Asimismo en su función de auditor tendrá las siguientes obligaciones: 1. Utilizar técnicas de auditoría apropiadas en sus evaluaciones; 2. Evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, la confidencialidad y la disponibilidad de los datos, como así también el cumplimiento con las especificaciones del manual de procedimientos y el plan de seguridad; 3. Verificar que se utilicen sistemas técnicamente confiables; 4. Emitir informes de auditoría con los hallazgos, conclusiones y recomendaciones en cada caso; 5. Realizar revisiones de seguimiento de las auditorías, para determinar si el organismo auditado ha tomado las acciones correctivas que surjan de las recomendaciones; 6. Emitir informes con las conclusiones de las revisiones de seguimiento de auditorías; 7. Intervenir en los simulacros de planes de contingencia; 8. Dar copia de todos los informes de auditoría emitidos al auditado.-

CAPITULO VI
DEL ENTE LICENCIANTE
ARTICULO 24º.- El Ente Licenciante es el órgano administrativo encargado de otorgar las licencias a los Certificadores Licenciados y de supervisar su actividad. Podrá, asimismo, actuar como Certificador Licenciado.-
ARTICULO 25º.- La correspondencia entre una clave pública, elemento del par de claves que permite verificar una firma digital, y el agente titular de la misma será acreditada mediante un certificado de clave pública emitido por el Ente Licenciante de la Provincia o por un Certificador Licenciado. Los requisitos y condiciones para la vigencia y validez de los certificados de clave pública, su emisión, aceptación, revocación, expiración y demás contingencias del procedimiento, así como las condiciones bajo las cuales deben operar las Autoridades de Registro serán los establecidos en este Decreto.-
ARTICULO 26º.- La Universidad de La Punta será Ente Licenciante de la Provincia de San Luis.-.
ARTICULO 27º.- Serán funciones del Ente Licenciante las siguientes: 1. Otorgar las licencias habilitantes para acreditar a los Certificadores Licenciados y emitir los correspondientes "Certificados de Clave Pública", que permiten verificar las firmas digitales de los certificados que éstos emitan; 2. Denegar las solicitudes de licencias a los Certificadores Licenciados que no cumplan con los requisitos establecidos para su autorización; 3. Revocar las licencias otorgadas a los Certificadores Licenciados que dejen de cumplir con los requisitos establecidos para su autorización; 4. Verificar que los Certificadores Licenciados utilicen sistemas técnicamente confiables, entendiéndose por tales a los que cumplan con los estándares tecnológicos que al efecto dicte la Autoridad de Aplicación; 5. Considerará para su aprobación el manual de procedimientos, el plan de seguridad y el de cese de actividades presentados por los Certificadores Licenciados; 6. Generar un plan de auditoría para los Certificadores Licenciados; 7. Disponer la realización de auditorías de oficio; 8. Resolver los conflictos individuales que se susciten entre el suscriptor de un certificado y un Certificador Licenciado emisor del mismo.-
ARTICULO 28º.- En su calidad de suscriptor de certificado y de Certificador Licenciado, el Ente Licenciante, tiene idénticas obligaciones que los Certificadores Licenciados, y además debe: 1.

Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a la Clave Privada de cualquier suscriptor de los certificados que emita; 2. Mantener el control de su propia clave privada e impedir su divulgación; 3. Revocar su propio certificado de clave pública frente al compromiso de su clave privada; 4. Permitir el acceso público permanente a los certificados de clave pública que ha emitido en favor de los Certificadores Licenciados, a la lista de certificados revocados, a la información sobre direcciones y números telefónicos de los Certificadores Licenciados, por medio de conexiones de telecomunicaciones públicamente accesibles; 5. Permitir el ingreso de los auditores, debidamente acreditados, a su local operativo. Poner a disposición de aquellos toda la información necesaria y proveer la asistencia del caso; 6. Publicar su propio certificado de clave pública en el Boletín Oficial y en dos (2) diarios de difusión nacional durante tres (3) días consecutivos a partir del día de su emisión; 7. Revocar los certificados emitidos en favor de los Certificadores Licenciados incursos en causales de revocación de licencia, o que han cesado sus actividades; 8. Revocar los certificados emitidos en favor de los Certificadores Licenciados, cuando las claves públicas que en ellos figuran dejan de ser técnicamente confiables; 9. Supervisar la ejecución del plan de cese de actividades de los Certificadores Licenciados que discontinúan sus funciones; 10. Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas.-

ARTICULO 29º.- El Ente Licenciante podrá arancelar los servicios que preste para cubrir total o parcialmente sus costos. Los recursos propios del Ente Licenciante 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 provincial. h) Los demás fondos, bienes o recursos que puedan serle asignados en virtud de las leyes y reglamentaciones aplicables.-

ARTICULO 30º.- Instrúyese a la Universidad de La Punta para que proceda a incluir en su presupuesto los fondos necesarios para que como Ente Licenciante 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 Provincial los costos de financiamiento del Ente Licenciante serán afrontados con el crédito presupuestario correspondiente a la Universidad de La Punta.-

CAPITULO VII

DEL CERTIFICADOR LICENCIADO

ARTICULO 31º.- El Certificador Licenciado es el ente público, ente privado u organismo de derecho público no estatal que emite Certificados de Clave Pública, entendiendo por tal al que asocia una clave pública con el suscriptor, durante el período de vigencia del certificado, haciendo plena prueba dentro de la Administración del Sector Público Provincial, los Poderes del Estado Provincial y el Sector Privado de la veracidad de su contenido.

El Certificador Licenciado proveerá, opcionalmente, el servicio de sellado digital de fecha y hora.-

ARTICULO 32º.- Será función del Certificador Licenciado emitir Certificados de Clave Pública.

Para emitir estos certificados de clave pública el Certificador Licenciado debe: 1. Recibir del aspirante una solicitud de emisión de certificado de clave pública firmada digitalmente con la correspondiente clave privada; 2. Verificar fehacientemente la información identificatoria del solicitante, la cual deberá estar siempre incluida en el certificado y toda otra información que según lo dispuesto en el manual de procedimientos del Certificador Licenciado, deba ser objeto de verificación, lo cual deberá realizarse de acuerdo a lo dispuesto en el citado manual; 3. Numerar correlativamente los certificados emitidos; 4. Mantener copia de todos los certificados emitidos, consignando su fecha de emisión.

El Certificador Licenciado puede, opcionalmente, incluir en un certificado información no verificada, debiendo indicar claramente tal cualidad.-

ARTICULO 33º.- El Certificador Licenciado será el responsable de revocar los certificados de clave pública emitidos por él mismo en las siguientes circunstancias: a) por solicitud de su suscriptor; b) por solicitud de un tercero que ostente un derecho subjetivo o interés legítimo; c) si llegara a determinar que un certificado fue emitido en base a una información falsa que en el momento de la emisión hubiera sido objeto de verificación; d) si llegara a determinar que las claves públicas

contenidas en los certificados dejan de ser técnicamente confiables; e) si cesa en sus actividades y no transfiere los certificados emitidos por él a otro Certificador Licenciado.
La solicitud de revocación de un certificado debe hacerse en forma personal, por escrito o por medio de un documento digital firmado digitalmente. Si la revocación es solicitada por el suscriptor deberá concretarse de inmediato. Si la revocación es solicitada por un tercero tendrá lugar dentro de los plazos mínimos necesarios para realizar las verificaciones del caso. La revocación debe indicar el momento desde el cual se aplica y no puede ser retroactiva o a futuro. El certificado revocado deberá incluirse inmediatamente en la lista de certificados revocados la cual debe estar firmada por el Certificador Licenciado. Dicha lista debe hacerse pública en forma permanente, por medio de conexiones de telecomunicaciones públicamente accesibles.
El Certificador Licenciado debe emitir una constancia de la revocación para el solicitante.-
ARTICULO 34º.- Serán Obligaciones del Certificador Licenciado, adicionalmente a sus obligaciones emergentes como suscriptor de su certificado emitido por el Ente Licenciante las siguientes: 1. Abstenerse de generar, exigir, o por cualquier otro medio, tomar conocimiento o acceder, bajo ninguna circunstancia, a la clave privada del suscriptor; 2. Mantener el control de su clave privada e impedir su divulgación; 3. Solicitar inmediatamente la revocación de su certificado, cuando tuviera sospechas fundadas de que su clave privada ha sido comprometida; 4. Solicitar al Ente Licenciante la revocación de su certificado cuando la clave pública, en él contenida, deje de ser técnicamente confiable; 5. Informar inmediatamente al Ente Licenciante sobre cualquier cambio en los datos contenidos en su certificado o sobre cualquier hecho significativo que pueda afectar la información contenida en el mismo; 6. Operar utilizando un sistema técnicamente confiable; 7.
Notificar al solicitante sobre las medidas necesarias que deberá obligatoriamente adoptar para crear firmas digitales seguras y para su verificación confiable; y de las obligaciones que aquel asume por el sólo hecho de ser suscriptor de un certificado de clave pública; 8. Recabar únicamente aquellos datos personales del suscriptor del certificado que sean necesarios y de utilidad para la emisión del mismo, quedando el solicitante en libertad de proveer información adicional. Toda información así recabada, pero que no figure en el certificado, será de trato confidencial por parte del Certificador
Licenciado; 9. Poner a disposición del suscriptor de un certificado emitido por éste Certificador
Licenciado, toda la información relativa a la tramitación del certificado; 10. Mantener la documentación respaldatoria de los certificados emitidos durante diez (10) años a partir de su fecha de vencimiento o revocación; 11. Permitir el acceso público permanente a los certificados que ha emitido y a la lista de certificados revocados por medio de conexiones de telecomunicaciones públicamente accesibles; 12. Publicar su dirección y sus números telefónicos; 13. Permitir el ingreso de los auditores acreditados a su local operativo, poner a su disposición toda la información necesaria, y proveer la asistencia del caso; 14. Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas; 15. En caso de Cese de Actividades los certificados emitidos por un Certificador Licenciado se revocarán a partir del día y la hora en que cesa su actividad, a menos que sean transferidos a otro Certificador Licenciado. El Certificador
Licenciado notificará mediante la publicación por tres (3) días consecutivos en el Boletín Oficial y
Judicial, la fecha y hora de cese de sus actividades, que no podrá ser anterior a los noventa (90) días corridos contados desde la fecha de la última publicación. La notificación, también, deberá hacerse individualmente al Ente Licenciante.
Cuando se hayan emitido certificados a entes, entidades o personas ajenas al Sector Público
Provincial, el Certificador Licenciado publicará durante tres (3) días consecutivos, en uno o más diarios de difusión nacional, el cese de sus actividades.
El Certificador Licenciado podrá disponer de medios adicionales de comunicación del cese de sus actividades para notificar a los suscriptores de certificados que son ajenos al Sector Público
Provincial. Si los certificados son transferidos a otro Certificador Licenciado, toda la documentación pertinente también deberá ser transferida a aquel.-
ARTICULO 35º.- La entidad que desee obtener una licencia como Certificador Licenciado deberá: 1. Presentar una solicitud; 2. Contar con un dictamen favorable emitido por el Organismo Auditante; 3. Someter a aprobación del Ente Licenciante el manual de procedimientos, el plan de seguridad y el de cese de actividades, así como el detalle de los componentes técnicos a utilizar; 4. Emplear para el ejercicio de las actividades de certificación personal técnicamente idóneo y que no se encuentre incurso en los supuestos de inhabilitación para desempeñar funciones dentro del Sector Público Provincial; 5. Presentar toda otra información relevante al proceso de otorgamiento de licencias que sea exigida por el Ente Licenciante.-
ARTICULO 36º.- La persona a cuyo nombre se emite un certificado, que resulta ser el titular de una clave privada correspondiente a la clave pública incluida en dicho certificado, es denominado en la infraestructura de firma digital como el suscriptor de un certificado de clave pública.
Son obligaciones de tal suscriptor: 1. Proveer todos los datos requeridos por el Certificador Licenciado, bajo declaración jurada; 2. Mantener el control de su clave privada e impedir su divulgación; 3. Informar inmediatamente al Certificador Licenciado, sobre cualquier circunstancia que pueda haber comprometido su clave privada; 4. Informar inmediatamente al Certificador Licenciado

cuando cambie alguno de los datos contenidos en el certificado que hubieran sido objeto de verificación.-
ARTICULO 37º.- El certificado de clave pública, deberá contener como mínimo, los siguientes datos: 1. Nombre del suscriptor del certificado; 2. Una identificación unívoca del suscriptor del certificado conteniendo tipo y número de documento, CUIT o CUIL, identificación del Organismo o número de licencia en el caso de certificados emitidos para Certificadores Licenciados; 3. Clave pública utilizada por el suscriptor; 4. Nombre del algoritmo que debe utilizarse con la clave pública en él contenida; 5. Número de serie del certificado; 6. Período de vigencia del certificado; 7. Nombre del Certificador Licenciado emisor del certificado; 8. Firma digital del Certificador Licenciado que emite el certificado, identificando los algoritmos utilizados; 9. Todo otro dato relevante para la utilización del certificado, se explicitará en el manual de procedimientos del Certificador Licenciado emisor.-
ARTICULO 38º.- El certificado de clave pública es válido únicamente si cumple con los siguientes recaudos: 1. Haber sido emitido por un Certificador Licenciado o por el Ente Licenciante; 2. No haber sido revocado; 3. No haber expirado.-

CAPITULO VIII
DE LA AUTORIDAD DE REGISTRO
ARTICULO 39º.- Las funciones relativas a la verificación de la identidad y demás datos correspondientes al aspirante a suscriptor del servicio, de registro de las presentaciones y trámites que les sean formuladas, así como la responsabilidad de las comunicaciones con el Ente Licenciante y/o el Certificador Licenciado en el proceso técnico de registración, podrán ser delegadas en una Autoridad de Registro.
La Autoridad de Registro será designada por la Autoridad de Aplicación entre aquellos que tengan idoneidad suficiente y no registren impedimento alguno.
ARTICULO 40º.- La Autoridad de Registro será 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. El cumplimiento de 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.
En el desarrollo de sus funciones la Autoridad de Registro deberá cumplir con la política de certificación dispuesta por la Autoridad de Aplicación así como con toda la normativa regulatoria emanada de aquella.-
ARTICULO 41º.- 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 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 IX
DISPOSICIONES COMPLEMENTARIAS
ARTÍCULO 42º.- Experiencia piloto. La Autoridad de Aplicación deberá instrumentar y efectivizar una prueba piloto de aplicación de firma digital en el ámbito del sector Público Provincial. Al finalizar deberá presentar al Poder Ejecutivo Provincial un informe detallado de la experiencia y su resultado con las propuestas que considere menester.-
ARTÍCULO 43º.- Cronograma de Implementación. Todo aquel organismo de la Administración
Pública Provincial comprendido en este Decreto, en virtud del alcance previsto en el art. 2, deberá presentar ante la Autoridad de Aplicación un cronograma de su proyecto de implementación de firma digital conteniendo el detalle de las aplicaciones previstas y los sujetos intervinientes, en un plazo de ciento ochenta (180) días contados a partir de su requerimiento por parte de la misma-
ARTICULO 44º.- Los organismos del Sector Público Provincial deberán informar a la Autoridad de Aplicación, con la periodicidad que ésta establezca, las aplicaciones que concreten de la tecnología regulada en este Decreto.-
ARTÍCULO 45º.- Proceso de despapelización. En razón del proceso de despapelización, contemplado en la Ley de Firma Digital de la Provincia de San Luis, todos los sujetos alcanzados

por aquella norma y este, su Decreto Reglamentario, deberán llevar adelante todas 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.-

ARTICULO 46º.- Asimismo deberán, dentro del plazo que establezca la Autoridad de Aplicación, poner en marcha los procesos que permitan que, en cada repartición, se opere con firma digital.

Debiendo, en el plazo indicado, desarrollar una detallada descripción de las políticas de certificación, normativas jurídicas internas, sistemas de seguridad y planes de contingencia, que resulten adecuados y eficaces para la implementación mencionada.-

ARTICULO 47º.- Con copia del presente decreto hacer saber a todos los Ministerios y a la Universidad de La Punta.-

ARTICULO 48º.- El presente decreto será refrendado por la Señora Ministro Secretario de Estado del Progreso.-

ARTICULO 49º.- Comunicar, publicar, dar al registro oficial y archivar.-

ALBERTO JOSÉ RODRÍGUEZ SAÁ
Alicia Bañuelos