PROVINCIA DE BUENOS AIRES - SECRETARIA LEGAL Y TÉNICA
CONSEJO FEDERAL DE INVERSIONES

FIRMA DIGITAL: ASPECTOS DE DERECHO PÚBLICO Y PROPUESTAS DE ADECUACION Y COORDINACIÓN

Informe Final

Diciembre de 2015

Asociación Civil Espacios Políticos - ACEP

ÍNDICE

1. INTRODUCCIÓN 3
2. MARCO NORMATIVO NACIONAL 5
2.1. Recopilación de antecedentes normativos en materia de Firma Digital 6
2.1.1. Introducción: el Gobierno Abierto 6
2.1.2. La Firma Digital 7
1.- Procedimientos Técnicos 8
a) Sistema de Criptografía Asimétrica 8
b) Resumen Hash 9
2.- Instrumentos Normativos 9
a) Certificado Digital 10
b) Infraestructura 11
b.1.- AUTORIDAD CERTIFICANTE RAÍZ operada por el Ente Licenciante. 12
b.2.- AUTORIDAD CERTIFICANTE operada por el Certificador Licenciado. 12
b.3.- AUTORIDAD DE REGISTRO 13
2.2. Relevamiento de la normativa vigente relacionada con la materia 14
2.3. Análisis de experiencias en Derecho Comparado 52
3. NORMATIVAS PROVINCIALES 64
3.1. Identificación de la normativa provincial regulatoria de la Firma Digital, con infraestructura propia y sin ella 65
4. **El caso de la Provincia de Buenos Aires** 74
ALTERNATIVA 81
- SECRETARÍA GENERAL DE LA GOBERNACIÓN 82
- SECRETARÍA LEGAL Y TÉCNICA 84
- MINISTERIO DE JEFATURA DE GABINETE DE MINISTROS 86
- CONSEJO PROVINCIAL PARA LA SOCIEDAD DE LA INFORMACIÓN 87

BIBLIOGRAFÍA 91

1. INTRODUCCIÓN

El presente documento constituye el Informe Final del estudio “Firma Digital: aspectos de Derecho Público y propuestas de adecuación y coordinación”, llevado adelante en el marco de la Secretaría Legal y Técnica de la Provincia de Buenos Aires.

La finalidad del proyecto mencionado consiste en favorecer la utilización de la herramienta de Firma Digital en la Administración Pública de la Provincia de Buenos Aires, a partir del análisis pormenorizado del marco regulatorio nacional y provincial, y la necesidad de armonización de las competencias nacionales y provinciales en pos de la previsibilidad, eficiencia, eficacia y certeza del sistema en su conjunto.

En dicho sentido, el objetivo principal del mismo es el de evaluar la necesidad de armonización de las competencias nacionales y provinciales en pos de la previsibilidad, eficiencia, eficacia y certeza del sistema en su conjunto, a partir del análisis de la regulación nacional de la tecnología de Firma Digital, así como también generar instancias superadoras de las dificultades encontradas y óptima coordinación de los diferentes niveles y actores involucrados.

Para ello, el estudio contempla un Plan de Tareas dividido en tres etapas:

1) Marco Normativo Nacional

a. Recopilación de antecedentes normativos en materia de Firma Digital.
b. Relevamiento de la normativa vigente relacionada con la materia.
c. Análisis de experiencias en Derecho Comparado.

2) Normativas Provinciales

a. Identificación de la normativa provincial regulatoria de la Firma Digital, con infraestructura propia y sin ella.
b. Construcción comparativa.

3) El caso de la Provincia de Buenos Aires

a. Compilación de antecedentes normativos
b. Análisis de la normativa vigente

c. Propuesta de adaptaciones y modificaciones al esquema vigente

De acuerdo al cronograma previsto, corresponde en el presente documento dar cuenta del avance registrado en lo que hace a:

1) Marco Normativo Nacional

a. Recopilación de antecedentes normativos en materia de Firma Digital.
b. Relevamiento de la normativa vigente relacionada con la materia.
c. Análisis de experiencias en Derecho Comparado

2) Normativas Provinciales

a. Identificación de la normativa provincial regulatoria de la Firma Digital, con infraestructura propia y sin ella.
b. Construcción de una matriz comparativa.

3) El caso de la Provincia de Buenos Aires

a. Compilación de antecedentes normativos
b. Análisis de la normativa vigente
c. Propuesta de adaptaciones y modificaciones al esquema vigente

En lo sucesivo, por tanto, el documento se divide en tres partes principales, cada una dedicada a exponer los detalles de los avances registrados en cada etapa, individualizando las tareas involucradas.

2. MARCO NORMATIVO NACIONAL

2.1. Recopilación de antecedentes normativos en materia de Firma Digital

2.1.1. Introducción: el Gobierno Abierto

El Gobierno Abierto, como enfoque de funcionamiento de las modernas administraciones, se basa en los principios de participación, colaboración y transparencia.

Esto significa que su fundamento está dado por una nueva forma de intercambio de información entre los gobiernos y la sociedad a la cual sirven, más libre, abierta y colaborativa. Bajo esta óptica, los datos son un insumo de acceso público a los efectos del intercambio, la rendición de cuentas de los mandatarios y la generación de valor a través de servicios derivados de ellos.

Resulta un enfoque más amplio que el de Gobierno Electrónico, al que podríamos considerar incluido en él.

Es decir, para la vinculación eficaz, inclusiva y eficiente entre los órganos de gobierno y los ciudadanos y organizaciones sociales, en pos de la deseada transparencia, colaboración y participación que oriente dicha relación, se torna imprescindible el diseño de mecanismos y herramientas innovadoras que incorporen las nuevas tecnologías de la información y el conocimiento (TICs) como medio para eliminar las barreras físicas al intercambio.

En definitiva, el objetivo es incrementar el caudal de información sobre las acciones de gobierno y su impacto real, fomentar la participación ciudadana e implementar mecanismos de colaboración con la finalidad de nutrir dichas acciones con la perspectiva de los actores que resultarán sus beneficiarios, o bien de asociaciones que relevantes en la materia por su compromiso y conocimiento técnico. Todo ello, con la finalidad última de optimizar las capacidades gubernamentales y políticas públicas en un marco de legitimidad social e integridad profesional.

Claro está que tal interrelación resulta muy dificultosa sin la incorporación de herramientas innovadoras que permitan un intercambio veloz y confiable en el ámbito de la sociedad de la información, acercando a los actores de gobierno con sus ciudadanos, allí donde estos últimos se encuentren, eliminando las distancias en un marco de inclusión y universalización de dichas prácticas.

De allí que resulte necesario adentrarnos en el estudio de tales herramientas, desentrañando su funcionamiento técnico, sus aspectos regulatorios y las dificultades

que se detectan para su progresiva utilización por parte de las áreas que conforman los niveles gubernamentales en su interrelación y prestación de servicios a los ciudadanos.

Como puede apreciarse, nos concentraremos principalmente en los aspectos de derecho público relacionados con la temática, para lo cual debemos previamente analizar la actual regulación, desentrañar cuáles son las normas de fondo que rigen las relaciones entre particulares, y en qué medida la herramienta se utiliza en procedimientos de carácter administrativo, los cuales son regidos por los derechos locales propios de cada estado subnacional autónomo.

Así, nos enfrentaremos a los conflictos interpretativos que pueden suscitarse ante el ejercicio de competencias provinciales en materia de transacciones digitales Estado-ciudadano, las cuales pueden -o no- ampararse en la legislación nacional; así como a las consecuencias que acarrea el apego o apartamiento de dicho régimen, en lo que hace a las presunciones de integridad y autoría que acompañan a los documentos digitales firmados.

2.1.2. La Firma Digital

Tal como se expuso con anterioridad, en las últimas décadas las TICs han ganado protagonismo a nivel mundial, brindando certeza y fluidez a las relaciones entre interlocutores sin ningún tipo de vinculación previa a través de herramientas que incrementan la velocidad de circulación de la información, simplifican operaciones complejas, y ofrecen un mejor nivel de servicios, reduciendo costos, aumentando productividad y competitividad.

Esto generó la necesidad de contar con un mecanismo que permita garantizar tanto la **integridad de un documento como la identidad de su autor**, dotando a las operaciones de seguridad y confianza.

Para dar solución a dicha problemática se diseñó el sistema de Firma Digital, que utiliza un mecanismo de claves asimétricas tendientes a otorgar a las transacciones electrónicas la responsabilidad personal que todo acto jurídico necesita.

Este sistema tiene por objetivo brindar seguridad en el intercambio de información en formato digital, otorgando garantía de autoría e integridad a los documentos, equiparándola con la rúbrica manuscrita.

De esta forma se posibilita el progresivo reemplazo de la documentación en papel, contribuyendo al proceso de "digitalización" de los procedimientos en pos de una mayor eficiencia en los servicios, economía de insumos y protección del medio ambiente.

Asimismo, en lo que hace a la actividad estatal, se dirige a dotar de transparencia y accesibilidad a los documentos públicos para su control por parte de la ciudadanía, y contribuir a optimizar la gestión posibilitando la realización de trámites por Internet en forma segura. Constituye así un pilar fundamental para el desarrollo del gobierno electrónico.

El concepto de Firma Digital comprende un conjunto de características técnicas y normativas. La herramienta se define en virtud de procedimientos técnicos que permiten su operatoria en el marco de instrumentos normativos que la validan, respaldando legalmente su aptitud para producir efectos jurídicos. Este procedimiento técnico permite asociar la identidad de una persona a un documento, comprobando como correlato de esta coincidencia su integridad.

De esta manera, y a través de un conjunto de presunciones legales, se produce el principal efecto jurídico de la Firma digital que es la instrumentación de la manifestación de voluntad respecto al contenido del documento digital.

1.- Procedimientos Técnicos

a) Sistema de Criptografía Asimétrica

El sistema que regula para la Firma Digital la Ley N° 25.506, conforme las referencias de los artículos 2, 7 y 9, es el de Criptografía asimétrica o Criptografía de Clave Pública.

Este sistema prevé la existencia de dos claves: una con la que se cifra el mensaje y otra que lo descifra. Ambas claves son asignadas a una misma persona, siendo una de ellas de conocimiento exclusivo del emisor (clave privada, utilizada para firmar) y otra accesible para terceros (clave pública, utilizada para constatar la firma digital). Ambas claves están vinculadas matemáticamente a través de una fórmula imposible de reproducir, y guardan entre sí una relación tal, que algo que sea encriptado por la clave privada de determinado emisor únicamente podrá ser desencriptado por su clave pública.

Para ello, todo el sistema deberá basarse en una infraestructura de manejo de claves que permita identificar de manera certera a cada usuario, con su clave pública, a través de terceras partes confiables.

El mecanismo descripto garantiza la integridad y autoría del documento firmado digitalmente, mas no su confidencialidad. Para que esto último sea posible, debería encriptarse el documento con la clave pública del receptor, para que cuando éste lo reciba, pueda leerlo únicamente si aplica su clave privada.

b) Resumen Hash

Al contenido del documento que se pretende firmar digitalmente con el sistema de criptografía asimétrica, el emisor le aplicará cierto algoritmo matemático, denominado *función hash,* y al resultado obtenido le aplicará su *clave privada*.

El *hash* es una función matemática o algoritmo criptográfico que transforma un documento digital en una secuencia de bits; es decir que transforma el documento digital en un extracto numérico llamado *resumen hash o digesto*.

A partir de un mismo documento, siempre se generará idéntico resumen *hash*, y correlativamente es imposible que existan dos resúmenes iguales de documentos distintos.

El destinatario, al recibirlo, utiliza la *clave pública* del emisor para descifrar el mensaje, consignando luego la misma función hash sobre el documento digital, obteniendo otro resumen *hash* que comparará con el adjuntado por el emisor al mensaje. Si los resúmenes coinciden, es porque el contenido del documento enviado no ha sido modificado.

Lógicamente, estas operaciones de cálculo y verificación posterior no son realizadas por el usuario, sino que las realiza automáticamente un *software* específico para la aplicación.

2.- Instrumentos Normativos

Como correlato de la operatoria técnica descripta, debe existir una estructura legal que brinde las presunciones que validen la factibilidad de producir efectos jurídicos por medio de actos instrumentados en formato digital. De conformidad con el

ordenamiento vigente, para que ciertamente podamos hablar de Firma Digital, será necesario contar con los siguientes elementos:

a) Certificado Digital

El receptor de un documento recibirá la clave pública del emisor, a través del *Certificado Digital* adjunto al mensaje, siendo esto lo que le otorga la validez legal a la Firma.

El Certificado Digital es un documento digital otorgado por la Autoridad Certificante que contiene los datos de identidad del firmante junto a su clave pública, el cual sirve para garantizar la veracidad de los datos contenidos, referentes a una persona física o jurídica.

Para que dicho certificado tenga la capacidad de atribuir efectos jurídicos a los documentos que acompañe, es necesario que sea expedido por una autoridad certificante habilitada por un ente certificante, y que el formato sea el utilizado internacionalmente (estándar internacional[1]).

Como hemos explicado *ut supra* el Certificado se basa en el método de criptografía asimétrica, en el cual las claves conforman un par único y se generan en el mismo momento por el usuario, ejecutando un programa provisto por la Autoridad de Certificación desde su sitio web.

Para aprobar un Certificado Digital, la Autoridad de Certificación firma con su Clave Privada la Clave Pública del Certificado Digital, constituyéndose así en la tercera entidad de confianza que asegura que la clave se corresponda con los datos del titular.

El titular del certificado debe mantener bajo su exclusivo poder la clave privada, ya que si ésta es sustraída, quien lo haga podría suplantar su identidad en la red.[2]

El certificado digital contendrá los siguientes datos:

a) Identificación de su titular (Nombre y DNI) y del certificador licenciado que lo emitió;

b) período de vigencia;

c) Clave Pública del titular, identificando el algoritmo utilizado;

---

[1]El artículo 18 de la Decisión Administrativa 927/14 (JGM) (B.O. 16/05/2014) prescribe que "Establécense como estándares operativos de la Infraestructura de Firma Digital de la REPUBLICA ARGENTINA, los contenidos en los Anexos II y III de la presente decisión administrativa, y como estándar tecnológico, el contenido en el Anexo IV, adoptándose en todos los casos estándares tecnológicos internacionales."

[2]En este caso, el titular deberá revocar el certificado lo antes posible. El proceso de revocación dependerá de la AC que haya emitido el certificado.

d) Número de serie del Certificado;

e) Dirección de Internet de la lista de Certificados revocados que mantiene el certificador que lo emitió[3];

f) identificación de la política de certificación bajo la cual fue emitido;

g) Firma Digital del certificador de la clave pública que emite el certificado.

Los Certificados pueden ser de distintos tipos, dependiendo de los requerimientos del usuario. Los denominados “de identificación” simplemente identifican o conectan una clave pública; aquellos llamados “de autorización”, validan un determinado hecho o que éste efectivamente ha ocurrido, por ejemplo determinar día y hora en que el documento fue digitalmente firmado.

b) Infraestructura

La infraestructura de firma digital (PKI[4]), es la que brinda validez legal y seguridad jurídica a la aplicación mediante el diseño del sistema de operaciones, la emisión de los certificados digitales, el establecimiento y actualización de estándares tecnológicos internacionales, la supervisión de la emisión de los certificados y hasta la aplicación de sanciones.

Al emitir un Certificado Digital, la Autoridad Certificante lo firma digitalmente con su propia clave privada. A su vez, dicha autoridad ha sido previamente autenticada mediante otro Certificado Digital emitido por otro organismo de mayor nivel, y así sucesivamente hasta una Entidad Certificante Raíz.

El mecanismo descripto da lugar a un encadenamiento de entidades certificantes que se autentican, denominado comúnmente como “cadena de confianza”.

Para fomentar la credibilidad, publicidad y transparencia en la firma del Certificador, algunos Estados prevén la publicación en un Boletín Oficial de la clave pública del prestador de Servicios de certificación, o de ciertos datos sobre el Certificado Raíz. Esto es lo que se conoce convencionalmente como Infraestructura de Clave Pública.

Las Autoridades Certificantes podrán actuar como tales sólo con la previa aprobación de una Autoridad Certificante estatal (Ente Licenciante) a través de un sistema de jerarquías.

[3]El listado de Certificados Revocados, sirve para que el destinatario pueda corroborar la vigencia del mismo.

[4]“Public Key Infrastructure”.

Recapitulando, la infraestructura descripta está constituida por una Autoridad Certificante raíz operada por el Ente Licenciante, por Autoridades Certificantes (AC) operadas por Certificadores Licenciados y por Autoridades de Registro (AR), que desarrollan funciones delegadas por los Certificadores Licenciados.

Con la PKI, se pretende asegurar: la *confidencialidad* de la información que acredita la identidad del titular del Certificado Digital, generando el par de claves (pública y privada) con absoluta reserva de su clave privada; la *integridad* de los datos que contiene el documento firmado, por medio de la generación del resumen hash o digesto, que permite chequear que el contenido no ha sido modificado; y la *identidad* del firmante.

En cuanto al sistema de reconocimiento de Certificados Extranjeros, se realiza mediante un método de Certificación Cruzada, en los cuales es necesario que Entidades Certificadoras sustancialmente equivalentes reconozcan los servicios prestados por la correlativa extranjera. Ello deberá ser reconocido y organizado por la legislación de cada país.

b.1.- AUTORIDAD CERTIFICANTE RAÍZ operada por el Ente Licenciante.

El Ente Licenciante es un organismo administrativo encargado de otorgar las licencias a los Certificadores y supervisar su actividad. Su función consiste así en autorizar a los Certificadores a emitir los Certificados Digitales y a prestar otros servicios relacionados con la Firma Digital.

Si lo representásemos gráficamente, se encontraría en el vértice de una pirámide, debajo de la cual actuarán los Certificadores Licenciados –a través de sus respectivas AC– y las Autoridades de Registro, en ejercicio de funciones delegadas por los anteriores, todo ello en el marco de la ya denominada “cadena de confianza”.

b.2.- AUTORIDAD CERTIFICANTE operada por el Certificador Licenciado.

La Autoridad Certificante interviene en la comunicación de documentos digitales como “tercera parte confiable”, emitiendo y revocando los Certificados Digitales, así como verificando su correspondencia con la identidad de su titular.

Tiene la misión dar fe de la utilización de la clave privada del remitente ante el destinatario del documento digital y responde de manera directa por su praxis.

Para ello deberá disponer de políticas de seguridad predeterminadas que infundan confianza –reguladas por la autoridad de aplicación del sistema-[5], utilizar tecnología acorde a su gestión y proporcionar altos niveles de calidad en atención y disponibilidad.

Puede tratarse de empresas privadas u organismos públicos, siempre que sean autorizados por el Ente Licenciante o Autoridad Certificante Raíz para emitir Certificados Digitales y prestar los servicios relacionados a ello.

Como ya fuera dicho, las Autoridades Certificantes disponen a su vez de sus propios Certificados Digitales emitidos por la Autoridad Certificante Raíz, mediante los cuales canalizan su propia actividad.

b.3.- AUTORIDAD DE REGISTRO

La Autoridad de Registro participa del proceso de verificación de datos de los particulares que solicitan la emisión de Certificados Digitales a la Autoridad Certificante.

Es decir que se encarga de comprobar la veracidad de los datos que aportan los solicitantes de Certificados Digitales, actuando así como una *"ventanilla de atención al público"*, para luego remitir la solicitud a la Autoridad Certificante de la cual dependen para la emisión del correspondiente certificado.

Tal Autoridad puede actuar dentro de la Autoridad Certificante –es decir, como una dependencia parte de ella-, o bien fuera de ella, ejerciendo funciones delegadas por los entes licenciantes o licenciatarios certificantes.

[5] La Autoridad de Aplicación del sistema es aquél organismo estatal dotado de competencia para reglamentar los detales técnicos vinculados a la infraestructura de Firma Digital. No debe confundírsela con las Autoridades Certificantes, quienes son parte de la cadena de confianza del sistema, es decir un actor más dentro de dicha infraestructura.

2.2. Relevamiento de la normativa vigente relacionada con la materia

A) Antecedentes

El primer antecedente legislativo en el país relativo a la materia que estamos tratando, data del año 1995, con la sanción de la Ley N° 24.624, que en su art. 30 autoriza el archivo y conservación de documentación en soporte electrónico u óptico indeleble dentro de la Administración Pública.

Durante el año 1997, se comenzaron a gestar las bases para la operatoria de la Firma Digital. Como primera medida, se dictó el Decreto N° 554/97, mediante el cual se declaró de interés Nacional el acceso de los ciudadanos a Internet. Ese mismo año, la Secretaría de la Función Pública, autorizó la incorporación de la tecnología de la Firma Digital en los procesos de información del sector público. También se concretaron varios proyectos referentes a la implementación de la Firma Digital y Documentos Digitales, a saber: el Ministerio de Trabajo y Seguridad Social dictó la Resolución N° 555/97[6], sobre Normas y Procedimientos para la Incorporación de Documentos con Firma Digital; la Superintendencia de Administradoras de Fondos de Jubilación y Pensiones dictó la Resolución N° 293/97, sobre la Incorporación del Correo Electrónico con Firma Digital; al mismo tiempo, el Ministerio de Justicia de la Nación dio inicio a la elaboración de proyectos concernientes a Instrumento Digital y Firma Digital.

En 1998, la Secretaría de la Función Pública elaboró un proyecto de decreto regulando la Infraestructura de Firma Digital para el Sector Público Nacional, que fue plasmado mediante el dictado del Decreto N° 427/98[7], de Firmas Digitales para la Administración Pública Nacional. Este antecedente es el puntapié inicial para toda la estructura que funciona actualmente.

[6] Resolución MTSS N° 555/97: define el documento digital, la firma digital, el certificador de clave pública, el certificado, la clave privada, la clave pública y dispone que los documentos digitales se considerarán válidos y eficaces, surtiendo todos los efectos legales y probatorios cuando estén firmados digitalmente.
[7] (BO 16/04/1998)

B) Marco Normativo Nacional

El marco normativo en la República Argentina en materia de Firma Digital está constituido por la Ley Nº 25.506[8], el Decreto Nº 2628/02 y un conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos.

A continuación se detallarán las mismas, expuestas en orden cronológico:

1.- LEY N° 25.506 • Ley de Firma Digital (B.O. 14/12/2001)

Sus lineamientos principales los examinaremos en detalle en el acápite correspondiente.

2.- Decreto Nº 1023/2001

En su Objeto (artículo 1º), se detalla que el Régimen de Contrataciones de la Administración Nacional, tendrá por objeto que las obras, bienes y servicios sean obtenidos con la mejor tecnología proporcionada a las necesidades, en el momento oportuno y al menor costo posible, como así también la venta de bienes al mejor postor, coadyuvando al desempeño eficiente de la Administración y al logro de los resultados requeridos por la sociedad.

En su artículo 21º permite la realización de las contrataciones comprendidas en el régimen, en formato digital firmado digitalmente.

3.- DECRETO N° 2628/2002 • Reglamentario de la Ley N° 25.506 (B.O. 20/12/2002)

Reglamenta la Ley N° 25.506 de firma digital y deroga el Decreto N° 427/98.

Detalla cuestiones vinculadas al establecimiento de la Autoridad de Aplicación, la creación de la Comisión Asesora para la Infraestructura de Firma Digital y el Ente Administrador de Firma Digital, el Sistema de Auditoría, Estándares Tecnológicos, Revocación de Certificados Digitales, Certificadores Licenciados, Autoridades de Registro y Disposiciones para la Administración Pública Nacional.

4.- DECRETO N° 283/2003 (B.O. 17/02/2003)

Autoriza a la Oficina Nacional de Tecnologías de la Información (ONTI), con carácter transitorio, a emitir Certificados Digitales para aquellos sectores de la Administración Pública que requieran firma digital.

[8] B.O. 14/12/2001

5.- Decreto Nº 152/2003 (B.O. 06/06/2003)

Otorga competencia a la Subsecretaría de la Gestión Pública para licenciar a los Certificadores, supervisar su actividad y dictar normas tendientes a asegurar el régimen de libre competencia en el mercado de los prestadores y la protección de los usuarios de firma digital.

6.- Decreto Nº 624/2003 (B.O. 22/08/2003)

Aprueba la estructura organizativa de primer nivel operativo de la Jefatura de Gabinete de Ministros.

Estable en su artículo 8°, que la Comisión Asesora para la Infraestructura de Firma Digital, creada por el artículo 28° de la Ley N° 25.506, actuará en la órbita de la Subsecretaría de la Gestión Pública de la Jefatura del Gabinete de Ministros.

También define las competencias de la Subsecretaría mencionada, y entre ellas establece, en el décimo punto: "*Actuar como autoridad de aplicación del Régimen Normativo que establece la Infraestructura de Firma Digital para el Sector Público Nacional, como así también en las funciones de organismo licenciante en la materia, supervisando su accionar*".

Finalmente, determina las competencias de ONTI, pudiendo mencionarse entre otras Acciones, las siguientes:

1. Entender en la elaboración del marco regulatorio del régimen relativo a la validez legal del documento y firma digital, así como intervenir en aquellos aspectos vinculados con la incorporación de estos últimos a los circuitos de información del sector público y con su archivo en medios alternativos al papel.

2. Ejercer las funciones de Autoridad Certificante de Firma Digital para el Sector Público Nacional.

7.- DECRETO N° 1028/2003 (B.O 10/11/2003)

Modifica el Decreto Reglamentario de la Ley 25.506, disolviendo el Ente Administrador de la Firma Digital - art. 11 -, y transfiere sus bienes patrimoniales y créditos presupuestarios a la ONTI, dependiente de la Jefatura de Gabinete de Ministros de la Nación.

Asimismo se le asignó al organismo la responsabilidad de intervenir en la definición de las normas y procedimientos reglamentarios del régimen Firma Digital, y la facultad de ejercer las funciones de Autoridad Certificante de la Firma Digital para el Sector Público Nacional.-

8.- RESOLUCIÓN N° 435/2004 • JEFATURA DE GABINETE DE MINISTROS

Aprueba el Reglamento de Funcionamiento de la Comisión Asesora para la Infraestructura de Firma Digital.

9.- DECRETO N° 160/2004 (B.O. 5/02/2004)

Designa a los integrantes de la Comisión Asesora para la Infraestructura de Firma Digital.

10.- DECRETO N° 409/2005 (B.O. 02/05/2005)

Establece que uno de los objetivos de la Subsecretaría de la Gestión Pública es actuar como autoridad de aplicación del régimen normativo de Firma Digital, así como desempeñar las funciones de entidad licenciante de certificadores.

11.- Decreto N° 378/2005 • Plan Nacional de Gobierno Electrónico (B.O 28/04/2005)

Dio impulso a la Firma Digital propiciando la digitalización de la documentación pública, en orden a un intercambio más fluido entre los ciudadanos y el Estado, y una mayor interoperabilidad en el ámbito interno de la Administración Pública.

12.- DECRETO N° 724/2006 (B.O. 13/06/2006)

Modifica el Decreto Reglamentario 2628/02, incorporando la gratuidad de los certificados emitidos por certificadores licenciados públicos, con el fin de evitar que se encarezcan innecesariamente los trámites de los particulares ante la Administración Pública. Incorpora la noción del tercero usuario.

13.- DECISIÓN ADMINISTRATIVA N° 6/2007 • JEFATURA DE GABINETE DE MINISTROS (B.O. 12/02/2007)

Establece el marco reglamentario aplicable al otorgamiento y revocación de las licencias, estableciendo los requisitos y procedimientos al respecto.

En tal sentido, aprueba los "Requisitos para el licenciamiento de certificadores" , los "Requisitos Mínimos para Políticas de Certificación", el "Perfil Mínimo de Certificados

y Listas de Certificados Revocados" , los "Contenidos Mínimos del Resumen de la Política de Certificación y del Manual de Procedimientos de Certificación para Suscriptores", los "Contenidos Mínimos de los Acuerdos con Suscriptores", los "Contenidos Mínimos de los Términos y Condiciones con Terceros Usuarios", los "Montos de aranceles y garantías", y los "Contenidos Mínimos de la Política de Privacidad".

Establece la estructura de la Firma Digital en Argentina, determinando sus cuatro componentes: a) el ente licenciante y su Autoridad Certificante Raíz, b) los certificadores licenciados, incluyendo sus Autoridades Certificantes y sus Autoridades de Registro, c) los suscriptores de los certificados digitales de esas Autoridades Certificantes y d) los terceros usuarios de esos certificados.

14.- Resolución SGP N° 63/2007

Establece la Política de Certificación de la Autoridad Certificante Raíz de la República Argentina.

15.-Resolución SGP N° 64/2007

Establece los procedimientos operativos para la instalación y puesta en marcha de la Autoridad Certificante Raíz de la República Argentina.

16.- Resolución SGP N° 62/2008

Determina que la ONTI, con el concurso de la Dirección de Infraestructura y de Recursos Informáticos, emitirá el dictamen legal y técnico previo al licenciamiento de certificadores.

17.- Resolución SGP N° 87/2008

Otorga a la Administración Nacional de la Seguridad Social la licencia para operar como Certificador Licenciado.

18.- Resolución SGP N° 88/2008

Otorga a la AFIP la licencia para operar como Certificador Licenciado.

19.- LEY N° 26.388 (B.O. 25/06/2008)

Establece que el término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.

Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente.

Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

20.- RESOLUCIÓN GENERAL AFIP N° 2651/2009

Establece el procedimiento para la solicitud, aprobación, emisión, aceptación y revocación del Certificado Digital de la Autoridad Certificante de la AFIP.-

21.- RESOLUCIÓN SGP N° 227/2010 • Oficina Nacional de Tecnologías de Información

Aprueba la Política de Certificación de la ONTI para Personas Físicas de Entes Públicos, Estatales o no Estatales, y Personas Físicas que realicen trámites con el Estado. También le otorga la Licencia para operar como Certificador Licenciado, y ordena su inscripción en el Registro de Certificadores Licenciados.-

23.- LEY N° 26.685 • Ley de comunicación electrónica judicial

Autoriza la utilización de expedientes electrónicos, documentos electrónicos, firmas electrónicas, firmas digitales, comunicaciones electrónicas y domicilios electrónicos constituidos, en todos los procesos judiciales y administrativos que se tramitan ante el Poder Judicial de la Nación, con idéntica eficacia jurídica y valor probatorio que sus equivalentes convencionales. Faculta a la CSJN y el Consejo de la Magistratura para que de manera conjunta reglamenten su utilización.-

24.- Ley N° 26.733 • Modificatoria del Código Penal

Sustituye el art. 77 del Código. En lo relativo a la FD, establece que “los *términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente”,* y que *“Los términos instrumento privado y certificado comprenden el documento digital firmado digitalmente*.”

C.- Análisis de la Ley N° 25.506, su Decreto Reglamentario N° 2628/2002, la Decisión Administrativa N° 6/2007 y la Decisión Administrativa 917/2014

La ley Nº 25.506 establece una Infraestructura de Firma Digital de alcance federal. La norma deroga el Decreto Nº 427/98, por cuanto cubre sus objetivos y alcance.

Más allá de que la normativa en análisis regula cuestiones de derecho de fondo (firma digital, documento electrónico), la invitación que el legislador establece en el art. 50 *"… a las jurisdicciones provinciales a dictar los instrumentos legales pertinentes para adherir a la presente*" genera interrogantes que intentaremos dilucidar a lo largo de este trabajo.

En el art. 1, a la vez que define el objeto de la ley, otorga validez jurídica tanto a la Firma Digital como a la Firma Electrónica.[9]

La Doctrina[10] ha criticado el empleo de la expresión "FIRMA DIGITAL", dado que con ella se limita su aplicación sólo a un sistema de encriptación fundado en la digitalización binaria. Por ello, siendo que la evolución tecnológica es constante y que en poco tiempo puede llegar a utilizarse otro procedimiento de identificación o reconocimiento – por ejemplo a través de la lectura del iris de las partes contratantes -, hay quienes estiman que era preferible – o de mayor corrección técnica - utilizar sólo la expresión "firma electrónica", dado que los impulsos eléctricos tienen un mayor futuro en cuanto a que seguirán siendo la base de todo sistema por un lapso mayor.

Esta interpretación crítica sobre los vocablos utilizados en la Ley es ciertamente opinable, puesto que lo concreto es que la definición que brinda sobre lo que se entiende por Firma Digital, es justamente un mecanismo de digitalización binaria, y no de reconocimiento de características físicas.

En el art. 2 la Ley describe lo que entiende por Firma Digital, como el "*resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control.*"

En el renglón siguiente, menciona las dos características básicas que tiene la Firma Digital, a saber: "…*ser susceptible de verificación por terceras partes, tal que dicha*

[9] ART. 1 - OBJETO. Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley**.**
[10] FARRÉS, Pablo; "*Firma* Digital", Buenos Aires, Ed. Lexis. Año 2005.

*verificación simultáneamente permita identificar al firmante (*autoría*) y detectar cualquier alteración del documento digital posterior a su firma.*" (Integridad).[11]

La Autoría significa que se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del CD[12]. La Integridad significa que se presume, salvo prueba en contrario, que este documento digital firmado digitalmente no ha sido modificado desde el momento de su firma[13]. Ambos caracteres, son la fuerza interna que hacen que la Firma Digital sea considerada como una alternativa válida a la exigencia de firma manuscrita[14], siendo ésta una de las cuestiones más trascendentes, ya que al equipararla con la firma ológrafa, está incorporando a nuestro derecho de fondo el instituto de la Firma Digital.

Asimismo puede entenderse válidamente que el requisito que se establece de "*encontrarse bajo control de su titular*", no hace a la esencia de la existencia de Firma Digital. Más allá de que ello tiene que ver con la seguridad jurídica del sistema y la imputación de efectos jurídicos al autor, no necesariamente se trata de un requisito que determine la existencia o no de la firma digital, siempre que se cumpla con la cadena de certificaciones impuesta por la Infraestructura.

El art. 2 continúa diciendo que "*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*." Según el Decreto N° 2628/02[15], la Autoridad de Aplicación será la Jefatura de Gabinete de Ministros.

El art. 3, como ya expresamos, equipara la Firma Digital a la firma manuscrita. En la normativa Civil, la firma es un elemento esencial para la validez de todo acto, ya que no puede ser reemplazada por signos o iniciales[16]. Lo mismo ocurre con los instrumentos públicos, a los cuales se los sanciona con la nulidad absoluta cuando carecieran de la firma de las partes[17]. Este artículo estaría modificando las

[11] También regulado en el punto 2 del Glosario del Decreto 2628/02.
[12] **ART 7º -** Presunción de autoría. Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma.
[13] **ART 8º —** Presunción de integridad. Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma.-
[14] **ART 3º —** Del requerimiento de firma. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia.
[15] ART. 4 a 6 Dec. 2628/02
[16] **ART. 1012** Código Civil Argentino.-
[17] ART. 988 y ART. 1004.

disposiciones mencionadas, salvo en lo que respecta a la aplicación de las excepciones contenidas en el art. 4[18] de la Ley 25.506, donde el legislador, en razón de la naturaleza de los actos allí enumerados, excluye la aplicación de la Ley, no sólo en lo atinente a la Firma Digital, sino también de la posibilidad de conservarse en soporte digital, porque quedan excluidos de todo el plexo normativo.

Atendiendo a la falta de claridad respecto al motivo que llevó al legislador a realizar dicha exclusión, parte de la doctrina, entre ellos Ventura, remarca que la exclusión de estos actos se debe a la falta de convencimiento respecto de la seguridad del sistema[19]. Lo cierto, es que las exclusiones de los incisos a, b y c parecen tener un hilo conductor o una justificación lógica que se vincula con el temor a su utilización fraudulenta en actos que son extremadamente sensibles a lo largo de la vida de las personas, lo cual efectivamente deja entrever que el legislador aún consideró en esos casos más segura la utilización de la firma ológrafa, impidiendo la utilización de una herramienta que podría redundar en forma beneficiosa en la celeridad y seguridad de muchos de esos actos.

En cuanto al inciso d, entendemos que la única interpretación coherente del mismo, que armonice dicha disposición con la del artículo 3 de cuerpo legal analizado, es aquella que entiende que se refiere sólo en los casos en que las disposiciones legales o convencionales tornen absolutamente imposible su implementación desde un punto de vista técnico, o bien la prohíban expresamente.

En el Proyecto de Código Civil y Comercial de la Nación recientemente sancionado, se incorpora este precepto, adaptando la normativa de fondo a la ley en estudio. Así, el art. 286 establece que: "*La expresión escrita puede tener lugar por instrumentos públicos, o por instrumentos particulares firmados o no firmados, excepto en los casos en que determinada instrumentación sea impuesta. Puede hacerse constar en cualquier soporte, siempre que su contenido sea representado con texto inteligible, aunque su lectura exija medios técnicos*".

---

[18] **ART 4º —** Exclusiones. Las disposiciones de esta ley no son aplicables:
a) A las disposiciones por causa de muerte;
b) A los actos jurídicos del derecho de familia;
c) A los actos personalísimos en general;
d) A los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes.-

[19] VENTURA, Gabriel "*ANÁLISIS EXEGÉTICO DE LA LEY*". Ver en http://www.cea.unc.edu.ar/

Asimismo, el art. 288 referido a la firma, establece que: "*La firma prueba la autoría de la declaración de voluntad expresada en el texto al cual corresponde. Debe consistir en el nombre del firmante o en un signo. En los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho si se utiliza una firma digital, que asegure razonablemente la autoría e inalterabilidad del instrumento*".
[20]

En este sentido, vemos que el proyecto no supera las discusiones sobre de la terminología utilizada, ya que se refiere textualmente a la firma digital, pero sí acerca de las dudas vinculadas a la seguridad de los sistemas de archivo y autenticación de identidad por medios electrónicos, ya que no efectúa ningún tipo de exclusión en función de los actos para los que se los utilice.

1.- Firma electrónica

En su art. 5, la Ley define a la "*firma electrónica*" como un "*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*".[21] De esta manera, cabe concluir que entre la Firma Electrónica y la Firma Digital existe una relación de género- especie, donde la Firma Digital aparece como la especie, contando con mayores exigencias y recaudos.

Si bien en el art. 1 se le reconoce validez jurídica tanto a la Firma Digital como a la Firma Electrónica, la diferencia entre una y otra es que a la Firma Electrónica le faltan alguno de los requisitos de validez establecidos en el art. 9 de la Ley. Es por ello que el valor probatorio atribuido a cada una de ellas es diferente, reconociéndose a la Firma Digital las presunciones de autoría e integridad[22]. De allí que, en el caso de la Firma Digital, el firmante no puede desconocerla sin probar en contrario a la validez del acto; mientras que en el caso de la Firma Electrónica, corresponde a quien la invoca acreditar su validez.

[20] CABULI, Ezequiel. "*Las Nuevas Tecnologías en el proyecto de código*" Buenos Aires, La Ley Año 2013.
[21] También definido en el punto 1 del Glosario del Decreto 2628/02.-
[22] Establecida en los art. 7 y 8 de la Ley 25.506 (B.O. 14/12/2001).-

De este modo, la Firma Digital otorga una identificación indubitable de quién es el autor del documento, y de que ese documento no ha sido modificado con posterioridad a su firma.

2.- Documento Digital

El art. 6 otorga reconocimiento jurídico al Documento Digital, ampliando lo normado por el ordenamiento de fondo.[23]

Citando a Lino Palacios, podemos caracterizar al documento como todo objeto susceptible de representar una manifestación del pensamiento, con prescindencia de la forma en que esa representación se exterioriza[24].

En nuestro derecho positivo, encontramos una definición de documento en el art. 77 del Código Penal, donde se establece que: "*el término documento comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión*".

El documento digital es una especie de documento electrónico que exige digitalización, es decir, que consiste en una secuencia informática de bits. Cabe así preguntarnos sobre la factibilidad de considerar documentos digitales a archivos almacenados con otros métodos y en su caso, firmar digitalmente este tipo de instrumentos. Nada impide que ello así sea en la medida en que puedan ser compatibilizados mediante algún proceso de transformación.

Al respecto, el art. 11 aclara un punto importante, en virtud de la controversia que pudiere surgir, equiparando como originales y con el mismo valor probatorio, a los reproducidos en formato digital firmados digitalmente, respecto de los originales de primera generación en cualquier otro soporte de los cuales los primeros deriven.[25]

---

[23] **ART 6—** Documento digital. 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.

[24] PALACIO, Lino Enrique. "*Manual de Derecho Procesal Civil*" Buenos Aires, Ed. Abeledo Perrot. 16° Ed. Año 2001. -

[25] **ART 11 —** Original. Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación.

Sin embargo, parte de la doctrina – a la cual adherimos - considera que esa solución es desacertada, ya que "…*el considerar originales a todas las reproducciones que de él se hicieren, constituye un error conceptual en cuanto a las posibilidades de ejecución del mismo: se ha advertido que la expresión usada, desde el punto de vista jurídico, se aplica al documento que genera la posibilidad de ejecutarse aun de una manera compulsiva; y, como las obligaciones contenidas en los documentos sólo pueden exigirse una sola vez, el documento debe perder eficacia, por cumplimiento, una vez prestado el servicio, entregada la cosa, etc.; es decir una vez cumplida la obligación instrumentada. Pero si los documentos son varios, esa primitiva y natural garantía, que constituye la enervación de eficacia del original, se ve seriamente perturbada, pues permanecerá intacta en el resto de los ejemplares "originales"*."[26]

El art. 12[27] norma lo relativo a la conservación de los documentos digitales, cuestión trascendente en virtud de que esos documentos deberán ser presentados en momento oportuno, sea para ejercer los derechos allí plasmados o para acreditar el cumplimiento de algún acto jurídico.

El art. 4 del Decreto Reglamentario establece que "…*será la Jefatura de Gabinete de Ministros la encargada de establecer las normas y procedimientos técnicos para la generación, comunicación, archivo y conservación del documento digital o electrónico*".

3.- Presunciones

Tal como ya dijéramos, la Firma Digital goza de una doble presunción iuris tantum que le otorga seguridad jurídica para tornarlo un medio altamente confiable. Este es el principal efecto de la Firma Digital y su diferencia básica con la Firma Electrónica.

[26] VENTURA, Gabriel "Análisis exegético de la Ley 25.506".-

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

El art. 7[28] de la Ley establece una presunción iuris tantum de *autoría*, por la cual se presume que la Firma Digital de un determinado documento pertenece al titular del Certificado Digital que va a permitir la verificación de la firma.

Junto con el Certificado Digital, ese documento digital firmado generará los efectos jurídicos allí establecidos, salvo que quién sea reputado como autor decida cuestionar judicialmente su autenticidad y pruebe que hubo alguna falla en la seguridad de la operatoria técnica.

Según Ventura[29], este artículo vendría a colocar al documento digital firmado, en una situación intermedia entre un instrumento público y uno privado, de acuerdo con la regulación establecida en el Código Civil. Sostiene que mientras el instrumento privado en el Código sólo genera vinculo jurídico una vez reconocida la firma, o dada por reconocida, según lo determina el artículo 1026 C.C., para lo cual el firmante está obligado a prestar esa declaración en sede judicial en caso de serle requerida, a tenor de lo previsto en el artículo 1031 del Código Civil; el documento digital debidamente firmado, cumpliendo con las previsiones de la norma que analizamos, genera ya el efecto jurídico invirtiendo “onus probandi”, por lo cual sólo caería la presunción de autoría frente a la prueba en contrario, sin que sea menester el reconocimiento previo.

Debemos destacar aquí que la dificultad que esto conlleva, debido a la complejidad técnica de todo el sistema y las contingencias que pueden suscitarse en torno a la guarda de la información confidencial propia del titular del certificado, sería un punto que abonaría la antes analizada postura del legislador de excluir, en el art. 4, determinados actos de la aplicación de la Firma Digital, a los efectos de no cargar con dicha obligación probatoria a las personas en actos particularmente sensibles.

Por su parte, el art. 8 consagra otra presunción, la de integridad e inalterabilidad del documento.[30] Ésta consiste en interpretar que, si el resultado de un procedimiento de verificación de una Firma Digital aplicado a un Documento Digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma.

[28] **ART. 7 -** Presunción de autoría. Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma.
[29] Ob. Cit. 24.-
[30] **ART 8º —** Presunción de integridad. Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma.

Nuevamente, la carga de la prueba (onus probandi) recaerá sobre la persona que alega la falsedad de un documento firmado digitalmente, o que el mismo ha sido firmado por interpósita persona. Por el contrario, cuando se desconoce la firma electrónica la carga de la prueba sobre su validez, recaerá sobre quien la alega.

También el art. 10 suma otra presunción al establecer que "*Cuando un documento digital sea enviado en forma automática por un procedimiento programado y lleve la firma digital del remitente, se presumirá, salvo prueba en contrario, que el documento firmado proviene del remitente*."

En este caso creemos que es una innecesaria reafirmación de lo ya establecido en el art. 7.

En conjunto, las presunciones mencionadas en este acápite, constituyen la denominada "garantía de no repudio", y otorgan a esta operatoria un alto grado de seguridad jurídica y confiabilidad en las transacciones que la incorporan, aún mayor que el que brinda la firma ológrafa

4.-Requisitos de validez de la Firma Digital

En el art. 9, se enumeran taxativamente los requisitos necesarios para que la Firma Digital sea válida:

a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante;

b) Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente;

c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la norma, por un certificador licenciado.

El contenido de este artículo nos lleva a reafirmar la definición expuesta al inicio de este trabajo, con referencia a la desagregación de los dos componentes esenciales: el técnico (inc. b – procedimiento de verificación que realiza el software) y el normativo (inc. a y c – certificado digital e infraestructura). Para que una Firma Digital sea considerada como tal – es decir, que sea válida – deberá reunir ambas características.

5.-Certificado Digital

El Certificado Digital, como ya se explicó en la introducción de este informe, conforma una identidad virtual a través de la asignación de una clave pública a una persona (física o jurídica) determinada. Se comporta como una especie de Documento de Identidad para manejarse en el ámbito cibernético.

La noción de Certificado Digital está inescindiblemente vinculada a la de Certificador Licenciado, ya que se define en virtud de él. Esta tercera entidad vinculada es la que le confiere la garantía de autenticidad y vigencia.

La ley lo define en el art. 13, y luego determina cuáles serán los requisitos de validez y de reconocimiento de los Certificados provenientes del exterior, cuestión esencial para relacionarse en el tráfico comercial en el ámbito internacional.

Según nuestra legislación, habrá Certificado Digital cuando estemos ante un "*… documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.*"[31] Su función es verificar que la clave pública específica pertenece efectivamente a un individuo determinado.

El art. 3 del Decreto Reglamentario N° 2628/02, establece que "*los CD contemplados en el art. 13 de la Ley serán aquellos cuya utilización permite disponer de una FD amparada por las presunciones de autoría e integridad establecidas en los art. 7 y 8 de la ley citada.*"; y en el art. 2 del mismo Decreto, se dispone que los Certificados Digitales emitidos por certificadores no licenciados serán válidos para producir los efectos jurídicos que la ley otorga a la firma electrónica.

Los requisitos de validez que establece el art. 14 son:

a) ser emitidos por un Certificador Licenciado por el Ente Licenciante.

En este caso, el inciso nos remite al art. 17 y al punto 5 del glosario del Decreto Reglamentario, en el cual se define al Certificador Licenciado, situándolo en el rol de entidad de confianza que sostiene la infraestructura de la Firma Digital.

[31] Art. 13 Ley 25.506 y punto 4 Glosario DR.-

b) Responder a formatos estándares reconocidos internacionalmente, fijados por la autoridad de aplicación.

Esto inserta a nuestra normativa en el ámbito internacional, abriendo un abanico de posibilidades para reconocer la autenticidad de los Certificados Digitales emitidos en el extranjero.

La autoridad de aplicación será la Jefatura de Gabinete de Ministros de la Nación[32]; el formato estándar reconocido internacionalmente es el "X.509" en su versión 3.

Luego, la Ley establece los recaudos que deben satisfacer los Certificados Digitales, enumerando: I) identificar indubitablemente a su titular y al certificador licenciado que lo emitió; II) indicar el período de vigencia; III) determinar que no ha sido revocado; VI) reconocer claramente la inclusión de información no verificada y; V) identificar la política de certificación[33] bajo la cual fue emitido.

En el art. 23 se identifican las situaciones en las cuales el Certificado Digital no será válido, tales los casos en que se lo utilice para: a) finalidad diferente a los fines para los cuales fue extendido; b) Para operaciones que superen el valor máximo autorizado cuando corresponda; c) Una vez revocado.

5.1- Vigencia

El art. 15[34] de la Ley, determina la validez del Certificado Digital en cuanto al tiempo de vigencia; esto nos lleva a analizar las causas mediante las cuales un Certificado Digital puede perder vigencia, a saber: la caducidad o la revocación.

[32] ART. 6 inc A) DR 2628/02 (B.O. 20/12/2002).-
[33] La política de Certificación está definida en el punto 6 del Glosario del DR como: "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)".
[34] **ART 15.** — Período de vigencia del certificado digital. A los efectos de esta ley, el certificado digital es válido únicamente dentro del período de vigencia, que comienza en la fecha de inicio y finaliza en su fecha de vencimiento, debiendo ambas ser indicadas en el certificado digital, o su revocación si fuere revocado.
La fecha de vencimiento del certificado digital referido en el párrafo anterior en ningún caso puede ser posterior a la del vencimiento del certificado digital del certificador licenciado que lo emitió.
La Autoridad de Aplicación podrá establecer mayores exigencias respecto de la determinación exacta del momento de emisión, revocación y vencimiento de los certificados digitales.

- Caducidad: cuando se agota el plazo de vigencia que estará indicado en el mismo certificado;

- Revocación: cuando por alguna causal de las enumeradas en el art. 19 de la Ley y el art. 23 del Decreto Reglamentario, se deja sin efecto el Certificado conferido. En virtud del necesario y permanente control que debe hacerse sobre este extremo, el Certificador Licenciado deberá confeccionar y publicar un listado con los Certificados revocados.-

En cuanto a las causales de revocación, el art. 19 establece las siguientes:

1) Solicitud del titular del certificado digital.

2) Si se determinara que un certificado digital fue emitido con base en una información falsa.

3) Si se determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.

4) Por condiciones especiales definidas en su política de certificación.[35]

5) Por resolución judicial o de la autoridad de aplicación.

El art. 23 del Decreto Reglamentario N° 2628/02 agrega:

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.

10) Por el cese de la relación de representación respecto de una persona.

[35] Es un conjunto de criterios que indican la aplicabilidad de un certificado a un grupo de usuarios o a un conjunto de aplicaciones con similares requerimientos de seguridad. La Jefatura de Gabinete de Ministros definirá el contenido mínimo de las políticas de certificación de acuerdo a estándares nacionales e internacionales vigentes.

La Ley establece, dentro de las obligaciones del titular del Certificado, la de "…s*olicitar la revocación de su certificado al certificador licenciado ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma*".[36]

En estos casos, el Certificador Licenciado deberá Publicar en Internet o en una red de acceso público, un listado en el cual se indique la fecha y la hora de la revocación.[37]

5.2.-Reconocimiento de los Certificados extranjeros

Como adelantáramos, en el art. 16[38] y en el art. 1 inc. d) del Decreto Reglamentario N° 2628/02[39] se establecen las bases sobre las cuales se les otorgará validez jurídica a los Certificados Extranjeros, con la finalidad de abrir el sistema a la realización de negocios jurídicos en el plano internacional.

Todas las legislaciones en la materia contienen este tipo de disposiciones que validan certificados extranjeros, ya que de alguna manera, estas operaciones - en el marco del proceso de globalización de la información - fueron las que dieron origen a las herramientas técnicas que hoy llamamos Firma Digital.

En virtud del art. 16, se considerará válido un Certificado Extranjero siempre que exista pacto de reciprocidad entre el país de origen y el nuestro. Asimismo se requiere que al certificado Extranjero, en su ámbito de origen, se le exijan los mismos recaudos que al nacional.

---

[36] Art. 25 inc. c) Ley 25.506.-
[37] Art. 19 inc. f) – art. 25 inc. k)
[38] **ART16.** — Reconocimiento de certificados extranjeros. Los certificados digitales emitidos por certificadores extranjeros podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley y sus normas reglamentarias cuando:
a) Reúnan las condiciones que establece la presente ley y la reglamentación correspondiente para los certificados emitidos por certificadores nacionales y se encuentre vigente un acuerdo de reciprocidad firmado por la República Argentina y el país de origen del certificador extranjero, o
b) Tales certificados sean reconocidos por un certificador licenciado en el país, que garantice su validez y vigencia conforme a la presente ley. A fin de tener efectos, este reconocimiento deberá ser validado por la autoridad de aplicación.-

[39] **art. 1. inc d)** Firma digital basada en certificados digitales emitidos por certificadores extranjeros que hayan sido reconocidos en los siguientes casos:
1. En virtud de la existencia de acuerdos de reciprocidad entre la República Argentina y el país de origen del certificador extranjero.
2. Por un certificador licenciado en el país en el marco de la presente reglamentación y validado por la Autoridad de Aplicación.

En cuanto a la competencia para la suscripción de esta clase de convenios de reciprocidad, el art. 28[40] del Decreto Reglamentario, faculta para ello a la Jefatura de Gabinete de Ministros de la Nación.

6.- Infraestructura de Firma Digital o de Clave Pública

Habiendo explicado ya las cuestiones técnicas - referidas a la criptografía, claves asimétricas - y la funcionalidad e importancia del Certificado Digital, debemos referirnos al sostén de todo ello, constituido por la Infraestructura de Firma Digital.

En nuestro país, la Infraestructura de Firma Digital (IFD o PKI) comenzó a delinearse con el dictado del Decreto N° 427/1998, que autorizó la utilización de la Firma Digital en la instrumentación de los actos internos de la administración, que no produzcan efectos jurídicos individuales en forma directa – vale decir entonces que no permitía la utilización de la herramienta en lo que técnicamente constituirían actos administrativos -, y equiparó sus efectos a la firma ológrafa. Dispuso que la Autoridad de Aplicación y órgano licenciante fuera la Secretaría de la Función Pública de la Jefatura de Gabinete de Ministros de la Nación (art. 6 y 9) y también instituyó a la Contaduría General de la Nación como Organismo Auditor del sistema (art.8).

A partir del año 2001, con la sanción de la Ley que analizamos, este diseño ha variado sustancialmente. La Ley N° 25.506 dedica la mayor parte de su articulado a establecer cómo funcionará la arquitectura de Firma Digital, al igual que su Decreto Reglamentario N° 2628/02.

La Ley de Firma Digital define a los actores de la Infraestructura de Firma Digital, enumerando:

- Ente Licenciante y su Autoridad Certificante Raíz.

[40] **Art. 28 DR 2628/02.** — Reconocimiento de certificados extranjeros. De acuerdo a lo establecido en el artículo 6° de la presente reglamentación, facúltase a la JEFATURA DE GABINETE DE MINISTROS a elaborar y firmar acuerdos de reciprocidad con gobiernos de países extranjeros, a fin de otorgar validez, en sus respectivos territorios, a los certificados digitales emitidos por certificadores de ambos países, en tanto se verifique el cumplimiento de las condiciones establecidas por la Ley N° 25.506 y su reglamentación para los certificados emitidos por certificadores nacionales.
Los certificadores licenciados no podrán reconocer certificaciones emitidas por certificadores extranjeros correspondientes a personas con domicilio o residencia en la República Argentina. El Ente Administrador de Firma Digital establecerá las relaciones que los certificadores licenciados deberán guardar entre los certificados emitidos en la República Argentina y los certificados reconocidos de certificadores extranjeros.

- Certificadores Licenciados, incluyendo Autoridades Certificantes y de Registro.

- Titulares de certificados digitales y terceros usuarios.

- Comisión Asesora.

- Sistema de Auditoría.

6.1.- Ente Licenciante

En nuestro país, la **Secretaría de Gabinete y Coordinación Administrativa** actúa como Ente Licenciante[41], otorgando, denegando o revocando las licencias de los certificadores licenciados, y supervisando su accionar[42].

El Decreto Reglamentario asigna al Ente las siguientes funciones:

- Otorgar las licencias habilitantes a los Certificadores.

- Fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los Certificadores Licenciados.

- Denegar las solicitudes de licencia a los prestadores de servicios de certificación que no cumplan con los requisitos establecidos.

- Revocar las licencias otorgadas a los Certificadores Licenciados que dejen de cumplir con los requisitos establecidos.

- Aprobar las políticas de certificación, el Manual de Procedimientos, los planes de seguridad, de cese de actividades y de contingencia presentados por los certificadores solicitantes de la licencia o licenciados.

- Solicitar los informes de auditoría en los casos que correspondiere.

- Realizar inspecciones a los Certificadores Licenciados por sí o por terceros.

- Homologar los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la presente reglamentación.

- Disponer la instrucción sumarial, la aplicación de sanciones e inhabilitar en forma temporal o permanente a todo certificador o licenciado que no respetare o que

[41] Ver Anexo I al Artículo 1º del Decreto Nº 357/02, sus modificatorios y complementarios —Organigrama de Aplicación de la ADMINISTRACION PUBLICA NACIONAL centralizada—, el Apartado XI, correspondiente a la JEFATURA DE GABINETE DE MINISTROS.
[42] Capítulo X, Normas de procedimiento, Art. 45 de la Decisión Administrativa Nº 6/2007.

incumpliere los requerimientos y disposiciones de la Ley N° 25.506, del Decreto Nº 2628/02 y sus normas complementarias.

- Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, números telefónicos, direcciones de Internet y certificados digitales de los Certificadores Licenciados, los certificadores cuyas licencias han sido revocadas y el Ente Administrador.

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

- Fijar el concepto y los importes de todo tipo de aranceles y multas previstos en la Ley N° 25.506.

- Solicitar la ampliación o aclaración de la documentación presentada por el certificador.

- 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.

6.1.1.- Autoridad Certificante Raíz

Es la Autoridad Certificante administrada por el Ente Licenciante que emite Certificados Digitales destinados a las Autoridades Certificantes de los Certificadores Licenciados (segundo grado) correspondientes a sus Políticas de Certificación aprobadas. Al otorgar la Licencia respecto a una Política de Certificación, el Ente Licenciante deberá a emitir a los Licenciados un Certificado Digital a través de su Autoridad Certificante Raíz.[43]

6.2.- Certificador Licenciado

La ley lo define en el art. 17, como "…*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*

[43] ART. 14 Decisión Administrativa 6/2007

público se prestará en régimen de competencia. El arancel de los servicios prestados por los certificadores licenciados será establecido libremente por éstos".[44]

Entonces el Certificador Licenciado deberá obtener una LICENCIA. El art. 20[45] de la Ley hace referencia a la necesidad de cumplir con una serie de requisitos para poder obtenerla. Esos requisitos están enumerados en el art. 24 del Decreto Reglamentario N° 2628/02, donde se dispone que para *"…obtener una licencia, los proveedores de servicios de certificación deberán particularizar las actividades para las cuales requieren la licencia y acreditar por los medios que este determine ante el Ente Administrador de Firma Digital:*

a) Documentación que demuestre:

1- En el caso de personas jurídicas su personería.

2- En el caso de registro público de contratos, tal condición

3- En el caso de organización pública, la autorización de su máxima autoridad para iniciar el proceso de licenciamiento y la correspondiente aprobación de la JEFATURA DE GABINETE DE MINISTROS, de acuerdo con lo dispuesto en el artículo 41 de la presente reglamentación.

b) El cumplimiento de las condiciones establecidas en la ley; este decreto y las normas complementarias.

c) Las políticas de certificación para las cuales solicita licencia que respaldan la emisión de sus certificados. Manual de Procedimientos, Plan de Seguridad, Plan de Cese de Actividades y Plan de Contingencia satisfactorias de acuerdo con las normas reglamentarias.

d) Toda aquella información o requerimiento, que demande la Autoridad de Aplicación."

Todo ello deberá ser examinado por el Ente Licenciante mediante un procedimiento en el cual se analizará detalladamente toda la documentación presentada.

[44] También está definido en el Punto 5 del Glosario DR 2628/02.-
[45] **ART. 20**: Para obtener una licencia el certificador debe cumplir con los requisitos establecidos por la ley y tramitar la solicitud respectiva ante el ente licenciante, el que otorgará la licencia previo dictamen legal y técnico que acredite la aptitud para cumplir con sus funciones y obligaciones. Estas licencias son intransferibles.

Por otro lado, la Decisión Administrativa Nº 6/2007 en el Capítulo X, Normas de Procedimiento (art. 41 a 46) y en su Anexo I, establece el procedimiento que debe realizarse para ser Certificador Licenciado, el cual comienza con la solicitud realizada por la Empresa u Organismo, acompañada de la documentación exigida. Luego, mediante un dictamen legal y técnico[46], se determinará la admisibilidad, otorgándose una licencia para cada política de certificación que presente el certificador.

La licencia durará 5 años y podrá renovarse, quedando los Licenciados sometidos a auditorías anuales[47].

El art. 27 del Decreto Reglamentario enumera las causales de caducidad de la licencia, determinando que la misma podrá ser dispuesta de oficio y en forma preventiva cuando:

a) Falte la Declaración Jurada anual.

b) La Declaración Jurada contenga datos falsos.

c) Exista dictamen desfavorable de auditoría basado en causales graves.

d) El informe de la inspección dispuesta por el Ente sea desfavorable con base en causales graves.

e) El Certificador Licenciado no permita la realización de auditorías o inspecciones.-

6.2.1.-Funciones del Certificador Licenciado

Los Certificadores Licenciados constituyen la columna vertebral del sistema de Firma Digital, y entre sus funciones[48] se destacan:

a) Recibir las solicitudes de emisión de Certificados Digitales, con los correspondientes datos de verificación del solicitante.

b) Emitir Certificados Digitales de acuerdo a lo establecido en sus políticas de certificación, y a las condiciones que la autoridad de aplicación indique en la reglamentación de la ley.

[46] El dictamen legal y técnico es el resultado de la evaluación de la aptitud del certificador para cumplir con las funciones y obligaciones inherentes al licenciamiento.
[47] Art. 26 del Decreto N° 2628/02 y art. 33 de la Ley N° 25.506.
[48] Definidas en el art. 19 de la Ley 25.506.-

Reiteramos que las políticas de certificación son los 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. Estas políticas de certificación integran el contenido de una suerte de contrato de adhesión al que quedaran vinculadas las partes, certificador y titular del certificado o usuario.

c) Identificar inequívocamente los certificados digitales emitidos.

d) Mantener copia de todos los certificados digitales emitidos, consignando su fecha de emisión y de vencimiento si correspondiere, y de sus correspondientes solicitudes de emisión.

e) Revocar los certificados digitales emitidos en los siguientes casos:

1) A solicitud del titular del certificado digital.

2) Si se determinara que un certificado digital fue emitido con base en una información falsa.

3) Si se determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.

4) Por condiciones especiales definidas en su política de certificación.

5) Por resolución judicial o de la autoridad de aplicación.[49]

f) Informar públicamente el estado de los Certificados Digitales por él emitidos. Los certificados revocados deben ser incluidos en un listado público, indicando fecha y hora de la revocación. La validez y autoría de dicha lista de certificados revocados deben ser garantizadas.

El art. 21 de la Ley y el art. 34 del Decreto Reglamentario, enumeran las obligaciones del Certificador Licenciado, las cuales pueden clasificarse en:

[49] Ver pág. 30 – Causales de revocación del CD -

a) OBLIGACIONES GENERALES, que son aquellas previas a la prestación del servicio en sí mismo, mencionadas en el art. 24 del Decreto Reglamentario - requisitos para obtener una licencia que ya han sido explicados -, y en el art. 21 de la Ley.[50]

Además, lo normado en el art. 32[51] del Decreto Reglamentario también debe ser considerado como una obligación, ya el Certificador Licenciado deberá acreditar que cuenta con los recursos profesionales, tecnológicos, financieros y de seguridad exigidos.

[50] Las obligaciones generales consistirán entonces en: Incorporar en su Política de Certificación los efectos de la revocación de su propio Certificado Digital o de la licencia que le otorgara a la autoridad de aplicación; informar inmediatamente al Ente Licenciante sobre cualquier cambio en los datos relativos a su licencia; permitir el ingreso de los funcionarios autorizados de la Autoridad de Aplicación, Ente Licenciante o auditores a su local operativo y poner a su disposición toda la información necesaria; emplear a personal idóneo con el conocimiento y la preparación suficientes para la prestación del servicio; someter a aprobación del Ente Licenciante el manual de procedimientos, plan de seguridad y el de cese de actividades, y los componentes técnicos a utilizar; y constituir domicilio en el país.

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

b) OBLIGACIONES PARTICULARES, son entendidas como aquellas que deben cumplirse al prestar el servicio, y durante toda la extensión del mismo.[52]

[52] Las obligaciones particulares consisten en informar a quien solicita un certificado con carácter previo a su emisión y utilizando un medio de comunicación las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de un sistema de licenciamiento y los procedimientos, forma que garantiza su posible responsabilidad patrimonial y los efectos de la revocación de su propio certificado digital y de la licencia que le otorgara el ente licenciante; abstenerse de tomar conocimiento o acceder bajo ninguna circunstancia a los datos de creación de firma digital de los titulares de certificados digitales por él emitidos; notificar el solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable , y las obligaciones que asume por el solo hecho de ser titular de un certificado digital; solicitar sólo los datos necesarios para emitir el certificado digital, informándolo de todo lo que se refiere a su tramitación; mantener la confidencialidad de la información que no figure en el certificado digital; mantener la documentación respaldatoria de los certificados digitales emitidos, por diez años a partir de su fecha de vencimiento o revocación; publicar la lista de certificados digitales revocados y el resultado de los informes de la última auditoría que se le haya efectuado; registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas; informar en las políticas de certificación si los certificados digitales por él emitidos requieren la verificación de la identidad del titular; verificar, de acuerdo con lo dispuesto en su manual de procedimientos, toda otra información que deba ser objeto de verificación, la que debe figurar en las políticas de certificación y en los certificados digitales; solicitar inmediatamente al ente licenciante la revocación de su certificado, o informarle la revocación del mismo, cuando existieren indicios de que los datos de creación de firma digital que utiliza hubiesen sido comprometidos o cuando el uso de los procedimientos de aplicación de los datos de verificación de firma digital en él contenidos hayan dejado de ser seguros y cumplir con toda otra obligación emergentes de su calidad de titular de la licencia adjudicada por el ente licenciante; 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; mantener a disposición permanente del público las Políticas de Certificación y el Manual de Procedimientos correspondiente; cumplir cabalmente con las políticas de certificación acordadas con el titular y con su Manual de Procedimientos; 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; informar al solicitante de un certificado digital, en un lenguaje claro y accesible, en idioma nacional, respecto de las características del certificado solicitado, las limitaciones a la responsabilidad, si las hubiere, los precios de los servicios de certificación, uso, administración y otros asociados, incluyendo cargos adicionales y formas de pago, los niveles de servicio al proveer, las obligaciones que el suscriptor asume como usuario del servicio de certificación, su domicilio en la República Argentina y los medios a los que el suscriptor puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema o presentar sus reclamos; disponer de un servicio de atención a titulares y terceros, que permita evacuar las consultas y la pronta solicitud de revocación de certificados; garantizar el acceso permanente, eficiente y gratuito de los titulares y terceros al repositorio de certificados revocados; mantener actualizados los repositorios de certificados revocados por el período establecido por el Ente Administrador; abstenerse de generar, exigir, tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada del suscriptor; informar al Ente Administrador de modo inmediato la ocurrencia de cualquier evento que comprometa la correcta prestación del servicio; respetar el derecho del titular del certificado digital a no recibir publicidad de ningún tipo por su intermedio, salvo consentimiento expreso de éste; publicar en el Boletín Oficial durante un día, el certificado de clave pública correspondiente a la política para la cual obtuvo licenciamiento; cumplir las normas y recaudos establecidos para la protección de datos personales; enviar periódicamente al Ente Administrador, informes de estado de operaciones con carácter de declaración jurada; contar con personal idóneo y confiable, con antecedentes profesionales acordes a

Analizando pormenorizadamente el texto de los artículos mencionados, observamos que existe una confusa redacción, que entremezcla las funciones (expuestas anteriormente) con las obligaciones, incurriendo en reiteraciones que quizás pudieran haberse subsanado unificando el texto en un solo artículo.

Además, su contenido debe complementarse armónicamente con lo dispuesto por la ley de Defensa del Consumidor Nº 24.240 y por la Ley de Protección de Datos Personales Nº 25.326, en función de las relaciones jurídicas entre los certificadores y los usuarios que derivarán de la aplicación del sistema.

6.2.2.- Responsabilidad

En cuanto a la responsabilidad de los sujetos involucrados en el sistema[53], es lógicamente de aplicación lo dispuesto en las Normas del Código Civil, sin perjuicio de lo cual el legislador consideró pertinente incluir disposiciones específicas en la Ley de Firma Digital.

El texto legal - así como el Decreto Reglamentario – reitera, como no podía ser de otra manera, los conceptos de responsabilidad Contractual en la vinculación con los usuarios (titulares de certificados) y extracontractual hacia terceros.

la función desempeñada; responder a los pedidos de informes por parte de un tercero respecto de la validez y alcance de un certificado digital emitido por él.

[53] **ART 37.** La relación entre el certificador licenciado que emita un certificado digital y el titular de ese certificado se rige por el contrato que celebren entre ellos, sin perjuicio de las previsiones de la presente ley, y demás legislación vigente.
ART 38. El certificador que emita un certificado digital o lo reconozca en los términos del artículo 16 de la presente ley, es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de ésta, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos, en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá al prestador del servicio demostrar que actuó con la debida diligencia

Regula también todo lo relativo a las limitaciones de la responsabilidad[54], y a la obligación de contar con un seguro acorde a las responsabilidades asumidas[55].

6.2.3.-Sanciones

En caso de que el Certificador Licenciado cometa alguna falta, el Ente Licenciante podrá instruir un sumario y aplicar sanciones, dentro de las previstas en el capítulo correspondiente de la Ley N° 25.506.

Las mismas podrán variar entre Apercibimiento, multa, caducidad de la licencia[56], e inhabilitación por el término de diez años para ser titular de licencias de certificador[57] según la gravedad de la falta. Más allá de la sanción aplicada, el Certificador Licenciado deberá responder ante terceros por los daños provocados por su conducta.

En el trámite del sumario, se aplicará lo dispuesto en la Ley Nacional de Procedimientos Administrativos (Ley N° 19.549).

6.2.4.- Cese del Certificado

[54] **Ley 25.506. ART 39.** — Limitaciones de responsabilidad. Los certificadores licenciados no son responsables en los siguientes casos:
a) Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstos en la ley;
b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;
c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el certificador pueda demostrar que ha tomado todas las medidas razonables.
DR 2628/02. Art. 31. — Responsabilidad de los certificadores licenciados. En ningún caso, la responsabilidad que pueda emanar de una certificación efectuada por un certificador licenciado, público o privado, comprometerá la responsabilidad pecuniaria del Estado en su calidad de Ente Administrador de la Infraestructura de Firma Digital

[55] **DR 2628/02: Art. 30.** — Seguros. El certificador licenciado debe contar con seguros vigentes acordes con las responsabilidades asumidas, que cumplan con los siguientes requisitos.
a) Ser expedidos por una entidad aseguradora autorizada para operar en la República Argentina.
b) Establecer la obligación de la entidad aseguradora de informar previamente al Ente Administrador de la Infraestructura de Firma Digital la terminación del contrato o las modificaciones que reduzcan el alcance o monto de la cobertura.
Los certificadores licenciados pertenecientes a entidades y jurisdicciones del sector público quedarán exentos de la obligación de constituir el seguro previsto en el presente artículo.

[56] ART. 14 LEY 25.506.-
[57] ART. 44 LEY 25.506.-

El art. 22 de la Ley enumera tres causales de cese del Certificador en su condición de tal:

a) Por decisión unilateral comunicada al ente licenciante.

b) Por cancelación de su personería jurídica.

c) Por cancelación de su licencia dispuesta por el ente licenciante.[58]

Cuando el Certificador Licenciado cesa en sus actividades, debe cumplir los recaudos que ha asumido al formular sus Planes de Cese de Actividades y de Contingencias, referidos a la forma en que efectivizará el corte de actividades.

6.2.5.- Autoridades Certificantes autorizadas en nuestro país

a.- Oficina Nacional de Tecnología de la Información ONTI.-

Es la Autoridad Certificante para la Administración Pública Nacional[59], y su misión principal es estructurar un esquema de confianza válido para los suscriptores de sus certificados y para los terceros que se relacionen con ella. El cumplimiento de todos los procedimientos operativos y de seguridad descriptos en la documentación técnica es un requisito básico para mantener la confiabilidad de dicho esquema.

Cuenta con Autoridades de Registro en las que delega 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.

[58] Esto se complementa con lo establecido por el art. 27 del Decreto Reglamentario, que dispone que será causal de la Cancelación de la Licencia: a) Falta de presentación de la declaración jurada anual; b) Falsedad de los datos contenidos en la declaración jurada anual; c) Dictamen desfavorable de auditoría basado en causales graves; d) Informe de la inspección dispuesta por el Ente Administrador desfavorable basado, en causales graves; y e) Cuando el certificador licenciado no permita la realización de auditorías o inspecciones dispuestas por el Ente Administrador.

[59] Conforme el Decreto N° 1038/03 tiene las siguientes funciones:
- Ejercer las funciones de Autoridad Certificante de Firma Digital para el Sector Público Nacional.
- Impulsar programas y brindar asistencia a fin de dar cumplimiento a lo establecido en la Ley N° 25.506 de Firma Digital, en lo relativo al uso de tecnologías informáticas por parte del Poder Ejecutivo Nacional, como así también en los demás poderes del Estado Nacional, en las provincias y en los municipios que lo requieran.
- Entender, asistir y supervisar en los aspectos relativos a la seguridad y la privacidad de la información digitalizada y electrónica del Sector Público Nacional.

b.- AFIP: Licenciada por Resolución N° 88/2008 de la Secretaría de Gabinete y Gestión Pública de la Jefatura de Gabinete de Ministros.

c.- ANSES: Licenciada por Resolución N° 62/2008 de la Secretaría de Gabinete y Gestión Pública de la Jefatura de Gabinete de Ministros.

En ambos casos, la Secretaría de Gabinete y Gestión Pública de la Jefatura de Gabinete de Ministros, otorga a los Organismos mencionados, la licencia para operar como Certificador Licenciado por haber cumplido con todos los recaudos exigidos.

Así las cosas en agosto de 2009, el organismo de recaudación fiscal dictó la Resolución General N° 2651[60] a los efectos de reglamentar el procedimiento para la emisión y aprobación de los certificados regulando los requisitos y formalidades a cumplir por parte del solicitante, del suscriptor y del tercero usuario de dichos certificados.

d.- ENCODESIN. Es un caso de empresa Certificadora Licenciada privada. El Certificador Licenciado es ENCODE S.A., y la Autoridad Certificante es ENCODESIN.

Tiene domicilio en la Provincia de Córdoba y se constituyó como Autoridad Certificante a través de la Resolución N° 184/12 de la Secretaría de Gabinete y Coordinación Administrativa de la Jefatura de Gabinete de Ministros de la Nación.-

e.- Poder Judicial de la Provincia de Chubut[61]

Por Acuerdo Nº 3268 del 24 de abril de 2002, el Poder Judicial de la Provincia de Chubut crea su Autoridad Certificante (https://ca.juschubut.gov.ar).[62]

Cabe destacar que existen también otras organizaciones que han sido admitidas en el proceso de licenciamiento, pero aún no han obtenido su aprobación definitiva, tales como la Suprema Corte de Justicia de la Provincia de Buenos Aires, EDICOM S.A. y Tecnología de Valores S.A., entre otras.[63]

[60] (BO 06/08/09)
[61] Esta información no surge de la Página Oficial de la Jefatura de Gabinete de Ministros de la Nación.-
[62] Dicha Autoridad Certificante tiene las siguientes funciones:
• Promover el uso de la Firma Digital en el ámbito del Poder Judicial de Chubut y la firma convenios con los operadores del derecho.
• Fomentar acuerdos de certificación cruzada con otras Autoridades Certificantes.
• Realizar acciones tendientes a mantener actualizado el sistema de Firma Digital.
[63] https://www.jefatura.gob.ar/ente-licenciante_p144

Al respecto, el inconveniente que aún no se ha superado en pos de la masificación del uso de esta herramienta, es que la política de registro estatal de los certificadores, propia de nuestro ordenamiento en la materia, y la complejidad que implica cumplir con los requisitos para el licenciamiento, se vuelven una barrera para su utilización fuera del ámbito estatal, e incluso para los poderes provinciales, afectándose así la pronta implementación de servicios que aprovechen la seguridad, celeridad y economía de insumos, derivados de la Firma Digital.

Ello sin mencionar que la constitución como Certificador Licenciado conlleva una gran inversión inicial, con lo cual no resulta ser un modelo de negocio del todo atractivo para los privados, volviéndose indispensable una política activa por parte del estado que tienda a la extensión de su aplicación en servicios al ciudadano, a sensibilizar a la sociedad acerca de los beneficios de la aplicación de las TICs en el intercambio de bienes y servicios, y a la capacitación de los eventuales actores del sistema para su uso.

6.3.- Autoridades de Registro

Son entidades que tienen a su cargo las funciones de validación de la identidad y otros datos de los suscriptores de certificados. Dichas funciones son delegadas por la Autoridad de Certificación, quién además deberá determinar cuál será el procedimiento a utilizar.

Su ámbito posible de competencia está demarcado por el art. 35 del Decreto Reglamentario N° 2628/02, donde se establece que: "…*Los Certificadores Licenciados podrán delegar en Autoridades de Registro las funciones de validación de identidad y otros datos de los suscriptores de certificados y de registro de las presentaciones y trámites que les sean formuladas, bajo la responsabilidad del Certificador Licenciado, cumpliendo las normas y procedimientos establecidos por la presente reglamentación.*

Una autoridad de Registro es una entidad responsable de las siguientes funciones:

a) La recepción de las solicitudes de emisión de certificados.

b) La validación de la identidad y autenticación de los datos de los titulares de certificados.

c) La validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador Licenciado.

d) La remisión de las solicitudes aprobadas al Certificador Licenciado con la que se encuentre operativamente vinculada.

e) La recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento al Certificador Licenciado con el que se vinculen.

f) La identificación y autenticación de los solicitantes de revocación de certificados.

g) El archivo y la conservación de toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el certificador licenciado.

h) El cumplimiento de las normas y recaudos establecidos para la protección de datos personales.

i) El cumplimiento de las disposiciones que establezca la Política de Certificación y el Manual de Procedimientos del Certificador Licenciado con el que se encuentre vinculada, en la parte que resulte aplicable."

Es decir que la Autoridad de Registro, como ya fuera dicho, se comporta como una suerte de ventanilla de atención, o puerta de entrada al sistema por parte de los eventuales usuarios (solicitantes de Certificados Digitales), así como asume también la función de custodio de la documentación pertinente para la acreditación de identidad de los titulares, y garante de la debida confidencialidad de los datos que aquella contiene.

6.4 Autoridades de sello de tiempo y Autoridades de competencia

Estas figuras fueron incorporadas mediante la Decisión Administrativa N° 927/2014 para la prestación de nuevos servicios de certificación.
Las primeras podrán emitir "sellos de tiempo", entendiéndose esto como la indicación de la fecha y hora cierta asignada a un documento o registro electrónico por una entidad habilitada a tal fin y firmada digitalmente por ella, según lo dispuesto en el Anexo I al Decreto Nº 2628/02 y sus modificatorios.
Las Autoridades de sello de tiempo podrán prestar sus servicios previa autorización del ente licenciante (art. 22, D.A. N° 927/2014).

Las segundas, denominadas Autoridades de competencia, podrán emitir “sellos de competencia” como herramienta para la confirmación de roles tales como condición de titularidad de las matrículas profesionales, o los cargos en distintas organizaciones o atribuciones de carácter similar.

Las Autoridades de competencia podrán brindar sus servicios constituyéndose como certificadores licenciados u obteniendo un certificado emitido por un certificador licenciado, previa autorización del ente licenciante, aclarándose que las autoridades de competencia pertenecientes al Sector Público sólo podrán emitir sellos de competencia para funcionarios y agentes públicos y cuando sea requerido para el ejercicio de sus funciones (art. 23, D.A. N° 927/2014).

A partir de lo precedentemente expuesto, entre los servicios de certificación digital que podrán brindarse en el marco de la Infraestructura de Firma Digital de la República Argentina, coexistirán certificados digitales que vinculan los datos de verificación de firma a su titular, y sellos de tiempo con indicación de la fecha y hora asignada a un documento o registro electrónico. Adicionalmente, podrán emitirse sellos de competencia, que indican cargo, rol o cualquier otra atribución de su titular.

6.5 Suscriptores de los Certificados

Así denomina la Decisión Administrativa N° 927/14 a los titulares de certificados digitales.

El acuerdo establecido entre el Certificador Licenciado y el suscriptor determina derechos y obligaciones de las partes en lo que respecta a la solicitud, aceptación y uso de los certificados digitales, estando los contenidos mínimos del mismo establecidos mediante Anexo V de dicha norma.

6.6 Terceros Usuarios

Son las personas físicas o jurídicas receptoras de un documento firmado digitalmente y que consultan para verificar la validez del certificado digital correspondiente.

Los terceros usuarios que sean personas jurídicas y que implementen aplicaciones que requieran Firma Digital, tienen la facultad de definir las características y requerimientos que deben cumplir las Políticas de Certificación a los efectos de

aceptar documentos electrónicos firmados digitalmente utilizando certificados digitales amparados por dichas Políticas.

Tales características y requerimientos deben ser manifestados previamente en forma clara y transparente a los titulares de certificados que pretendan operar con ellos.[64]

6.7.- Autoridad de Aplicación

Está determinada en el art. 29 de la Ley N° 25.506, y es la Jefatura de Gabinete de Ministros, quien estará facultada a establecer las normas y procedimientos técnicos necesarios para la efectiva implementación de la ley[65].

6.7.1.- Funciones

Están enumeradas en el art. 30 de la Ley, asignándosele – entre otras – la de dictar las normas reglamentarias y de aplicación; así como dictar normas relativas a estándares tecnológicos y de seguridad aplicables en consonancia con estándares internacionales[66] en armonía con lo dispuesto en el art. 6 del Decreto Reglamentario[67].

---

[64] Art. 34 bis, Decreto Reglamentario N° 2628/02, incorporado mediante Decreto N° 724/06.

[65] ART. 4 Decreto Reglamentario N° 2628/02.-

[66] Estándar "X.509" es el que ha determinado la Jefatura de Gabinete de Ministros.

[67] **Art. 6°** — Regulación. Facúltase a la JEFATURA DE GABINETE DE MINISTROS a establecer:
a) Los estándares tecnológicos y de seguridad aplicables en consonancia con estándares internacionales.
b) Los procedimientos de firma y verificación en consonancia con los estándares tecnológicos definidos conforme el inciso precedente.
c) Las condiciones mínimas de emisión de certificados digitales.
d) Los casos en los cuales deben revocarse los certificados digitales.
e) Los datos considerados públicos contenidos en los certificados digitales.
f) Los mecanismos que garantizarán la validez y autoría de las listas de certificados revocados.
g) La información que los certificadores licenciados deberán publicar por internet.
h) La información que los certificadores licenciados deberán publicar en el Boletín Oficial.
i) Los procedimientos mínimos de revocación de certificados digitales cualquiera que sea la fuente de emisión, y los procedimientos mínimos de conservación de la documentación de respaldo de la operatoria de los certificadores licenciados, en el caso que éstos cesen su actividad.
j) El sistema de auditoría, incluyendo las modalidades de difusión de los informes de auditoría y los requisitos de habilitación para efectuar auditorías.
k) Las condiciones y procedimientos para el otorgamiento y revocación de las licencias.
l) Las normas y procedimientos para la homologación de los dispositivos de creación y verificación de firmas digitales.
m) El reglamento de funcionamiento de la Comisión Asesora para la Infraestructura de Firma Digital.
n) El procedimiento de instrucción sumarial y la gradación de sanciones previstas en la Ley N° 25.506, en virtud de reincidencia y/u oportunidad.
o) Los procedimientos aplicables para el reconocimiento de certificados extranjeros.
p) Las condiciones de aplicación de la presente ley en el Sector Público Nacional, incluyendo la autorización para prestar servicios de certificación
digital para las entidades y jurisdicciones de la Administración Pública Nacional.

También será la encargada de determinar el procedimiento de firma y verificación, conforme al estándar tecnológico y las condiciones mínimas de emisión de los certificados. Se la faculta para revocar los Certificados del Certificador Licenciado y del Ente Licenciante, y podrá instrumentar acuerdos Internacionales para validar las certificaciones expedidas por certificadores licenciados del país o para que las que se expidan en el exterior puedan producir efectos en el ámbito Nacional.

Ejercerá facultades de contralor de los Certificadores Licenciados y del Ente Licenciante; dictaminará sobre las pautas de auditoría y los niveles de licenciamiento; fiscalizará el cumplimiento de la Ley y las reglamentaciones, pudiendo aplicar las sanciones que correspondan; otorgará y revocará las licencias; y podrá homologar los dispositivos de creación y verificación de Firma Digital.

6.7.2.- Obligaciones

El art. 31 enumera las obligaciones de la Autoridad de Aplicación, haciendo expresa remisión a las disposiciones incluidas en los arts. 21 y 25 de la Ley. Además incluye otros supuestos, a saber:

a) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder, bajo ninguna circunstancia, a los datos utilizados para generar la firma digital de los certificadores licenciados;

b) Mantener el control exclusivo de los datos utilizados para generar su propia firma digital e impedir su divulgación;

c) Revocar su propio certificado frente al compromiso de la privacidad de los datos de creación de firma digital;

d) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios,

---

q) Los contenidos mínimos de las políticas de certificación de acuerdo con los estándares nacionales e internacionales y las condiciones mínimas que deberán cumplirse en el caso de cese de actividades de un certificador licenciado.
r) Los niveles de licenciamiento.
s) Reglamentar el uso y los alcances de los certificados de firma digital emitidos por los Registros Públicos de Contratos.
t) Exigir las garantías y seguros necesarios para prestar el servicio previsto.
u) Las condiciones de prestación de otros servicios en relación con la firma digital y otros temas cubiertos en la ley

números telefónicos y direcciones de Internet, tanto de los certificadores licenciados como los propios, y su certificado digital;

e) Supervisar la ejecución del plan de cese de actividades de los certificadores licenciados que discontinúan sus funciones.

Dentro del ámbito de la Autoridad de Aplicación[68], el art. 28 de la Ley[69] crea la Comisión Asesora para la Infraestructura de la FD, que será la encargada de emitir recomendaciones sobre los aspectos técnicos referidos al funcionamiento de la Infraestructura. Específicamente, está regulada en el Capítulo VIII de la Ley, en el cual se detalla su integración y funciones. La Comisión será multidisciplinaria[70] y su cantidad de miembros no podrá ser superior a siete, designados por el Poder Ejecutivo[71].

En el art. 36 de la Ley se consignan sus funciones, vinculadas a la emisión de recomendaciones, por iniciativa propia o a solicitud de la autoridad de aplicación, sobre:

a) Estándares tecnológicos.

b) Sistema de registro de toda la información relativa a la emisión de certificados digitales.

c) Requisitos mínimos de información que se debe suministrar a los potenciales titulares de certificados digitales de los términos de las políticas de certificación.

d) Metodología y requerimiento del resguardo físico de la información.

---

[68] **DR 2628/02 Art. 7°** — Comisión Asesora para la Infraestructura de Firma Digital. En el ámbito de la JEFATURA DE GABINETE DE MINISTROS funcionará la Comisión Asesora para la Infraestructura de Firma Digital, que se constituirá de acuerdo a lo dispuesto por el artículo 35 de la Ley N° 25.506.

[69] **ART 28. Ley 25.506** — Comisión Asesora para la Infraestructura de Firma Digital. Créase en el ámbito jurisdiccional de la Autoridad de Aplicación, la Comisión Asesora para la Infraestructura de Firma Digital

[70] DR 2628/02 **Art. 8°** — Integración. La Comisión Asesora para la Infraestructura de Firma Digital estará integrada multidisciplinariamente por profesionales de carreras afines a la actividad, de reconocida trayectoria y experiencia, provenientes de organismos del Estado Nacional, Universidades, Cámaras, Colegios u otros entes representativos profesionales. Para integrar la Comisión Asesora para la Infraestructura de Firma Digital se deberán reunir los siguientes requisitos:
a) Poseer título universitario, expedido por Universidad Nacional o privada reconocida por el Estado, correspondiente a carrera profesional de duración no inferior a cuatro (4) años, con incumbencias relacionadas con la materia.
b) Antecedentes académicos y/o profesionales o laborales en la materia

[71] El Decreto Reglamentario, exige como recaudos para integrar la Comisión:
a) Título Universitario correspondiente a carrera profesional de duración superior a cuatro años.-
b) Antecedentes académicos y profesionales en la materia.

e) Otros que le sean requeridos por la autoridad de aplicación.

7.- Sistema de Auditoría

Conforme lo regulado en el art. 27[72] de la Ley, el sistema de auditoría será establecido por la autoridad de aplicación con el concurso de la Comisión Asesora, y su objeto es evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de datos, como así también el cumplimiento de las especificaciones del manual de procedimientos y planes de seguridad y contingencia aprobados por el Ente Licenciante.

En cuanto a los Sujetos pasivos, están establecidos en el art. 33 de la Ley[73], que determina que se auditará al Ente Licenciante y a los Certificadores Licenciados.

Las auditorías podrán hacerse directamente por la Autoridad de Aplicación, o a través de terceras personas habilitadas expresamente a tal efecto; pudiendo tales terceros habilitados ser las Universidades y organismos científicos o tecnológicos nacionales o provinciales, colegios y consejos profesionales que acrediten experiencia profesional en la materia[74]. La Jefatura de Gabinete de Ministros convocará a un Concurso Público para la precalificación de entidades de auditoría, elaborando un Pliego Estándar de Precalificación de Entidades de Auditoría[75].-

Los resultados de la auditoría serán comunicados a la Autoridad de Aplicación, quién determinará si los sistemas utilizados por el Certificador Licenciado cumplen o no con los requerimientos de la Ley N° 25.506 y sus normas reglamentarias.

---

[72] **ART 27. —** Sistema de Auditoría. La autoridad de aplicación, con el concurso de la Comisión Asesora para la Infraestructura de Firma Digital, diseñará un sistema de auditoría para evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, así como también el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y de contingencia aprobados por el ente licenciante.

[73] **ART 33. —** Sujetos a auditar. El ente licenciante y los certificadores licenciados, deben ser auditados periódicamente, de acuerdo al sistema de auditoría que diseñe y apruebe la autoridad de aplicación. La autoridad de aplicación podrá implementar el sistema de auditoría por sí o por terceros habilitados a tal efecto. Las auditorías deben como mínimo evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y, disponibilidad de los datos, así como también el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y, de contingencia aprobados por el ente licenciante.

[74] ART. 34 LEY 25.5096.-

[75] ART. 18 LEY 25.506.-

Por último, el art. 21 del Decreto Reglamentario establece el deber que rige para los auditores de mantener la confidencialidad sobre la información amparada bajo normas de confidencialidad del Certificador Licenciado.

8.- Técnica Legislativa

La Ley N° 25.506 utiliza una técnica amplia, es decir, regula únicamente el marco legal (método amplio), a fin de poder adaptar la normativa vigente al progreso tecnológico que pudiera experimentar el software aplicable a la Firma Digital, consagrando el principio de neutralidad tecnológica (art. 2).

Cabe aclarar, que esa neutralidad es tal en tanto y en cuanto comprendamos que regula únicamente la herramienta de Firma Digital, no así otros métodos biométricos que pudieran aplicarse a los efectos del reconocimiento de identidad, tal como se aclarase al comienzo de este trabajo al referirnos a las críticas formuladas a la terminología utilizada por parte de la doctrina.

En tal sentido, recepta los principios establecidos internacionalmente de libertad económica, y de equivalencia entre el medio electrónico y el documento en soporte papel y la no discriminación de los medios electrónicos.

Al respecto, enseña Illescas Ortiz[76] que "…*el significado de la regla de la equivalencia funcional debe formularse de la siguiente manera: la función jurídica que en toda su extensión cumple la instrumentación escrita y autógrafa –o eventualmente su expresión oral- respecto de cualquier acto jurídico lo cumple igualmente su instrumentación electrónica a través de un mensaje de datos, con independencia del contenido, alcance y finalidad del acto así instrumentado. La equivalencia funcional, en suma, implica aplicar a los mensajes de datos electrónicos una pauta de no discriminación respecto de las declaraciones de voluntad o ciencia manual, verbal o gestualmente efectuadas por el mismo sujeto: los efectos jurídicos apetecidos por el*

[76] ILLESCAS ORTIZ, Rafael, "Derecho de la Contratación electrónica" Ed. Civitas, España, 2001, pág.41.Esta autor recuerda que la primera formulación positiva de la regla tuvo lugar en el artículo 11.2 de la Convención de las Naciones Unidas sobre Garantías independientes y cartas de crédito contingente de 1995, el que establece: "La promesa podrá disponer, o el garante/emisor y el beneficiario podrán convenir en otra parte, que la devolución al garante emisor del documento que contenga la promesa, o algún trámite funcionalmente equivalente a esa devolución, de haberse emitido la promesa en forma que no sea sobre papel, será necesaria para la extinción del derecho a reclamar el pago".

emisor de la declaración deben de producirse con independencia del soporte escrito –eventualmente oral- o electrónico en el que la declaración conste".

Estos principios (equivalencia y no discriminación) constituyen dos caras de una misma moneda. Decir que el documento digital tiene el mismo valor probatorio que el documento escrito, o decir que una declaración de voluntad emitida mediante un mensaje de datos no puede ser discriminado jurídicamente por el sólo hecho de serlo, es defender, mediante técnicas diferentes, al nuevo medio de expresión.

2.3. Análisis de experiencias en Derecho Comparado

El primer antecedente de sanción de una ley vinculada con la temática que analizamos, lo encontramos en el Estado de Utah - Estados Unidos de América -, donde en el año 1995 se dictó una ley que regulaba la Firma Electrónica.[77]

Posteriormente, en el año 1996, la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional emitió una ley modelo, que sirve como guía para los distintos Estados al momento de regular la institución, siendo su principal misión eliminar los soportes materiales de los documentos por los cuales se instrumenten transacciones comerciales.

Por su parte, en Europa el primer país en reglar legalmente la firma electrónica fue Alemania[78], donde en el año 1997 se aprobó una ley que contempla el ya analizado concepto de criptografía asimétrica, como el equivalente funcional de los documentos electrónicos.

Posteriormente, en mayo de 1999 se dictó para la Comunidad Europea la Directiva sobre un Sistema Común para firmas electrónicas[79], la que debió ser transpuesta a los distintos estados al 19 de julio del 2003.

77 Ley Utah título 46, capítulo 3 (1996)- regula la firma electrónica sobre la base del sistema de criptografía, establece una autoridad licenciante de los certificadores, y reconoce efectos jurídicos a las firmas electrónicas homologándola a la firma manuscrita.-
78 Junto con la "Ley de Multimedia" (de la cual la Ley de firma digital constituyó el Artículo 3), la Ley fue debatida en el parlamento durante 1997 y sancionada como Ley el 1ro. de agosto de 1997. El objetivo y propósito de esta Ley fue crear las condiciones generales para las firmas digitales bajo las cuales se las pueda considerar seguras y que las falsificaciones de firmas digitales y las falsificaciones de información firmada puedan ser verificadas sin lugar a duda.
79 Directiva 1999/93/CE del Parlamento Europeo y del Consejo.

La normativa comunitaria impone a los Estados miembros la obligación de reconocer plenamente los efectos jurídicos y validez de la firma electrónica, siempre y cuando ésta cumpla los requisitos que en ella se explicitan.[80]

A) Firma electrónica en España

En España la aplicación de la Firma Digital fue temprana, siendo uno de los países pioneros en la utilización de la herramienta regulada en aquel momento por el Real Decreto-ley 14/1999. Fue uno de los primeros países de la Unión Europea que legisló la materia, incluso antes que la Directiva Europea sobre Firma Digital fuese oficialmente publicada.

El Marco normativo español está compuesto por:

1.- La Ley N° 34/2002 de servicios de la sociedad de la información y de comercio electrónico.

2.- La Ley N° 59/2003 de firma electrónica, por al cual se regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

3.- La Ley N° 56/2007, de Medidas de Impulso de la Sociedad de la Información.

La citada Ley N° 59/2003, clasifica a la Firma Electrónica distinguiendo tres tipos:

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

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

- La firma *electrónica reconocida*, descripta como "*…la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La firma electrónica reconocida tendrá respecto de los*

[80] Art. 5.1 de la Directiva 1999/93/CE.

datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel".

Vemos entonces que la firma electrónica reconocida es la única que tiene eficacia equivalente a la firma manuscrita.

En su normativa de aplicación, se define como *Certificados Reconocidos* a los certificados electrónicos expedidos por un Prestador de Servicios de Certificación que cumpla los requisitos establecidos por la Ley N° 59/2003 en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes, y a la fiabilidad y las garantías de los servicios de certificación.[81]

El Prestador de Servicios de Certificación es la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica. En la legislación española, la prestación de estos servicios no está sujeta a autorización previa, y se realizará en un régimen de libre competencia.[82]

Asimismo se prohíbe el establecimiento de restricciones para los servicios de certificación que procedan de otro Estado miembro del Espacio Económico Europeo.

Conforme lo dispuesto por el artículo 2.11 de la Directiva 1999/93/CE, los Proveedores de Servicios de Certificación, son "...*la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica. También son conocidos como prestadores de servicios de certificación o entidades de certificación."*

La Ley 59/2003 (art. 2) por su parte, los define como *"…la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica*."

Más allá de que los servicios de certificación no requieran licencia previa del Estado, deben cumplir con requisitos y obligaciones vinculados a estándares tecnológicos y políticas de seguridad, en pos de garantizar la confianza del sistema.

Entre los requisitos y obligaciones que deben cumplimentar los Prestadores de Servicios de Certificación, pueden citarse:

[81] Art. 11 Ley 59-2003
[82] ART. 5 Ley 59-2003

- No almacenar ni copiar los datos de creación de firma de la persona.

- Proporcionar al solicitante, antes de la expedición del certificado, la información mínima que establece la Ley de forma gratuita. (Declaración de Prácticas de Certificación y Políticas de Certificación).

- Mantener un directorio actualizado de certificados en el que se indiquen los certificados expedidos y su vigencia.

- Disponer de un servicio de consulta pública sobre la vigencia de los certificados que sea rápido y seguro.

Para aquellos Prestadores de Servicios de Certificación Reconocidos, la exigencia es aún mayor, debiendo:

- Disponer de las medidas técnicas y organizativas que garanticen la fiabilidad y seguridad de los servicios (hardware, software, procedimientos de operación y personal empleado).

- Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años.

- Constituir un seguro de responsabilidad civil (o garantía mediante aval bancario o seguro de caución) por un importe de al menos 3.000.000 de euros, para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados que expidan.

En cuanto a su responsabilidad, como principio general, los Prestadores responden civilmente por los daños y perjuicios que pudieran causar a sus usuarios o a terceros cuando actúen con negligencia en el cumplimiento de sus obligaciones.[83]

[83] Art. 26, Ley N° 59/2003.

En cuanto a su extensión, parte de la doctrina española[84] coincide que existen límites a la responsabilidad de los Prestadores, que pueden vincularse a su utilización, emitiendo el certificado únicamente para un uso determinado, excluyendo así su responsabilidad cuando el Certificado se aplique en alguna operación diferente; o bien a la cuantía, atento al importe hasta el cual podrán realizar operaciones los titulares de los Certificados emitidos.

En cuanto a la supervisión, conforme lo estipula el art. 29 de la Ley Española, el Estado, a través de la dependencia competente, controlará el cumplimiento por los prestadores de servicios de certificación de las obligaciones establecidas en la ley, y supervisará el funcionamiento del sistema.

En dicho marco, la Ley N° 17/2009, transposición de la Directiva 2006/123/CE, prevé que las Administraciones Públicas pongan en marcha un sistema de ventanilla única a través del cual los prestadores de servicios podrán llevar a cabo en un único punto, por vía electrónica y a distancia, todos los procedimientos y trámites necesarios para el acceso a las actividades de servicios y su ejercicio.

En este sentido, y a efectos de facilitar el uso transfronterizo de las ventanillas únicas con arreglo a la Directiva 2006/123/CE del Parlamento Europeo y el Consejo, relativa a los servicios en el mercado interior, se prevé que cada Estado miembro de la UE publique una «Lista de confianza» que contenga una información mínima referente a los prestadores de servicios de certificación que expidan certificados reconocidos al público, supervisados en ese Estado. Esta Lista debe cumplir las especificaciones técnicas recogidas en el Anexo de la Decisión de ejecución de la Comisión 2013/662/UE, por la que se modifica la Decisión 2009/767/CE en lo relativo al establecimiento, el mantenimiento y la publicación de listas de confianza de proveedores de servicios de certificación supervisados o acreditados por los Estados Miembros.

[84] DIAZ BERMEJO, Guillermo "*La Firma electrónica y los servicios de Certificación*". En publicación de Noticias Jurídicas (en línea) Diciembre 2007. Disponible en Internet: http://noticias.juridicas.com/articulos/20-Derecho-Informatico/200712-123456789.html

En el ámbito de la UE, los certificados de seguridad han sido expresamente definidos como: "...*la certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de ésta...*"[85].

La Ley española define al certificado electrónico en su artículo 6 como "…*un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad".*

Estos certificados son emitidos por los Prestadores de Servicios de Certificación o Autoridades de Certificación. Como ya se adelantara, al existir una firma electrónica general y otra cualificada, habrá, correlativamente *certificados ordinarios* y *certificados reconocidos*. Éstos últimos son certificados que ofrecen mayores garantías, ya que reúnen una serie de requisitos que aumentan su seguridad:

En el art. 11 de la referida Ley N° 59/2003 se establecen los datos que contendrá el certificado reconocido:

- La indicación de que se expiden como tales.
- El código identificativo único del certificado.
- La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.
- La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.
- La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellido completo y su número de documento nacional de identidad, o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.
- Los datos de verificación de firma que correspondan a sus datos de creación, que se encuentren bajo el control del firmante.
- El comienzo y el fin del período de validez del certificado.
- Los límites de uso del certificado, si se establecieran.

[85] Artículo 2.9 de la Directiva 1999/93/CE

- Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecieran.

Si los certificados reconocidos admiten una relación de representación deben incluir una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente[86].

En cuanto a su vigencia, los propios certificados indican la fecha y hora del inicio y de la finalización de su validez. El período de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma. En el caso de los certificados reconocidos este período no podrá ser superior a cuatro años.

Por regla general, los certificados serán revocados una vez que cumplan el período temporal de validez por el cual fueron creados. Sin embargo, también cabe la posibilidad de que el certificado sea objeto de una revocación anticipada, generalmente cuando la clave privada ha sido puesta en peligro (perdida o extraviada), por lo que puede ser utilizada por personas no autorizadas o para fines ilegítimos.

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

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

2. Resolución judicial o administrativa que lo ordene.

3. La existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los certificados contempladas en los párrafos c y g del art. 8 de la Ley.-

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

[86] art. 13 apartado 2 Ley 29-2003

Asimismo, la Ley 59/2003 reseña como otras causas de extinción, además del vencimiento del plazo por el que fueron emitidos, las siguientes:

- Revocación formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.
- Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por un tercero.
- Resolución judicial o administrativa que lo ordene.
- Fallecimiento o extinción de la personalidad jurídica del firmante; fallecimiento o extinción de la personalidad jurídica del representado; incapacidad sobreviniente, total o parcial, del firmante o de su representado; terminación de la representación; disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica.
- Cese en la actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos por aquél sean transferidos a otro prestador de servicios de certificación.
- Alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.
- Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

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

Respecto de la Autoridad Certificante Raíz, al no necesitar en el caso español autorización estatal para funcionar, la misma Autoridad emite su Certificado Digital, es decir que la entidad raíz se auto-firma su certificado de clave pública. De la misma forma, dentro de la jerarquía tiene la capacidad de emitir certificados para Autoridades de Certificación subordinadas e intermedias, y también podrá emitir Certificados al usuario.

B) Firma Digital en Brasil (ASSINATURA DIGITAL)

En Brasil, con el dictado del Decreto N° 3587 del 5 de septiembre de 2000, se instruye la creación de la infraestructura de Claves Públicas del Poder Ejecutivo Federal, mediante un sistema de Firma Digital basado en criptografía asimétrica, para ser usado en el sector de la Administración Pública Federal.

La Infraestructura de Firma Digital está regulada a través de una medida provisoria (nº 2.200-2), figura legislada en el art. 62 de la Constitución de la República Federativa de Brasil, por la cual se habilita al Presidente a dictar medidas provisorias por razones de necesidad y urgencia, debiendo dar inmediatamente intervención al Congreso. Cuentan con la misma fuerza que las leyes, resultando un equivalente a los Decretos de Necesidad y Urgencia propios de nuestro ordenamiento nacional.

Sancionada en el año 2001, aprueba la Infraestructura de Firma Digital con el objetivo de dotar de validez jurídica, y garantizar de integridad y autenticidad de documentos electrónicos y de las aplicaciones que utilicen Certificados Digitales.

La ICP- Brasil (Infraestructura chave publica do Brasil) está formada por la autoridad Gestora de Políticas, la Autoridad Certificante Raíz, las Autoridades Certificantes, y las Autoridades de Registro. Pero reconoce también Autoridades Certificantes independientes de la ICP Brasil[87], es decir, sin vínculos jerárquicos respecto de ella. Esto fue viable a raíz de una enmienda producida en la Medida Provisoria original, luego de que muchos sectores de la doctrina Brasilera criticaran el monopolio estatal de la actividad certificadora.

La Medida Provisoria designa como Autoridad Gestora de Políticas -lo que en nuestro ordenamiento se conoce habitualmente como Autoridad de Aplicación - al Comité

[87] Art. 10 2do párrafo MP 2.200-2/2001

Gestor de la ICP- Brasil, dependiente de la Presidencia de la República, que se encargará de:

1.- Adoptar las medidas necesarias y coordinar la implantación y funcionamiento de la ICP- Brasil.

2.- Establecer la política, criterios y normas técnicas para el licenciamiento de las Autoridades Certificantes, Autoridades de Registro y demás prestadores del servicio de soporte de ICP Brasil, en todos los niveles de la cadena de certificación.

3.-Establecer la política de certificación y las reglas operacionales de la Autoridad Certificante Raíz.

4.- Homologar, auditar y fiscalizar a la Autoridad Certificante Raíz y sus prestadores de servicios.

5.- Establecer directrices y normas técnicas para la formulación de políticas de certificados y reglas operacionales de la Autoridad Certificante y de las Autoridades de Registro y definir los niveles de la cadena de certificación.

6.- Aprobar las políticas de certificación, las reglas operacionales, y licenciar y autorizar el funcionamiento de las Autoridades Certificantes y las Autoridades de Registro.-

7.- Identificar y avalar las políticas de ICP externas, negociar y aprobar acuerdos de certificación bilateral, certificación cruzada, reglas de interoperabilidad y otras formas de cooperación internacional. Podrá certificar, cuando fuera el caso, su compatibilidad con la ICP Brasil, observando lo dispuesto en tratados o acuerdos internacionales.-

8.- Actualizar, ajustar y revisar los procedimientos y prácticas establecidas para la ICP Brasil, garantizando su compatibilidad, y promover la actualización tecnológica del sistema y su conformidad con las políticas de seguridad.

La función básica de la Autoridad Certificante Raíz es ejecutar las políticas de certificación y normas técnicas y operacionales aprobadas por el Comité Gestor, actuando en la emisión, expedición, distribución, revocación y gerenciamiento de Certificados Digitales de Autoridades Certificantes de nivel inmediatamente inferior al suyo, llamadas Autoridades Certificantes Principales. También se encarga de la lista de Certificados revocados, emitidos y vencidos, y de la fiscalización y auditoría de las

Autoridades Certificantes, Autoridades de Registro, o prestadoras de servicio de soporte habilitadas en el marco de la ICP- Brasil.

La Medida Provisoria designa al Instituto Nacional de Tecnología de la Información como Autoridad Certificante Raíz, dotándolo de autarquía. Está Integrado por un Presidente, una Dirección de Tecnología de la Información, una Dirección de Infraestructura de Clave Pública, y una Procuraduría general.

En ejercicio de sus atribuciones, tiene potestades fiscalizadoras y sancionatorias.

Las Autoridades Certificantes tienen competencia para emitir, expedir, revocar y gerenciar los Certificados, colocar a disposición de los usuarios las listas de Certificados Digitales revocados y mantener el registro de sus operaciones. El par de claves criptográficas emitido, será generado por el titular, y su clave privada de FD será de su exclusivo control, uso y conocimiento.

Son auditadas por la Autoridad Certificante Raíz antes de iniciar la prestación del servicio. Mediante una auditoría, se constatará que se cumplan con las exigencias previstas para la ICP- Brasil, y luego se les otorgará el licenciamiento.

Con posterioridad a su licenciamiento, también deben ser auditadas de manera anual, donde el Instituto verifica que se estén cumpliendo con las normas y exigencias impuestas por la legislación de la ICP Brasil.

Las Autoridades de Registro –al igual que en los sistemas ya descriptos- están operacionalmente vinculadas a determinada Autoridad Certificante. Les corresponde identificar y registrar a los usuarios de Certificados Digitales y son las responsables del proceso final en la cadena de Certificación Digital, atendiendo a los interesados en adquirir Certificados y recolectando la documentación pertinente. Son también auditadas por el ITI (Instrucción Normativa nº 07/2006).[88]

La Medida Provisoria, permite que sean Autoridad Certificante y Autoridad de Registro de la ICP- Brasil todos los órganos o entidades públicas y personas jurídicas de

[88]Web del Gobierno de Brasil, ver: http://www.iti.gov.br/images/icp-brasil/Normas%20ICP-Brasil/Documentos%20principais/DOC-ICP-03_Credenciamento_das_Entidades_Integrantes_da_%20ICPBrasil_Versao_4.6.pdf

Derecho Privado que cumplan con los requisitos establecidos por el Comité Gestor para licenciarse.

Las declaraciones de los documentos en formato electrónico producidos con la utilización de certificación en el marco de la ICP Brasil, se presumen válidos en relación a los signatarios en la misma forma en que lo determina el Código Civil. Esto significa que los Certificados emitidos por una Autoridad Certificante no perteneciente a la ICP Brasil, no tienen la misma investidura que los emitidos por una Autoridad Certificante que sí depende de ella.

En lo que hace al ámbito de la Administración Pública Federal, el Decreto N° 4414/2002 reglamenta la prestación de Servicios de Certificación Digital, estatuyendo que solamente mediante previa autorización del Comité Ejecutivo del Gobierno Electrónico los órganos y las entidades de la Administración Pública Federal podrán prestar o contratar servicios de Certificación Digital, debiendo hacerlo en el marco de la ICP- Brasil.-

Especial interés reviste el caso Brasileño, a nivel de derecho comparado, en relación con su organización federal. Su ordenamiento de competencias establece claramente que la sanción de la ley es competencia de la “unión” (Nación) ya que la firma es el medio por el cual se le confiere autenticidad a los documentos privados y públicos, y es materia civil. Ello es atribución de las autoridades nacionales, tanto desde el punto de vista normativo, como desde el punto de vista de su ejecución - al reglamentar una infraestructura de Claves Públicas -.

En el mismo sentido, los Estados locales (entendidos como equivalentes a las provincias en nuestra organización política) no pueden rechazar Autoridades Certificantes o de Registro sin violar las reglas de la ICP Brasil. Estas autoridades integran un sistema público centralizado que tiene como primera autoridad de la cadena a la Autoridad Certificadora Raíz. Así, los Estados reconocen en su normativa local de procedimientos administrativos, la validez de los Certificados emitidos respetando la infraestructura nacional.

3. NORMATIVAS PROVINCIALES

3.1. Identificación de la normativa provincial regulatoria de la Firma Digital, con infraestructura propia y sin ella

A) Provincias con Infraestructura de Firma Digital propia.

1.- Ciudad Autónoma de Buenos Aires

La Ciudad Autónoma de Buenos Aires adhirió a la Ley Nacional mediante la Ley N° 2751 del año 2008. Ese mismo año, dicta su Decreto Reglamentario Nº 1181/08.-

Por su intermedio, se designa como Autoridad de Aplicación a la Jefatura de Gabinete de Ministros del gobierno de la Ciudad Autónoma de Buenos Aires, como Autoridad Certificante a la Agencia de Sistemas de Información (art. 9 del Decreto Reglamentario) y como Autoridad de Registro a la Dirección General de la Escribanía General. El ámbito de aplicación se limita en principio al Poder Ejecutivo, pero en el art. 15 del Decreto Reglamentario se invita a los demás poderes a dictar las normas que resulten necesarias a fin de implementar la Firma Digital.

Ese mismo año 2008, mediante Decreto 417/08 se instituye la obligatoriedad de la utilización del correo electrónico institucional como medio de comunicación fehaciente para comunicaciones internas no productoras de efectos jurídicos directos – nuevamente se excluye así a los actos administrativos en sentido estricto -, entre organismos que integran la administración pública de la ciudad.

En el año 2009, a través de la Resolución 17/09 se establece la reglamentación para los procedimientos de solicitud, emisión, uso, renovación y revocación de los Certificados Digitales para el empleo de la Firma Electrónica[89], y se formula la Política de Certificación para el empleo de la misma en el ámbito del Gobierno de la Ciudad Autónoma de Buenos Aires.

En el año 2013 la Legislatura de la Ciudad Autónoma dicta la Ley N° 4.736 de Firma Digital del Gobierno de la Ciudad Autónoma de Buenos Aires, regulando la implementación de la misma en todo el sector público de la Ciudad de Buenos Aires.

[89] Al no contar aún la Ciudad con un Certificador Licenciado por el Ente Licenciante nacional, en el marco de la Ley N° 25.506, las herramientas que aplicaba carecían de uno de los requisitos necesarios para ser consideradas Firma Digital, formando parte entonces del género Firma Electrónica.

En su art. 3, designa al Poder Ejecutivo como licenciante y como encargado de implementar la Infraestructura de Firma Digital del Gobierno de la Ciudad Autónoma de Buenos Aires, coordinando con los Poderes Legislativos y Judicial su operatividad y puesta en funcionamiento.[90]

Mediante el Decreto N° 518/14 se estableció que la Secretaría Legal y Técnica será el Ente Licenciante del Gobierno de la Ciudad Autónoma de Buenos Aires, conservándose a la Agencia de Sistemas de información (ASI) como Autoridad Certificante. Las Autoridades de Registro serán la Dirección General de Escribanía General y la Dirección General de Mesa de Entradas, salidas y archivo, ambas dependientes de la Secretaría Legal y Técnica del Gobierno de la Ciudad de Buenos Aires.

Luego la Secretaría Legal y Técnica, en su calidad de Ente licenciante dictó la Resolución nº 283/14 que aprobó la política de certificación del Gobierno de la Ciudad Autónoma de Buenos Aires.

Los certificados emitidos por la Autoridad Certificante podrán usarse para la firma electrónica o cifrado de cualquier informe o documento, y como mecanismo de identificación ante servicios o aplicaciones informáticas implementados por el gobierno de la Ciudad Autónoma de Buenos Aires.-

Quienes podrán suscribir Certificados así emitidos serán:

1.- personas físicas que requieran un Certificado Digital del GCABA para su desempeño como funcionarios o agentes del Sector Público de la Ciudad de Buenos Aires

2.- personas físicas que requieran un Certificado Digital del GCABA para el ejercicio de los derechos y obligaciones que resulten de los procesos de contrataciones de bienes y servicios y de obra pública iniciados en el Sector Público de la Ciudad de Buenos Aires

[90] Art. 2º. Ley N° 4.736: Ámbito de Aplicación. La presente Ley es de aplicación a todas las dependencias del sector público de la Ciudad de Buenos Aires incluidas en las previsiones del artículo 4º de la Ley 70.
Art. 3º. Ley N° 4.736: Infraestructura de Firma digital. El poder Ejecutivo, en su carácter de licenciante, implementa la infraestructura de firma digital del Gobierno de la Ciudad Autónoma de Buenos Aires, que debe ser utilizada por la totalidad de las dependencias alcanzadas por esta Ley, conforme se establece en el artículo 2º, coordinando con los Poderes Legislativo y Judicial su operatividad y puesta en funcionamiento.

3.-personas físicas que requieran un Certificado Digital del GCABA para utilizar los servicios del Sector Público de la Ciudad de Buenos Aires.

Finalmente, cabe puntualizar que los certificados emitidos en el marco de la Política de Certificación del GCABA, verifican la autoría e integridad de:

a) documentos electrónicos presentados por personas físicas externas al Sector Público de la Ciudad de Buenos Aires.

b) documentos electrónicos emitidos por el Sector Público de la Ciudad de Buenos Aires.

Por el Decreto N° 589/09 se aprobó la implementación del Sistema de Administración de Documentos Electrónicos (SADE) como sistema de caratulación, numeración, seguimiento y registración de movimientos de todas las actuaciones y expedientes del Gobierno de la Ciudad Autónoma de Buenos Aires, como solución horizontal de Administración Electrónica. El Decreto designa a la Secretaría Legal y Técnica como administradora del SADE, y en consecuencia le atribuye las siguientes competencias:

- Administrar en forma integral el Sistema.
- Habilitar a los administradores locales.
- Actualizar el nomenclador de actuaciones y de tratas.
- Actualizar las tablas referenciales.
- Asignar usuarios y permisos.
- Auditar y controlar el funcionamiento, los usuarios y el ingreso de datos al sistema.
- Capacitar y prestar asistencia a los administradores locales del sistema.

Para la implementación y funcionamiento del SADE se facultó a la Secretaría Legal y Técnica a dictar las normas reglamentarias, aclaratorias y complementarias. Entre otras, se dictaron la Resolución N° 96-SECLyT-2009 y la Resolución N° 138/SECLyT/2010, que modifican el Reglamento para el inicio, ordenamiento, registro y circulación de expedientes y actuaciones administrativas, definiendo los tipos de

documentación administrativa que utiliza la Administración en los distintos procedimientos de gestión.

Posteriormente, el Decreto N° 765/10 instruyó a todos los organismos del Poder Ejecutivo de la Ciudad Autónoma de Buenos Aires a utilizar, del SADE, el módulo "Generador de Documentos Electrónicos Oficiales -GEDO" como medio de creación, registro y archivo de informes y providencias.

En ese marco, la Resolución N° 1/SECLyT/11 aprobó el reglamento para la Generación de Documentos Electrónicos Oficiales (GEDO) y el procedimiento para las altas, bajas y modificaciones de usuarios del SADE. Se estableció también que los Documentos Electrónicos Oficiales generados en GEDO son encriptados mediante tecnología de firma digital, utilizando identificación y clave de usuario y archivados en el repositorio único de imágenes del Gobierno de la Ciudad Autónoma de Buenos Aires. A su vez, quedó establecido que la Secretaría Legal y Técnica definiría las especies y subespecies de documentos iniciados en el Módulo "GEDO", conforme la incorporación de las nuevas herramientas de tecnología de firma digital al sistema.

Posteriormente, por el Decreto N° 6/11 se instruyó a todos los organismos del Poder Ejecutivo a utilizar del SADE, el módulo GEDO como medio de creación, registro y archivo de Disposiciones.

Así se llega al Expediente Electrónico, cuya implementación fue definida en el Decreto N° 196/11, en los términos del Plan de Modernización aprobado por la Ley 3.304. A fin de avanzar y completar lo dispuesto en el Decreto N° 6/11, el Decreto N° 424/12 instruyó a todos los organismos del Poder Ejecutivo a utilizar del SADE, el módulo GEDO como medio de creación, registro y archivo de Resoluciones.

La Ley de Ministerios N° 4.013 crea el Ministerio de Modernización, y reemplaza a la Jefatura de Gabinete como autoridad de aplicación del Plan de Modernización de la Administración Pública, facultándolo además para "*diseñar e implementar las políticas de incorporación y mejoramiento de los procesos, tecnologías, infraestructura informática y sistemas y tecnologías de gestión del Gobierno de la Ciudad Autónoma de Buenos Aires*". La misma norma define que le "*corresponde a la Jefatura de Gabinete de Ministros, en forma conjunta con el Ministerio de Modernización diseñar, coordinar y verificar la implementación de las políticas de gobierno electrónico y tecnologías de la información para el Poder Ejecutivo del Gobierno de la Ciudad*". La

Ley reserva a la Secretaría Legal y Técnica, entre otras, las acciones de "*organizar y administrar la Mesa General de Entradas, Salidas y Archivo del Gobierno de la Ciudad Autónoma de Buenos Aires y los Sistemas de Administración de Documentos Electrónicos"*, y "*entender en la planificación, administración y ejecución de la prestación de los servicios de producción gráfica y digital, formularios e impresos de las distintas reparticiones del Gobierno de la Ciudad Autónoma de Buenos Aires*".

De esta manera, muchas de las aplicaciones que utilizan la tecnología de Firma Digital derivan de una acción conjunta entre la Jefatura de Gabinete de Ministros, el Ministerio de Modernización y la Secretaría Legal y Técnica.

En la actualidad, varias normas han autorizado e impulsado el uso de Firma Digital. Entre ellas se destacan:

- Decreto 105/13 aplicar expediente electrónico a los proyectos de Ley a remitir por el Poder Ejecutivo a la Legislatura de la Ciudad Autónoma de Buenos Aires, y los proyectos de Ley sancionados por la Legislatura de la Ciudad Autónoma de Buenos Aires, comunicados al Poder Ejecutivo. El mismo acto instruye a la Secretaría Legal y Técnica, al Ministerio de Modernización y a la Jefatura de Gabinete de Ministros para que, en forma conjunta, adopten las medidas necesarias para que todos los documentos tramiten de conformidad a las normas y procedimientos aplicables al Expediente Electrónico.
- Decreto 398/13: dispuso, a partir del 1° de octubre de 2013, que los Decretos del Poder Ejecutivo, mensajes y proyectos de Ley con iniciativa legislativa del Poder Ejecutivo de la Ciudad Autónoma de Buenos Aires se suscriban con tecnología de firma digital. A su vez, encomendó al Jefe de Gabinete de Ministros y al Secretario Legal y Técnico, en forma conjunta, dictar las demás normas aclaratorias, interpretativas y complementarias que resulten necesarias para su implementación.

2.- San Luis

La provincia de San Luis Adhirió a la Ley Nacional mediante la Ley V-0591-2007 y DR 428- MP- 2008, designando a la Universidad de La Punta como Autoridad de

Aplicación del mencionado régimen legal, así como también Ente Licenciante de la Provincia de San Luis, lo cual constituye una particularidad a destacar por no tratarse de una dependencia de la Administración Pública central.

Por Resolución Rectoral Nº 2020013-ULP-2009, de fecha 2 de febrero de 2009, se creó en la órbita de la Universidad de La Punta, el Instituto de Firma Digital de la Provincia de San Luis al que se le asignaron las funciones de Ente Licenciante Provincial, encargado principalmente, de otorgar las licencias a los Certificadores y de supervisar su actividad.

En esta medida – constitución de un Ente Licenciante propio -, se advierte una clara contradicción con la Ley nacional, la cual seguramente se debe a que, aun cuando en el plano formal el Estado Provincial adhirió a la normativa nacional, no pudo conseguir la autorización que emite la Oficina Nacional de Tecnologías de Información (ONTI) para funcionar como Certificador Licenciado conforme lo establece el artículo 17 de la ley referenciada.

Así, al igual que en el caso de la CABA, resulta motivo de análisis la verdadera naturaleza de la herramienta reglamentada, ya que aun cuando a nivel local se la denomine como Firma Digital, lo cierto es que para la normativa nacional sus efectos se reducirían a los reconocidos a la Firma Electrónica, distinción que surge de los artículos 2 y 5 de la Ley N° 25.506.

B) Provincias sin infraestructura propia

1.- Neuquén

Adhirió a la Ley nacional por medio de la sanción de la Ley N° 2578, reglamentada por el Decreto N° 444/2011.

La normativa provincial, no organiza una infraestructura propia, sino que reconoce a la ONTI como Organismo Certificante (AC), designándose como Autoridades de Registro provinciales al Poder Judicial y a la Secretaria de Gestión Pública.

Su ámbito de aplicación está conformado por el Poder Judicial y el Poder ejecutivo, respectivamente.

2.- San Juan

Formuló su adhesión a la Ley Nacional mediante la sanción de la Ley N° 8128, del año 2010, reglamentada mediante el Decreto N° 1/2014.

El art. 5 del Decreto Reglamentario, instituye como Autoridad de Aplicación de la Firma Digital en el ámbito provincial a la Secretaría de Gestión Pública, a través de la Dirección General de Recursos Humanos y Organización, facultándola para constituirse en Autoridad de Registro de la Autoridad Certificante ONTI.

3.- Santa Fe

El 17 de marzo del año 2005, se firmó un Convenio de Cooperación en materia de Firma Digital entre la Subsecretaría de Gestión Pública de la Jefatura de Gabinete de Ministros de la Nación y el Gobierno de la Provincia de Santa Fe, aprobado por la Legislatura provincial mediante la sanción de la Ley N° 12.492.-

En diciembre de ese mismo año, y sobre las bases del Convenio citado, se sanciona la Ley de adhesión a la Ley Nacional de Firma Digital Nº 12.941.-

En ese derrotero, mediante la Resolución N° 0386/07 del Ministerio de Hacienda y Finanzas provincial, se designó como Oficiales de Registro de la Autoridad de Registro dependiente de la Autoridad Certificante ONTI, a la Dirección General de Recursos Humanos de la Provincia[91].

4.- Tierra del Fuego

Originariamente adhirió a la Ley Nacional mediante la sanción de la Ley Provincial Nº 633/2004. Esta ley nunca fue reglamentada, y finalmente, en el año 2013, se dictó la Ley N° 955 que implementó la Firma Digital en la Provincia.

Su reglamentación fue instrumentada a través del Decreto N° 1/2014, designándose como Autoridad de Aplicación a la Secretaría de Informática y telecomunicaciones (art. 2 del anexo del Decreto Reglamentario). Al igual que en los casos anteriores, se reconoce la infraestructura nacional y se designan como Autoridades de Registro,

[91] La ONTI, por Disposición N° 0015/07 convalidó las designaciones del personal de la Dirección General de Recursos Humanos de la Provincia como Oficiales de Registro.

dependientes de la Autoridad Certificante nacional ONTI, a los Poderes Ejecutivo y Judicial de la provincia.

5.- Tucumán

Adhirió a la normativa nacional mediante la sanción de la Ley N° 7.291, reglamentada por Decreto N° 1190/10. El marco provincial se limitó a reconocer la Infraestructura nacional, designándose como Autoridad de Registro de la Autoridad Certificante ONTI al Poder Judicial, a la Legislatura y a la Secretaría de Coordinación y Gestión Pública.

6.- Chaco

La Legislatura provincial sancionó la Ley de adhesión Nº 6.711 en el año 2010, reglamentándose a través del dictado del Decreto N° 99/11.

Reconoce en una primera instancia en su totalidad la Infraestructura nacional hasta tanto exista un Organismo provincial con licencia y en condiciones de certificar la Firma Digital, facultando a cada poder del Estado para que, a través del área de Recursos Humanos, se constituya en Autoridad de Registro. Así, hasta el día de la fecha, en este marco transitorio y según el listado actualizado de las Autoridades de Registro dependientes de la Autoridad Certificante ONTI, sólo se han constituido como Autoridad de Registro dentro de la Provincia el Poder Ejecutivo y el Poder Judicial.

Provincias que han adherido a la Ley Nacional de Firma Digital son:

Provincia	N°	Fecha de publicación
Buenos Aires	13666	02/05/2007
Ciudad de Buenos Aires	2751	15/07/2008
Formosa	1454	23/09/2004
Jujuy	5425	22/09/2004
La Pampa	2073	31/10/2003
Mendoza	7234	04/08/2004
Neuquén	2578	*S/D*
Río Negro	3997	20/10/2005
San Luis	V-0591-2007	*S/D*
Santa Fe	12491	21/12/2005
Tierra del Fuego	633	04/08/2004
Tucumán	7291	07/11/2003

4. El caso de la Provincia de Buenos Aires

Marco general

Al igual que lo que sucede a nivel nacional, en el ámbito provincial existen diversas normas relativas a la firma digital.

En primer lugar debemos mencionar la Ley N° 13.666 por la que se adhiere al régimen instaurado por la Ley nacional N° 25.506, con el propósito de asimilar al derecho local los institutos regulados por leyes nacionales que resulten necesarios a los efectos de garantizar la vigencia de la normativa de fondo. Esta ley se encuentra reglamentada por el Decreto N° 305, del 9 de mayo de 2012, derogatorio del Decreto N° 1388/08.

Por el decreto reglamentario se ha dispuesto que la autoridad de aplicación de la Ley N° 13.666 sea la Secretaría General de la Gobernación. [92]

La ley local señala como ámbito de aplicación a los Poderes Ejecutivo, Legislativo y Judicial de la provincia, los Municipios, la Administración Centralizada y Descentralizada, los Organismos de la Constitución, Entes Autárquicos y todo otro Ente en que el Estado Provincial o sus Organismos Descentralizados tengan participación suficiente para la formación de sus decisiones. La autoridad de aplicación ejercerá la coordinación de las acciones vinculadas a la implementación y utilización de la firma digital en el ámbito de aplicación de la ley.

Con respecto a los estándares tecnológicos y de seguridad aplicables, la Autoridad de Aplicación será la encargada de determinar dichos criterios, así como los procedimientos de firma, verificación, certificación y auditoria, los que deberán ser consecuentes con los utilizados por el Gobierno Nacional y las regulaciones internacionales.[93]

Por otra parte, el Decreto Reglamentario destina un artículo a la Infraestructura de Firma Digital del Gobierno provincial, la que estará conformada por Organismos Certificadores, Autoridades de Registro, titulares de certificados digitales y el conjunto de equipamiento, software, normas, políticas y procedimientos requeridos para la generación, almacenamiento y publicación de los Certificados Digitales.[94]

El Organismo Certificador previa autorización de la Autoridad de Aplicación, podrá inscribirse como Certificador Licenciado en los términos de la Ley Nacional Nº 25.506 y Decreto Reglamentario Nacional Nº 2.628/02. Para el cumplimiento de las

[92] Decreto N° 305/12, artículo 2°.
[93] Ley N° 13.666, artículos 3 y 4.
[94] Decreto N° 305/12, artículo 4.

responsabilidades a su cargo, el Organismo Certificador deberá delegar en Autoridades de Registro las funciones de recepción y registro de las presentaciones y trámites que le sean formuladas, y la validación de identidad y otros datos de los suscriptores de certificados.

En este punto, el decreto reglamentario designa a la Secretaría General de Gobernación como Organismo Certificador para la Administración Pública Provincial central, autorizándosela a requerir su reconocimiento como Certificador Licenciado.[95]

En cuanto a los certificados digitales, el artículo 7 de la Ley determina que las certificaciones para agentes de la Administración Pública Provincial y Municipal, destinados a la gestión interna de los Organismos, y la Certificación de particulares para cumplimiento de trámites ante la Administración Pública Provincial y Municipal, con la correspondiente generación de la clave pública, serán emitidas por el Organismo Provincial ya aludido.

Sin perjuicio de ello, la Secretaría General de Gobernación podrá reconocer certificados de particulares emitidos por certificadores de otras jurisdicciones para la realización de trámites ante la Administración Pública Provincial y Municipal, mediante la firma de convenios con otras jurisdicciones para el reconocimiento recíproco de certificados emitidos por sus propios certificadores.

La titularidad de los Certificados Digitales podrá recaer en todos los agentes y funcionarios del Estado Provincial, así como las personas físicas o jurídicas que se relacionen con la misma.[96]

Por último, se establece que las Autoridades de Registro asociadas a Organismos Certificadores Licenciados, sean éstos provinciales o nacionales, podrán ser constituidas previa notificación a la Secretaría General de Gobernación; y finalmente designa a la Dirección Provincial de Personal de la Provincia de Buenos Aires y sus Delegaciones Sectoriales como Autoridad de Registro para el ámbito de la Administración Pública Provincial central.[97]

2.- Modificaciones introducidas por el Decreto N° 305/12

[95] Decreto N° 305/12 artículo 8.
[96] Decreto N° 305/12 artículo 7.
[97] Decreto N° 305/12 artículo 10.

Como enunciáramos anteriormente el Decreto N° 305/12 vino a reglamentar la Ley N° 13.666, derogando de ese modo la anterior reglamentación del citado cuerpo legal, que había sido dispuesta por Decreto N° 1388/08 del Poder Ejecutivo Provincial.

Nos propondremos en este acápite analizar los cambios introducidos por la nueva reglamentación, a la luz del régimen que estaba anteriormente vigente.

No se observan cambios en lo que respecta a los estándares tecnológicos y de seguridad aplicables y a los procedimientos de firma, verificación, certificación y auditoría, ya que en ambos supuestos se previó que estuvieran en consonancia o conformidad con los utilizados a nivel nacional y las regulaciones internacionales (artículos 2 y 5 del Decreto N° 1388/08 y artículo 3 del Decreto N° 305/12).

Con relación a la Infraestructura de Firma Digital no se registran alteraciones sustanciales, toda vez que la misma está integrada por similares elementos: a) Organismos Certificadores, b) Autoridades de Registro, c) titulares de certificados digitales y d) el conjunto de equipamiento, software, normas, políticas y procedimientos requeridos para la generación, almacenamiento y publicación de los certificados digitales. Sólo se advierte que el Decreto N° 1388/08 se refiere a la figura de Autoridad Responsable de la Infraestructura Tecnológica (Dirección Provincial de Comunicaciones, conforme lo establecido en los artículos 26 y 27 del referido Decreto), cuestión soslayada en su similar N° 305/12. Sin perjuicio de ello, estimamos que esta omisión resulta irrelevante en la medida que el Decreto N° 666/12 asigna a la Dirección Provincial de Sistemas de Información y Tecnologías la responsabilidad de asistir al Secretario General y a las restantes áreas que integran la jurisdicción, así como a los restantes organismos y jurisdicciones que integran la Administración Pública Provincial y Municipal, en los asuntos vinculados al desarrollo de la Firma Digital Ley Nº 13.666, su reglamentación y dictado de normas modificatorias y complementarias en lo que hace a la competencia de sistemas y tecnologías.

Adentrándonos ya en el terreno de las diferencias, debemos señalar fundamentalmente que el Decreto derogado preveía la existencia de un Certificado Digital Raíz del Estado Provincial, el cual daba origen y sostén a la infraestructura de firma digital. El titular de dicho Certificado resultaba ser el Poder Ejecutivo Provincial y su administración quedaba a cargo de la Autoridad de Aplicación (Secretaría General de la Gobernación).

También se hablaba de un Certificado Digital Raíz del Organismo Certificador, el cual era asignado por el Administrador del Certificado Digital Raíz del Estado Provincial. Conforme surge del artículo 17 del Decreto derogado la Escribanía General de Gobierno de la Provincia de Buenos Aires era la autoridad designada como Organismo Certificador para todo el ámbito de aplicación descripto en el artículo 2 de la Ley. Es decir que era una autoridad única para todo el Poder Legislativo y Judicial, Municipios, Administración Centralizada y Descentralizada, Organismos de la Constitución, Entes Autárquicos y todo otro Ente en el que el Estado Provincial - o sus Organismos Descentralizados - tuviera participación suficiente para la formación de sus decisiones.

Luego cada Poder debía designar, en el ámbito de su competencia, al Organismo que cumpliría en rol de Autoridad de Registro, para los agentes y funcionarios de su jurisdicción (artículo 20). En el ámbito del Poder Ejecutivo se asignó dicha función a la Dirección Provincial de Personal de la Provincia de Buenos Aires, y como Autoridades de Registro de cada Repartición, a sus Delegaciones Sectoriales (artículo 21).

Esta mención al Certificado Raíz provincial, ponía a la provincia en una situación similar a los casos analizados anteriormente de la Ciudad Autónoma de Buenos Aires y de la provincia de San Luis, ya que aun cuando legislativamente se hubiese adherido a la normativa nacional, cierto es que el sistema provincial escapaba a sus previsiones basándose en un certificado primigenio que no había sido emitido por el ente Licenciante nacional.

Es decir que, conforme la ley nacional de Firma Digital, los certificados emitidos por las Autoridades Certificantes que se constituyeran a nivel provincial, no serían válidos como Firma Digital, sino que caerían en el género Firma Electrónica, no contando por ello – fuera del ámbito de la provincia de Buenos Aires – con las presunciones que otorgan seguridad jurídica a transacciones informáticas firmadas digitalmente.

Para subsanar dicha incongruencia, el Decreto N° 305/12 modificó las cuestiones apuntadas evitando la mención al concepto de Certificado Digital Raíz del Estado Provincial propio del anterior Decreto.

La actual reglamentación (artículo 8) se designa como Organismo Certificador para la Administración Pública central a la Autoridad de Aplicación (Secretaría General de la Gobernación).

Asimismo, el artículo 7 encomienda a la Autoridad de Aplicación la designación de los Organismos que actuarán como Organismos Certificadores Licenciados en los términos de la Ley Nacional Nº 25.506 para el ámbito de aplicación de la Ley Nº 13.666, estableciendo que los Organismos designados serán autorizados por la Autoridad de Aplicación para requerir su reconocimiento como Certificadores Licenciados ante la autoridad nacional competente, en el plazo que la misma fije al efecto.

También se dispone (artículo 8 *in fine*) que la Autoridad de Aplicación podrá desempeñarse como Organismo Certificador Licenciado respecto de cualquiera de los entes enumerados en el artículo 2° de la Ley Nº 13.666 que así lo requieran.

La infraestructura descripta, nos permite entonces advertir nuevas diferencias respecto de la reglamentación anterior. En el régimen anterior el Organismo Certificador (Escribanía General de Gobierno) era único para todo el ámbito de aplicación de la Ley, y por ende el mismo para todos los poderes que sólo podían designar sus Autoridades de Registro; mientras que el actual permite la constitución de otros Certificantes Licenciados ante las autoridades nacionales, previa autorización de la Autoridad de Aplicación.[98]

3.- Resolución SG N° 23/13[99]. Prueba Piloto de Firma Digital

Con la finalidad de avanzar en la sensibilización de los agentes y funcionarios que componen la Administración provincial, la Secretaría General de la Gobernación diseñó en el año 2013 una prueba piloto, -aprobada mediante el dictado de la Resolución SG N° 23/13 - por la cual se constituyó, a través de la Dirección Provincial de Sistemas de Información y Tecnologías, en Autoridad de Registro dependiente del Certificador Licenciado ONTI (de nivel nacional, como ya se explicara anteriormente).

Este proyecto, tal como se desprende de la motivación de la Resolución que lo origina, tiene como objetivo avanzar en el proceso de digitalización de los

[98] En el régimen actual cada poder puede establecer y solicitar el reconocimiento de su propio Organismo Certificador, previa autorización de la Secretaria General de la Gobernación y siempre que se obtenga el dictamen favorable del ente licenciante raíz (Jefatura de Gabinete de Nación), tal como acontece en el expediente actualmente en trámite bajo el N° 2100-13558/12
[99] B.O. 25-09-2013.

procedimientos administrativos y servicios que brinda la Administración Pública provincial, a través de la progresiva utilización de la tecnología de Firma Digital, con un horizonte temporal de dos años estimado suficiente para lograr la estabilización de la infraestructura necesaria para constituirse la propia Secretaría General en Autoridad Certificante, tal como se reglamentara oportunamente.

Al respecto, debe destacarse que, en virtud de la atribución conferida por el artículo 2° del Decreto N° 305/12, le corresponde a la Secretaría General de la Gobernación – como Autoridad de Aplicación - coordinar las acciones tendientes a implementar la utilización de Firma Digital en el ámbito de aplicación definido por el artículo 2° de la Ley Nº 13.666, quedando facultada para el dictado y aprobación de la normativa que resulte necesaria a tal efecto.

Es en virtud de dichas atribuciones es que se procedió al desarrollo de la prueba piloto, la cual no hace más que generar una instancia transitoria a los efectos de dotar de plena validez y eficacia jurídica a los certificados digitales a ser utilizados durante su transcurso, permitiendo en forma inmediata obtener avances en la despapelización y digitalización de las comunicaciones internas de la administración y la prestación de servicios a los ciudadanos, en un esquema similar al aplicado en los casos ya analizados de provincias que no cuentan con infraestructura propia.

Tales adelantos, constituirán un cúmulo de información y experiencia que permitirán un paso no traumático hacia la generalizada utilización de la Firma Digital, una vez que la Secretaría General de la Gobernación se encuentre habilitada por el Ente Licenciante nacional para operar como Certificador Licenciado.

ALTERNATIVA

En virtud de los antecedentes reseñados, y el estado actual de las gestiones tendientes a la implementación de la tecnología de firma digital, se pone a consideración una alternativa que busca el cumplimiento de los siguientes objetivos para el período 2014 – 2015:

- *OBJETIVO GENERAL*

  Extender el uso de la tecnología de firma digital en el ámbito de la Administración Pública provincial, orientándola a la mejora de procesos internos y organizacionales, así como a la prestación de servicios a los ciudadanos.

- *OBJETIVOS ESPECÍFICOS*

  A. Propiciar la gestión y administración masiva de documentos electrónicos, avanzando en la digitalización de la comunicación de los documentos administrativos de uso corriente, facilitando la despapelización y avanzando hacia el expediente digital.
  B. Incorporar progresivamente la tecnología de Firma Digital a los procesos de creación, registración, comunicación y archivo de los actos administrativos.
  C. Brindar asistencia técnica (funcional y tecnológica) a los Organismos de la Administración Pública Provincial, Organismos de la Constitución, Entes Descentralizados y Municipios para el diseño, desarrollo y puesta en producción de aplicaciones de firma digital en sus procesos de gestión.

En tal sentido, se proponen una serie de cambios en las estructuras y dispositivos institucionales vigentes, a fin de establecer mecanismos de coordinación e implementación conjunta que permitan avanzar rápidamente hacia el uso masivo de la tecnología de Firma Digital.

- SECRETARÍA GENERAL DE LA GOBERNACIÓN

De acuerdo al Decreto N° 666/12, distintas dependencias de la Secretaría General cuentan con acciones destinadas a intervenir dos áreas clave para dar impulso al proceso en cuestión:

- *Firma Digital*: la Subsecretaría para la Modernización del Estado, por intermedio de la Dirección Provincial de Gestión Pública, la Dirección de Innovación en la Gestión y la Dirección de Seguimiento y Evaluación de la Gestión, debe entender en el desarrollo de la Firma Digital. Por otro lado, la Dirección Provincial de Sistemas de Información y Tecnologías (DPSIT) tiene la responsabilidad de asistir al Secretario General y a las restantes áreas que integran la jurisdicción, así como a los restantes organismos y jurisdicciones que integran la Administración Pública Provincial y Municipal, en los asuntos vinculados al desarrollo de la Firma Digital Ley Nº 13.666, su reglamentación y dictado de normas modificatorias y complementarias en lo que hace a la competencia de sistemas y tecnologías. A través de la Dirección de Desarrollo de Sistemas y Asistencia Técnica debe elaborar, desarrollar, asistir y controlar la implementación de programas y proyectos relacionados con la Firma Digital, en coordinación con la Dirección de Innovación en la Gestión Pública. Tal como se indicó previamente, la Resolución N° 23/13 del Secretario General aprueba el desarrollo de la Prueba Piloto de Firma Digital, estableciendo además que la elección de las aplicaciones y/o procedimientos administrativos a los que se incorpore Firma Digital en el marco de la Prueba Piloto, serán oportunamente individualizados y aprobados por Resolución del Secretario General de la Gobernación. La DPSIT será la Autoridad de Registro de la ONTI, y estará encargada de conformar unidades de asesoramiento técnico en materia de Firma Digital para aquellos Municipios.
- *Sistema de Expedientes*: la Dirección de Sistemas y Asistencia Técnica de la DPSIT debe desarrollar y mantener en adecuado funcionamiento un sistema único de mesa de entradas de la Administración Pública Provincial. La Subsecretaría para la Modernización del Estado debe entender en el desarrollo e implementación del Sistema Único de Mesa

de Entradas y en el Sistema Único de Seguimiento de Expedientes, ello en el marco de la oferta de servicios digitales al ciudadano y a los organismos que integran la Administración Pública Provincial. Por medio de la Dirección de Innovación de la Gestión tiene que participar y colaborar con la Dirección de Desarrollo de Sistemas y Asistencia Técnica de la DPSIT en el desarrollo de un sistema único de mesa de entradas y un sistema único de seguimiento de expedientes, y coordinar su implementación desde la perspectiva de la gestión pública.

Cabe mencionar que, de manera general, la DPSIT debe evaluar e intervenir en el dictamen de los planes, programas y proyectos en materia de incorporación y difusión del uso de sistemas de información y tecnologías en el ámbito de la Administración Pública Provincial.

Se propone que la Secretaría General de la Gobernación, en conjunto con la SLyT y el Ministerio de Jefatura de Gabinete de Ministros (MJGM), propicie los siguientes avances y modificaciones:

- Revisión del Decreto N° 300/06 y N° 2200/06: a fin de establecer los tipos de documentación administrativa que utiliza la Administración en los distintos procedimientos de gestión, y contemplar el soporte digital.
- Revisión del Decreto N° 16236/54 de Reglamento para las Mesas de Entradas y Salidas de la Administración Provincial sobre Numeración Única y Carátula Uniforme para Expedientes: a fin de elaborar un nuevo Reglamento para el inicio, ordenamiento, registro y circulación de expedientes y actuaciones administrativas, adaptado a los tiempos que corren y las tecnologías disponibles.
- Implementación, en conjunto con la SLyT, de un nuevo Sistema de Gestión Interna de Documentación, que combine seguimiento y gestión de actuaciones y documentos, y permita avanzar hacia la implementación del expediente electrónico, en un reemplazo gradual del sistema vigente.

- SECRETARÍA LEGAL Y TÉCNICA

La Secretaría Legal y Técnica, de acuerdo a lo establecido en el Decreto N° 218/10 cumple en asistir en materia legal y técnica a la actividad administrativa de la Provincia. En ese marco, le corresponde llevar tanto el despacho de los actos de alcance general y particular que se sometan a consideración del Poder Ejecutivo, analizando y ordenando su trámite, como así también evaluar y elaborar, en su caso, proyectos de actos administrativos, anteproyectos de ley, iniciativas y convenios que le encomiende el Señor Gobernador. Asimismo, en el ámbito específico de las relaciones entre el Poder Ejecutivo y Legislativo, es el organismo encargado de tramitar los anteproyectos y proyectos de ley sancionados.

Se encarga a su vez de llevar el registro y protocolización de los actos administrativos individuales y generales, los actos de promulgación de leyes (o, en su caso vetos), los actos de funcionarios en ejercicio de competencia delegada, como así también los convenios. Adicionalmente, interviene con carácter previo a la celebración de pactos, convenios, protocolos, tratados y cualquier otro acuerdo que suscriba el Poder Ejecutivo.

En una función transversal, cumple también el rol de coordinar el control de gestión general de los aspectos legales, técnicos, normativos y jurídicos de las distintas áreas de gobierno, en cuyas tareas es el organismo encargado de mantener las relaciones funcionales del Poder Ejecutivo Provincial con Asesoría General de Gobierno y los Organismos de la Constitución.

A fin de cumplir acabadamente con estas acciones, la SLyT ha avanzado decididamente en procesos de modernización y mejora de la gestión[100], los que han sido incluso plasmados en un Plan Estratégico de Sistemas de Información y Tecnología (PESIT). A fin de potenciar la implementación de Firma Digital en la Provincia por medio de mejoras en la coordinación e implementación conjunta, la experiencia comparada indicaría que podrían llevarse adelante las siguientes modificaciones:

- ❖ Organizar y administrar, conjuntamente con la Subsecretaría para la Modernización del Estado, y la Dirección Provincial de Sistemas de Información y Tecnologías (DPSIT), los Sistemas de Administración de

[100] Para mayor información, acceder a http://www.tecno.slyt.gba.gov.ar/

Documentos Electrónicos. La SLyT, habiendo diseñado, instalado y puesto en práctica un Sistema de Gestión Interna de Documentación, debería impulsar su adaptación y escala a toda la administración pública provincial, gradualmente. Para ello, podría administrar conjuntamente con la DPSIT el nuevo Sistema Provincial de Gestión Documental, con facultades para dictar todas las normas reglamentarias, aclaratorias y complementarias, así como la definición de los actos administrativos que, paulatinamente, incorporen la tecnología de firma digital, y la tramitación del expediente electrónico.

- *Impulsar, junto con la SG, la aprobación del Expediente Electrónico*: una vez avanzada la implementación del Sistema de Gestión Interna de Documentación, y la implementación de Firma Digital, la SG, como Autoridad de Aplicación definida Decreto N° 305/12, junto con la SLyT, deberán propiciar el dictado de una norma que dé inicio al Expediente Electrónico. La SG establecerá los estándares tecnológicos y de seguridad aplicables, los procedimientos de firma, verificación, certificación y auditoría, y la SLyT dictará todas las normas reglamentarias, aclaratorias y complementarias correspondientes a esta nueva modalidad.

- *Modificación de la Dirección de Registro Oficial* [101]: otorgándole las acciones de coordinar las actividades de guarda y custodia de los textos originales de las Leyes, Decretos, Resoluciones y documentos públicos; conformar y actualizar en forma permanente la base de datos de normativa provincial que constituye el Registro Oficial, coordinando conjuntamente con la Dirección de Planificación, las acciones para el acceso, la consulta y la difusión de legislación bonaerense en el marco del sistema de informática jurídico-legal; administrar la publicación del Boletín Oficial e implementar su difusión por los medios oficiales de comunicación. De esta manera, pasaría a ser la *Dirección de Registro y Boletín Oficial*, incorporando la estructura de la Dirección de Boletín

[101] Este modelo se corresponde con aquellos dispuestos para las Secretarías Legal y Técnica, o dependencias que hacen sus veces, en Ciudad de Buenos Aires; Tierra Del Fuego; Santa Cruz; Formosa; Salta; Tucumán; San Luis; Rio Negro; Córdoba; y Mendoza, entre otras.

Oficial, Subdirección de Boletín Oficial, y el Departamento Agencias de Boletín Oficial de la Subsecretaría de Gobierno del Ministerio de Jefatura de Gabinete de Ministros. La SLyT podrá entonces determinar un Régimen de Publicación del Boletín Oficial, incorporando el uso de la Firma Digital a su edición electrónica, y al sistema de informática jurídico-legal.

- *Incorporación a la Dirección de Planificación:* agregar el *Departamento Boletín Oficial Electrónico e Informática Jurídica*, y la *Subdirección De Informática Jurídico Legal*, a fin de organizar y mantener la base de datos que constituye el servicio de biblioteca y búsqueda virtual de normativa provincial; verificar el ingreso, la carga y puesta en línea de las ediciones del Boletín Oficial para su difusión electrónica; actualizar en forma permanente la temática y vigencia de normas sancionadas en la Provincia.

- MINISTERIO DE JEFATURA DE GABINETE DE MINISTROS

El Ministerio de Jefatura de Gabinete de Ministros (MJGM), en cumplimiento de lo dispuesto en la Ley 13.757 debe, entre otras cuestiones, asistir al Gobernador de la Provincia en la coordinación con los diferentes Ministerios, Secretarías y demás organismos, comisiones y acciones interministeriales, así como también coordinar la relación entre las distintas reparticiones ministeriales, secretarías y organismos de la administración provincial, centralizada y descentralizada; proponer la creación de Comisiones interministeriales o de cualquier nivel de integración, que hagan a la mejor ejecución y coordinación de los planes, programas y proyectos emanados del Poder Ejecutivo; y diseñar, coordinar y evaluar los programas interministeriales, interorganizacionales e interjurisdiccionales, en concurrencia con las áreas con competencias afines.

En el marco de la presente propuesta, el MJGM debería efectuar las siguientes acciones y adecuaciones:

- Conformación de una Comisión o Mesa Interministerial para la Implementación de la Firma Digital y el Expediente Electrónico, integrada por representantes de SG, SLyT, MJGM y aquellas

Jurisdicciones de la Administración Pública Provincial que se encuentren interesadas en el avance de estas soluciones.

- *Adecuación de la Dirección Provincial de Impresiones del Estado y Boletín Oficial*: como contrapartida a las modificaciones de la SLyT. Mantendría toda la estructura y acciones que corresponden a Impresiones del Estado, modificando su denominación a "Dirección Provincial de Impresiones del Estado", con las siguientes dependencias: Subdirección Administrativo Contable; Departamento Contable y Financiero; Departamento Administrativo y Personal; Dirección de Impresiones Y Publicaciones del Estado; Subdirección de Gestión Integrada de Salud y Seguridad Ocupacional, Medio Ambiente y Gestión de la Calidad; Departamento de Salud; Departamento Medio Ambiente Laboral e Higiene y Seguridad en el Trabajo; Departamento Gestión de la Calidad; Departamento Diseño Grafico; Departamento Programación de la Producción; Departamento General de Talleres; Departamento Escuela de Aprendices; Departamento de Impresiones de Seguridad; Dirección De Gestión Comercial; Departamento de Comercialización.

- CONSEJO PROVINCIAL PARA LA SOCIEDAD DE LA INFORMACIÓN

El Decreto N° 110/08 crea el Consejo Provincial para la Sociedad de la Información (CPSI), derogando el Plan Estratégico de Gobierno Electrónico para la Provincia de Buenos Aires (Decreto N° 1824/02). El CPSI incorporó a las distintas jurisdicciones del Poder Ejecutivo con incumbencia en cuestiones tecnológicas, así como también se invitó a participar a actores sociales, económicos y académicos, en pos de "proponer al Poder Ejecutivo una agenda de orientaciones estratégicas destinada a promover que los ciudadanos, las empresas, las organizaciones de la sociedad civil y el Gobierno alcancen, mediante la incorporación de las Tecnologías de la Información y la Comunicación (TICs), la transformación de los tradicionales mecanismos de gestión del Estado, la resolución de urgencias sociales aumentando la competitividad industrial y la generación de empleo calificado, a fin de lograr una sociedad más equitativa, integradora y democrática"[102]

[102] Artículo 1 del Decreto Nº 110-08

En este contexto, parecían quedar definidos los elementos necesarios para el desarrollo de una Estrategia de Gobierno Electrónico, una Agenda Digital, como parte de un proyecto de Provincia, y como una política pública de Estado que, por su propia naturaleza, requiere del alcance de ciertos consensos básicos. Sin embargo, no se avanzó más allá de la formulación de intenciones y objetivos generales, y no pudieron elaborarse a partir de ellos iniciativas concretas que alimenten la Agenda Digital del Gobierno de la Provincia de Buenos Aires. El trabajo del CPSI se vio entorpecido por una serie de factores (internos y externos) que fueron diluyendo su actividad.

Por el lado de las dificultades internas, resultó sumamente difícil comprometer a todos los actores involucrados en un esquema de trabajo sostenido. En el caso de los representantes de la Administración, salvo excepciones, no llegaban a comprender del todo la importancia del tema, y debían dedicar parte de su tiempo a una actividad extraña a sus funciones habituales. Además, la estructura del CPSI hacía necesario que el impulso del trabajo proviniera de la SG, pero dificultades políticas y de gestión fueron relegando al Consejo a un lugar cada vez menos importante. Ello sumado a que no existía un equipo de trabajo dedicado exclusivamente a las tareas derivadas del CPSI. Si bien el modelo aplicado siguiendo el caso chileno sentaba sus bases en la multisectorialidad, careció de un equipo de profesionales y expertos en la materia que tuvieran dedicación exclusiva e incentivos para llevar adelante una tarea compleja y de largo plazo, como sí existe en Chile, lo cual tornaba aún más difícil la continuidad de las acciones.

El interés original de algunas Cámaras y empresas del sector fue disminuyendo, quizá como resultado de la poca continuidad del trabajo, o bien porque tomaron conciencia que no se trataba de un espacio en el cual aparecerían oportunidades comerciales con la Provincia. Algo similar ocurrió con el gremio de los trabajadores estatales, cuyos miembros desde el primer momento participaron de los encuentros, pero solían manifestar cuestiones y reclamos que estaban fuera de los objetivos del CPSI. Ello generaba discusiones y planteos que no colaboraban con el trabajo de definición de una Agenda Digital.

Como resultado final, las expectativas originales no fueron satisfechas, y que no fue posible siquiera contar con la aprobación del Reglamento Interno, o un óptimo

funcionamiento del foro, ya que sólo se publicó la información de contacto de los coordinadores de las Comisiones, sus objetivos, careciendo por completo de actualización.

Al no registrarse avances en las actividades del CPSI, debería evaluarse la conveniencia de derogar el Decreto N° 110/08, o modificarlo, en pos de una estructura dinámica puesta al para la obtención resultados concretos en materia de aplicación de nuevas tecnologías.

CONSIDERACIONES FINALES

Hemos procurado a lo largo de la investigación realizada analizar los aspectos técnicos y legales vinculados a la firma digital, con el objetivo de comprender cabalmente el instituto, emprendiendo luego la tarea de relevar la realidad de su aplicación a nivel provincial.

Como corolario de ello, podemos afirmar que si bien los avances han sido sustanciales a lo largo de la última década, no se ha conseguido aún la utilización generalizada de los sistemas electrónicos de identificación que aseguren la mayor velocidad de las transacciones entre privados, así como una eficiencia creciente en la prestación de servicios por parte de la administración pública.

Sin duda ello se debe a múltiples factores que exceden al marco de este trabajo, sin perjuicio de los cual podemos señalar, como ruta para futuros estudios complementarios, la necesidad de clarificar la naturaleza de las disposiciones legales vinculadas con la firma digital y, derivado de ello, la instancia regulatoria – nacional o local – a la cual le compete su dictado y organización.

Claro es que, allí donde nos encontramos ante transacciones entre particulares, la firma digital se comporta como un instituto de fondo, resultando el legislador nacional su natural regulador.

Pero mayores dificultades ha suscitado su utilización por las autoridades locales en el ejercicio de función administrativa, ello en razón de las competencias atribuidas por el marco regulatorio de la firma digital a órganos que conforman la administración nacional, sujetándose, a primera vista la implementación de la firma digital en los procedimientos locales a determinados requisitos de autorización ante

entes nacionales que pueden resultar contradictorios con el carácter local de los procedimientos administrativos.

En una primera aproximación al tema, podríamos aventurar que la invitación sin más a adherir que efectuó el legislador nacional a las jurisdicciones locales, sólo podría referirse a preceptos de carácter administrativo, ya que tratándose de cuestiones de fondo, ninguna necesidad existe para ello.

Ahora bien, en aquello que hace los actos que vinculen a los particulares con los gobiernos locales en ejercicio de función administrativa, no debemos perder de vista que todo aquello atinente a su regulación resulta exclusivo resorte de las autoridades provinciales, debiendo por ello la normativa de fondo – de carácter nacional – evitar interferir en dicha autonomía mediante la imposición de trámites y autorizaciones que no hacen a la naturaleza del instituto regulado.

En función de ello, dado el inevitable cruce de competencias regulatorias de distinto nivel, y la dispar aplicación de la herramienta, según se trate de actos de derecho privado o administrativos, resultaría adecuada una revisión integral del sistema que considere la experiencia recogida y, mediante mecanismos de concertación federal, proyecte alternativas superadoras de las dificultades constatadas.

Este punto debe ser profundizado, no por un mero apego a las cuestiones teóricas, sino porque del relevamiento efectuado acerca de la evolución local de la utilización de la firma digital surge que allí se han suscitado las más arduas discusiones, marchas y contramarchas, demorándose el objetivo común de agilizar los servicios que se brindan al ciudadano.

BIBLIOGRAFÍA

- AIRTON, Roberto Guelfi. "Análise de elementos jurídico – tecnológicos que compoem a assinatura digital certificada digitalmente pela Infra-estrutura de chaves publicas do brasil –ICP- Brasil." Universidade de sao Paulo. Escola Politécnica. Sao Paulo 2007.-

- ARAUJO CASTRO, Aldemario. "O Documento eletrônico e a assinatura digital (Uma visão geral). Disponible en: www.aldemario.adv.br/doceleassdig.htm

- Autoridad Certificante de la Administración pública. https://pki.jgm.gov.ar/app/

- BARBERÁN, BARBERÁN, BONTEMPO, LENS, PEREZ WILIAMS, SCATTOLIN, "Firma Digital". Master en Dirección de Empresas- Universidad del Salvador (Argentina) – Universidad Deusto (España)- Cátedra Marco Legal – Año 2004. Disponible en http://www.hfernandezdelpech.com.ar/PUBLICAtrabajosFirmaDigital.htm

- BAUZÁ MARTORELL, Felio José "Acceso Electrónico de los ciudadanos a los servicios públicos liberalizados"- España- Disponible en: http://estuderecho.com/sitio/?p=1097

- CABULI, Ezequiel, "Las nuevas tecnologías en el Proyecto de Código". Publicado en LA LEY 22/02/2013. AR/DOC/6066/2012.-

- DIAZ BERMEJO, Guillermo "La Firma electrónica y los servicios de Certificación". En publicación de Noticias Jurídicas. Diciembre 2007. Disponible en Internet: http://noticias.juridicas.com/articulos/20-Derecho-Informatico/200712-123456789.html

- FARRÉS, Pablo; "Firma Digital", Buenos Aires, Ed. Lexis. Año 2005.

- FERRARO, Ricardo H. "AFIP implementó la gestión de autorizaciones electrónicas para firma digital". AR/DOC/5276/2012.-

- GONZALEZ GOMEZ, Pedro M. "Equiparación a la ológrafa de la firma informática argentina" Publicado en: Sup. Act. 12/04/2007.-

- ILLESCAS ORTIZ, Rafael, "Derecho de la Contratación electrónica" Ed. Civitas, España. Año 2001.-

- Instituto Nacional de Tecnologia da Informação. Disponible en www.iti.gov.br

- Jefatura de Gabinete de Ministros de la Nación- Proyecto de Modernización del Estado. Disponible en: http://www.jefatura.gob.ar/archivos/pme/actividades/467.pdf

- Ley modelo de la CNUDMI sobre firmas electrónicas. La guía para su incorporación al derecho interno. Disponible en: www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf

- LYNCH, Horacio M., "Comentario a la ley 25.506 de firma y documento digital." Publicado en ADLA 2002-A, 1555. Ed. La Ley, Boletín informativo año 2001, Nro. 34.-

- MOLINA QUIROGA, Eduardo. "Ley de expedientes digitales y notificaciones electrónicas judiciales". LA LEY 22/06/2011.-

- MORA, Santiago, "Documento digital, firma electrónica y digital" Publicado en LA LEY 31/12/2013 – Enfoques 2014 (Febrero)- AR/DOC/3995/2013.-

- Observatorio de políticas públicas - Coordinación general del cuerpo de Administradores gubernamentales – Jefatura de gabinete de ministros. "E autenticación. Firma Digital y Firma electrónica. Panorama en la República Argentina. Agosto 2007.-

- RAUEK DE YANZÓN, Inés. "La implementación del principio procesal de digitalización" Publicado en: Sup.Act 07/12/2006.-

- TEMPERINI, Marcelo. "Firma Digital en Argentina: manteniendo la ilusión"- Disponible en: http://www.elderechoinformatico.com/publicaciones/mtemperini/Firma_Digital_en_Argentina_Temperini.pdf

- VENTURA, Gabriel O. "Firma Digital Análisis exegético de la ley 25.506" Disponible en: www.acaderc.org.ar

- VERNET, Tomás. "FIRMA DIGITAL" Universidad Abierta Interamericana. Sede Regional Rosario, Facultad de Derecho. Agosto 2003.-