elDial.com
Biblioteca Jurídica Online

¿Relanzamiento de la firma digital en Argentina? Decisión Administrativa N° 927/2014 JGM, cinco aspectos a considerar(*)

Por Alejandro Batista(**)

El pasado lunes 3 de noviembre de 2014 se publicó en el Boletín Oficial la **Decisión Administrativa** (en adelante DA) **Nº 927/2014** de la **Jefatura de Gabinete de Ministros de la Nación[1]**, que finalmente deroga su similar **DA N° 006/2007[2]**; estableciendo algunas modificaciones importantes en el esquema técnico-jurídico que hace a las posibilidades de ampliación del uso de firma digital en los términos de la **Ley N° 25.506**[3].-

En los párrafos que siguen, sin pretensión de ser exhaustivos, pues incluso algunos detalles todavía requerirán de un nivel inferior de reglamentación; se señalan los cinco cambios más relevantes, desde el punto de vista funcional, y en particular sus posibles implicancias prácticas para los abogados.-

I- Contexto normativo.-

El conjunto de elementos que determina el ámbito de aplicación y las condiciones de validez de una arquitectura de firma digital está dado por *componentes técnicos*, por una parte, y por *elementos normativos* por la otra.-

En este sentido, para el momento de sanción de la Ley Nacional 25.506[4], los aspectos técnicos vinculados a los diferentes sistemas bajo los cuáles es factible aplicar firma digital se encontraban lo suficientemente maduros, adoptando nuestra ley el ***sistema de doble clave, clave pública o criptografía asimétrica***[5].-

Si bien con la Ley y la posterior promulgación de su **Decreto Reglamentario N° 2628/2002**[6] se inició el camino de implementación de soluciones de firma digital, lo cierto es que más allá de los avances y pruebas puntuales, el cuadro se completó finalmente con la referida **DA N° 006 del año 2007**, que estableció ***el marco normativo aplicable al otorgamiento y revocación de las licencias de certificadores.-***

El proceso de actualización.-

Con posterioridad a la DA N° 006/2007, varios fueron los ámbitos en los que se señaló la necesidad de su adecuación *y se proyectaron más de un borrador a tales fines*; sin embargo pasaron siete años hasta que dicha reforma finalmente se concretara.-

Durante su vigencia solamente se establecieron y autorizaron a operar tres (3) Autoridades de Certificación (en adelante AC), además de la **Autoridad de Certificación de la Administración Pública ACAP**, dependiente de la propia **Oficina Nacional de Tecnología de la Información - ONTI**-.

Ellas son la **Autoridad de Certificación de la AFIP[7]**, la de la **ANSES[8]** y una del ámbito privado, **ENCODE[9]**, enfocada específicamente en la esfera de las relaciones laborales, en el contexto de la **Resolución Nº 1455/2011 del MTESS.[10]**

II.- Principales modificaciones.-

Sin ahondar en los detalles netamente técnicos, entre los principales aspectos a considerar en materia funcional, que se introducen con la DA Nº 927/2014, podemos mencionar los siguientes:

1.- Interoperabilidad plena de certificados.-

A los fines prácticos, se trata posiblemente del principal avance en el impulso que se quiere dar a la utilización de firma digital. En efecto, hasta ahora y tal como lo hemos señalado en otra oportunidad, el alcance de cualquier implementación de firma digital estaba acotado por el ámbito de vigencia de las **Políticas de Certificación**.-

Este término ha sido justamente uno de los elementos distintivos a la hora de comparar el uso y los efectos de la ***firma ológrafa con la digital***. Ya que si bien en el "*mundo de los átomos*", solamente tenemos una "firma" valida a todos los efectos, en el "*mundo de los bits*" (NEGROPONTE, 1995), se podía dar la circunstancia (como de hecho sucede en otros países como España) de tener que ***tramitar y utilizar múltiples firmas digitales dependiendo del tipo de aplicación que puedo darle, es decir del alcance de la Política de Calificación.-***

Si bien en los hechos no se conocen inconvenientes de esta índole, ello es básicamente por la poca difusión que ha tenido hasta ahora el uso de firma digital, traducido en la inexistencia de Certificadores Licenciados en el ámbito privado, a excepción de la mencionada ENCODE, que a su vez se encuentra habilitada exclusivamente para emitir certificados a ser utilizados en relaciones laborales, más concretamente a la operatoria de emisión de ***recibos de haberes digitales***, según la **Resolución Nº 1455/2011 del MTESS.[11]**.-

A partir del escenario marcado por la nueva DA Nº 927/2014, los certificados que se emitan por cualquier de las **Autoridades de Certificación que se habiliten** serán plenamente válidos para cualquier función; así lo determina expresamente su **Artículo 12**:

Art. 12. — Los certificados digitales emitidos por certificadores licenciados, en el marco de la Infraestructura de Firma Digital de la REPUBLICA ARGENTINA, podrán ser utilizados por sus titulares para firmar digitalmente cualquier documento o transacción, pudiendo ser empleados para cualquier uso o aplicación, como así también para autenticación o cifrado.-

Esta idea se refuerza en los Anexos de la Norma, por caso en el **punto 1.4 del Anexo III, Política Única de Certificación**.-

Esto implica que el Titular de un certificado digital puede ahora aplicarlo a ***cualquier transacción, documento o trámite***, y la misma mantendrá los efectos de la ***firma digital*** de los artículos 7º y 8º de la Ley 25.506.-

Esta misma situación bajo la vigencia de la DA Nº 006/07, ***tornaba esa firma digital en firma electrónica*** conforme el artículo 5º de la Ley, pues se utilizaba por fuera de los alcances de la

Política de Certificación.-

Si bien el documento firmado electrónicamente goza de algunos de los atributo de la ley como puede ser la "***integridad***" no es lo mismo que ostentar además la presunción de ***autoría***, de la firma digital y con ello la ***condición de no repudio***.-

2.- Política Única de Certificación.-

Es uno de los presupuestos que fundan lo expresado en el punto anterior, ya que precisamente unificar las políticas de certificación y requerir de la adhesión de los Certificadores Licenciados, permite por una parte facilitar la constitución de nuevas *AC* pero fundamentalmente habilita hacer efectivo la meta de plena interoperabilidad.-

Esta exigencia se plasma en el **Artículo 9º**:

Art. 9° — Establécese una Política Única de Certificación que será de cumplimiento obligatorio para todos los certificadores licenciados que integran la Infraestructura de Firma Digital de la REPUBLICA ARGENTINA.-

El texto pertinente se aprueba en el Anexo III de la DA.-

Los dos siguientes puntos son de particular interés para los abogados.-

El primero tiene que ver con la regulación de la constitución de **Autoridades de Tiempo** que puedan operar emitido ***sellos de tiempo*** o servicios de ***timestamping***.-

3.- Sello de Tiempo.-

Como se recordará la utilización de certificados digitales, otorga a un documento firmado digitalmente la cualidades de "***integridad*** y ***autoría***" *es decir que su contenido no ha sido modificado desde que fue firmado y que su autor es quien dice ser*; **pero nada podemos colegir de la fecha de su firma**, pues la misma corresponderá a la del dispositivo utilizado para aplicarla.-

Así software como Adobe Reader, al ejecutar y verificar la firma digital contenida en un documento PDF firmado digitalmente, de manera expresa advierte al tercero que ***esa verificación no cubre el dato de la fecha.-***

Naturalmente en ciertas circunstancias especialmente en materia jurídica y para utilizar el título de un artículo de Patricia Prandini, sobre *timestamping*, (que por cierto recomendamos su lectura) "***el cuándo***" es tan relevante como "***el qué y el quien***"[12].-

Básicamente el funcionamiento de un sello de tiempo es el siguiente: "*Para solicitar un sello de tiempo, el interesado envía a la TSA el hash o resumen criptográfico del documento o contenido electrónico que desea fechar. Al recibirlo y luego de verificar que cumple con los requisitos técnicos establecidos, la TSA le adiciona el registro de fecha y hora obtenido de una fuente confiable. Luego vuelve a calcular un nuevo hash de la combinación de ambos elementos, procediendo a firmar*

digitalmente dicha porción de información. Obtiene de esta manera el sello de tiempo, el cuál devuelve a la TSA".-

Al recibirlo, el solicitante procede a verificar la firma digital de la TSA. Si verifica correctamente, procede a comparar el hash obtenido con el hash calculado sobre el hash del documento original y el registro de fecha y hora. Si ambos coinciden, puede afirmarse que el sello de tiempo es correcto. (PRANDINI, MAGGIORE, FAUSTO, & ROGINA, 2009)

La DA Nº 927/2014 contempla este tipo de certificados en su **Artículo 10**, al decir:

(…) Los certificados digitales que permitan identificar en forma fehaciente en internet o cualquier otra red informática, a los servidores que establezcan conexiones seguras, son también certificados de aplicaciones. b) Sellos de tiempo, siendo éstos los que indican fecha y hora cierta asignadas a un documento o registro electrónico.-

Esta novedad debería ser bienvenida en el ámbito judicial pues abre interesantes perspectivas en cuanto a la posibilidad de extender los supuestos de ***notificación electrónica*** actualmente en vigencia tanto a nivel Federal[13] (Acordada 11/2014) como de la provincia de Buenos Aires.[14] (Acuerdo 3540/11).-

Recordemos que en rigor de verdad estas experiencias descansan los efectos jurídicos de las notificaciones en la tradicional notificación que se verifica ***los días de nota***.-

Por otra parte, y a los efectos de la verificación de fecha y hora de las transacciones que los profesionales generan utilizando los sistemas electrónicos de presentaciones, están basadas hasta donde sabemos, en *la fecha y hora del servidor de la Corte Nacional o su par de la Provincia*, pero ello no reemplaza una certificación como la que se establece mediante una Autoridad de Tiempo.-

4.- Sello de competencias.-

La otra novedad que incumbe directamente a los colegios y asociaciones profesionales, es la incorporación a la infraestructura de firma digital de las denominadas Autoridades de Competencias, previstas en el **Artículo 14**:

Art. 14. — Componen la Infraestructura de Firma Digital de la REPUBLICA ARGENTINA: a) El ente licenciante y su Autoridad Certificante Raíz, b) Los certificadores licenciados, incluyendo sus autoridades certificantes y sus autoridades de registro, según los servicios que presten, c) Las autoridades de sello de tiempo, ***d) Las autoridades de competencia****, e) Los suscriptores de los certificados y f) Los terceros usuarios, según lo dispuesto en el Anexo I del Decreto Nº 2628 del 19 de diciembre de 2002 y su modificatorio.-*

Esto se vincula estrechamente con otro aspecto, más de índole técnica, que tiene que ver con los *campos que debe contener el certificado digital de una persona física*.-

Desde ahora esos campos estarán limitados a:

"commonName" (OÍD 2.5.4.3: Nombre común): DEBE estar presente y DEBE corresponderse con el nombre que figura en el Documento de identidad del suscriptor, acorde a lo establecido en el punto 3.2.3.-

"seriaINumber" (OÍD 2.5.4.5: Nro. de serie): DEBE estar presente y DEBE contener el tipo y número de identificación del titular, expresado como texto y respetando el siguiente formato y codificación: "[tipo de documento]" "[nro. de documento]"

Los valores posibles para el campo [tipo de documento] son:

En caso de ciudadanos argentinos o residentes: "CUIT/CUIL": Clave Única de Identificación Tributaria o Laboral.-

Cabe destacar que a la fecha, la solicitud de un certificado de firma digital por caso, a la ACAP, *implica no solamente establecer los datos filiatorios del suscriptor* sino además su ***cargo o función***. Así surge del formulario on line en el que se gestionan los certificados[15], y también de los Manuales de los Oficiales de Registro, en los que como requisito para el trámite ante las Autoridades de Registro, se exigen dos certificaciones una de servicios a suscribir por el área de Recursos Humanos y otra que debe ser firmada por el funcionario o autoridad a la que reporta el solicitante.-

A partir de la nueva política, esos roles serán acreditados por estas nuevas ***Autoridades de Competencias***, básicamente como mencionamos, los Colegios y Asociaciones Profesionales, tengan o no (en este caso requiriendo autorización previa para ejercer esta opción) el *control de la matricula*; pero también las *oficinas públicas respecto de las competencias que se vinculan con sus funcionarios o empleados.-*

Art. 39. — Las entidades que controlan la matrícula u otras que actúen como autoridades de competencia, podrán optar por utilizar un certificado digital emitido por un certificador licenciado o cumplir con el proceso de licenciamiento a fin de constituirse como certificador licenciado. Para la prestación del servicio de emisión de sellos de competencia, quienes no ostenten la facultad para la acreditación de tal competencia, deberán celebrar el correspondiente convenio con dicha entidad para la emisión de los respectivos certificados. En todos los casos deberá mediar autorización previa y expresa del ente licenciante.-

Art. 40. — Las entidades comprendidas en el artículo precedente que pretendan prestar servicios de emisión de sellos de competencia deberán solicitar una licencia al ente licenciante, en las condiciones que éste establezca.-

Un sello de competencia permitirá también asociar a una persona física con una jurídica o de existencia ideal:

Art. 43. — La vinculación entre una persona física y una persona jurídica podrá ser acreditada a través de un sello de competencia emitido a tal fin.-

Resta conocer el detalle de la puesta en práctica de este punto de la iniciativa y la manera en la que ***esas competencias se correlacionarán con la firma digital del suscriptor***. La nueva reglamentación solo menciona que estas Autoridades podrán gestionar un certificado provisto por un certificador licenciado, o bien iniciar y solicitar su propia habilitación como Autoridad de Certificación.-

Art. 23. — 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.-

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.-

En el contexto de la DA Nº 006/2007 éste era el único camino posible[16], si es que tales profesionales no se encontraban incluidos como en el supuesto de los abogados, por políticas de certificación que les fueran aplicables, como los ejemplos citados de Ambas Cortes, de Nación y

Provincia de Buenos Aires.-

5.- Infraestructura tecnológica compartida.-

Para finalizar este breve comentario de los cinco puntos (a nuestro criterio) más relevantes de la nueva **DA Nº 927/2014**, es importante destacar el cambio completo de opinión respecto de la *posibilidad de compartir infraestructura tecnológica por parte de dos AC diferentes*,

Dicha situación estaba expresamente prohibida en la DA Nº 006/2007 en el segundo párrafo de su Artículo 17:

Art. 17: (…)

No se admitirá compartir infraestructuras tecnológicas entre distintos certificadores.-

Ahora según se desprende del **Artículo 16 de la DA Nº 297/2014**, es posibilidad se acepa, siempre por supuesto que se esgriman razones atendibles.-

Art. 16. — La infraestructura tecnológica del certificador licenciado podrá ser compartida por otros certificadores licenciados siempre que existan motivos que así lo justifiquen, se cumplan los requisitos de seguridad establecidos en la presente decisión administrativa y se garanticen procesos confiables de gestión del ciclo de vida de los certificados. En todos los casos deberá mediar autorización previa y expresa del ente licenciante.-

Recordemos qué implica la Infraestructura Tecnológica:

Art. 13. — Se entiende por infraestructura tecnológica del certificador licenciado, al conjunto de servidores y otros equipamientos informáticos relacionados, software y dispositivos criptográficos utilizados para la generación, almacenamiento y publicación de los certificados enumerados en el artículo 10 de la presente decisión administrativa, y para la provisión de información sobre su estado de validez.-

La Infraestructura tecnológica que soporta los servicios del certificador utilizada tanto en el establecimiento principal como en el alternativo destinado a garantizar la continuidad de sus operaciones, deberá estar situada en territorio argentino, bajo el control del certificador licenciado y afectada exclusivamente a las tareas de certificación.-

Esto indudablemente puede significar la oportunidad para sectores, organismos u organizaciones que *por escala no pueden plantearse la alternativa de inversión que implica montar una AC y que por la particularidad de su actividad no se encuentran comprendidas en ninguna de las AC vigentes.-*

III.- Conclusiones.-

Como en otros aspectos de la vida, el derecho o la norma por sí misma, no siempre puede modificar la realidad, no obstante las adecuaciones y reformas normativas pueden propender o facilitar ciertos cambios. Éste pareciera ser el objetivo de la Decisión Administrativa Nº 927/2014.

En todo caso habrá que estar atentos a los tiempos de implementación previstos para que los cambios se tornen operativos[17] y verificar si en efecto, estamos a las puertas de una

generalización de uso de firma digital, que significaría además de contar con circuitos y procesos mucho más eficientes y plazos más breves (tanto en el ámbito de lo que se denomina Gobierno Electrónico, como en el sector privado); un salto de calidad y seguridad en todos los trámites y transacciones que se operan electrónicamente.

Referencias

BATISTA, A. (2007). Derecho y Nuevas Tecnologías. Los desafíos de la Abogacía en la Sociedad de la Información. *Revista ANALES FCJyS-UNLP. Año 4 Nº 37*.-

BATISTA, A. (2009). Experiencia de aplicación de firma digital en el Instituto Nacional de Servicios Sociales para Jubilados y Pensionados – PAMI. *38 Jornadas Argentinas de Informática JAIIO Mar del Plata 2009 y en 2do Congreso Provincial de Ciencias Jurídicas .* Mar del Plata y La Plata.-

BATISTA, A. (2010). La responsabilidad civil de los Certificadores Licenciados en el marco de la Ley 25.506 de Firma Digital La culpa de Bíró! *Suplemento de Derecho de Alta Tecnología - elDial.com - DC1347*.-

BATISTA, A. (2011). Derecho 2.0 de la formación analógica a las problemáticas digitales. *Revista ANALES FCJyS-UNLP Nº 41*, 282 a 294.-

BATISTA, A. (2011). La Ley 25.506, la Resolución 1455/2011 del MTESS y los recibos de haberes digitales. *Suplemento de Derecho de Alta Tecnologia - elDial.com - DC1790.-*

LOPEZ TALLON, A. (2010). *El manual práctico de supervivencia en la Administración Electrónic@.* Bajo licencia CC.-

NEGROPONTE, N. (1995). *Ser Digital.* Buenos Aires: Atlántida.-

PIANA, R. S. (2007). *Gobierno electronico. Gobierno, tecnologias y reformas.* La Plata: EDULP - Editorial de la Universidad Nacional de La Plata.-

PRANDINI, P., MAGGIORE, M., FAUSTO, E., & ROGINA, P. (2009). Qué y quién… pero también cuándo: Sellos de tiempo. *elDial.com - DC120E.-*

(*) Decisión Administrativa 927/2014 - FIRMA DIGITAL - Certificaciones Digitales. Política, Contenidos, Requisitos y Formularios. Aprobación.

Bs. As., 30/10/2014
Publicación en B.O.: 03/11/2014

(**) Abogado (UNLP), Especialista en Derecho de Alta Tecnología (UCA-SMB), Magister en Finanzas Públicas (FCE-UNLP), Docente de Grado y Posgrado en temáticas de Sociología Jurídica, Nuevas Tecnologías, Plantificación y Gestión, etc., en la Universidad Nacional de La Plata. Presidente de la Comisión de Derecho, Tecnología e Innovación del Colegio de Abogados de La Plata, y actualmente Coordinador de Políticas Digitales del INSSJP-PAMI.

@batista1088

[1]Ver: http://www.boletinoficial.gov.ar/Avisos/VerPDF.castle?f=20141103&s=01&pd=1&ph=0&sup=Falsey sus correspondientes Anexos en: http://www.boletinoficial.gov.ar/Displaypdf.aspx?s=A&tid=4708795&i=1

[2]Ver: http://www.boletinoficial.gov.ar/Avisos/VerPDF.castle?f=20141103&s=01&pd=1&ph=0&sup=False

[3]Ver: http://www.infojus.gob.ar/25506-nacional-ley-firma-digital-lns0004621-2001-11-14/123456789-0abc-defg-g12-64000scanyel

[4]La Ley 25.506 se publicó en noviembre de 2001, naturalmente el complicado proceso político y social que vivió Argentina entre ese año y el 2003, hacen que no pueda achacarse la demora en su implementación a una mera falta de iniciativa.

[5]Ver más en: http://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica

[6]Ver: http://www.infojus.gob.ar/2628-nacional-decreto-reglamentario-ley-25506-sobre-firma-digital-dn20022002628-2002-12-19/123456789-0abc-826-2002-2002soterced

[7]Ver: https://acn.afip.gov.ar/afipacn/p_Home.seam

[8]Ver: http://www.anses.gob.ar/firmadigital/index.html

[9]Ver en: http://www.encode.com.ar/

[10] Ver: http://www.boletinoficial.gov.ar/Avisos/VerPDF.castle?f=20111201&s=01&pd=11&ph=0&sup=False

[11]Al respecto de puede ampliar en “La Ley 25.506, la Resolución 1455/2011 del MTESS y los recibos de haberes digitales”, BATISTA, A. en http://www.eldial.com/nuevo/resultados-detalle-doctrina.asp?id=6084&base=50&resaltar=batista

[12]Ver “Qué y quién… pero también cuándo: Sellos de tiempo”. Por Patricia Prandini, Marcia Maggiore, Emiliano Fausto y Pablo Rogina. http://www.eldial.com/nuevo/resultados-detalle-doctrina.asp?id=4658&base=50&resaltar=prandini

[13]Ver: https://sau.pjn.gov.ar/sau/Inicio.do#_

[14]Ver: http://www.scba.gov.ar/servicios/notiypresen.asp

[15]Ver: https://pki.jgm.gov.ar/app/Signature/Request/CertificateRequest.aspx

[16]Conteste con el Artículo 18 de la Ley 25.506: **Certificados por profesión. ARTICULO 18. -** Las entidades que controlan la matrícula, en relación a la prestación de servicios profesionales, podrán emitir certificados digitales en lo referido a esta función, con igual validez y alcance jurídico que las firmas efectuadas en forma manuscrita. A ese efecto deberán cumplir los requisitos para ser certificador licenciado.

[17] Art. 63. — A partir de los CIENTO VEINTE (120) días hábiles administrativos del dictado de la presente, los certificadores licenciados sólo podrán emitir certificados de acuerdo a lo establecido en la Política Única de Certificación.

Citar: elDial DC1E08

Publicado el: 12/11/2014