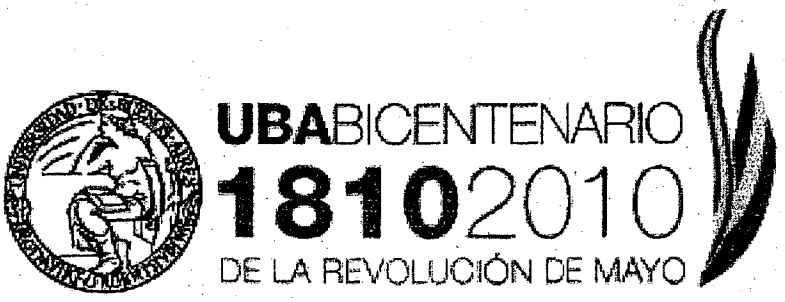
Cod. 1502/0461



MAESTRÍA EN ADMINISTRACIÓN PÚBLICA

Facultad de Ciencias Económicas

UNIVERSIDAD DE BUENOS AIRES

TESIS

"Infraestructura de Firma Digital Argentina: Factores que explicarían su escasa masividad a 10 años de implementación en el Estado"

Director: Lic. Guillermo Schweinheim

Autora: AG Mercedes Rivolta

Año 2011

INDICE

"But I am also a teacher. If my writing produces angry reactions, then it might also effect a more balanced reflection. These are hard times to get it right, but the easy answers to yesterday's debate won't get it right".
LESSIG, Lawrence: Code 2.0, Prólogo.

Agradecimientos

Dedicada a la Lic. Cristina Bottinelli y al Dr. Carlos Domínguez Molet, a quienes le debo mi formación como Administradora Gubernamental.

Mi agradecimiento al Lic. Guillermo Schweinheim, mi Director de Tesis.

I.- INTRODUCCION

Identificación del tema general

El presente trabajo de investigación aborda el tema de la firma digital en la República Argentina desde tres perspectivas: la tecnológica, la jurídica y la organizacional-administrativa.

Constituye un aporte original al conocimiento existente sobre el tema en la medida que lo encara desde estas tres miradas. Hasta el momento, se pueden encontrar estudios que abordan el tema desde los aspectos tecnológicos (KHUN et all, NIST: 2001; GUTMANN: 2002; ELLISON, SCHNEIER: 2000; CLARKE: 2001; ADAMS: 2004). También es dable encontrar trabajos jurídicos sobre la firma digital (LORENZETTI: 2001; DEVOTO: 2001; FISCHER-DIESKAU, WILKE: 2006; TELLEZ VALDEZ: 2004; PRANDINI, RIVOLTA: 2002; MASON: 2006; RIVOLTA, FRAGA: 2007; RIVOLTA, SCHAPPER, VEIGA MALTA: 2006; UNCITRAL: 2009). Incluso algunos trabajos abordaron ambos aspectos, el tecnológico y el legal (MARTA, PRANDINI, RIVOLTA: 2003; RIVOLTA, SCHAPPER: 2004; BUGONI, RIVOLTA: 2007). Pero este es el primer trabajo de investigación que además de dichos aspectos, analiza al tema de la firma digital desde la perspectiva de su organización administrativa en el Estado.

Este enfoque pluridisciplinario permitirá comprender más cabalmente la problemática de la firma digital en Argentina. Conectar múltiples enfoques y teorías brinda un panorama más acabado y un entendimiento más profundo de la evolución de la Infraestructura de Firma Digital que un abordaje apoyado en una sola disciplina.

Argentina fue un país pionero en la materia. En 1997 emitió la primera norma que daba valor jurídico a la firma digital, aunque restringida al Sector Público Nacional. Sin embargo, pasados 10 años desde la firma del Decreto N° 427/98, el desarrollo de la firma digital en nuestro país se encuentra detenido. Este trabajo

presentará los factores que pudieran explicar los motivos de este estancamiento, según la opinión de expertos.

Por otra parte, el tema es relevante desde la perspectiva de políticas públicas por varios motivos, entre los que cabe mencionar los siguientes:

- La firma digital es un mecanismo de autenticación electrónica en las aplicaciones de gobierno electrónico.

- El régimen legal de la firma digital es el marco normativo del comercio electrónico y del gobierno digital.

- La autoridad de aplicación de la firma digital es un organismo del Estado, actualmente, la Secretaría de la Gestión Pública de la Jefatura de Gabinete de Ministros.

Antecedentes

Desde mediados de los años 90, la aparición de Internet y el constante avance de las tecnologías de la información y de las comunicaciones han producido un nuevo modo de vinculación entre las personas. Internet permite realizar transacciones en forma simultánea entre personas ubicadas en lugares remotos. (RIVOLTA; 2008: 3)

Este avance tecnológico, que facilitó los procesos de globalización y de internacionalización con fuerte impacto en los mercados, tuvo múltiples efectos en la vida cotidiana de las personas. Estos procesos fueron acompañados con una adecuación de los aspectos institucionales tanto del sector privado como del público (OSZLAK, MALVICINO; 2001: 2).

En este nuevo escenario de "mutación acelerada" (KLIKSBERG; 2000: 1), las empresas debieron adaptarse y hacer uso de estas tecnologías para insertarse en los mercados, y los gobiernos debieron enfrentar por un lado, la necesaria regulación de las transacciones electrónicas y de los aspectos vinculados a estos nuevos elementos como Internet, telecomunicaciones, comercio electrónico, y por el otro, adaptar su organización e incorporar el uso de estas nuevas herramientas. Concomitantemente, los postulados de la Nueva Gerencia Pública apoyaban el uso de las tecnologías en la gestión de los gobiernos. Así surgieron nuevas fronteras tecnológicas en gerencia, que expresaban nuevas demandas referidas al perfil del Estado, a cómo lidiar con la complejidad y la incertidumbre. (KLIKSBERG; 2000: 6)

Este avance tecnológico generó la necesidad de dar seguridad jurídica a las transacciones que se realizaban por medios electrónicos, lo cual motivó la adecuación de los marcos legales de los países. (BUGONI, RIVOLTA, 2007: 15). El principal objetivo de la legislación sobre comercio electrónico o firma electrónica, ha sido remover los obstáculos para el uso de la legislación tradicional interna de cada país, en las nuevas aplicaciones basadas en transacciones electrónicas. Con ese propósito, los países han desarrollado legislación específica que proporciona nuevas

alternativas a las firmas manuscritas, basadas tanto en las Leyes Modelo de Uncitral sobre Comercio Electrónico (1996) y sobre Firma Electrónica (2001), cuanto en la Directiva 99/93 de la Unión Europea, en la Ley de Firma Electrónica de Estados Unidos conocida como E-Sign, o en una combinación de ellas. (RIVOLTA, SCHAPPER; 2004: 33), (UNCITRAL; 2009: 40).

Gran número de países han desarrollado legislación específica sobre comercio electrónico o sobre firmas electrónicas. Los enfoques que se adoptaron están basados en cada sistema legal en particular de cada uno de los países. En aquellos países cuyos regímenes jurídicos pertenecen al common law, en los cuales la regulación es más abierta, ha menudo ha sido necesario solamente reconocer el no repudio de un documento electrónico (electronic record) o de una firma electrónica (tal como lo establece la Ley de Firma Electrónica de Estados Unidos de América – E-Sign). En aquellos países con regímenes de derecho civil codificado, se han formulado tipos muy prescriptivos de legislación sobre firmas electrónicas o comercio electrónico, con énfasis en normas técnicas y operacionales y en las formalidades de los actos, específicamente basados en firmas digitales (RIVOLTA, SCHAPPER: 2004: 34).

Es así como a fines de los 90 y comienzos del nuevo siglo, gradualmente los países[1] aprobaron leyes que complementan sus ordenamientos jurídicos vigentes y

[1] Ver la Ley Argentina sobre Firma Digital Nº 25.506, la Ley de la República Dominicana sobre Comercio Electrónico, Documentos Electrónicos y Firmas Digitales Nº 126-02, la Ley Peruana sobre Firma Digital Nº 27269, la Medida Provisoria de Brasil Nº 2200-2, la Ley de Chile sobre Firmas Electrónicas Nº 19.979, la Ley Colombiana sobre Comercio Electrónico y Firmas Digitales Nº 527-1999, la Ley de Ecuador sobre Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, la Ley Venezolana de Mensajes de Datos y Firmas Electrónicas. A enero de 2007, se había adoptado legislación que aplicaba disposiciones de la Ley Modelo de la CNUDMI sobre Comercio Electrónico al menos en los siguientes países: Australia, Ley de operaciones electrónicas (1999); China, Ley de firmas electrónicas (2004); Colombia, Ley de comercio electrónico (1999); Ecuador, Ley de comercio electrónico, firmas electrónicas y mensajes de datos (2002); Eslovenia, Ley de comercio electrónico y firma electrónica (2000); Filipinas, Ley de comercio electrónico (2000); Francia, Loi 2000-230 portant adaptation du droit de la preuve aux technologies de l´information et relative à la signature électronique (2000); India, Ley de tecnología de la información (2000); Irlanda, Ley de comercio electrónico (2000); Jordania, Ley de operaciones electrónicas (2001); Mauricio, Ley de operaciones electrónicas (2000); México, Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en materia federal , del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de protección al consumidor (2000); Nueva Zelandia, Ley de operaciones electrónicas (2002); Pakistán, Ordenanza de operaciones electrónicas, 2002; Panamá, Ley de firma digital (2001); República de Corea, Ley Marco de comercio electrónico (2001); República Dominicana, Ley sobre comercio electrónico, documentos y firmas digitales Nº 126-02 (2002); Singapur, Ley de operaciones electrónicas (1998); Sri Lanka, Ley de operaciones electrónicas (2006); Sudáfrica, Ley de comunicaciones y operaciones electrónicas (2002); Tailandia, Ley de operaciones electrónicas (2001); Venezuela (República Bolivariana de), Ley sobre mensajes de datos y firmas electrónicas (2001); y Viet Nam, Ley de operaciones electrónicas (2006). La Ley Modelo ha sido adoptada también en las dependencias de la Corona británica de la Bailía de Guernsey (Ley de operaciones electrónicas (Guernsey), 2000), la Bailía de Jersey (Ley de comunicaciones electrónicas (Jersey), 2000) y la Isla de Man (Ley de operaciones electrónicas, 2000); en los territorios de ultramar del Reino Unido de Gran Bretaña e Irlanda del Norte de las Bermudas (Ley de operaciones electrónicas, 1999), las Islas Caimán (Ley de operaciones electrónicas, 2000) y las Islas Turcas y Caicos (Ordenanza de operaciones electrónicas, 2000); y en la Región Administrativa Especial de Hong Kong de China (Ordenanza de operaciones electrónicas (2000)).

reconocen el valor legal de estas transacciones electrónicas. En particular, fueron leyes llamadas de comercio electrónico o de firma electrónica o digital, que remueven los obstáculos que presenta la antigua legislación para este reconocimiento jurídico. Dichos obstáculos principalmente estaban vinculados con la exigencia de una firma en un documento, con la consideración del carácter de "original" al documento suscripto por las partes intervinientes, con la conservación del documento, y con la propia naturaleza del documento que se exigía fuera "escrito". *"La noción de documento escrito, que lleva la firma del autor como único medio para atribuir la declaración de voluntad, se ha ido ampliando. ... Esta tendencia es coincidente en todo el mundo y bastante homogénea, lo cual tiene sentido si se piensa que la estandarización permite una mejora sustancial en las relaciones económicas internacionales"*. (LORENZETTI; 2001: 61)

Estas primeras leyes de firma electrónica o firma digital, se basaban en el criterio del "equivalente funcional" con la firma manuscrita, es decir, reconocían el valor legal equiparable a la firma para aquellas tecnologías que permiten la autenticación de las personas en entornos electrónicos. Dichas tecnologías recibieron por imperio de la ley la definición de "firma electrónica" y de "firma digital", según se apoyaran o no en Infraestructuras de Clave Pública. A la firma digital las leyes le asignaron dos presunciones iuris tantum, es decir, que admiten prueba en contrario: la de autoría y la de integridad del mensaje. Dichas consecuencias son relevantes en función de la posibilidad de repudiar transacciones. (LORENZETTI, 2001: 81-82)

Surgieron entonces dos tipos de leyes de comercio electrónico: un primer modelo legislativo basado en la criptografía, y el otro, apoyado en el principio de analogía y no discriminación. Dicho principio, reconocido por la Ley Modelo de UNCITRAL de Comercio Electrónico (1996), a partir del análisis de los objetivos y funciones del documento en papel, admite distintas variaciones en el soporte técnico. En ese sentido, plantea que no se le negarán efectos jurídicos, validez o eficacia a una información solamente porque esté bajo forma de mensaje electrónico (art. 5º), o, cuando la ley requiera que conste por escrito, este requisito se considerará cumplido por un mensaje electrónico (art. 6º). (LORENZETTI; 2001: 60).

En lo referido a la Administración Pública, a partir de la sanción de estas leyes, surgió el concepto de "gobierno electrónico" esto es, el uso que los gobiernos dan a las nuevas tecnologías y que permiten mejorar la calidad de los servicios, aumentar la transparencia, incrementar la eficiencia y eficacia de las organizaciones públicas, ampliar la participación democrática, y en general, acercar el Estado al ciudadano (RIVOLTA; 2008: 4). Este trabajo no se referirá al tema de gobierno electrónico que de por sí merece una investigación específica, pero sí destacamos la íntima relación que tiene el tema de la firma digital con el tema de gobierno electrónico, por ser la Ley Nº 25.506 de Firma Digital el marco legal que otorga valor jurídico a los documentos electrónicos.

Como se mencionó, a fines de los ´90, los países fueron adecuando sus marcos jurídicos adaptándolos con normas específicas de comercio electrónico o firma digital. El objetivo era remover los obstáculos que representaban las normas tradicionales contenidas en los Códigos para el desarrollo del comercio realizado por

medios electrónicos, en los cuales el uso papel ya no tenía un lugar primordial (RIVOLTA, SCHAPPER: 2004: 36).

Se partía de la base que no era necesario escribir todo el derecho nuevamente, que los códigos civiles y comerciales eran aplicables en lo sustantivo, ya que la actividad comercial no variaba en su naturaleza, solamente variaba el soporte en el cual se instrumentaban los contratos y las transacciones. Se iniciaba así un cambio cultural profundo: pasar de la cultura del papel, de más de 4000 años, a la cultura digital, que irrumpía vertiginosamente en la vida cotidiana a nivel planetario. (RIVOLTA, 2008: 4)

Las primeras aproximaciones de adecuación legal tuvieron como eje dar respuesta a la preocupación del momento, relativa al potencial repudio que las transacciones digitales pudieran generar. En efecto, se pensaba que dada la naturaleza del documento electrónico, fácilmente modificable, las personas repudiarían sus actos. Se elaboraron así las primeras normas que tenían como principal objetivo garantizar el no repudio de las transacciones electrónicas. Es así como surgieron las primeras normas, en los Estados de Utah y California en Estados Unidos, Alemania e Italia y Argentina, a fines de 1997 (RIVOLTA; 2008:4).

Situación de la firma digital en Argentina

En abril de 1998, Argentina sanciona el Decreto Nº 427 que establecía una Infraestructura de Firma Digital para el Sector Público Nacional. A partir de esta experiencia, que se desarrolló en la entonces Secretaría de la Función Pública de la Jefatura de Gabinete de Ministros, se puso en operación una Autoridad Certificante Raíz, se licenció una Autoridad Certificante de la Oficina Nacional de Tecnologías Informáticas, se desarrolló un software de autoridad certificante de libre disponibilidad que se entregó gratuitamente a distintos organismos públicos, nacionales, provinciales, Poderes Judiciales y Universidades. Con el objetivo de difundir el uso de la firma digital se montó un Laboratorio de Firma Digital, se levantó en Internet una página web con información, se publicó un newsletter que se mantiene en Internet hasta la fecha. A fin de ampliar el alcance jurídico de la firma digital a todo tipo de transacciones, se elaboró y presentó ante el Congreso en 1999 el primer proyecto de ley de Firma Digital, que fue tomado como modelo para los distintos proyectos presentados por más de diez diputados y senadores, proceso que culminó exitosamente con la sanción de la Ley No. 25.506 de firma digital, la cual constituye el marco legal para el comercio electrónico y el gobierno digital en Argentina (RIVOLTA, 2008: 5).

Actualmente, la Infraestructura de Firma Digital de la República Argentina cuenta con una Autoridad Certificante Raíz, administrada por la Oficina Nacional de Tecnologías de Información, ha licenciado dos autoridades certificantes de los organismos de recaudación tributaria y de seguridad social (AFIP y ANSES) y se encuentran en proceso de licenciamiento la autoridad certificante de la Oficina Nacional de Tecnologías de Información y tres solicitudes del sector privado.

Desde ese momento hasta la fecha, la firma digital no ha avanzado en Argentina. La investigación pretende dar cuenta de las razones por las cuales la firma digital no ha llegado a ser masiva en la República Argentina después de 10 años de vigencia normativa. En ese orden de ideas, la pregunta de indagación de la presente investigación apunta a identificar algunos factores que estarían rezagando el uso masivo de la firma digital en la Argentina, de acuerdo con la percepción de expertos en el tema.

Relevancia de la Investigación

El tema elegido está presente en otros países. Tanto en Europa, EEUU, Asia, Australia y los países de la región han sancionado normas de comercio electrónico o firma digital (UNCITRAL; 2009: 40). Estos países, en mayor o menor medida, disponen de Infraestructuras de Firma Digital. A su vez, en su casi totalidad los países han implementado planes de gobierno electrónico que pueden o no tener relación con el uso de la firma digital. Sin embargo, la firma digital no se ha masificado en ningún país. A escala internacional no se cuenta con una variedad de estudios que permitan explicar este fenómeno.

Por ello, la relevancia del presente estudio radica en que puede constituir un aporte original para la interpretación de políticas públicas vinculadas a gobierno electrónico y a comercio electrónico, así como también, un elemento interesante a ser considerado en el análisis y formulación de políticas específicas sobre firma digital en nuestro país y en el entorno Mercosur.

Esta investigación intenta aportar elementos para clarificar los motivos por los cuales los esquemas de autenticación basados en firma digital no son masivos. Se han realizado algunos pocos estudios que tratan sobre el escaso desarrollo de la firma digital en Europa y a nivel de usuarios angloparlantes en el ciberespacio. (HANNA; 2003), (ADAMS; 2004), (COMUNIDAD EUROPEA, 2006), (UNCITRAL; 2009).

La presente Tesis se ha apoyado en una encuesta internacional realizada en el año 2003 (HANNA; 2003), con un agregado para su aplicación en Argentina, con el fin de determinar si los factores que pudieran estar obstaculizando el desarrollo de la firma digital son los mismos que se han identificado internacionalmente, o si, por el contrario, existen factores vernáculos específicos, o una combinación de ambos.

Por otra parte, la formulación del proyecto se apoya en una vasta exploración ya realizada previamente a fin de delinear tres enfoques sobre la unidad de análisis. Dichos enfoques permiten identificar a priori tres posibles factores que podrían incidir en el escaso uso masivo de la firma digital. De los trabajos preliminares ya realizados, se han identificado tres factores:

- Factores tecnológicos.
- Factores normativos.

- Factores organizacionales – administrativos.

La relevancia del presente proyecto también radica en su enfoque multidisciplinario. Se ha analizado el tema de la firma digital desde sus aspectos tecnológicos, jurídicos y de organización administrativa. Esta mirada comprende tres disciplinas diferentes: la tecnología, la legal y la de ciencias de la administración, y se ha propuesto relacionar sus componentes para intentar dar una explicación respecto de los factores que pudieran estar afectando el desarrollo de la firma digital.

Si bien el enfoque puede parecer complejo, es absolutamente necesario para lograr una adecuada comprensión de las causas que influyen en la escasa masificación de la firma digital. Ello así pues se espera que la investigación sea leída por no expertos, o expertos en uno solo de los campos. El esfuerzo se ha centrado en elaborar un documento que pueda ser entendido por expertos en ciencias de la administración, por expertos informáticos y por gente del derecho, sin perder rigor en los contenidos técnicos pero con un vocabulario que permita un amplio entendimiento.

Desde esta perspectiva, no sería posible llegar a la identificación de los factores que estarían impidiendo la masificación de la firma digital sin hacer previamente una descripción acabada de los componentes de una Infraestructura de Clave Pública, como sistema técnico – jurídico - administrativo que se compone de elementos tecnológicos, elementos normativos y elementos de gestión pública.

Las respuestas, entonces, serán fruto de los resultados de las encuestas y del análisis teórico sobre los factores. Como corolario de la investigación se presentan conclusiones a ser presentadas en foros de expertos y policy makers, a nivel sub nacional, nacional, regional e internacional. Por las razones expuestas, la presente investigación se enmarca en los alcances e incumbencias de las tesis a ser presentadas en la Maestría de Administración Pública de la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

Estrategia general de investigación

La investigación se propuso presentar un estudio de caso referido a la firma digital en la República Argentina, dentro del período comprendido desde 1997, momento en el cual se aprueba la primera norma argentina en la materia, hasta noviembre de 2008. El estudio pretende en primer lugar, describir en todo su potencial y complejidad los aspectos involucrados en una Infraestructura de Firma Digital (en adelante, PKI por sus siglas en inglés: Public Key Infrastructure), a saber:

- Marco normativo, tanto nacional como internacional, que define los alcances jurídicos.
- Marco tecnológico, que en forma sencilla explica los componentes técnicos involucrados en una PKI, de modo de facilitar el entendimiento de las dificultades que su implementación conlleva.

- Marco organizacional - administrativo, que describe los aspectos de gerencia pública involucrados en el caso argentino, con su correspondiente contextualización teórica.

Además de la descripción de los tres aspectos señalados, se ha realizado una encuesta a expertos sobre los obstáculos para la masificación del uso de la firma digital, basada en un formulario de encuesta realizada en 2003 por el Comité Técnico de la Sección PKI de OASIS[2]. Se ha utilizado el mismo formulario a fin de poder realizar una comparación entre ambos resultados, al cual se anexó un ítem específico sobre el caso argentino.

Los aspectos metodológicos se describen con más detalle en el Anexo I.

Hipótesis de la Investigación

La unidad de estudio de la presente investigación es la Infraestructura de Firma Digital de la República Argentina. Intenta dar respuesta al interrogante que se plantea respecto de la identificación de algunos factores que estarían rezagando el uso masivo de la firma digital en Argentina, a 10 años de su vigencia.

A tal fin, se han delineado varias hipótesis, que han permitido el desarrollo de la investigación en todas las facetas necesarias para dar respuesta a la pregunta originaria.

Una **primera hipótesis**, explica el escaso uso de la firma digital por la inadecuación normativa sobre el tema. Se analizaron para ello los contenidos del marco jurídico, tanto de la ley como de los decretos reglamentarios y normas inferiores, su consistencia interna y también en relación con las leyes modelo de UNCITRAL que inspiraron la regulación internacional.

Una **segunda hipótesis** explica el escaso uso de la firma digital a partir de la inmadurez de los estándares de la tecnología de clave pública. A tal fin, se han analizado los principales componentes tecnológicos involucrados en la operación de una Infraestructura de Firma Digital, los estándares aplicables internacionalmente aceptados, y sus riesgos potenciales.

Una **tercera hipótesis** para explicar el uso limitado de la firma digital se vincula con la inexistencia de un órgano exclusivo para el desarrollo de las funciones de Autoridad de Aplicación de la Infraestructura de Firma Digital, es decir, como

---

[2] OASIS (Organization for the Advancement of Structured Information Standards) es una organización sin fines de lucro que impulsa el desarrollo, convergencia y adopción de estándares abiertos para la sociedad global de la información. Fundada en 1993, OASIS cuenta con más de 5000 participantes que representan más de 600 organizaciones y miembros individuales en 100 países.

sistema técnico administrativo. Para ello se analizaron las competencias de los organismos que desempeñan el rol de Autoridad de Aplicación.

II.- LA INFRAESTRUCTURA DE FIRMA DIGITAL COMO SISTEMA TECNICO JURIDICO ADMINISTRATIVO

El presente capítulo se propone contextualizar a la Infraestructura de Firma Digital como un sistema técnico-jurídico-administrativo. Se analizan los aspectos tecnológicos y jurídicos involucrados, que son los más difundidos actualmente. Pero también, y en esto reside el aporte de este trabajo, se identifican los componentes organizacionales – administrativos a partir de una primera aproximación que no agota todos los aspectos institucionales, sino aquellos que, en función del estado de situación en Argentina, se consideran como más relevantes a los fines de esta investigación.

Sistemas técnico – jurídico - administrativos

La tecnología de la información ha sido definida como aquella "*basada en computadora para el almacenamiento, acceso, procesamiento y comunicación de información*"(MOLLOY, 1995).

PEREZ SEDEÑO aporta una interesante dimensión del término "tecnología", del cual identifica al menos tres sentidos. "*En primer lugar, la tecnología es una forma de conocimiento que contiene conceptos científicos, datos problemáticos.... También utilizamos "tecnología" para referirnos al conjunto de objetos físicos reales tales como coches, aspiradores u ordenadores. Pero esos objetos no son nada sin personas que sepan cómo usarlos. Así pues, "tecnología" también refiere a lo que la gente hace y a lo que sabe, forma parte de las actividades humanas: un ordenador sin programa ni programador es un conjunto de trozos de metal, plástico y silicio. Pero la tecnología no tiene que ver sólo con conocimiento, actividad o construcción de artefactos. Es una institución e incluye prácticas.*" (PEREZ SEDEÑO, 2008: 16).

Así, se advierte que la Tecnología contiene una dimensión operacional, que incluye prácticas, procedimientos, actividades realizadas por el hombre, al mismo tiempo que alude a los objetos en sí mismos tecnológicos. En cuanto a los objetos, alude tanto a los artefactos con los cuales se procesa la información (redes teleinformáticas, computadoras, programas informáticos, teléfonos, etc.) como a los datos que la componen. Esta concepción resulta adecuada pues contempla los variados aspectos contenidos en la tecnología.

Ya a mediados de los 90 KLIKSBERG señalaba el impacto que tiene el desarrollo tecnológico en las formas de producción, en los estilos de gerencia y en las estructuras organizativas, tanto del sector privado como público. Tal como menciona, estos cambios tecnológicos "*afectan a lo cotidiano, que impactan todas las organizaciones y que inciden fuertemente en los parámetros en los que se mueve cualquier tipo de gerencia. Así, se están produciendo revoluciones en el campo tecnológico que están variando fundamentalmente lo que podríamos denominar la*

matriz tecnológica de las actividades centrales de las sociedades organizadas. El impacto de las revoluciones tecnológicas en curso -en campos como entre otros la biotecnología, la microelectrónica, la informática, la robótica, las comunicaciones- está cambiando decisivamente la manera en que se producen bienes y servicios, así como el modo en que se comercializan, se utilizan y se consumen. Ello está modificando el paisaje de las organizaciones industriales y de servicios de toda índole a lo largo del planeta." (KLIKSBERG, 2000:2). En ese orden, las administraciones públicas no han quedado atrás en este proceso. Han reaccionado al avance tecnológico en dos sentidos: por una parte, incorporando estas herramientas en su gestión diaria, y por la otra, produciendo políticas públicas relacionadas con la tecnología.

OZSLAK explica que la actividad de las organizaciones públicas en realidad no está centrada en ejecutar una serie de normas, sino más bien en intentar *"compatibilizar los intereses de sus clientelas, y los suyos propios, con aquellos sostenidos en sus "proyectos políticos" por regímenes que sucesivamente se alternan en el control del Estado."* (OZSLAK, 1980:208)

Por otra parte, todo proyecto político pretende actuar sobre la sociedad, y también dentro del aparato estatal del cual se vale para implementar sus políticas. Esto significa que cada cambio de gobierno necesariamente actuará sobre y a través de un aparato estatal preexistente. Esta acción puede significar alterar el statu quo, tanto de las jurisdicciones como de las personas, lo cual genera una natural resistencia al cambio. Si entendemos a la configuración organizativa del Estado como el *"conjunto de relaciones de dominación que suponen una determinada alianza de clases para el desarrollo"* (SCHWEINHEIM, 2010: 4), se podrá inferir que la ausencia de una adecuada organización puede no ser casual, sino responder a dichas relaciones de dominación.

Señala OZSLAK que *"Al privilegiar determinados sectores o intereses, todo nuevo proyecto político interioriza en el aparato estatal en tanto concede privilegios automáticamente a ciertos organismos y programas oficiales en detrimento de otros. Las políticas que traducen esa voluntad sesgada del régimen, originan, dentro de la burocracia, un gran número de reacomodamientos y ajustes derivados de la variable inclinación o posibilidades objetivas de sus diversas unidades en el sentido de materializar dichas políticas."* (OZSLAK, 1980:209)

Estos comportamientos adaptativos de las organizaciones estatales, generados a partir de los cambios que se intentan introducir con las nuevas políticas, son percibidos como resistencias en la medida que intentan mantener un statu quo y seguir sirviendo a los intereses anteriores. A su vez, estos comportamientos influyen en los niveles gobernantes, generando nuevos comportamientos adaptativos que buscan superar las desviaciones o bloqueos presenta la organización.

Si entendemos que el gobierno electrónico, puesto en acto a partir de proyectos tecnológicos concretos, es el uso de tecnologías de la comunicación y de la información para mejorar el funcionamiento del gobierno, es claro que dichos proyectos tendrán un impacto directo sobre la gestión administrativa, con lo cual es de esperar el surgimiento de resistencias.

Por otra parte, tal como señala OZSLAK, si entendemos que el Estado, como instancia de articulación y dominación de la sociedad, "condensa y refleja sus conflictos y contradicciones a través tanto de las variables tomas de posición (o políticas) de sus instituciones, como de la relación de fuerzas existentes entre éstas. Si visualizamos el ámbito institucional del Estado como una privilegiada arena de conflicto político, donde pugnan por prevalecer intereses contrapuestos y se dirimen cuestiones socialmente problematizadas, concluiremos que su fisonomía y composición no pueden ser sino un producto histórico, un "resumen oficial" de la sociedad civil como lo caracterizara Marx. (OZSLAK, 1980: 209)

En consecuencia, el aparato estatal no es un conjunto de organismos con competencias y recursos racionalmente asignados, sino más bien el producto de variados proyectos políticos sumado al resultado específico de la propia burocracia para sobrevivir. No es el resultado de un proceso racional de diferenciación estructural y especialización funcional. La organización estatal es más el resultado de una sinuosa trayectoria en la cual han interactuado los sectores sociales que lograron imponer una cuestión como política pública, las autoridades con sus proyectos políticos y una burocracia que pugna por su permanencia y el mantenimiento del statu quo. (OZSLAK, 1980:209)

Corroborando estas características (aunque referidas a las políticas de género), RODRIGUEZ GUSTA apunta que *"los entornos tecno-políticos impulsados por el gobierno aún no han logrado que la transversalidad de género en el Estado alcance un ángulo más colectivo y deliberativo. Las sociedades actuales necesariamente conllevan el desarrollo de organizaciones e instituciones complejas, estratificadas e interrelacionadas, y las prácticas deliberativas no están pensadas para reemplazar a estas instituciones. No obstante, las instituciones generan su propia inercia estructural, crean intereses propios y muchas veces cuentan con canales más abiertos o permeables para algunas voces y no otras."* (RODRIGUEZ GUSTA, 2008: 160)

Como se ha visto entonces, el desarrollo tecnológico ha producido un cambio profundo en los esquemas de trabajo de las organizaciones. Específicamente en el sector público, se ha visto que la implantación de cambios genera reacomodamientos y resistencias. En ese marco, se analizará la institucionalización de la Infraestructura de Firma Digital como organismo de la administración nacional.

La Ley Nº 25.506 crea la Infraestructura de Firma Digital y designa como autoridad de aplicación a la Jefatura de Gabinete de Ministros. Esto es así debido al reconocimiento que el legislador hace a la trayectoria en el tema de la Oficina Nacional de Tecnologías de Información. ONTI, la cual depende de dicha jurisdicción. Ahora bien, en el cuerpo legal no se define la forma de organización de dicha Infraestructura.

La ley mencionada asigna obligaciones y facultades a la Jefatura de Gabinete en su calidad de Autoridad de Aplicación. Estas competencias podrían clasificarse en tres rubros:

- **Competencias tecnológicas**: cumplir el rol de autoridad certificante, emitir certificados digitales, controlar el cumplimiento de las calidades tecnológicas requeridas a los certificadores licenciados, etc.

- **Competencias jurídicas**: emitir dictamen legal para el licenciamiento, dictar normas que regulan el valor legal del documento electrónico referidas a conservación, celebrar acuerdos de reconocimiento mutuo con otros países referidos a certificados digitales, resolver recursos administrativos, etc.

- **Competencias organizacionales - administrativas**: administrar sus recursos, dictarse normas de funcionamiento, publicar en Internet, contar con personal especializado, etc.

Como se verá más adelante con mayor detalle, la Infraestructura de Firma *Digital* cumple un rol fundamental tanto desde el punto de vista tecnológico como jurídico. Desde lo tecnológico, el esquema de licenciamiento que presenta se basa en la emisión de un certificado digital para aquellas entidades que son licenciadas. Esto implica constituir y administrar una autoridad certificante raíz que posee un nivel de complejidad tecnológica importante, pues un compromiso en la seguridad podría acarrear la caída de todo el sistema de firma digital.

Por otra parte, el organismo designado como Autoridad de Aplicación de la Infraestructura de Firma Digital, es el órgano que interpreta la norma y tiene la capacidad de regular los aspectos vinculados con el comercio electrónico, el valor jurídico de los documentos digitales, y en general, el marco regulatorio del comercio electrónico y del gobierno digital. Esto es, excede el marco de la administración nacional, alcanzando a la totalidad de las transacciones realizadas en formato electrónico, tanto públicas como privadas.

Qué es una Infraestructura de Firma Digital

Una Infraestructura de Firma Digital, o PKI por sus siglas en inglés (Public Key Infrastructure) es *"una combinación de tecnología (hardware y software), procesos (políticas, prácticas y procedimientos) y componentes legales (acuerdos) que asocian la identidad del poseedor de una clave privada con su correspondiente clave pública, usando la tecnología de criptografía asimétrica"* (KOORN; 2002:1). Los usos de una PKI en entornos digitales pueden ser múltiples: proteger la confidencialidad (mediante la encripción de comunicaciones o de datos almacenados), autenticar la identidad de una persona u organización, informar sobre la integridad de un mensaje o documento electrónico, y garantizar el no repudio de mensajes o transacciones electrónicas.

Una Infraestructura de Firma Digital puede definirse como el conjunto de políticas, procedimientos, hardware, software y recursos humanos entrenados con el

propósito de administrar certificados digitales y pares de claves públicas y privadas, incluyendo las actividades vinculadas con la creación, administración, almacenamiento, distribución y revocación de certificados digitales de clave pública. (GASSON et all, 2005: 16)

Una Infraestructura de Clave Pública vincula claves públicas con entidades (personas físicas o jurídicas), permite a otras entidades verificar las relaciones con dichas claves públicas y provee los servicios necesarios para la administración permanente de las claves en un sistema distribuido. PKI integra certificados digitales, criptografía de clave pública y autoridades de certificación en una completa arquitectura organizacional en red. Una organización típica de PKI abarca la emisión de certificados digitales a usuarios individuales y servidores; software de inscripción de usuarios finales; integración con directorios de certificados; herramientas para la administración, renovación y revocación de certificados; y servicios conexos y asistencia técnica de apoyo. (KUHN et all, 2001:15)

Una PKI se define como el "*conjunto de políticas, procesos, plataformas de servidores, software y estaciones de trabajo utilizados para el propósito de administrar certificados y pares de claves públicas y privadas, incluyendo la habilidad de emitir, mantener y revocar certificados de clave pública*". (KUHN et all, 2001:51)

Una PKI efectiva debe abarcar más que el conjunto de dispositivos y medidas informáticas para manejar claves, pues requiere establecer y mantener relaciones entre esas claves y entidades y acciones del mundo real (CLARKE, 2001: 4.1).

Podría definirse entonces a la PKI como el conjunto de hardware, software, personas, políticas y procedimientos necesarios para crear, administrar, almacenar, distribuir y revocar certificados de clave pública basados en criptografía asimétrica, que facilitan la creación de una asociación verificable entre una clave pública y la identidad (u otro atributo) del tenedor de su correspondiente clave privada. (RIVOLTA, SCHAPPER, 2004: 16). Una falla en cualquiera (una o varias) de estas áreas podría causar la caída de todo el sistema.

Desde el punto de vista tecnológico, los esquemas de firma digital son procesos criptográficos que cumplen funciones similares en relación con los documentos electrónicos que las firmas manuscritas en relación con los documentos en papel. Esta función es la de garantizar la autenticidad del documento a su receptor (autenticación de la autoría del documento), de modo tal que éste podría probar su autenticidad ante terceros, por ejemplo, en un juicio. Un elemento esencial para el uso de las firmas digitales es la disponibilidad de una PKI. Validar una firma digital requiere una clave pública del usuario auténtica. Los certificados (que en términos generales son claves públicas firmadas digitalmente) organizados dentro de una PKI, habilitan la construcción de una relación de confianza sin necesidad de autenticar manualmente cada clave.

Usualmente, una firma digital descansa en tres algoritmos:

- Algoritmo de generación de claves: genera el par de claves (pública y privada)
- Algoritmo de firmado digital del documento: encripta el documento con la clave privada, y genera la firma.

- Algoritmo de verificación de la firma: toma la firma digital del documento (y a veces también el documento), la desencripta y verifica si el procedimiento de verificación es exitoso o no. (GASSON et all, 2005: 20)

Componentes de la Infraestructura de Firma Digital

Las tecnologías de clave pública no pueden garantizar por sí solas la identificación de las personas en el mundo real, ya sea la identificación de personas físicas, organizaciones públicas y privadas o atributos de entidades de todo tipo, tales como servidores.

Para ello, deben adoptarse adicionalmente otras medidas, además de la tecnología de clave pública. Cuando se habla de Infraestructura de Claves Públicas (sinónimo de Infraestructura de Firma Digital), se está aludiendo a este conjunto de elementos que comprende a los pares de claves asociados con una identificación en el mundo real. Asimismo, abarca los mecanismos para generar los pares de claves, los resguardos de seguridad para alojar la clave privada, y en este sentido cabe mencionar los dispositivos de generación y almacenamiento de la clave privada, así como los mecanismos de resguardo de la clave privada, que pueden ser desde una simple password, una passphrase, o bien basarse en biometría (por ejemplo, la huella dactilar).

Una característica distintiva de la PKI es que el receptor del mensaje debe tener acceso a la clave pública de la persona que lo remite. Es así como surge el concepto de certificado digital, así como la necesidad de contar con directorios en los cuales se publiquen dichos certificados digitales, y que sean accesibles para su consulta pública.

A fin de satisfacer los requerimientos detallados en el punto precedente, una PKI contempla los siguientes elementos:

- Estándares y protocolos;
- Software para implementar un gran número de funciones y protocolos;
- Protección de las claves privadas;
- Un repositorio de claves públicas, su creación, mantenimiento y uso;
- Los elementos que permitan firmar digitalmente los certificados por la entidad de certificación;
- Un marco legal que regule y apoye la infraestructura y su operación y
- Servicios para apoyar la operación de aplicaciones que utilicen firma digital.

Para el Grupo de Trabajo en Tecnologías de Seguridad del National Institute Standards Technology – NIST (organismo del gobierno de Estados Unidos que fija estándares tecnológicos), desde el punto de vista funcional, los componentes de una PKI incluyen a las autoridades de certificación (CA por sus siglas en inglés Certification Authorities), Autoridades de Registro (RA por sus siglas en inglés – Registration Authorities), repositorios y archivos. Distingue dos tipos de usuarios: los suscriptores de certificados y las terceras partes que confían en el certificado.

Adicionalmente, podría considerarse a las Autoridades de Atributo como un componente opcional (KUHN et all; 2001: 16).

En síntesis, una infraestructura de clave pública incluye:

- Una Autoridad Certificante (CA por sus siglas en inglés), también denominada Entidad de Certificación o Certificador, según la distinta legislación. La CA emite y garantiza la autenticidad de sus Certificados Digitales. Un Certificado Digital incluye la clave pública u otra información respecto de la clave pública.

- Una Autoridad de Registro (RA por sus siglas en inglés) – valida los requerimientos de Certificados Digitales. La Autoridad de Registro autoriza la emisión del certificado de clave pública al solicitante por parte de la Autoridad Certificante.

- Un sistema de administración de certificados – una aplicación de software provisto por el vendedor de PKI.

- Un directorio en el cual los certificados y sus claves públicas son almacenados.

- El Certificado Digital incluye el nombre de su titular y su clave pública, la firma digital de la Autoridad Certificante que emite el certificado, un número de serie y la fecha de expiración.

- Suscriptores: son las personas o entidades nombrados o identificados en los certificados de clave pública, tenedores de las claves privadas correspondientes a las claves públicas de los certificados digitales.

- Usuarios: son las personas que validan la integridad y autenticidad de un documento digital o mensaje de datos, en base al certificado digital del firmante.

La importancia del tema radica en que un certificado digital, o certificado de clave pública, es por lo tanto una versión electrónica de un documento de identificación personal que *"establece las credenciales de una persona o entidad y autentica su conexión"*. (RIVOLTA, SCHAPPER; 2004: 24).

Cabe destacar que el certificado digital contiene la firma digital de la Autoridad Certificante para permitir a cualquier receptor la confirmación de su autenticidad. Por su parte, la firma digital de la Autoridad Certificante en sí misma puede requerir verificación. La verificación de autenticidad de la firma digital de la AC se realiza *"mediante una jerarquía entre las diferentes Autoridades Certificantes, en la cual la Entidad de Certificación de más alto nivel (Autoridad Certificante Raíz o Root CA en inglés) tiene sólo un certificado autofirmado. Este certificado puede ser transmitido fuera de línea o de otra manera encontrarse ya incorporado en los navegadores"* de internet (RIVOLTA, SCHAPPER; 2004: 24).

III.- FACTORES TECNOLOGICOS DE LA INFRAESTRUCTURA DE FIRMA DIGITAL

En el presente capítulo se presentan en forma breve y accesible los conceptos de criptografía simétrica y asimétrica y tecnología de clave pública, subyacentes en la firma digital. También, se describe sencillamente el procedimiento de firma digital de un documento electrónico.

A fin de transmitir una acabada idea de la complejidad de una Infraestructura de Firma Digital, se identifican y describen en forma accesible sus principales componentes técnicos: Autoridades de Certificación, Autoridades de Registro, certificados digitales, listas de certificados, etc.

En igual sentido se identifican los principales usos de la tecnología de clave pública: confidencialidad, seguridad, autenticación, conservación de documentos. Asimismo, se describen mecanismos de autenticación en entornos electrónicos alternativos. (KUHN et all; 2001), (CLARKE; 2001), (RIVOLTA, SCHAPPER; 2004), (BUGONI, RIVOLTA; 2007),

Nociones elementales de Criptografía Simétrica y Asimétrica

La criptografía, voz de origen griego que significa "escritura oculta", es el arte y la ciencia que estudia la transformación (encripción) de información legible (texto plano) en otra que no se puede leer directamente por estar en un formato ininteligible (texto cifrado). En este proceso la información es codificada (cifrada) para evitar que sea leída o alterada por terceras personas. La información cifrada será ininteligible para todo aquel que no tenga capacidad de descifrarla. Esta encripción protegerá la confidencialidad de la información tanto al ser transmitida como archivada (RIVOLTA, SCHAPPER; 2004: 13).(REYES KRAFT; 2005: 115).

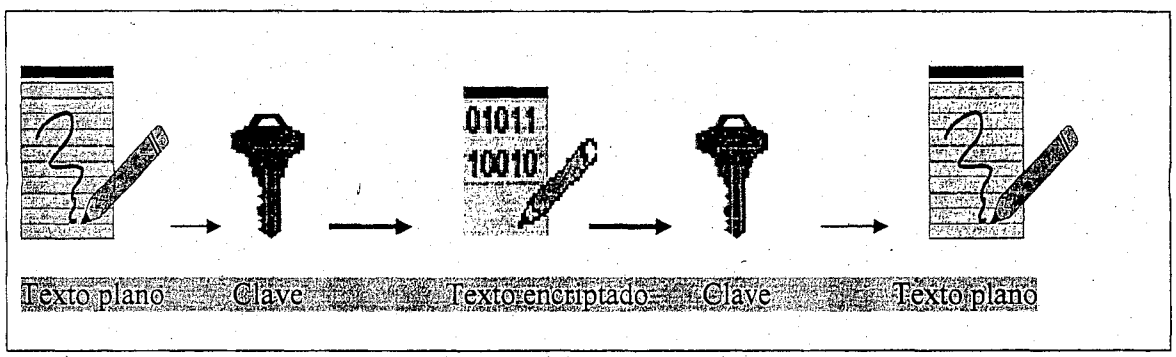
El cifrado y descifrado requieren una formula matemática o algoritmo y una clave, para convertir los datos "en claro" a datos cifrados y viceversa.

Dentro de la criptografía disputan permanentemente dos ramas: los criptógrafos, dedicados a inventar algoritmos, y los criptoanalistas, dedicados a romper dichos algoritmos. Esta puja permanente brinda seguridad respecto de la potencia de los algoritmos de encripción. "*Durante dos mil años, los creadores de cifras han luchado por preservar secretos, mientras que los descifradores se han esforzado por revelarlos. Ha sido siempre una carrera reñida..... La invención de la criptografía de clave pública y el debate político en torno al uso de criptografía potente nos traen al momento presente, y es evidente que los criptógrafos están ganando la guerra de la información.*" (SINGH; 2000: 317).

Criptografía Simétrica

La criptografía simétrica aplica una misma clave para encriptar y desencriptar un documento. Se trata de una clave compartida, una password, en nuestros días por ejemplo, la clave con la cual accedemos a los cajeros electrónicos, y que es compartida por el administrador del sistema. (RIVOLTA, SCHAPPER; 2004: 13) (KUHN et all; 2001: 9)

Figura Nº 1: CRIPTOGRAFIA SIMETRICA



Fuente: Elaboración propia

La criptografía de claves simétricas, usa una sola clave que ambas partes poseen, dicha clave debe ser comunicada de una parte a la otra, es decir, que ambas partes deben conocer la misma clave que encripta y desencripta (RIVOLTA, SCHAPPER; 2004: 14).

Criptografía Asimétrica

A partir de los años ´70, surgió una nueva rama de la criptografía, la criptografía asimétrica, la cual se basa en dos claves íntimamente relacionadas entre sí pero diferentes: la clave pública y la clave privada. La criptografía asimétrica intenta superar los problemas que presenta la tradicional criptografía simétrica, esto es, la dificultad para proteger la confidencialidad de la clave, y la complejidad de su distribución segura.

La prehistoria de la criptografía asimétrica se remonta al paper presentado por Diffie y Hellman en 1976, quienes proponían un Directorio de Claves que los usuarios podrían consultar para conocer las claves públicas de otros usuarios. El esquema de firma digital fue completado por Kohnfelder in 1978, quien propuso el concepto de certificados. (ADAMS, 2004: 2), (GUTMANN; 2002:1)

La criptografía asimétrica utiliza algoritmos que emplean dos claves diferentes pero matemáticamente vinculadas: una clave para encriptar los datos y otra clave para desencriptarlos. Dado que ambas claves son casi imposibles de derivar una de la otra, se considera que la criptografía asimétrica cumple la condición de "irreversibilidad" (RIVOLTA, SCHAPPER; 2004: 15). (KUHN et all; 2001: 11)

Cómo se generan las claves asimétricas

La clave privada es solamente conocida por su titular, y la clave pública es de acceso público. Ambas claves, se generan a partir de dos números primos seleccionados al azar. El producto de ambos números primos es la clave pública, y la clave privada se calcula en base a una operación de aritmética modular basada en ambos números primos. A continuación se presenta un ejemplo:

Número primo p=
1306932240210065546037290586095547112555655572202791827140049682054
3230709995361923264497263426673522981355324446575560717217090794993
4640728118 5886210303

Número primo q=
1154329170630485499128205326655648234534038128324936193803563507212
3140767619879947055794178155878831076988621881878883273530930538636
731138191162287228337

Clave Pública:
n= p*q
=
1508630008911927413198409146685444644675143717844390704505767449193
2959261191279542290348151510881966475744276056713725950587892510033
5308535018685795925041443616170203299241549726752965481817691505256
8550945498569688334837087443627547192152419453307 31
e= 5

Clave Privada:
d= e-1 mod ((p-1)(q-1))
=
6034520035647709652793636586741778578700574871377562818023069796773
1837044765118169161392606043527865902977104226854903802351570040134
1234140074743183700067324008247191155159579070501814113387178273006
3112573616833477632693490669900513965319921633287 42

Dónde se alojan las claves

La generación del par de claves (pública y privada) requiere de precauciones especiales.

Cuando se crea el par, una de las claves, que es en realidad una secuencia muy larga de números, es designada como clave privada, o sea la que en el futuro se empleará para firmar los mensajes, por ello su almacenamiento requiere máxima seguridad debido a que no debe ser conocida ni utilizada por nadie, excepto por su titular (quien la generó).

En consecuencia, la clave privada se encripta y protege mediante una contraseña y se la guarda en un disco, diskette o, idealmente, en una tarjeta inteligente (smart card) o dispositivo criptográfico (token). Para proteger mejor la clave privada, se utiliza una clave simétrica para encriptarla y desencriptarla. Esta clave simétrica puede ser una password, una passphrase o un dato biométrico como la huella dactilar.

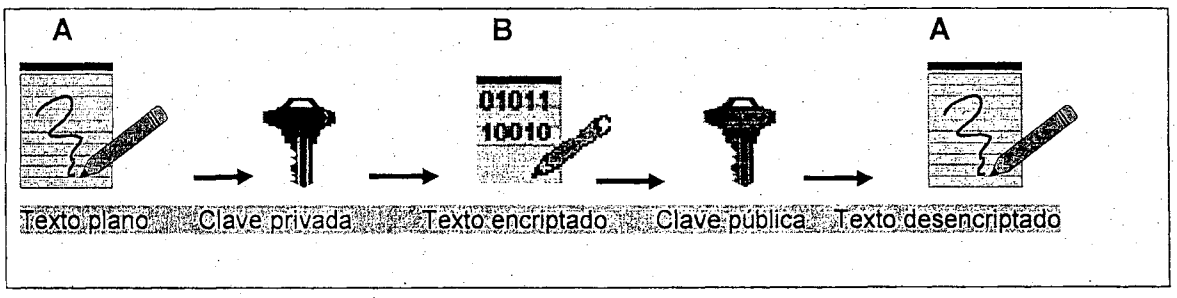
La clave pública, en cambio, debe ser conocida por todos, por tal motivo es enviada a una Autoridad de Certificación (que actúa como tercera parte confiable), quien la incluye en un certificado digital.

A su vez, los certificados digitales son publicados en el sitio de internet de la autoridad certificante, para ser consultados acerca de su validez.

Cómo se encripta y desencripta un documento con ambas claves

En el caso de la criptografía asimétrica, se emplean ambas claves, la privada y la pública para encriptar y desencriptar el documento digital.

Figura Nº 2: CRIPTOGRAFIA ASIMETRICA



Fuente: Elaboración propia

Dado un documento A en claro (texto plano), se encripta con la clave privada solamente conocida por el titular y se obtiene un documento encriptado (B). Para poder desencriptarlo, es necesario aplicar la clave pública relacionada con aquella clave privada que se usó para encriptar. Caso contrario, por ejemplo, si se utilizara la misma clave privada usada para encriptar, no se podría obtener nuevamente el documento en claro. Solamente con la aplicación de la clave pública correspondiente, se podrá desencriptar el documento (A). (KHUN et all; 2001: 11)

Qué es una firma digital

Como se mencionó, el proceso de firma digital de un documento requiere la existencia de un par de claves, una privada y una pública. Además, es necesario garantizar la relación de la clave pública con una persona determinada, lo cual permitirá identificar al firmante de un documento electrónico. Esto se logra mediante una serie de procedimientos técnicos y administrativos que las autoridades de certificación aplican para emitir certificados digitales. Más adelante se verán estos procedimientos y demás características de un certificado digital.

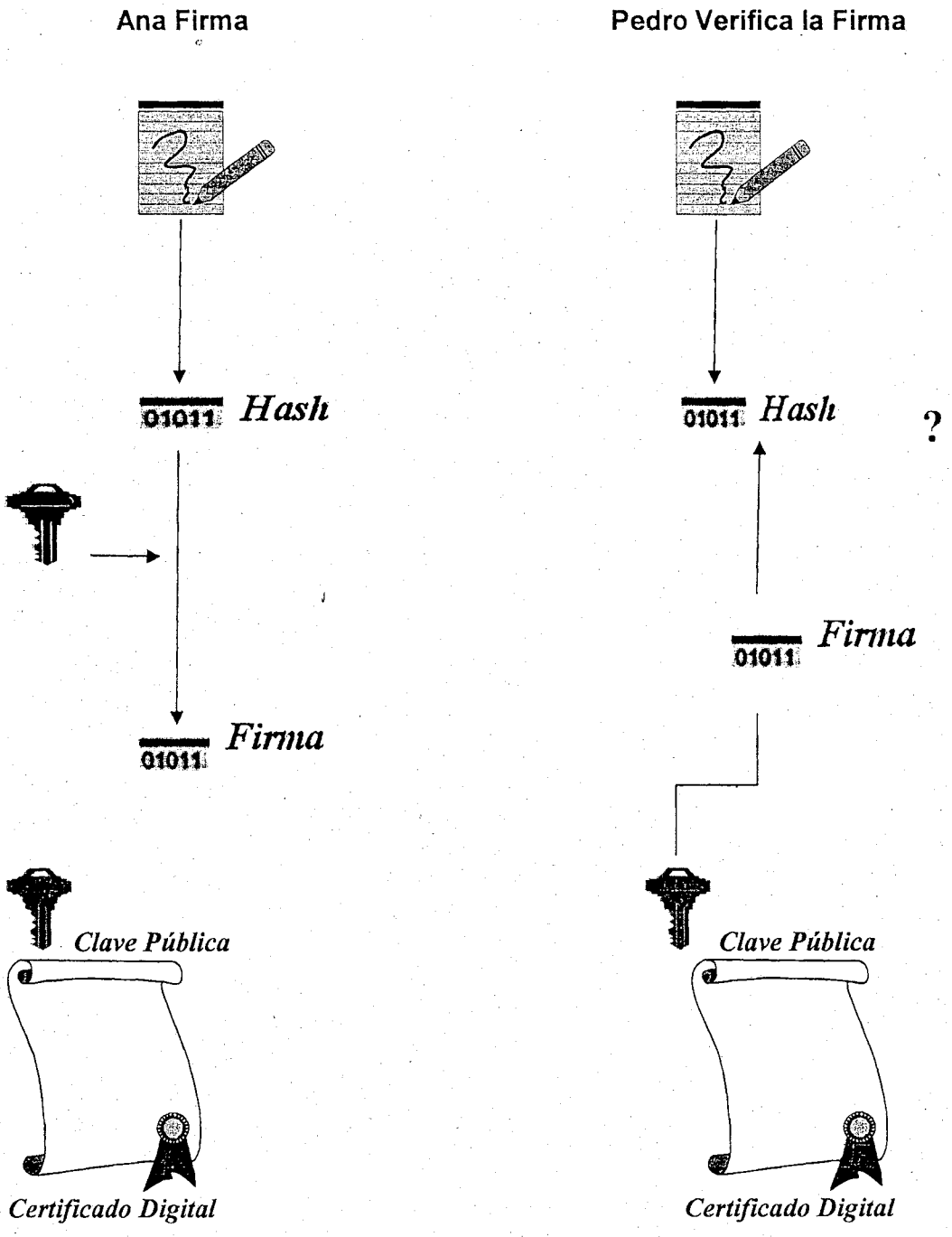
Ahora se analizará el proceso de firmado digital de un documento electrónico. Según la Ley argentina, el proceso de firmado digital de un documento electrónico presenta dos momentos:

- un primer momento en el cual el suscriptor de un certificado digital firma digitalmente un documento electrónico

- un segundo momento en el cual un tercero, receptor de ese documento electrónico firmado digitalmente, verifica la autoría e integridad del mensaje.

Las firmas digitales son una aplicación muy importante de esta tecnología de claves públicas. En efecto, la persona que remite un mensaje utiliza su clave privada para encriptar el digesto seguro del mensaje (obtenido mediante el cálculo de la función de hash del mensaje). Remite al receptor el mensaje, el digesto seguro encriptado y su certificado digital que contiene su clave pública. El receptor desencripta el digesto utilizando la clave pública del emisor del mensaje, la cual se corresponde con la clave privada del mismo. El receptor del mensaje, verifica la firma digital del mensaje, para lo cual recalcula la función de hash de este, y si ambos resultados coinciden, verifica que el mensaje no ha sido alterado, con lo cual puede tener certeza de su integridad. Si fue posible desencriptar el digesto con la clave pública correspondiente al emisor del mensaje, verifica la autoría del documento electrónico firmado digitalmente. (RIVOLTA, SCHAPPER; 2004: 17) (KUHN et all; 2001: 11)

Figura Nº 3: Firma digital de un documento



Fuente: Elaboración propia

Certificados digitales

Un Certificado Digital o Certificado de Clave Pública, en adelante, CD, es un documento electrónico emitido y firmado digitalmente por una Autoridad de

Certificación, que identifica unívocamente a un suscriptor durante un período determinado (el período de vigencia del certificado) y que contiene la clave pública de su titular, correspondiente con la clave privada que utiliza para firmar digitalmente. (RIVOLTA, SCHAPPER; 2004: 20)

Los certificados digitales contienen en general los siguientes datos:

- Firma digital de la Autoridad de Certificación que lo emite;
- Nombre y dirección electrónica del suscriptor;
- Identificación del suscriptor nombrado en el certificado;
- Nombre, dirección electrónica y lugar donde realiza actividades la Autoridad de Certificación, y los antecedentes de la autorización obtenida;
- Clave pública del suscriptor;
- Metodología utilizada para verificar la firma digital del suscriptor;
- Número de serie del certificado;
- Fecha y hora de emisión y expiración del certificado; e,
- Identificación de la Política de Certificación bajo la cual el certificado fue emitido.

Vigencia

Para que una firma digital sea legalmente válida, es necesario que el certificado se encuentre vigente al momento de la verificación. Esto constituye un problema para implementaciones administrativas, ya que con el correr del tiempo el certificado pierde validez, pues es emitido por un período determinado. Podría ocurrir, por ejemplo, en el caso de licitaciones electrónicas, que el sistema requiera la firma digital de la oferta por parte del licitante. En el momento de enviar la oferta, la firma digital verifica correctamente. Pero al cabo de cinco años, al haber caducado el certificado digital con el cual fue firmada, la verificación no será exitosa.

Revocación

Los certificados digitales pueden ser revocados, suspendidos y refirmados. Algunas legislaciones contemplan la suspensión de certificados, pero en general no es común, pues introduce confusiones. Se consideran los certificados vigentes, los certificados revocados y los certificados expirados. Las Autoridades de Certificación tienen la obligación de publicar en sus sitios de Internet las listas de certificados revocados para que las terceras partes que confían consulten si el certificado se encuentra vigente o no. Esta consulta puede automatizarse, pero implica disminución de performance de los sistemas, aun en el caso de que todo funcione perfectamente bien.

Clases de certificados

Existen varios tipos de certificados, tipificados según la información que se controla para su emisión. Desde los más simples, en los cuales solamente se verifica la existencia de una cuenta de correo electrónico, hasta más fuertes en los cuales se requiere de la presencia física y presentación de documentación para acreditar la identidad de la persona que lo solicita.

Los **certificados clase 0**, en los cuales se solicita solamente una cuenta de correo electrónico, no tienen ningún valor de seguridad pues no se controla la veracidad de la información contenida en ellos.

Los **certificados digitales avanzados**, suponen la verificación de los datos de identidad del solicitante, quien debe presentarse personalmente ante la Autoridad de Certificación o de Registro, munido de la documentación que acredite su identidad.

Si el **certificado** contuviese **atributos**, por ejemplo, el poder de representación de la persona otorgado por una empresa, deberá además presentar el poder en papel certificado por notario. El **problema** se presenta respecto de la **vigencia de los poderes**, pues podría haber sido emitido el certificado en forma correcta, pero el poderdante podría revocar el poder antes de la expiración de la vigencia del certificado, con lo cual el uso del certificado no garantiza la autoría del documento, en la medida que la persona no mantiene el poder de representación de la empresa.

Otro **problema** se deriva de la exigencia de **presentarse en persona** para obtener el certificado digital, lo cual podría representar un **serio obstáculo** para aquellas personas ubicadas en zonas remotas. Esto constituye un problema para la implementación del gobierno electrónico y de las compras públicas electrónicas. Colisiona con el principio de no discriminación que promueve la mayor accesibilidad a los servicios e informaciones del gobierno. En efecto, por ejemplo en el tema de licitaciones públicas podría significar una merma de la competencia de proveedores locales por este motivo. Respecto de las licitaciones internacionales, al hecho de requerir la presencia física para emitir el certificado al potencial proveedor, se suma el tema de la **validez de los documentos que acreditan la identidad y la personería**. En efecto, qué documentos se les va a exigir, los válidos en el país de origen, los válidos internacionalmente, además de la apostilla o el visado consultar, las traducciones, las certificaciones de las traducciones, etc.

Autoridades de Certificación

Desde una perspectiva legal, un Certificador Licenciado (en adelante, AC por la denominación usual internacional Autoridad de Certificación), es aquella institución o persona jurídica que está facultada por un órgano del Estado para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales

Desde el punto de vista técnico, el Certificador Licenciado es el pilar básico de la PKI. Se compone de hardware, software, procedimientos y personal que lo opera. Los Certificadores o Autoridades de Certificación son conocidos por dos atributos: su nombre y su certificado digital. (KUHN et all; 2001: 17)

Son funciones de una AC:

- Emitir certificados de clave pública, lo cual implica la creación y firma digital de los mismos.
- Mantener información sobre el estatus de los certificados y emitir listas de certificados revocados.
- Publicar en su sitio web la lista de certificados vigentes (no expirados ni revocados) y las listas de certificados revocados, para ser consultadas por las terceros partes que confían en dichos certificados, y
- Mantener archivos y resguardar la información contenida en los certificados expirados emitidos.

Estas funciones pueden ser realizadas por la AC o bien ser delegadas en otros componentes de la PKI, tales como las Autoridades de Registro.

Una Autoridad de Certificación puede emitir certificados a usuarios, a otras autoridades de certificación o a ambos. Cuando una AC emite un certificado digital, se entiende que el suscriptor del mismo (la persona nombrada en el certificado) posee la clave privada que se corresponde con la clave pública contenida en el certificado. Si la AC incluye información adicional en el certificado, la AC está afirmando que dicha información corresponde también a la persona titular del mismo. Esta información adicional puede ser información de contacto (una dirección de correo electrónico), o información sobre la política bajo la cual el certificado fue emitido (por ejemplo, aplicaciones para las cuales puede ser utilizado el certificado). Cuando la persona titular del certificado es otra AC, la AC que lo emite afirma que los certificados digitales que la otra AC emitirá en el futuro, son confiables.

La AC inserta su nombre en cada certificado y lista que emite, las cuales son firmadas digitalmente con la clave privada de la AC.

Para que una tercera parte que confía en un certificado pueda verificar exitosamente la firma digital, es necesario que previamente, confíe a su vez en el certificado digital de la Autoridad de Certificación que lo emitió. Esto constituye un problema para el uso masivo de la firma digital, y se trata de superar mediante esquemas cerrados de firma digital que admiten solamente certificados emitidos por AC determinadas. La divulgación masiva de los certificados digitales de las AC es uno de los desafíos pendientes. Este certificado en nuestro país es emitido por la Autoridad de Aplicación de la Ley N° 25.506 de firma digital para los certificadores licenciados, a partir de la Autoridad Certificante Raíz.

Una AC debe contar con documentos técnicos aprobados por el órgano estatal habilitante, que establezcan los procedimientos a seguir para el desarrollo normal de sus actividades y ante casos de contingencia, y además contar con un manual específico de seguridad. Estos documentos son:

- **Manual de Procedimientos**: Es el conjunto de prácticas utilizadas por la Autoridad de Certificación en la emisión y administración de los certificados. En inglés, Certification Practice Statement (CPS);
- **Plan de Cese de Actividades**: Es el conjunto de actividades aprobadas por el ente público habilitante, a desarrollar por la Autoridad de Certificación en caso de finalizar la prestación de sus servicios;
- **Plan de Contingencias**: Es el conjunto de procedimientos a seguir por la Autoridad de Certificación ante la ocurrencia de situaciones no previstas que puedan comprometer la continuidad de sus operaciones;
- **Plan de Seguridad**: Es el conjunto de políticas, prácticas y procedimientos destinados a la protección de los recursos de la Autoridad de Certificación;
- **Políticas de Certificación**: Es el conjunto de información relativa al cumplimiento de los requisitos de emisión de los certificados digitales, que constituyen el contrato entre la Autoridad de Certificación y el suscriptor. Se vinculan con cada clase de certificado digital.

Actualmente en la Infraestructura de Firma Digital de la República Argentina son Autoridades de Certificación licenciadas las de AFIP y ANSES para las aplicaciones de sus propios organismos. En la ONTI funciona desde el año 2000 una Autoridad Certificante para el Sector Público Nacional que aún no ha sido licenciada.

Autoridades de Registro

Se denomina **Autoridad de Registro** a toda persona u organización privada o pública, que tiene por función validar los datos de identidad de las personas físicas y jurídicas, suscriptoras de certificados. En inglés se denomina Registration Authority (RA). (RIVOLTA, SCHAPPER; 2004: 20)

La Autoridad de Registro es una entidad que participa de la cadena de confianza de las Autoridades de Certificación, verificando los datos, documentación e identidad de los suscriptores de certificados. (KUHN et all; 2001: 17). Puede ser parte o no de la misma. En general, las áreas de recursos humanos cumplen esta función respecto de las Autoridades de Certificación de organismos públicos.

Cada Autoridad Certificante puede tener una lista de Autoridades de Registro acreditadas, las cuales participan de su cadena de confianza. Cada Autoridad de Registro se da a conocer ante la Autoridad Certificante por su nombre y por el certificado de clave pública. La Autoridad de Certificación verifica cada vez la firma digital de la Autoridad de Registro lo cual le permite mantener un circuito seguro de emisión de certificados.

La información que analiza la Autoridad de Registro puede provenir directamente del suscriptor del certificado, como por ejemplo, su documento nacional de identidad, o bien de una tercera parte, como por ejemplo, la función que desempeña en el organismo al que pertenece.

Algunas de las funciones de las Autoridades de Registro son:

a) Recibir las solicitudes de emisión de certificados digitales;

b) Validar la identidad y la documentación respaldatoria de los datos de los solicitantes de certificados digitales;

c) Validar otros datos de los solicitantes de certificados digitales que se presenten ante ella cuya verificación delegue la Autoridad de Certificación, para el otorgamiento de certificados digitales con atributos determinados, como por ejemplo, calidad de representante de una persona jurídica, calidad de funcionario de una organización, calidad de miembro de un colegio profesional, entre otros;

d) Remitir las solicitudes aprobadas a la Autoridad de Certificación con la que se encuentre operativamente vinculada;

e) Recibir y validar las solicitudes de suspensión o revocación de certificados digitales, y su posterior envío a la Autoridad de Certificación con la que se vinculen, una vez que se realicen las verificaciones de identidad correspondientes;

f) Identificar y autenticar a los solicitantes de suspensión o revocación de certificados digitales emitidos por la Autoridad de Certificación;

g) Conservar y archivar toda la documentación de respaldo del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por la Autoridad de Certificación;

h) Cumplir las normas legales aplicables así como las que pudiera dictar el órgano público habilitante en relación con la protección de datos personales, la confidencialidad de la información y otros temas vinculados con la actividad;

i) Cumplir las disposiciones que establezca la Política de Certificación y el Manual de Procedimientos de la Autoridad de Certificación con la que se encuentre vinculada, en la parte que resulte aplicable; y,

j) Colaborar para la realización de inspecciones o auditorías por parte de la Autoridad de Certificación o el órgano estatal habilitante.

Una Autoridad de Registro puede constituirse como una única unidad o como varias unidades dependientes jerárquicamente entre sí, pudiendo delegar su operación en otras Unidades de Registro, siempre que medie la aprobación de la Autoridad de Certificación y la respectiva autorización del ente público habilitante.

Actualmente existen 61 Autoridades de Registro dependientes de la Autoridad Certificante de la ONTI, pertenecientes en general a los poderes judiciales de las provincias (en virtud del Convenio de Comunicación Electrónica Interjurisdiccional firmado entre el Ministerio de Justicia y los Superiores Tribunales de Justicia de todo el país en el año 2000), aplicaciones de la Administración Nacional y de otras jurisdicciones y gobiernos.[3]

[3] Son Autoridades de Registro de la Autoridad Certificante de la ONTI: Ministerio Público Nacional: Procuración General de la Nación, Defensoría General de la Nación. Consejo de la Magistratura CABA, Superiores Tribunales de Justicia de las Provincias de Catamarca, Chaco, Córdoba, Entre Ríos, Jujuy, La Rioja, Mendoza, Neuquén, Río Negro, Salta, Santa Fé, Santiago del Estero, Tierra del

Ente público habilitante y de control

Si bien desde el punto de vista técnico, la existencia de una Autoridad Certificante es libre, y no requiere más que una importante inversión en recursos tecnológicos, desde la perspectiva legal, en aquellos países que han apoyado sus normas de comercio electrónico en estructuras de PKI, como la de Argentina y en la mayoría de la región, existen órganos del Estado cuya función es regular, controlar y autorizar su funcionamiento.

Estos órganos rectores en firma digital, son los que aprueban los estándares, y habilitan a las Autoridades de Certificación para emitir certificados digitales que permitan a las personas firmar digitalmente. (RIVOLTA, SCHAPPER; 2004: 24)

Respecto del grado de intervención del Estado, existen tres criterios en este tema:

1.- Criterio de libertad de mercado

2.- Criterio de acreditación voluntaria

3.- Criterio de licenciamiento obligatorio

1.- Criterio de libertad de mercado:

Las Autoridades de Certificación funcionan por su propio riesgo, y basan su desarrollo en el prestigio que obtienen por su desempeño. Así han funcionado hasta ahora sin mayores problemas, librados a las fuerzas del mercado que premian al más competente. Las grandes empresas de certificación digital no están supervisadas por ningún órgano público, y fundan su prestigio en la

---

Fuego, Antártida e Islas del Atlántico Sur y Tucumán. Administración Nacional: Presidencia de la Nación: Secretaría General, Administración de Parques Nacionales, Sistema de Identificación Nacional Tributario y Social, Secretaría de Programación para la Prevención de la Drogadicción y la Lucha contra el Narcotráfico; Jefatura de Gabinete de Ministros: Oficina Nacional de Tecnologías de Información, Oficina Nacional de Contrataciones; Ministerio de Defensa: Ministerio de Defensa, Estado Mayor General del Ejército; Ministerio de Desarrollo Social: Lotería Nacional S.E.; Ministerio de Economía y Producción: Subsecretaría de Presupuesto, Superintendencia de Seguros, Instituto Nacional de la Propiedad Industrial, Instituto Nacional de Vitivinicultura; Ministerio de Educación: Universidad Tecnológica Nacional - Facultad Regional Mendoza; Ministerio de Ciencia, Tecnología e Innovación Productiva; Ministerio del Interior: Ministerio del Interior, Agencia Nacional de Seguridad Vial; Ministerio de Justicia, Seguridad y Derechos Humanos: Ministerio de Justicia y Derechos Humanos, Servicio Penitenciario Federal; Ministerio de Planificación Federal, Inversión Pública y Servicios: Ministerio de Planificación Federal, Inversión Pública y Servicios, Comisión Nacional de Energía Atómica, Comisión Nacional de Comunicaciones, Fondo Fiduciario Federal de Infraestructura Regional, Nucleoeléctrica Argentina; Ministerio de Relaciones Exteriores, Comercio Internacional y Culto: Comisión Nacional de Actividades Espaciales; Ministerio de Salud: Instituto Nacional Unico Coordinador de Ablación e Implante (INCUCAI), Superintendencia de Servicios de Salud, Administración de Programas Especiales; Ministerio de Trabajo, Empleo y Seguridad Social: Ministerio de Trabajo, Empleo y Seguridad Social, Superintendencia de Riesgos del Trabajo; Banco Central de la República Argentina; Sindicatura General de la Nación. Otras Jurisdicciones / Otros Poderes: Auditoría General de la Nación, Gobiernos de las Provincias de Corrientes y Chubut.

solidez de sus servicios, de hecho, son las principales proveedoras de certificados digitales para autenticación de sitios web. Ejemplo: sistema Estados Unidos.

2.- Criterio de acreditación voluntaria:

Existe un órgano público que emite licencias para autoridades certificantes, pero la acreditación es voluntaria, aunque difiere el valor legal de los certificados que emiten. Si la Autoridad Certificante está habilitada por el Estado, sus certificados tendrán el reconocimiento jurídico suficiente para producir firmas digitales. Si por el contrario, la Autoridad de Certificación no se ha licenciado ante el órgano rector, sus certificados tendrán un reconocimiento legal limitado a firma electrónica. Ejemplo: sistema argentino.

3.- Criterio de licenciamiento obligatorio:

Existe un órgano rector que emite licencias para funcionar. Todas las autoridades certificantes deben ser licenciadas ante el mismo, en un esquema similar al de telefonía. Ejemplo: sistema República Dominicana.

Los mencionados órganos públicos rectores tienen amplias facultades para definir estándares aplicables, políticas de certificación, procedimientos. Tienen facultades de auditoría y control sobre las autoridades certificantes y tienen poder sancionatorio.

Desde el punto de vista tecnológico, la intervención del Estado respecto de la habilitación de Autoridades Certificantes puede darse de dos formas:

- **Acreditación tecnológica, operando como Autoridad Certificante Raíz**, en la cual el órgano rector en materia de firma digital emite el certificado de las autoridades certificantes que habilita, como en el caso de Brasil y Argentina, o

- **Acreditación administrativa**, en la cual el Estado supervisa y aprueba los recursos y documentación de cada Autoridad Certificante, pero ésta emite su propio certificado, como el ejemplo de República Dominicana.

En el primer esquema el riesgo es mayor, pues el compromiso de la clave de la AC Raíz haría caer todo el sistema.

En síntesis, el órgano público rector es *"responsable, dentro de lo que establece la ley, de:*

- *Otorgar licencias, establecer requisitos mínimos de las políticas de certificación y dar formal reconocimiento a los estándares técnicos.*

- *Autorizar, regular o brindar otro reconocimiento gubernamental o legal al conjunto de Autoridades Certificantes, las cuales son administradas por los respectivos responsables de Políticas y Operacionales.*

*La **Acreditación** es el procedimiento por el cual un cuerpo con autoridad declara los criterios bajo los cuales serán evaluados los componentes de la PKI y los responsables de realizar dichas evaluaciones.*

La Autoridad de Acreditación es una entidad que gerencia la PKI, con la autoridad para permitir a una entidad subordinada de la PKI (como por ejemplo, una Autoridad Certificante) a operar dentro de un dominio particular" (RIVOLTA, SCHAPPER; 2004: 29).

Sistema de auditoria

Una vez que se implementa una Infraestructura de Claves Públicas, se requieren garantías respecto de la calidad del diseño de los sistemas y de la efectividad del ambiente de control de las Autoridades de Certificación. Esto es cierto tanto para los suscriptores y usuarios reales o potenciales de los certificados digitales, como para los directivos de entidades involucradas o para aquellos terceros que deben confiar en los certificados digitales. Por consiguiente, se hace necesaria la realización de evaluaciones independientes que permitan comprobar el cumplimiento de los requerimientos tecnológicos y de procedimiento por parte de las Autoridades de Certificación, mediante la realización de auditorías especializadas. (MARTA, PRANDINI, RIVOLTA; 2003: 22)

Los países que han emitido normas referidas a la implementación de estas tecnologías, han concluido que las auditorías son cruciales para determinar el cumplimiento de lo establecido en las normas que regulan los esquemas nacionales de acreditación. (MARTA, PRANDINI, RIVOLTA; 2003: 22)

Las auditorías son procesos formales y necesarios para las Autoridades de Certificación, que tienen por objeto verificar el cumplimiento oportuno de las normas, políticas y procedimientos relacionados con la prestación de los servicios de certificación, y evaluar si se han implementado los controles necesarios para garantizar un ambiente confiable para la administración del ciclo de vida de los certificados.

Constituyen **objetivos de control** (KOORN; 2002: 2):

a. **Ambiente de Control de la Autoridad de Certificación**: comprenden, entre otros, aquellos objetivos relacionados con las políticas de certificación, los manuales de procedimientos y demás documentación técnica, la administración de la seguridad física y lógica, del personal y de los accesos a los sistemas, la clasificación y el control sobre los activos, el desarrollo y mantenimiento de las aplicaciones de la Autoridad de Certificación y la continuidad del negocio.
b. Controles sobre la administración del **ciclo de vida de las claves criptográficas**: incluyen, entre otros, los controles relacionados con la generación, administración, backup, recuperación, distribución y destrucción de las claves de la Autoridad de Certificación, la administración del hardware criptográfico y los servicios de generación de claves del suscriptor provistos por la Autoridad de Certificación.
c. Controles sobre el **ciclo de vida del certificado**: comprenden, entre otros, aquellos controles relacionados con la solicitud, emisión, distribución,

administración, renovación, suspensión y revocación de los certificados emitidos por las Autoridades de Certificación y la publicación del estado de los mismos.

En los casos en los que el órgano rector actúa como Autoridad Certificante Raíz, también debe ser objeto de auditorías como tal. En estos casos, sin embargo, se produce una paradoja en el sentido de que las auditorías no son independientes, ya que el propio órgano de control es autocontrolado. La confiabilidad de todo el sistema descansa sobre las auditorías que el órgano rector se hace a sí mismo. Otro problema surge en virtud de la escasa madurez del tema en general, ya que actualmente no existen demasiadas experiencias de auditorías sobre firma digital, con lo cual se dificulta su implementación.

Las auditorías pueden ser realizadas por auditores individuales o por cuerpos de auditores reconocidos por el órgano de acreditación de PKI. *"El órgano de acreditación de PKI es el responsable de evaluar el cumplimiento de las Autoridades Certificantes de los requisitos operacionales, procedimentales y de administración en relación con las políticas establecidas, los manuales de procedimientos, estándares y criterios y de producir el informe de auditoría correspondiente"* (RIVOLTA, SCHAPPER; 2004: 29).

Suscriptor del certificado digital

Se entiende por suscriptor o titular de certificado digital a la persona que contrata con una Autoridad de Certificación la expedición de un certificado de clave pública. (RIVOLTA, SCHAPPER; 2004: 20)

Las legislaciones establecen derechos y obligaciones para los suscriptores, fundamentalmente, la principal obligación es mantener en secreto su clave privada.

En general, las normas autorizan la emisión de certificados solamente a personas físicas, contemplando la inclusión de ciertos atributos dentro del cuerpo del certificado, como por ejemplo, la calidad de representante de una persona ideal. Otras legislaciones admiten en cambio, tanto la emisión de certificados a personas físicas, como a personas jurídicas, como a servidores en representación de la persona que lo ha programado.

Usuarios de los certificados digitales

Se considera usuario a la persona que, sin ser suscriptor y sin contratar los servicios de emisión de certificados de una Autoridad de Certificación, utiliza el certificado de clave pública del originador de un documento electrónico para validar su integridad y autoría. También se las denomina terceras partes que confían. (RIVOLTA, SCHAPPER; 2004: 20) (KUHN et all; 2001: 18)

Para ello, el usuario debe:

- Reconocer previamente el certificado digital de la Autoridad de Certificación que emitió el certificado de clave pública del remitente del mensaje.

- Verificar que dicho certificado digital se encuentra vigente, mediante consulta ante los repositorios que las Autoridades de Certificación mantienen en internet.

- Efectuar el proceso de verificación de la firma digital adjunta al documento que ha recibido.

Las aplicaciones en general utilizan solamente una autoridad de certificación a los efectos de facilitar su uso por los usuarios, y básicamente no utilizan firma digital para la autenticación de usuarios, debido, entre otros, a este problema. Si utilizan firma digital para autenticar sitios web, y para obviar este inconveniente, usan certificados digitales emitidos por autoridades de certificación internacionalmente aceptadas, aunque no cuenten con autorizaciones de órganos públicos para funcionar. Ello es así, pues los navegadores las reconocen previamente.

Repositorios o listas de certificados digitales

Los repositorios o listas de certificados son sistemas de información para el almacenamiento y recuperación de certificados u otro tipo de información relevante para la expedición y validación de los mismos. (KUHN et all; 2001: 18)

- **Repositorio:** es la base de datos de certificados activos de una Autoridad de Certificación. El objetivo primordial de un repositorio es proveer datos que permita a los usuarios o terceras partes que confían confirmar el estado del certificado digital que han recibido adjunto a un mensaje o documento electrónico.

- **Archivo:** es la base de datos que contiene información a ser utilizada en futuras disputas. El objetivo del archivo es almacenar y proteger la información necesaria y suficiente para determinar si la firma digital en un antiguo documento puede ser confiable.

- **Listas de Certificados Revocados: (o CRLs**, por sus siglas en inglés – Certificate Revocation Lists), son listas de aquellos certificados que han sido revocados. Estas listas usualmente son firmadas digitalmente por la misma Autoridad de Certificación que ha emitido el certificado. Los certificados se revocan, por ejemplo, cuando se compromete la clave privada con la cual se firma, o cuando la persona deja de pertenecer a la organización para la cual estaba delegada, o cambia alguno de los atributos de la persona, por ejemplo, el nombre. El hecho de que la lista de Certificados Revocados no incluya a un certificado vigente, hace presumir que el mismo es válido.

Las Autoridades de Certificación mantienen accesibles por internet las 24 horas las listas de certificados emitidos y las listas de certificados revocados. Con ello, el usuario puede consultar en cualquier momento si el certificado que está utilizando para verificar autoría e integridad del mensaje que ha recibido, está vigente, es decir, no ha expirado, o bien no ha sido revocado. (KOORN; 2002: 2). Asimismo, el manejo y conservación de documentación resultará crítica en el futuro.

Sin embargo, este punto constituye un **problema** que aún no ha sido analizado en profundidad, y es que, una vez expirado el certificado, la firma no verifica. Con lo cual, pasado un cierto tiempo, todo el andamiaje se desmorona. Veamos un ejemplo: se realiza una notificación judicial electrónica a través de una aplicación web de un Tribunal. Si se usa firma digital, el mensaje que contiene la notificación puede ser firmado con un certificado de servidor o personal de la persona del juzgado habilitada a tal efecto. El certificado digital tiene un período de vigencia determinado, digamos que de un año. Si luego de ese lapso, alguna de las partes quisiera impugnar la validez de la notificación, debería probar que la misma no se realizó de la manera correcta. En este caso, en la fecha de la impugnación, con el certificado vencido, no se podría verificar la firma digital original del documento, por el mero transcurso del tiempo. Se debería acudir a otras medidas de prueba.

Por otra parte, el archivo de documentos electrónicos trae aparejado otro problema: la conservación y accesibilidad a través del tiempo. En efecto, el permanente cambio tecnológico torna obsoletos formatos en forma permanente. También cambian los dispositivos en los cuales se almacenan documentos electrónicos. Hace 10 años atrás, se almacenaban documentos digitales en diskettes, hoy en desuso. Ya las computadoras personales no poseen disqueteras. Si tuviéramos un documento electrónico almacenado en un diskette, digamos en un formato antiguo, sería necesario transformarlo a un formato más actualizado de modo que fuera posible leer su contenido en los software actuales. Ello implica una transformación del documento electrónico. Y la consecuente no verificación de su firma digital. (BUGONI, RIVOLTA; 2004: 63)

Ambas situaciones (certificados vencidos y actualización de formato) constituyen **obstáculos tecnológicos para el desarrollo de la firma digital**. Al menos hasta el momento, no se ha podido encontrar respuestas a estas preguntas.

Las aplicaciones basadas en PKI son dependientes de un directorio subyacente para la distribución de certificados y la información sobre su estado. Estos directorios proveen el medio de conservación, administración y distribución de certificados. Estos directorios deben basarse en estándares internacionalmente aceptados, ya que la potencia de las aplicaciones de firma digital descansa sobre su interoperabilidad. Sin esa interoperabilidad, una tercera parte que confía no podrá consultar los certificados o listas de certificados revocados del sitio web de la Autoridad de Certificación para la verificación de la firma digital que ha recibido.

Este, sin embargo, es uno de los problemas pendientes de resolver, por la carencia de estándares de alcance internacional de aceptación uniforme.

Estándares Tecnológicos

Tal como sucede en otros ámbitos, las tecnologías de clave pública se apoyan en estándares. A medida que las iniciativas e infraestructuras de clave pública van proliferando, comienzan a aparecer modificaciones a los estándares utilizados

inicialmente para poder ampliar su funcionalidad o para hacerlos más específicos y con un contenido semántico mas claro.

Distintos organismos, basados normalmente en estándares iniciales comunes, van realizando sucesivas especificaciones, aumentando el valor semántico de los formatos de documentos o certificados definidos. Del mismo modo, distintas normas recogen estos estándares y los definen en forma mucho más específica.

Estas especificaciones más detalladas son establecidas a través de diversos mecanismos, en algunos casos se los define como un estándar tecnológico, en otros el órgano regulador establece las características de las políticas que deben utilizarse. Por ejemplo, Brasil establece 4 políticas de certificación para firma electrónica avanzada, en las cuales se expresa de manera obligatoria la inclusión de determinados atributos y extensiones en los certificados a emitir.

Sin embargo, esta atomización de especificaciones detalladas podría derivar en un obstáculo para la interoperabilidad internacional, y constituye uno de los problemas con los que se enfrenta la firma digital.

Una vez que se implementa una Infraestructura de Firma Digital o PKI, se requieren garantías respecto de la calidad del diseño de los sistemas y a la efectividad del ambiente de control de las prestadoras de servicios de certificación. Por consiguiente, se hace necesaria la realización de evaluaciones independientes que otorguen esas garantías, bajo la forma de auditorías especializadas. (KOORN; 2002: 2)

Sin embargo, si bien es compartido el criterio respecto de la necesidad de establecer mecanismos de control sobre los distintos componentes de las Infraestructuras de Firma Digital, incluyendo por ejemplo, revisiones independientes que aseguren el cumplimiento de las normas y verifiquen la existencia de un ambiente de control adecuado, existe un tratamiento dispar en cuanto a la manera en que deben efectuarse dichas revisiones. (MARTA, PRANDINI, RIVOLTA; 2003:22)

Los estándares se refieren, entre otros, a los siguientes componentes (CLARKE; 2001: Apendix I):

- Estándares para algoritmos de encripción y algoritmos de hash.
- Protocolos para parámetros acordados asociados con los algoritmos de encripción y algoritmos de hash.
- Protocolos para facilitar el acceso de usuarios a las claves públicas.
- Protocolos para facilitar el acceso de usuarios a las noticias de revocación
- Estándares para la generación segura de pares de claves
- Estándares y protocolos para apoyar el mecanismo de sincronización y fechado con valor probatorio (time stamping)
- Estándares para el software de:
    - Generación de pares de claves
    - Almacenamiento de claves privadas
    - Almacenamiento de claves públicas
    - Acceso de usuarios a claves públicas

  - Generación de digestos seguros de mensajes
  - De encripción de mensajes
  - De creación de mensajes
  - De solicitud de claves públicas
  - De verificación de claves públicas: de su validez, de su vigencia, de no haber sido revocadas
  - De desencripción de mensajes
  - De desencripción de digestos seguros
  - De comparación de digestos desencriptados
  - De tiempo
  - De protección de claves privadas
  - Contra intrusiones cuando están almacenadas
  - Contra intrusiones cuando están en la memoria principal
  - Contra invocaciones no autorizadas
- De Directorio si es utilizado como Repositorio de claves públicas:
  - Protocolos para insertar datos y mantener datos en el repositorio
  - Protocolos para acceder a los datos del repositorio
- De los certificados de la Autoridad de Certificación:
  - Estándares para formatos de certificados
  - Perfiles para aplicación de los estándares en contextos particulares
- Protocolos para la comunicación de certificados a las partes que los necesiten
- Medios por los cuales los receptores de mensajes pueden evaluar si chequean la firma digital del certificado
- Medios por los cuales los receptores de mensajes pueden chequear la firma digital del certificado
- Medios por los cuales los receptores de mensajes pueden evaluar la extensión de las afirmaciones contenidas en el certificado
- Si los certificados son firmados por Autoridades de Certificación:
- Estándares para Autoridades de Certificación
- Estándares y procedimientos para registro y auditoría de Autoridades de Certificación
- Procedimientos para recurrir contra la Autoridades de Certificación
- Seguros que deben contratar las Autoridades de Certificación

Si el marco legal vincula un par de claves con algo del mundo real como parte de una PKI, más allá de un nivel de aplicación informática (como es el caso argentino y la mayoría de las legislaciones latinoamericanas), entonces la PKI debe contener los medios para establecer la asociación del par de claves con un dispositivo, persona física, persona jurídica, atributo, agencia pública o lugar.

Los elementos involucrados deberían comprender: (CLARKE; 2001)

- Estándares para autenticar la relación invocada
- Procedimientos para autenticar la relación invocada
- Los medios para comunicar la relación invocada y autenticada
- Un número suficiente de autoridades de registro operativas que provean los servicios de autenticación
- Una declaración de las garantías que proveen las autoridades de registro y las autoridades de certificación
- Los medios de comunicación de las garantías mencionadas.

Tal como se vio, el grado de madurez de los estándares es aún incipiente, con lo cual no existe un marco de estándares internacionalmente aceptados que facilite un esquema de interoperabilidad. La descripción anterior demuestra otro de los **obstáculos para el desarrollo de la PKI**, dada la complejidad tecnológica asociada y la inexistencia de estándares internacionalmente aceptados.

Usos de la firma digital

La tecnología de clave pública se utiliza en múltiples aplicaciones. A continuación se enumeran las más comunes. Cabe destacar que si bien la tecnología es la misma, existe una amplia gama de combinaciones de sus herramientas, aunque desde el punto de vista legal cuando se habla de firma digital solamente se esté aludiendo a una combinación específica y muy regulada. (BUGONI, RIVOLTA; 2007: 58)

Para autenticarse

Un uso posible de los certificados digitales es para la autenticación de la persona en el mundo digital. La posesión y uso de un certificado digital avanzado, permite identificar a una persona tal como si fuera un documento nacional de identidad en el mundo del papel. Esto se produce pues, además de la tecnología (generación de claves pública-privada) interviene un tercero de confianza – las Autoridades de Certificación, que mediante un procedimiento riguroso, verifican la identidad de la persona a la cual le van a emitir el certificado digital. Dichos procedimientos son los aprobados por la autoridad estatal regulatoria en materia de firma digital.

La autenticación es parte de un proceso de seguridad de sistemas que además contempla autorizaciones, administración de derechos, control de accesos y auditorías. La autenticación depende de la existencia de uno o más de los siguientes factores: algo que la persona conoce (v.g. un secreto compartido como por ejemplo una palabra clave o password), algo que la persona tiene (v.g. un dispositivo criptográfico o una tarjeta inteligente) y algo que la persona es (v.g. un dato biométrico o un conjunto de atributos tales como peso, edad y altura). (OCDE; 2007: 17).

La importancia del concepto de autenticación radica en que *"Una vez producida la autenticación, se asignan ciertos derechos y sus correspondientes obligaciones. La autenticación debe ser bi-direccional y ofrecer garantías a ambas partes de la transacción. Más generalmente, en el caso de la autenticación de una persona, el interés radica en la autenticación de la identidad de la persona."* (OCDE; 2007: 17)

Se entiende por autenticación al proceso de *"verificación de la autenticidad de identificadores alegada por o para tanto una entidad como una persona u organización"*. El proceso de autenticación es el segundo paso luego de que la

persona ha presentado un identificador ante un sistema de seguridad informática y se ha presentado o generado información que corrobora el vínculo entre la entidad que se autentica y el identificador. (RIVOLTA, SCHAPPER; 2004: 9)

Este procedimiento supone la constatación fehaciente de:

- Documentación que acredite la identidad
- Presencia física de la persona

La Autoridad de Certificación efectúa dicha comprobación por sí o por medio de las Autoridades de Registro, requiriendo la comparecencia personal y directa del solicitante o de su representante legal si se tratare de una persona jurídica.

La comprobación de los datos de identidad de las personas que soliciten la emisión de un certificado digital seguro, se efectuará en base al número del documento nacional que acredite la identidad de las personas en cada país. Sin embargo, qué ocurre cuando la persona no es nacional del país. Cuál es el documento que se tomará en consideración? Algunas legislaciones requieren el pasaporte. Sin embargo, qué ocurre con aquellas personas que no poseen un pasaporte?

Sin embargo, surgen varios **problemas** relativos a estos aspectos.

El primero es la diferente forma en la cual los países acreditan la identidad de sus ciudadanos. Por ejemplo, existen países en los cuales una licencia de conducir alcanza para verificar la identidad (por ejemplo, Estados Unidos). En otros países, *como* Argentina, se identifica a las personas con documentos nacionales de identidad, obligatorios. Por lo tanto, no hay un criterio universal establecido sobre la validez de los documentos que acreditarán la identidad de los suscriptores de certificados. (BUGONI, RIVOLTA; 2007: 59)

Otro problema se presenta respecto de los certificados que contienen atributos, por ejemplo, de representación de una determinada empresa. Antes de emitir el certificado, la Autoridad de Registro debe verificar la validez de los poderes, pero dado que cada país tiene disposiciones específicas, cuál criterio se utilizará? Una Autoridad de Registro de un país con derecho continental, que deposita la fé pública en escribanos, puede validar un poder emitido mediante una simple nota intervenida por notario de un país de derecho anglosajón, función que no requiere las solemnidades otorgadas en el primer caso? En todos los casos la documentación debe ser apostillada o intervenida consularmente?

Además de la evidente complejidad que la instrumentación de mecanismos de autenticación mediante certificados digitales representa por los puntos mencionados, existe otro factor que podría disminuir el grado de confiabilidad del sistema. En efecto, suponiendo que el poder fue bien otorgado, que el certificado fue emitido correctamente verificando documentos de identidad, presencia física y documentación que acredite personería debidamente otorgada, traducida, certificada y apostillada, pudiera ocurrir que el poder fuera revocado. Sin embargo, esto no se reflejaría en el certificado, con lo cual la persona, podría seguir autenticándose usando dicho certificado. Si bien es cierto que, una vez descubierta la maniobra, todos los actos serían nulos por el vicio de falta de personería. En otras palabras, autenticarse mediante el uso de certificados digitales no garantiza 100% autoría. (BUGONI, RIVOLTA; 2007: 60)

Estos problemas constituyen serios **obstáculos para el desarrollo de la firma digital,** dado que no existen criterios comunes para la identificación de las personas con validez en distintos países. Otro obstáculo es la necesidad de la presencia física de una persona ubicada en un lugar remoto. Estos problemas se presentarían cuando fuera necesario interactuar con personas ubicadas en distintas jurisdicciones.

Para encriptar y garantizar confidencialidad de la información

El uso más difundido de la tecnología de clave pública es para encripción. El uso del par de claves soluciona el problema de la distribución de la clave, con lo cual se mantiene el secreto sin aumentar los riesgos de que dicha clave se difunda. En efecto, el documento se encripta con la clave pública de la persona a la cual se dirige el mensaje y este lo desencripta con su clave privada. La operación no es reversible, y garantiza la confidencialidad de la información pues solamente el poseedor de la clave privada que se corresponde con la clave pública puede desencriptar el mensaje.

Sin embargo, el uso de la encripción en forma metódica implica políticas de certificación específicas, repositorios de claves para la posterior desencripción de documentos, políticas de recuperación de claves o key scrow, que permitan acceder a los documentos encriptados en un lapso prolongado. (BUGONI, RIVOLTA; 2007: 61)

Estas políticas para certificados de encripción son distintas de las políticas de certificación para firma digital. Mientras que la firma digital requiere el secreto de la clave privada, una aplicación que utilice encripción necesita tener repositorios de claves para desencriptar a lo largo del tiempo. Es por ello que algunos países han aprobado políticas diferentes o directamente, no contemplan la encripción dentro de las PKI. 4 (BUGONI, RIVOLTA; 2007: 60)

Para fortalecer la seguridad informática: identificación de sitios web, sesiones seguras.

Uno de los aspectos más complejos del uso de internet es el vinculado con la seguridad informática: esto es, garantizar la autenticidad de una página web (que no haya sido robada su identidad) y garantizar la confidencialidad de las comunicaciones entre el servidor y la persona que se contacta con el sitio. Veamos un ejemplo: la banca electrónica nos permite realizar transacciones en nuestras cuentas bancarias por internet. Esto requiere por un lado, estar seguros de que el sitio de internet al cual estamos accediendo sea el de nuestro banco y no de otra persona que podría fraudulentamente haber accedido ilegalmente a dicho sitio. Por otra parte, dado que la información que circula por la sesión es de carácter

4 El primer caso, Brasil, tiene políticas específicas para certificados de encripción. Argentina es un ejemplo del segundo supuesto, ya que la PKI se refiere a la firma digital y requiere el secreto de la clave.

confidencial (como nuestro número de tarjeta de crédito) es necesario garantizar un canal seguro para el intercambio de datos sensibles.

Las sesiones de internet en general utilizan claves simétricas para autenticar al usuario (passwords) y utilizan certificados digitales internacionalmente reconocidos para autenticar el sitio y para encriptar las comunicaciones con el usuario (sesiones seguras). "La seguridad tanto de la criptografía simétrica como de la asimétrica, descansa sobre la sofisticación de algoritmos conocidos públicamente y sobre el secreto de las claves. La autenticación se deriva del grado en el cual se administran y del grado de capacidad tecnológica que permiten proporcionar confianza en el vínculo entre la clave secreta y una entidad del mundo físico – un individuo o una organización" (RIVOLTA, SCHAPPER; 2004: 22).

En el campo de la seguridad informática en redes se ha dado un amplio y difundido uso de los certificados digitales. Dicho uso de vincula con la autenticación de páginas de internet y con el establecimiento de sesiones seguras. El uso de la tecnología de clave pública permite definir direcciones de Internet seguras al acceder a una web con el encabezado https, el navegador le informará con una imagen que representa una llave o candado cerrado.

Este hecho indica que la comunicación se establece con un sitio Web que tiene un certificado digital de servidos que lo identifica. Normalmente estos certificados son de empresas reconocidas internacionalmente, con lo cual todos los navegadores tienen incorporado el certificado digital de dicha empresa, lo cual permite verificar el certificado del sitio de internet al cual se accede. (BUGONI, RIVOLTA; 2007: 61)

Paradójicamente, esta situación constituye un **obstáculo para el desarrollo de la firma digital** ya que si el certificado digital que autentica a un sitio web no estuviera incluido en los navegadores de uso masivo, no serviría en los hechos para dar garantía de que el sitio es el correcto.

Para firmar documentos: garantizar el no repudio respecto de la identidad del firmante y de la integridad del contenido.

Finalmente, se presenta la aplicación legal de la tecnología de clave pública: el firmado digital de documentos electrónicos, el cual brinda un cierto grado de certeza respecto de su autoría e integridad.

Ya se han analizado en profundidad los componentes que se requieren para la firma digital de un documento. Analizaremos ahora los procesos específicos de la firma digital.

"El proceso de firma digital de un documento electrónico es una moneda con dos caras. Una cara, el proceso de firma propiamente dicho. La otra cara, el proceso de verificación de la firma realizado por un usuario." (BUGONI, RIVOLTA; 2007: 62)

A continuación se presenta una síntesis de los requisitos y pasos involucrados en el proceso de firmado digital de un documento:

Persona / Requisitos	Firma	Verificación
Firmante del documento	1. Generar par de claves 2. Albergar clave privada en forma segura 3. Enviar clave pública a Autoridad de Certificación 4. Solicitar emisión certificado digital 5. Presentarse con documentos ante Autoridad de Registro para acreditar identidad 6. Recibir certificado clave pública 7. Instalar certificado clave pca. de la Autoridad Certificante en su PC 8. Instalar su certificado digital en su PC 9. Disponer de software para firmar documentos 10. Calcular el hash del documento 11. Acceder a su clave privada alojada en dispositivo seguro mediante clave simétrica o password 12. Encriptar el hash del documento con su clave privada 13. Enviar documento firmado a un tercero 14. Enviar certificado digital al tercero	

Receptor del documento		15. Recibir documento firmado 16. Recibir certificado digital del firmante 17. Instalar certificado digital de la autoridad certificante que emitió el certificado digital del firmante 18. Desencriptar el has del documento con la clave pública del firmante 19. Recalcular el hash del documento 20. Verificar resultados del hash 21. Verificar en la CRLs de la Autoridad Certificante que el certificado digital del firmante se encuentra vigente

En total: 21 escalones para firmar digitalmente un documento.

Complejidades asociadas a la firma digital

"La idea de PKI es sumamente simple y ha sido desarrollada hace más de veinte años atrás. Hoy, se aplica con varios estándares y protocolos. Cada día, la gente visita sitios de Internet para comprar o realizar operaciones bancarias y PKI es parte de esas conexiones seguras. No obstante, es evidente que tanto la administración como la dimensión legal de PKI son complejas, aún sin el desarrollo requerido para extender la validez legal de los certificados digitales entre diferentes países y diferentes sistemas de acreditación". (RIVOLTA, SCHAPPER; 2004: 29).

Por otra parte, el supuesto subyacente en la criptografía de clave pública, y en los sistemas basados en PKI, es que la clave secreta siempre permanece secreta. En realidad, esto necesitaría hardware y software exclusivamente diseñados para la función de firmado de documentos. En la medida que las claves privadas (teóricamente secretas) sean alojadas en máquinas de usos múltiples, con los consiguientes problemas de seguridad, en la práctica podrían dejar de ser secretas, con lo cual no sería posible garantizar el no repudio. (GASSON et all, 2005: 24)

Se presentan a continuación los problemas identificados inherentes al concepto de PKI, a partir de los exhaustivos análisis realizados por reconocidos autores (GASSON, GUTMANN, ELLISON, SCHNEIER, SCHAPPER) y de la propia experiencia en el tema. Se exponen las complejidades identificadas en respuesta a la pregunta de investigación sobre los motivos que pudieran estar afectando el uso masivo de la firma digital.

Relativas a la implementación de PKI

La transferencia segura de información implica un intercambio entre partes identificables. La criptografía de clave pública por sí misma solamente se refiere a las operaciones matemáticas sobre dichos datos. No provee por sí misma una conexión con las aplicaciones ni con el entorno tales como comercio electrónico, correo electrónico, o la web. Esa conexión requiere de elementos adicionales, que en su conjunto, conforman una Infraestructura de Firma Digital (ADAMS, JUST; 2004: 2).

GUTMANN ha señalado que las PKI originales, y aún algunas actuales, parten del concepto de tratar de constreñir al mundo real para adaptarse a la PKI, en lugar de adaptar el diseño de la PKI al mundo real. (GUTMANN; 2002: 1)

Expertos en PKI han asegurado que, en los hechos, PKI tiene un alcance acotado. Aunque PKI puede usarse para autenticar personas, brindar seguridad en transferencias electrónicas comerciales y proteger la privacidad de correos electrónicos y comunicaciones telefónicas mediante la encripción de los mensajes, existen barreras que limitan su uso, entre las cuales pueden citarse la escasez de aplicaciones, altos costos, dificultad para entender su complejidad y los problemas de interoperabilidad. (RIVOLTA, SCHAPPER; 2004: 30).

Con el propósito de detectar los principales obstáculos para el uso y despliegue de PKI, el Comité Técnico de PKI de OASIS desarrolló una encuesta en Junio de 2003. Se logró la participación de un gran número de encuestados calificados, quienes identificaron los obstáculos específicos según su propio criterio. (DOYLE, HANNA; 2003: 12)

Los cinco primeros obstáculos para el despliegue y uso de PKI identificados por los encuestados fueron:

1. Las aplicaciones no disponen de un software que lo sostenga
2. Costos muy altos
3. PKI es escasamente entendida
4. Demasiado focalizada en tecnología, no en necesidades
5. Pobre interoperabilidad

Se solicitó a los encuestados que describieran en sus propias palabras las causas de los obstáculos señalados. Los factores principales mencionados fueron:

- Apoyo inconsistente para PKI. A menudo, no existe para aplicaciones y sistemas operativos. Cuando existe, hay una amplia diferencia de su alcance. Esto incrementa sustancialmente el costo y la complejidad y torna la interoperabilidad en una pesadilla.

- Los estándares actuales de PKI son inadecuados. En algunos casos (por ejemplo, la administración de certificados), hay demasiados estándares. En otros (por ejemplo, smart cards) son escasos. Cuando existen, los estándares son demasiado flexibles y complejos. Debido a ello, las aplicaciones de diferentes proveedores raramente son interoperables.

ELLISON y SCHNEIER identificaron, en un estudio realizado en el año 2000, diez riesgos inherentes a la implementación de PKI:

Riesgo #1 ("En quién confiamos, y por qué?") previene que el certificado emitido por una AC podría no ser automáticamente confiable para un gran número de aplicaciones basadas en niveles de riesgo, como por ejemplo, realizar pagos mínimos o firmar millonarias órdenes de compra. (ELLISON, SCHNEIER; 2000: 1)

Riesgo #2 ("Quién está usando mi clave?") previene respecto de la seguridad del almacenamiento de la clave privada. (ELLISON, SCHNEIER; 2000: 2)

Riesgo #3 ("Qué tan segura es la computadora que verifica?") analiza la cuestión de la inseguridad pero desde la perspectiva de quien recibe el documento firmado y verifica la firma digital del documento. (ELLISON, SCHNEIER; 2000: 2)

Riesgo #4 ("Cuál Juan Fernández es él?") previene que el nombre en el certificado podría no ser tan valioso como parece. Los usuarios en el entorno electrónico, así como en el mundo físico, necesitan poder relacionar el nombre con la identidad de una persona, con PKI o sin ella. PKI asocia un identificador con una clave pública. La asociación entre el identificador con una identidad, o con atributos dentro del contexto en el cual se utiliza la aplicación, está afuera del alcance de PKI, así ha sido siempre. Las aplicaciones que confían en PKI para autenticación necesitan reconocer que este tema no ha sido resuelto por PKI. (ELLISON, SCHNEIER; 2000: 3)

Riesgo #5 ("La Autoridad de Certificación es una autoridad?") previene respecto de que una Autoridad de Certificación puede no ser, y usualmente no lo es, una autoridad sobre los datos contenidos en el certificado. No es el órgano que asigna nombres a empresas, ni que emite documentos nacionales de identidad a las personas; su principal función es asociar un identificador con una clave pública. (ELLISON, SCHNEIER; 2000: 3)

Riesgo #6 ("El usuario es parte del diseño de seguridad?") previene respecto de que los usuarios frecuentemente toman decisiones de seguridad (por ejemplo, comprar por Internet en una página web segura) sin haber visto el certificado de dicha página, o sin saber si existe alguna relación con lo que se muestra en la pantalla. (ELLISON, SCHNEIER; 2000: 4)

Riesgo #7 ("Era una Autoridad de Certificación o una Autoridad de Certificación más una Autoridad de Registro?") previene respecto de que el modelo "AC+AR" admite que, una entidad (la AC) que no es la autoridad sobre los contenidos, forje un certificado con tales contenidos. (ELLISON, SCHNEIER; 2000: 4)

Riesgo #8 ("Cómo identificó la Autoridad de Certificación al poseedor del certificado?") previene sobre la posibilidad de que la Autoridad de Certificación podría no haber usado buena información para verificar la identidad de la entidad que solicita el certificado, o podría no haber asegurado que esta entidad realmente está en control de la clave privada correspondiente a la clave pública que está siendo certificada. (ELLISON, SCHNEIER; 2000: 4)

Riesgo #9 ("Cuán seguras son las prácticas de certificación?") previene, en síntesis, que los certificados deben ser usados correctamente si el usuario quiere seguridad. (ELLISON, SCHNEIER; 2000: 6)

Riesgo #10 ("Por qué usamos el proceso de la Autoridad de Certificación, de todas maneras?"), previene sobre el hecho de que PKI no resuelve todos los problemas de seguridad, aunque a veces es publicitada y vendida bajo estas premisas. (ELLISON, SCHNEIER; 2000: 7)

Además de los problemas mencionados, respecto de los procedimientos de emisión del certificado, existen una serie de cuestiones asociadas al proceso de verificación que aún no han sido resueltas, tales como:

- Listas de Certificados Revocados (CRLs):
  - administración de las listas de certificados revocados.
  - Estándares.
  - Actualización de las listas.
  - Valor de la consulta.
  - Celeridad en la consulta y demoras en las aplicaciones.

- Almacenamiento y Manejo de claves privadas.
  - Estándares para dispositivos criptográficos.
  - Costos.
  - Mantenimiento y actualización.
  - Accesos a las claves mediante passwords.

- Proceso de verificación de la firma digital de un documento:
  - aceptación del certificado de la autoridad certificante en los navegadores de los usuarios que verifican
  - complejidad del software en función de la naturaleza del negocio
  - qué ocurre posteriormente a la expiración del certificado, no verifica la firma digital

Relativas a la aceptación del uso por no expertos

El modelo de negocio de una PKI requiere al usuario que disponga de:

- Un software de administración de certificados a ser instalado y configurado en la máquina del usuario y del firmante
- El pago del certificado digital del firmante
- Elevados conocimientos para el manejo de claves y certificados

Sin embargo, la PKI brinda al usuario una escasa confiabilidad en la información contenida en los certificados, toda vez que son comunes las cláusulas de exención de responsabilidad para las autoridades de certificación, incorporadas en los contratos que firman con los suscriptores.

Tal como se vio anteriormente la firma de un documento implica subir 21 escalones, que si bien algunos están automatizados, otros deben ser realizados por el usuario. Esto es complejo aún para informáticos, pero rápidamente pueden ser entrenados para la operación.

Mayor dificultad se presenta en aquellas aplicaciones cuyos usuarios no son expertos informáticos. Por ejemplo, en los sistemas de compras públicas electrónicas, cuyo objetivo es adquirir bienes y servicios ampliando la participación de oferentes, muchas veces las empresas, especialmente las pequeñas y medianas, no cuentan con personal altamente capacitado en sistemas.

Es por ello, que en consideración de los principios que rigen la contratación pública, relativos a la transparencia, publicidad, libre concurrencia y competencia, sea necesario contemplar que los sistemas electrónicos sean amigables para usuarios no expertos. Establecer condiciones de uso restrictivas y complejas deriva en una restricción de la competencia que no se condice con los principios de la contratación administrativa.

La banca electrónica es una aplicación amigable, de uso masivo y exitosa. En unos pocos años se ha masificado el uso de los cajeros automáticos o ATM, y ha producido una aceptación entre personas no expertas que podría ser contemplada por otras aplicaciones de manera sinérgica, aprovechando las infraestructuras existentes e interactuando con las fuentes de información. Coordinación, sinergia y sencillez, deberían ser los ejes para la instalación de cualquier sistema de compras públicas electrónicas.

Por otra parte, el alto costo de mantener una PKI operativa, con el alto riesgo inherente que implica el compromiso de la clave de la autoridad certificante raíz o las claves de las autoridades de certificación, lo cual harían caer todo el sistema, no resulta compatible con una política que pretenda fomentar el comercio electrónico, superar la brecha digital e promover la inclusión digital de la mayor cantidad de empresas en todo el territorio nacional.

Relativas a la interoperabilidad

GUTMANN menciona una serie de problemas que presenta el escenario actual de la PKI.

Además de los relativos a la emisión de certificados, a la administración, distribución y verificación de las listas de certificados revocados y a la revocación misma de certificados, plantea las dificultades que se observan en relación a la interoperabilidad.

El problema de la interoperabilidad se presenta en aquellos esquemas de autenticación que se apoyan en PKI. En efecto, una PKI implica la existencia de cadenas de certificados, que representan el camino de confianza.

En una estructura jerárquica, como por ejemplo, la de Brasil o la de Argentina, en la cual el órgano publico regulador de PKI emite los certificados de las Autoridades de Certificación, el camino que un usuario debe recorrer para verificar la firma digital de un documento es el siguiente:

1.- Verificar la vigencia del certificado del firmante – Consultar la CRL de la AC que emitió el certificado
2.- Verificar la vigencia del certificado de la AC - Consultar a la AC Raíz
3.- Verificar la vigencia del certificado raíz

En cuyo caso, los problemas mencionados se multiplican por la extensión de la cadena de confianza. Según apunta GUTMANN, la complejidad del proceso de verificación del certificado es proporcional al tamaño y profundidad de la estructura jerárquica de emisión. (GUTMANN; 2002: 10)

El problema aumenta si existen varias estructuras jerárquicas, pues en ese caso la cadena se corta en la autoridad certificante raíz de cada una. Si dos personas pertenecientes a dos estructuras jerárquicas diferentes quisieran interoperar, cuál podría ser la solución para la verificación de sus firmas digitales? Este no es un caso teórico, pues es el escenario que en poco tiempo podría llegar a plantearse en la región, básicamente en los sistemas electrónicos de compras públicas que asumieran como mecanismo de autenticación un esquema PKI.

Una alternativa es la certificación cruzada, en la cual la AC 1 reconoce y firma el certificado emitido por la AC 2, y viceversa, en tanto hayan celebrado un acuerdo de reconocimiento recíproco y cuenten con las respectivas autorizaciones de los órganos rectores estatales de cada país. El problema que se presenta es que a partir de la certificación cruzada, cada certificado tiene dos emisores, con lo cual se multiplica la complejidad señalada anteriormente, y las rutas de confianza se convierten en una maraña..... Según GUTMANN, la certificación cruzada es el agujero negro de la PKI, en el cual se rompen todas las reglas y donde nadie sabe qué hay dentro..... (GUTMANN; 2002: 10)

Otra alternativa es la certificación cruzada en los navegadores, mediante la incorporación de las AC. El tema es que el criterio con el cual los navegadores incorporan AC no es uniforme. No están solamente las habilitadas para funcionar por

los órganos públicos del estado, sino que ya existen una cantidad de AC de diferentes categorías, que han cumplido los requisitos solicitados por el navegador, y pagado la tasa correspondiente. Algunos debieron someterse a auditorías.

En resumen, los problemas que presenta el estado actual de PKI se refieren a:

- Muy escasa interoperabilidad y/o compatibilidad con aplicaciones
- Ausencia de expertise en el desarrollo y uso de aplicaciones basadas en PKI para autenticación
- No es administrable
- Requiere de enormes infraestructuras: muy pocas organizaciones han comprendido cuánto dinero, tiempo y recursos requieren las aplicaciones basadas en PKI
- El lema "PKI acabará con las passwords" no es real, ya que las aplicaciones actuales utilizan passwords + clave privada (la venganza de las passwords....)
- La revocación de certificados no funciona bien en los hechos.

Relativas a la conservación de documentos

La conservación de documentación es un aspecto relevante, ya que constituye la evidencia en juicio que prueba la realización del contrato. En materia de compras públicas, también es importante pues es la materia sobre la cual trabajarán los organismos de control del Estado para realizar sus auditorías. Por ello, la conservación de documentos electrónicos es un tema que tiene suma importancia para el ejercicio del control público sobre los procedimientos de adquisiciones, y también como evidencia documental frente a posibles litigios.

Al contrario de lo que ocurre con la documentación en papel, el valor de seguridad de los documentos electrónicos firmados digitalmente decrece con el tiempo. Esto se debe en principio al constante desarrollo tecnológico de los algoritmos criptográficos, pero también a que con el correr del tiempo se pierde la posibilidad de verificar correctamente la firma digital de un documento electrónico, al expirar el certificado de clave pública correspondiente. A esto se suma la constante y vertiginosa evolución del mercado del software y hardware, que dificultan, cuando no impiden, el acceso a los documentos electrónicos antiguos. (FISCHER, WILKE; 2006)

La implementación del comercio y del gobierno electrónicos genera un nuevo escenario para la conservación documental. Surgen nuevas cuestiones que requieren soluciones:

- los procedimientos y técnicas de conservación y archivo de documentos digitales

- la admisibilidad de evidencia digital en juicio

- la producción de evidencia digital

- la interpretación de la evidencia digital por parte de los jueces

- la aparición de una nueva rama del derecho: la informática forense

Estas cuestiones requieren un análisis pormenorizado, específico, que permita identificar aquellos aspectos que, vinculados con la aplicación en sí misma, tengan consecuencias en materia de conservación documental y producción de evidencia digital.

En efecto, la implementación de un sistema de comercio o de gobierno *electrónico*, implica determinadas características funcionales para su operación, pero al mismo tiempo, debería considerarse aquellas funcionalidades que cubran los requerimientos legales de conservación documental y producción de evidencia digital.

La producción de evidencia digital requiere de sistemas confiables. Sin embargo, actualmente existen limitaciones técnicas para garantizar la integridad e inalterabilidad del documento electrónico. Un adecuado sistema debería contener un módulo específico de conservación, que en forma confiable conserve documentos, archivos y logs con valor legal, que pudieran ser presentados como prueba y ser objeto de control por parte de los organismos auditores.

En un entorno tradicional, basado en documentos instrumentados en papel, las principales cuestiones a resolver para una adecuada conservación, es la calidad del papel y la administración del entorno de almacenamiento (lugares ventilados, sin roedores, archivos accesibles para consulta, etc).

La conservación de documentos electrónicos presenta otras cuestiones más complejas.

En primer lugar, se requiere probar la autenticidad e integridad del documento digital, tanto en el momento de su generación, como a través del lapso de conservación impuesto por las leyes, en su mayoría de 10 o más años.

Una fuerte corriente ha impulsado el uso de la firma digital, afirmando que la misma garantiza la integridad e inalterabilidad del contenido del documento. Numerosas leyes han recogido esta solución. Sin embargo, el problema presenta algunas cuestiones que no son resueltas por la firma digital, más aún, algunas cuestiones que surgen de la aplicación de la firma digital y que generan más problemas en materia de conservación.

Se han identificado los siguientes riesgos del uso de firma digital relacionados con la conservación de documentos electrónicos (BUGONI, RIVOLTA; 2007: 78):

Riesgo #1: "La firma digital no impide la alteración del documento":

En efecto, la firma digital es una operación matemática basada en criptografía asimétrica que permite determinar con algún grado de certeza la autoría e integridad del documento digital. No impide que el documento sea alterado, suprimido o dañado. Impedir el acceso no autorizado al documento, su alteración o supresión es materia de seguridad informática. Un buen sistema de compras electrónicas debiera contemplar firewalls, antivirus, procedimientos de niveles de acceso restringido, almacenamiento y archivo de documentación. Pero nada tiene que ver con la firma digital del documento.

Riesgo # 2: "Pérdida de potencia del hash, algoritmos criptográficos y generación de números primos":

El constante avance tecnológico permite suponer que en un lapso de cinco años, las actuales soluciones para calcular el hash, los algoritmos criptográficos y la selección de números primos para generar las claves serán superadas por otras más complejas y robustas. Al mismo tiempo, considerando el avance del criptoanálisis, las actuales soluciones seguras podrían tornarse vulnerables. Lo que hoy no puede ser quebrado, podría ser casi transparente dentro de cinco años.

Riesgo # 3: "Disponibilidad de directorios gigantes por 10 o más años":

La administración, consulta y acceso a las listas de certificados emitidos y de certificados revocados es un tema que aún no tiene una solución estandarizada. Imaginar un escenario futuro en el cual deban procesarse listas por 10 años, que permitan consultar si en determinado momento del pasado, un certificado se encontraba vigente, si el certificado de la autoridad certificante que lo emitió se encontraba vigente, y cuál era la política bajo la cual el certificado fue emitido, parece una pesadilla.

Riesgo # 4: "No verifica la firma digital al expirar el certificado":

Aún suponiendo que los riesgos anteriores no se hubieran producido, es decir, que el documento electrónico no fue alterado, que la potencia de hash, algoritmos y selección de números primos sea la misma, y que se haya logrado administrar eficientemente los directorios de certificados, subsiste un problema crucial. En efecto, la verificación de la firma digital de un documento requiere de una clave pública contenida en un certificado digital. Los certificados tienen un período de vigencia, no mayor a dos años en general, pues se teme la pérdida de potencia de la clave por el avance tecnológico. Es decir que si, por ejemplo, tomamos una oferta de una licitación de hace cinco años, tendremos el certificado expirado. Esto hará que no verifique. Con lo cual, el uso de la firma digital para firmar la oferta no da certeza de autoría ni de integridad más allá del lapso de vigencia del certificado.

Riesgo # 5: "Transformación permanente de formatos de documentos electrónicos":

El constante avance produce que los formatos de documentos electrónicos cambien, así como los dispositivos de almacenamiento. Hace unos pocos años atrás, se utilizaban diskettes. Hoy muchas computadoras ni siquiera traen disquetera. Es así que un adecuado sistema debiera prever la actualización

permanente de formatos y dispositivos de almacenamiento. Ahora bien, el traspaso de un formato a otro genera a su vez delicadas cuestiones. En primer lugar, debiera estar enmarcada en procedimientos rigurosos que permitan tener algún grado de certeza sobre la integridad de la información. Por otra parte, si el documento electrónico se encuentra firmado digitalmente, al transformar su formato, la firma no verifica en el nuevo formato. Esto genera una pérdida del grado de certeza obtenida originalmente respecto de autoría e integridad del contenido del documento electrónico. Al pasarlo al nuevo formato, se pierde la firma digital.

Una solución a este problema se ensayó en Alemania, donde se re-firma el documento electrónico. Esta segunda firma digital, no pertenece a la persona que la firmó originalmente como expresión de su consentimiento, sino que es una firma digital de una tercera parte de confianza que avala el procedimiento de traspaso de formato, certificando la relación entre ambos documentos y que el segundo se corresponde con el primero y sus contenidos coinciden. Esta segunda firma digital del documento, no es una declaración de voluntad sino una medida de seguridad informática.

La conservación de documentos electrónicos ha sido identificada como una de las causas del escaso desarrollo de la firma digital (firma electrónica avanzada) en Europa. En efecto, en 2006 la Comunidad Europea elaboró un informe acerca del desarrollo de la firma electrónica avanzada en el marco de Europa. Uno de las razones prácticas detectadas para explicar la resistencia a implementar aplicaciones con firma digital se debe a que se considera que el archivo de documentos firmados digitalmente es un proceso muy complejo e incierto. La obligación legal de conservar documentos por períodos extensos, que pueden llegar hasta 30 años, requieren de costosas y engorrosas tecnologías y procedimientos para asegurar su posterior accesibilidad y lectura, y la verificación pasado dicho período de tiempo. (EUROPE; 2006: 8)

Relativas al reconocimiento de certificados digitales emitidos en el extranjero

Los esquemas de PKI actualmente tienen alcance local. Las leyes de comercio electrónico o firma digital se aplican a las operaciones realizadas totalmente dentro del territorio de cada país, como derecho interno.

Ahora bien, el avance de Internet facilita la realización de operaciones entre partes ubicadas en distintos países. Se plantea así una cuestión que requiere ser abordada para no entorpecer el comercio electrónico.

Qué ocurre con aquellas operaciones en las que las partes se encuentran en distintos países? Por ejemplo, en el caso de los sistemas de compras electrónicas, los regímenes legales de los países contemplan la figura de la licitación pública internacional. Pero si el sistema requiere de firma digital para autenticarse, qué ocurre con aquellos licitantes que poseen un certificado digital en su país, distinto del país comprador, y tiene intenciones de participar en una licitación?

En general, las leyes que se basan en esquemas de PKI, admiten dos mecanismos para el reconocimiento de certificados digitales emitidos en el extranjero:

Mediante acuerdos de reconocimiento mutuo entre gobiernos.

Se contempla la posibilidad de que dos o más gobiernos celebren acuerdos de reciprocidad, cuyo objeto sea otorgar validez, en sus respectivos territorios, a los certificados digitales emitidos por autoridades de certificación autorizadas de ambos países, en tanto se verifique el cumplimiento de las condiciones establecidas por la normativa interna de cada país.

Mediante el reconocimiento formulado por una autoridad de certificación nacional.

En este caso, dicho reconocimiento debe estar aprobado por el órgano público rector en materia de firma digital. La Autoridad de Certificación nacional, debe probar que los certificados a ser reconocidos por ella, han sido emitidos por un prestador de servicios de certificación no establecido en el país que cumple con normas técnicas y de procedimientos equivalentes a las establecidas en la normativa nacional para el desarrollo de la actividad.

Un **problema sustancial** se presenta con el requisito de presencia física para la emisión del certificado, requisito presente en la normativa argentina y que, dada la alta probabilidad de que las transacciones electrónicas se realicen entre personas situadas en diferentes países, podría constituir un **obstáculo** para la masificación de la firma digital.

IV.- FACTORES JURIDICOS DE LA INFRAESTRUCTURA DE FIRMA DIGITAL

El presente capítulo aborda los aspectos jurídicos involucrados en la Infraestructura de Firma Digital de la República Argentina. Después de presentar un panorama general, se analiza el marco normativo argentino, su impacto en la legislación civil y las normas administrativas que regulan a los organismos competentes de la Administración Central. Se menciona también el marco normativo de las provincias argentinas, aunque sin profundizar en ellos.

Se explican brevemente los conceptos de documento electrónico y firma electrónica y su virtualidad jurídica en el derecho argentino, así como las *presunciones* legales asociadas a la firma digital y a la firma electrónica.

Posteriormente, se hace una breve reseña de los esquemas normativos internacionales, ya que la temática involucra el desarrollo del comercio electrónico en un escenario globalizado.

Antecedentes del marco normativo que reconoce el valor legal del documento electrónico

En los últimos años, los países han aprobado una serie de leyes que complementan su legislación interna civil y comercial, con el propósito de reconocer la validez jurídica de los contratos celebrados por internet que permitiera construir un entorno jurídico seguro del comercio electrónico.

En efecto, el surgimiento del comercio electrónico, del gobierno electrónico y de las formas transaccionales en medios digitales, ha encontrado obstáculos jurídicos representados por algunas disposiciones contenidas en las normas de derecho interno de los países que regulan los contratos y las formas de los actos jurídicos y administrativos.

Los sistemas jurídicos imperantes, previos a la aparición de las nuevas tecnologías, se basaban en el soporte papel como base para la instrumentación de las manifestaciones de voluntad de las personas. Establecían determinados requisitos de forma para los actos jurídicos. En general, requerían que las declaraciones de voluntad se manifestaran por escrito, y que fueran acompañadas de la firma manuscrita de las personas involucradas. Otras disposiciones relativas a la conservación de los documentos, el archivo, la consideración de originales y copias, se vinculaban con el esquema basado en la única tecnología conocida en ese momento, el papel y el trazo de la mano del hombre.

Con el inicio de Internet, en los años 90, se había detectado que los principales obstáculos que los ordenamientos jurídicos internos presentaban al

desarrollo del comercio electrónico, se vinculaban con la exigencia de que la manifestación del consentimiento se realizara mediante documento escrito y se confirmara mediante una firma manuscrita. (BUGONI, RIVOLTA; 2007: 36)

Es así como surgieron normas específicas del entorno electrónico, las cuales se conocen como leyes de comercio electrónico, de firma electrónica o de firma digital, según la corriente que adoptara cada país. Estas disposiciones se apoyan en el criterio del equivalente funcional entre el entorno papel y su correlato en el entorno digital. (RIVOLTA, SCHAPPER; 2004: 28)

Concepto técnico legal de Documento Electrónico

Las nuevas leyes de comercio electrónico reconocen el valor jurídico del documento electrónico, o documento digital o mensaje de datos. Estos conceptos, similares entre sí, se refieren a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Asimismo, dichas normas establecen que un documento digital también satisface el requerimiento de escritura.

De esta manera, las leyes equiparan el documento electrónico con los instrumentos privados por medio de los cuales las personas manifiestan su voluntad en papel. Al reconocer su eficacia jurídica, alcanzan a la totalidad de operaciones que se realicen por Internet o en entornos informáticos cerrados.

Desde el punto de vista tecnológico, constituye un documento electrónico cualquier manifestación de voluntad que se exprese en formato digital, como por ejemplo:

- Un mensaje enviado por correo electrónico,
- Un archivo en procesador de texto, como word,
- Un archivo en base de datos, como excel,
- Una base de datos completa,
- Una grabación digital de video,
- Los archivos contenidos en un CD, en un diskette, en un disco rígido, etc.

Al considerar que el documento electrónico satisface el requisito de escritura, las leyes equiparan su valor jurídico al documento escrito sobre papel.

La Convención de Naciones Unidas sobre Comunicaciones Electrónicas en Contratos Internacionales, adoptada por la Asamblea en noviembre de 2005, con el propósito de fomentar la seguridad jurídica y la previsibilidad comercial cuando se utilicen comunicaciones electrónicas en la negociación de contratos internacionales, establece la validez del documento electrónico en su artículo 8. Aunque no lo menciona específicamente, dispone el reconocimiento del valor jurídico de las comunicaciones efectuadas por medios electrónicos. 5

---

[5] *Convención de las* Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en Contratos Internacionales:

Artículo 8: Reconocimiento jurídico de las comunicaciones electrónicas:

Respecto del requisito de forma escrita, la Convención dispone en su Artículo 9 que para los casos en los cuales la ley requiera que una comunicación o un contrato conste por escrito, o prevea consecuencias en el caso de que eso no se cumpla, una comunicación electrónica cumplirá ese requisito si la información consignada en su texto es accesible para su ulterior consulta.

Concepto técnico legal de Firma Electrónica

El término "firma electrónica" se aplica a cualquier sonido, símbolo o proceso, adjunto o lógicamente asociado a un documento electrónico que exprese el consentimiento de una persona emitido en formato digital, y ejecutado o adoptado por dicha persona con el propósito de firmar el documento electrónico.

La ley federal de Estados Unidos sobre firma electrónica, la E-Sign, define como "firma electrónica" a todo sonido, símbolo o proceso, adjunto o lógicamente asociado con un contrato u otro archivo electrónico y ejecutado o adoptado por una persona con la intención de firmar el archivo.

En general, las leyes denominan "firma electrónica" a cualquier mecanismo de autenticación que no cumpla alguno de los requisitos exigidos para una firma digital, que se verán más adelante. "Firma electrónica" es el término genérico y neutral para referirse al universo de tecnologías que una persona puede utilizar para expresar su consentimiento con el contenido de un documento. La "firma electrónica" puede adoptar diversas formas: una firma manuscrita digitalizada, una identificación biométrica, escribir el nombre al final de un documento electrónico o de un correo, el uso de una clave compartida como por ejemplo en los cajeros automáticos, o el uso de criptografía asimétrica con certificados de clave pública emitidos por certificadores no reconocidos en esquemas de PKI estatales. (TELLEZ VALDEZ; 2004: 203)

En Estados Unidos, la Ley de Despapelización Gubernamental (Government Paperwork Elimination Act - GPEA) define como firma electrónica a "cualquier método de firma de un mensaje electrónico que identifique y autentique a la persona que es la fuente del mensaje y que indique su aprobación de los contenidos" del mismo. (KUHN et all; 2001: 5)

Las partes pueden acordar cuál mecanismo reconocerán para autenticarse al enviar y recibir documentos electrónicos. Constituye firma electrónica, por ejemplo:

- El nombre escrito al final de un correo electrónico
- Una palabra clave (password que se utiliza, por ejemplo, para acceder a la banca electrónica o home banking)

---

1. No se negará validez ni fuerza ejecutoria a una comunicación o a un contrato por la sola razón de que esa comunicación o ese contrato esté en forma de comunicación electrónica.
2. Nada de lo dispuesto en la presente Convención hará que una parte esté obligada a utilizar o a aceptar información en forma de comunicación electrónica, pero su conformidad al respecto podrá inferirse de su conducta.

- Una frase clave (passphrase que se utiliza, por ejemplo para entrar en una base de datos)
- Una pregunta y respuesta para autenticarse en un sitio web si se olvidó la contraseña (por ejemplo, en las cuentas de correo electrónico)
- Pulsar el botón "aceptar" en una aplicación web, etc.

Generalmente, los mecanismos de firma electrónica que acuerdan las partes están definidos en los términos y condiciones de uso de un sistema informático, y constan de varios pasos y cruces de información con el propósito de aumentar la seguridad.

Por ejemplo, cuando accedemos a la aplicación de banca electrónica de nuestro banco, nos solicita que, como paso previo para autenticarnos en la página web del Banco, tramitemos nuestra palabra clave en el cajero automático localizado en alguna sucursal. Para acceder al cajero automático, debemos presentar nuestra tarjeta electrónica (algo que tengo) e ingresar nuestra palabra clave de acceso (algo que sé). Una vez abierta la sesión, el cajero automático nos solicita que determinemos una nueva palabra clave específica para banca electrónica, la cual luego deberemos ingresar en el sitio web. Una vez que ingresamos en la página de Internet del Banco, y ya identificados por esta clave obtenida en el cajero automático, la aplicación cruza información con las bases de datos del Banco, y con información adicional de nuestro número de documento, más la palabra clave, nos solicita que definamos una nueva palabra clave con la cual nos autenticaremos en el sistema. Es un mecanismo sencillo, amigable para no expertos, que se apoya en dispositivos ya existentes (tarjeta de débito, cajeros automáticos) y que evidentemente, funciona sin repudios.

En síntesis, la autenticación es un elemento necesario en las comunicaciones formales que se celebran entre partes, incluyendo transacciones de pago. En el sistema bancario, el PIN (personal identification number) provee la autenticación electrónica suficiente para las transacciones en cajeros automáticos (ATM). Este PIN es, desde el punto de vista criptográfico, una clave simétrica, compartida entre el titular y el banco. Desde el punto de vista legal, es una firma electrónica, por la cual el titular expresa su consentimiento para realizar las transacciones en su cuenta bancaria que él mismo realiza a través de la máquina.

Las leyes de comercio electrónico contemplan la figura de firma electrónica, algunas, además, introducen la firma digital, asignándole presunciones respecto de la autoría e integridad de contenidos del documento electrónico firmado.

En general, las aplicaciones en Internet y cajeros automáticos, utilizan la firma electrónica como mecanismo de autenticación. Excepcionalmente, se utiliza firma digital para aplicaciones consideradas de altísimo riesgo.

Dada la evolución del comercio electrónico, que básicamente adopta la firma electrónica como mecanismo de autenticación en el ciberespacio, UNCITRAL ha incorporado dicha figura en su Convención sobre Comunicaciones Electrónicas en Contratos Internacionales.

Esta Convención, aplicable a contratos celebrados entre personas ubicadas en distintos países e instrumentado por medios electrónicos, dispone que para aquellos casos en los cuales la ley requiera que una comunicación o un contrato sea firmado por una parte, o prevea consecuencias en el caso de que no se firme, ese requisito se dará por cumplido respecto de una comunicación electrónica:

a) Si se utiliza un método para determinar la identidad de esa parte y para indicar la voluntad que tiene tal parte respecto de la información consignada en la comunicación electrónica; y

b) Si el método empleado:

i) O bien es tan fiable como sea apropiado para los fines para los que se generó o transmitió la comunicación electrónica, atendidas todas las circunstancias del caso, inclusive todo acuerdo aplicable; o

ii) Se ha demostrado en la práctica que, por sí solo con el respaldo de otras pruebas, dicho método ha cumplido las funciones enunciadas en el apartado a).

Esto implica que, siguiendo el principio jurídico aplicable a los contratos que establece la autonomía de la voluntad de las partes, por una parte, y reconociendo el avance tecnológico y las prácticas del comercio electrónico, por la otra, la citada Convención reconoce el valor legal de la firma electrónica en la medida que haya sido voluntariamente consignada en el documento, con el propósito de dar consentimiento al contenido del mismo. Respecto del mecanismo tecnológico, se basa en el criterio del riesgo, es decir, que se considera válido tanto si el mecanismo es razonable, como si las mismas partes reconocen que han dado su consentimiento para el uso de tal mecanismo.

En este aspecto hay un viraje importante en el concepto de firma, pues en los años 90 la principal preocupación giraba alrededor del potencial repudio de las transacciones electrónicas. Debido a ello, las legislaciones buscaban definir mecanismos tecnológicos que hicieran imposible el repudio. *"Una propiedad adicional a menudo definida como esencial para el e-business es el no repudio, el cual es simplemente un producto de la autenticación combinado con integridad y se entiende que representa un compromiso que goza de la presunción de validez."* (RIVOLTA, SCHAPPER; 2004: 11)

Es así como surgieron las primeras normas de firma digital, que ataban el reconocimiento de la firma a las tecnologías de clave pública y al control del Estado. Transcurridos 10 años, con un comercio electrónico en geométrico avance, no se verificó la hipótesis inicial de que iban a producirse masivos repudios de las transacciones. Por el contrario, y tal como ocurre en el comercio tradicional, las operaciones se desenvolvieron sin inconvenientes. Debido a ello, se elaboró la mencionada Convención, en la cual se privilegia el acuerdo de partes, la neutralidad tecnológica y la matriz de riesgo para autenticación. 6

---

[6] Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en Contratos Internacionales, Artículo 9 inciso 3

Concepto técnico legal de Firma Digital

En general, las leyes entienden por firma digital al mecanismo de autenticación que, basado en criptografía asimétrica, es decir, que usa dos claves, una pública y una privada, permite identificar al firmante y garantizar la integridad del contenido del documento electrónico firmado. Además, para ser considerada legalmente firma digital, ese mecanismo debe haber sido aplicado mediante el uso de un certificado digital emitido por una entidad de certificación acreditaba por el órgano rector del Estado en dicha materia.

Si cumple todos esos requisitos, este mecanismo de autenticación será considerado ante la ley como firma digital, y gozará de dos presunciones asociadas, la presunción de autoría del documento electrónico, y la presunción de integridad de los contenidos del mismo. Sin embargo, estas presunciones son iuris tantum, es decir, admiten prueba en contrario.

Si el mecanismo que aludimos no cumpliera con alguno de los requisitos que la ley exige para considerarlo firma digital, entonces tiene el valor de una firma electrónica, pues ha sido utilizado mediante acuerdo de partes, para identificarse en el entorno digital y para expresar su consentimiento con el contenido del documento electrónico firmado.

Una firma digital es un conjunto de datos asociados a un mensaje o documento digital que permite asegurar la identidad del firmante y la integridad del mensaje.

La firma digital no garantiza la confidencialidad del documento electrónico, ya que no implica que el mensaje esté encriptado. El mensaje está en claro, y puede ser leído por otras personas. Si se lo desea encriptar, si bien se utilizan certificados de clave pública, el procedimiento es el inverso y además, no pertenece a la infraestructura de firma digital.

La firma digital en un documento electrónico tampoco impide que el mensaje sea alterado, no garantiza su inviolabilidad, pero sí da la certeza de que el contenido del mensaje es íntegro o no lo es: permite saber con exactitud si el mensaje es el mismo que fue emitido por el signatario o fue alterado en el camino.

Procedimientos para originar una firma digital

El proceso que culmina con la firma digital y posterior verificación de autoría e integridad de un documento contempla varias etapas, que se detallan a continuación.

Paso 1.- Procedimiento de generación de claves

La firma digital es el resultado de un procedimiento que utiliza un par de claves: una clave privada que se encuentra bajo el exclusivo control de la persona que firma, y una clave pública conocida por todos que permite la verificación de la firma digital.

La clave privada es una clave numérica creada por un algoritmo de generación de claves.

Al mismo tiempo que se genera la clave privada, este algoritmo genera otra clave, diferente, pero que está íntimamente asociada con la anterior, denominada clave pública. Esta clave pública funciona como complemento de la clave privada. Ambas claves, la privada y la pública, se calculan a partir de dos números primos suficientemente grandes, seleccionados al azar. La clave pública es el resultado de multiplicar ambos números primos. La clave privada, es el resultado de una operación de aritmética modular basada en los mismos números primos con los que se calculó la clave pública. Por eso, ambas claves están íntimamente relacionadas, pero no es posible derivar una de la otra.

La clave privada debe permanecer bajo el exclusivo control de su propietario siendo este el único capaz de tener acceso a ella, esta característica es lo que permite que una firma digital identifique en forma unívoca al firmante, la clave pública por otra parte es la que permite verificar a un tercero el origen de la firma y la no alteración del mensaje.

Paso 2.- Procedimiento de emisión de un certificado digital

El propósito de identificar a una persona no estaría cumplido si no se pudiera asociar indubitablemente una clave pública con una persona determinada. Esto se logra mediante la inclusión de la clave pública en un certificado digital a nombre del firmante, emitido por una entidad de certificación habilitada por un órgano rector del Estado para tal fin. Previamente, dicha autoridad certificante, por sí o a través de una autoridad de registro, tuvo ante sí los datos de identificación del firmante, documento nacional que acredite la identidad del suscriptor del certificado, quien mediante su presencia física ante dichas autoridades prueba que es quien dice ser.

Un certificado digital es un documento electrónico emitido y firmado digitalmente por una autoridad certificante habilitada por el Estado para tal fin, el cual incluye la clave pública del suscriptor, entre otros datos. Tiene un plazo de validez, normalmente entre uno y dos años, y contiene información sobre el suscriptor y sobre la autoridad que lo emitió.

Paso 3.- Procedimiento de firmado digital de un documento electrónico

Hasta ahora se vio cómo se generan las claves, cómo se emite un certificado digital en base a un proceso de identificación basado en la presencia física del suscriptor del certificado. Ahora analizaremos el procedimiento de firma digital.

El procedimiento utilizado para firmar digitalmente un mensaje es el siguiente:

- La persona que va a firmar un documento electrónico, ya sea un mail, un documento word, etc, aplica sobre dicho documento (el cual en definitiva es un conjunto de números) una función de hash, logrando un resultado, que se conoce como digesto seguro del documento.

- Este digesto seguro del mensaje se encripta con la clave privada del firmante, y el resultado es lo que se denomina firma digital. Esta firma digital se envía adjunta al mensaje original.
- El firmante remite al destinatario el mensaje, la firma digital del mensaje, y su certificado digital el cual contiene su clave pública. De esta manera el firmante adjunta al documento una marca que es única para ese documento y que sólo él es capaz de producir.

Paso 4.- Verificación de la autoría e integridad del mensaje

El receptor del mensaje podrá comprobar que el mensaje no fue modificado desde su creación y que el firmante es quién dice serlo mediante la verificación de la firma digital. Para ello, realiza el siguiente procedimiento: en primer término recalculará la función de hash del mensaje recibido, obteniendo el digesto seguro. Luego desencriptará la firma digital del mensaje utilizando la clave pública del firmante y obtendrá de esa forma el digesto seguro del mensaje original; si ambos digestos seguros coinciden, significa que el mensaje no fue alterado y que el firmante es quien dice serlo.

Con este procedimiento se verifica la integridad y autoría del mensaje, garantizando su no repudio.

Validez jurídica de una firma digital

Desde el punto de vista legal, para ser válida jurídicamente, la firma digital debe cumplir estos requisitos:

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 por una autoridad de certificación habilitada para funcionar como tal por un órgano del Estado.

Estos requisitos son los que constituyen el principal obstáculo para el desarrollo del comercio electrónico, pues son de alcance local, requieren presencia física, y los certificados de por sí tienen períodos de vida muy breves, uno o dos años, con lo cual al cabo de dicho lapso, las firmas digitales no son válidas, aunque lo hayan sido en el momento que se produjeron.

Marco legal internacional

Ya culminando la primera década del S XXI, puede afirmarse que está superado el dilema que se presentaba a mediados de los 90 con la irrupción de Internet, respecto de si debía ésta auto regularse o los Estados debían generar normas. La primera clasificación del derecho en el mundo digital, podría sintetizarse en dos corrientes, la corriente ontológica que sostenía que el fenómeno de Internet demandaba un derecho diferente, y la corriente instrumental, que simplemente traslada las normas existentes del derecho tradicional por analogía. (LORENZETTI, 2001: 37).

Estas posiciones se han visto superadas por el avance legislativo a nivel mundial. Todos los países hoy cuentan con leyes de comercio electrónico, de firma electrónica o de firma digital, así como normas penales referidas a delitos informáticos, normas tendientes a la protección de datos personales, y normas de gobierno electrónico. En tal sentido, es dable observar la existencia de un eje común en la evolución del derecho de Internet alrededor de la necesidad de regular los potenciales conflictos que pudieran surgir a partir del uso de las tecnologías. Esta tercera opción, supera la debilidad de los dos enfoques anteriores. En efecto, el enfoque ontológico no toma en cuenta que el nuevo medio electrónico no *suprime* los conflictos, y el enfoque instrumental no considera que, si bien los conflictos perduran, el medio utilizado los modifica. (LORENZETTI, 2001: 44).

Una tercera alternativa, que permite alcanzar una mejor comprensión de la relación entre derecho e Internet, se focaliza en los conflictos perdurables y su problematicidad específica en el medio tecnológico, considerando la analogía a nivel de principios y la diversidad a nivel de reglas. Es decir, que problemáticas tales como exclusión social, monopolio, discriminación, etc, deben estudiarse analizando el impacto derivado del uso de las tecnologías. Los valores y principios del derecho, permanecen tanto en el mundo físico como en el espacio virtual, en cambio, las reglas son diferentes, difieren las reglas aplicables al mundo virtual respecto de las normas tradicionales basadas en medios físicos como el papel. (RIVOLTA; 2008: 25)

La aparición y extraordinario crecimiento de Internet en los años 90 generó nuevos medios para realizar transacciones, los que fueron reemplazando paulatinamente el tradicional uso del papel. En ese orden, los países comenzaron a adecuar su derecho interno, con el fin de otorgar pleno valor legal a los contratos celebrados mediante el uso de medios electrónicos.

Comisión de Naciones Unidas para el Desarrollo del Derecho Mercantil - UNCITRAL

Desde mediados de los años 80, la Comisión de Naciones Unidas para el Desarrollo del Derecho Mercantil, UNCITRAL por sus siglas en inglés, ha elaborado normas modelo tendientes a facilitar las transacciones en formato electrónico. (BUGONI, RIVOLTA; 2007: 37)

UNCITRAL ha desarrollado leyes modelo sobre comercio electrónico y firma electrónica, así como una ley modelo de compras gubernamentales. Actualmente, ha aprobado una Convención sobre comunicaciones electrónicas en contratos internacionales, que no es una ley modelo, sino que es una norma que, a medida que los países vayan adhiriendo, constituirá derecho interno.

La importancia del trabajo de UNCITRAL se ha traducido en un rol preponderante en materia de comercio electrónico. En efecto, todas las leyes internas de los países sobre comercio electrónico han tomado como guía a las leyes modelo de UNCITRAL, tanto la de comercio electrónico como la de firma electrónica, introduciendo cada país las modificaciones que consideraba pertinentes.

Sin embargo, si bien contar con leyes de comercio electrónico ha sido un gran avance para el desarrollo de las actividades por Internet, se trató de un primer paso. En efecto, todas las leyes de comercio electrónico, firma electrónica o firma digital son normas locales, de derecho interno de cada país. Su alcance se limita a las fronteras, con lo cual, queda sin regularse una importante cantidad de transacciones que se realizan cada día por Internet, localizadas las partes en distintos países.

Ley Modelo de Comercio Electrónico

A mediados de los 90 UNCITRAL formuló su Ley Modelo de Comercio Electrónico con el objeto de asistir a los países miembros en el esfuerzo de dotar a las transacciones realizadas por medios digitales de un marco jurídico adecuado. En ese momento, el derecho interno de cada país, diseñado en base a la tecnología del papel y la pluma, no contemplaba estos nuevos medios que el avance de las tecnologías de la comunicación y la información brindaban. Con el explosivo desarrollo de Internet, fue necesario dotar al derecho civil y comercial de cada país, del complemento necesario para despejar las dudas que pudieren existir respecto de la validez legal de las transacciones electrónicas.

En este marco, la iniciativa de UNCITRAL apuntaba a superar el problema que se presentaba cuando las leyes civiles tradicionales requerían que un documento constara por escrito, se guardara su original, y estuviera firmado. Dos mil años de cultura del papel resultaban así conmovidos. Ahora, el soporte era otro, digital. De esta manera, UNCITRAL identificó los principales aspectos a ser considerados para dotar al comercio electrónico de un reconocimiento legal suficiente. Es así como elaboró en 1996 la Ley Modelo de Comercio Electrónico, basándola en dos principios:

- Neutralidad tecnológica, también conocido como no discriminación.
- Equivalente Funcional

El principio de neutralidad tecnológica tiene como principal objetivo permitir la vigencia temporal de la norma. Dado que los tiempos difieren entre el constante avance tecnológico y el proceso de aprobación de leyes, cabe suponer que una ley que define una tecnología determinada quedará rápidamente obsoleta.

Para superar este problema, se abordó el tema buscando el equivalente funcional de las figuras jurídicas tradicionales, esto es, documento, firma, original. Determinadas las funciones que tiene cada figura en el entorno en papel, se requieren similares características a la solución tecnológica que reemplace dichos conceptos. La Ley Modelo advierte que *"la adopción de este criterio del equivalente funcional no debe dar lugar a que se impongan normas de seguridad más estrictas a los usuarios del comercio electrónico (con el consiguiente costo) que las aplicables a la documentación consignada sobre papel."* (UNCITRAL; 1996: 21)

Así es como la Ley Modelo de Comercio Electrónico otorga valor legal a los mensajes de datos, o documentos electrónicos, es decir, a los documentos instrumentados por medios electrónicos, considerando que los mismos cumplen el requisito de escritura y constituyen originales.

Respecto de autenticación, aborda el tema de la firma. (RIVOLTA, SCHAPPER; 2004: 31). En su artículo 7, la Ley Modelo establece un criterio amplio para reconocer la validez de la firma electrónica, reconociendo igual valor al de la firma ológrafa, en los siguientes casos:

- si se utiliza un método para identificar a la persona y para indicar que esa persona aprueba el contenido del mensaje de datos o documento electrónico.
- si ese método es tan fiable como sea apropiado para los fines del mensaje de datos, teniendo en cuenta todas las circunstancias del caso, inclusive el acuerdo de partes.

Esta solución, amplia y general, coincide con lo que ocurre en el entorno de papel, donde tradicionalmente, existen una serie de métodos considerados "firmas" que se aplican según las situaciones. En efecto, la Ley Modelo en su Guía para la Incorporación menciona que, *"... junto con la firma manuscrita tradicional, existen varios tipos de procedimientos (por ejemplo, estampillado, perforado), a veces denominados también "firmas", que brindan distintos grados de certeza. Por ejemplo, en algunos países existe el requisito general de que los contratos de compraventa de mercaderías por encima de cierto monto estén "firmados" para ser exigibles."* (UNCITRAL; 1996: 39)

Sin embargo, el concepto de la firma adoptado en ese contexto es tal que un sello, un perforado o incluso una firma mecanografiada o un membrete puede considerarse suficiente para satisfacer el requisito de la firma. En el otro extremo del espectro, existen requisitos que combinan la firma manuscrita tradicional con procedimientos de seguridad adicionales como la confirmación de la firma por testigos." (UNCITRAL; 1996: 39)

Seguidamente, sugiere la aplicación de criterios comerciales para evaluar los métodos de autenticación que pueden ser utilizados, citando entre otros, los siguientes factores técnicos, jurídicos y comerciales a ser considerados (RIVOLTA, SCHAPPER; 2004: 32):

1) la perfección técnica del equipo utilizado por cada una de las partes;
2) la naturaleza de su actividad comercial;
3) la frecuencia de sus relaciones comerciales;
4) el tipo y la magnitud de la operación;

5) la función de los requisitos de firma con arreglo a la norma legal o reglamentaria aplicable;
6) la capacidad de los sistemas de comunicación;
7) la observancia de los procedimientos de autenticación establecidos por intermediarios;
8) la gama de procedimientos de autenticación que ofrecen los intermediarios;
9) la observancia de los usos y prácticas comerciales;
10) la existencia de mecanismos de aseguramiento contra el riesgo de mensajes no autorizados;
11) la importancia y el valor de la información contenida en el mensaje de datos;
12) la disponibilidad de otros métodos de identificación y el costo de su aplicación;
13) el grado de aceptación o no aceptación del método de identificación en la industria o esfera pertinente, tanto en el momento cuando se acordó el método como cuando se comunicó el mensaje de datos; y
14) cualquier otro factor pertinente.

El Artículo 7 establece una norma mínima de autenticación entre las partes, que no considera si existe o no una relación comercial entre ellas.

Ley Modelo sobre Firma Electrónica

En 2001, UNCITRAL elaboró la Ley Modelo sobre Firmas Electrónicas, complementaria de la Ley Modelo de Comercio Electrónico. Esta nueva Ley Modelo se propone complementar al artículo 7 de la mencionada Ley Modelo de Comercio Electrónico, regulando específicamente los casos de firma electrónica basada en certificados de clave pública. (BUGONI, RIVOLTA; 2007: 41)

Contempla dos aspectos relevantes referidos al tema de autenticación que nos ocupa:

1.- Respeta el principio de neutralidad tecnológica, aceptando cualquier método de autenticación acordado entre las partes. Dicho principio también se conoce como de No Discriminación.

2.- Establece la validez transfronteriza de las firmas digitales en la medida que respondan a criterios de fiabilidad equivalentes, tomando en cuenta normas internacionales reconocidas u otros factores pertinentes.

En el nuevo contexto de comercio electrónico, los países han ido resolviendo el tema de la firma electrónica de diferente manera, ante esta situación, UNCITRAL advierte acerca del *"...riesgo de que distintos países adopten criterios legislativos diferentes en relación con las firmas electrónicas exige disposiciones legislativas uniformes que establezcan las normas básicas de lo que constituye en esencia un fenómeno internacional, en el que es fundamental la armonía jurídica y la interoperabilidad técnica."* (UNCITRAL; 2002:10)

La Ley Modelo de Firma Electrónica, si bien regula en detalle las Infraestructuras de Firma Digital, pretende establecer un marco de neutralidad respecto de los medios técnicos utilizables. En la Guía para la Incorporación, en el punto 82, menciona que *"....Ante la evolución de las innovaciones tecnológicas, la Ley Modelo establece criterios para el reconocimiento jurídico de las firmas electrónicas independientemente de la tecnología utilizada (a saber, firmas electrónicas basadas en la criptografía asimétrica; los dispositivos biométricos (que permiten la identificación de personas por sus características físicas, como su geometría manual o facial, las huellas dactilares, el reconocimiento de la voz o el escáner de la retina, etc.); la criptografía simétrica; la utilización de números de identificación personal (NIP); la utilización de "contraseñas" para autenticar mensajes de datos mediante una tarjeta inteligente u otro dispositivo en poder del firmante; versiones digitalizadas de firmas manuscritas; la dinámica de firmas; y otros métodos, como la selección de un signo afirmativo en la pantalla electrónica mediante el ratón). Las diversas técnicas enumeradas podrían combinarse para reducir el riesgo sistémico."* (UNCITRAL; 2002: 43)

Asimismo, la Ley Modelo establece el principio de No discriminación de las firmas electrónicas extranjeras. Establece como principio básico que el lugar de origen en sí no debe ser en ningún caso un factor para determinar si puede reconocerse la capacidad de los certificados extranjeros o las firmas electrónicas para tener eficacia jurídica en un Estado promulgante. La determinación de si un certificado o una firma electrónica pueden tener eficacia jurídica, y hasta qué punto pueden tenerla, no debe depender del lugar en que se haya emitido el certificado o la firma electrónica sino de su fiabilidad técnica.

La Ley Modelo de Firma Electrónica no fija un criterio específico para determinar la equivalencia de fiabilidad técnica entre certificados emitidos por certificadores nacionales y extranjeros. Por el contrario, establece un marco general referido a las normas internacionales reconocidas u otros factores equivalentes. En su Guía para la Incorporación, explica que el concepto de "norma internacional reconocida" debe interpretarse con amplitud para que abarque las normas internacionales técnicas y comerciales (por ejemplo, las dependientes del mercado), las normas y reglas adoptadas por órganos gubernamentales o intergubernamentales y las "normas voluntarias".

Es interesante el concepto de "Normas internacionales reconocidas", que pueden ser declaraciones de prácticas técnicas, jurídicas o comerciales aceptadas, desarrolladas por el sector público o el privado (o por ambos), que tengan carácter normativo o interpretativo, generalmente aceptadas para su aplicación internacional. Esas reglas pueden adoptar la forma de requisitos, recomendaciones, directrices, códigos de conducta o declaraciones de prácticas óptimas o de normas.

Convención sobre Comunicaciones Electrónicas en Contratos Internacionales

Desde que surgió la Ley Modelo de Comercio Electrónico en 1996, los países han ido adoptando leyes sobre la materia. Sin embargo, dichas leyes tienen un alcance limitado, pues se aplican a las transacciones internas de cada país,

quedando sin regular una amplia gama de operaciones transfronterizas, que se realizan a través de Internet.

Para superar este problema, UNCITRAL elaboró un proyecto de Convención sobre Comunicaciones Electrónicas Internacionales que actualmente ha sido firmado por 18 naciones entre las que se encuentran China, Rusia y Corea, y de la Región, Paraguay, Colombia, Honduras y Panamá.

Dicha Convención, adoptada por la Asamblea General el 23 de noviembre de 2005, tiene por objeto fomentar la seguridad jurídica y la previsibilidad comercial cuando se utilicen comunicaciones electrónicas en la negociación de contratos internacionales. Regula la determinación de la ubicación de la parte en un entorno electrónico; el momento y lugar de envío y de recepción de las comunicaciones electrónicas; la utilización de sistemas de mensajes automatizados para la formación de contratos; y los criterios a que debe recurrirse para establecer la equivalencia funcional entre las comunicaciones electrónicas y los documentos sobre papel, incluidos los documentos sobre papel "originales", así como entre los métodos de autenticación electrónica y las firmas manuscritas. (BUGONI, RIVOLTA; 2007: 46)

La Convención de UNCITRAL *"respeta el principio de neutralidad tecnológica, admitiendo todo método de autenticación que permita por una parte, establecer la identidad de la persona y por la otra, establecer la manifestación de la voluntad de esa persona. Admite asimismo, los acuerdos de parte, los antecedentes, la proporcionalidad entre medios y fines, la prueba posterior inclusive. Considera a tales métodos como el equivalente funcional de la firma que solicitan las leyes tradicionales."* (BUGONI, RIVOLTA; 2007: 46).

MERCOSUR

En el ámbito del MERCOSUR, con su conformación original de cuatro miembros (Argentina, Brasil, Paraguay y Uruguay), se comenzó a tratar el tema de firma digital en el Subgrupo de Trabajo Nº 13 de Comercio Electrónico, en cuyo marco se aprobaron dos resoluciones relativas a la firma digital.

Resoluciones sobre Comercio Electrónico

En 2006, el Subgrupo de Trabajo Nº 13 de Comercio Electrónico del MERCOSUR, aprobó dos Resoluciones sobre Firma Digital. La primera de ellas, la Resolución Nº 34/06, establece las Directrices para la celebración de acuerdos de reconocimiento mutuo de firmas electrónicas avanzadas en el ámbito del MERCOSUR.7 La segunda, la Resolución Nro. 37/06, contempla la eficacia jurídica del documento electrónico, de la firma electrónica y de la firma electrónica avanzada en el ámbito del MERCOSUR.8

[7] Disponible en http://www.mercosur.int/msweb/Normas/normas_web/Resoluciones/ES/RES%20034-2006.pdf

[8] Disponible en http://www.mercosur.int/msweb/Normas/normas_web/Resoluciones/ES/GMC_2006_RES-037_ES_EficaciaFirmaDigital.pdf

Ninguna de estas Resoluciones tiene efecto práctico, por cuanto la primera, si bien no requiere la incorporación al derecho interno, no establece un acuerdo de reconocimiento en sí mismo sino que fija pautas a tal fin. La segunda, requiere se su incorporación al derecho interno para tener eficacia jurídica, con lo cual, representa solamente una declaración general sin efectos jurídicos. (BUGONI, RIVOLTA; 2007: 46)

Resolución Nº 34/06

Establece las directrices a ser consideradas en futuros acuerdos de reconocimiento de certificados emitidos por los países miembros entre sí.

Esta Resolución establece los estándares a ser tenidos en cuenta, mencionando concretamente cada uno de ellos. Debido al constante avance tecnológico, y las distintas velocidades entre dicho cambio y los procesos de aprobación de las normas, incluyendo las del MERCOSUR, permite augurar una pronta obsolescencia para esta Resolución, al estar muy enfocada en la tecnología.

Define asimismo los criterios de seguridad física y lógica de los prestadores de servicios de certificación, los criterios de auditoria y control a ser aplicables a los certificadores, los criterios de emisión de certificados reconocidos y hasta recomendaciones para la verificación segura de firmas electrónicas avanzadas.

En términos generales, esta Resolución no toma en consideración el distinto enfoque que cada país del bloque ha dado al tema de comercio electrónico.

En efecto, mientras Argentina cuenta con una ley sobre firma digital vigente, no ha implementado aun una infraestructura de firma digital. Brasil, por el contrario, no cuenta con un marco legal, sino que por Decreto presidencial, ha creado una Infraestructura de Claves Públicas muy potente en la cual se basan numerosas aplicaciones. Paraguay no tiene legislación aprobada en la materia, aunque proyectos de ley se encuentran bajo tratamiento legislativo, basados en PKI. Uruguay, sigue otro enfoque más moderno, dispone de una infraestructura de firma digital pero no como requisito para otorgar validez a los actos emitidos en forma electrónica. (BUGONI, RIVOLTA; 2007: 48)

Dicho de otra manera, el enfoque del comercio electrónico no debió pasar por un abordaje tecnológicamente sesgado como el que se traduce de la presente resolución, sino que más bien debió buscar los comunes denominadores que permitieran posteriores acuerdos respetando las diferencias.

Resolución Nº 37/06

Esta Resolución necesita ser incorporada al derecho interno de cada país para ser efectiva. Se trata de una declaración general sobre la intención de los Estados de reconocer eficacia jurídica al documento electrónico, la firma electrónica y la firma digital.

En su artículo 2, establece los principios siguientes:

1. Autonomía operativa y coordinación permanente entre las Infraestructuras nacionales;

2. Interoperabilidad basada en estándares internacionales;

3. Intercambio de información y documentación digital entre los Estados Partes en condiciones técnicas seguras, con validez legal y valor probatorio;

4. Transparencia en la gestión de la certificación digital;

5. Tratamiento neutro en las leyes nacionales con relación a las diversas tecnologías utilizadas en las actividades previstas en la presente Resolución, de modo de permitir la adaptación al ritmo del desarrollo tecnológico inherente a esas actividades (neutralidad tecnológica);

6. Interpretación funcional de los términos y conceptos, a fin de asegurar que no sean negados efectos jurídicos a un proceso o tecnología utilizado por un Estado Parte, por el sólo hecho de que se le atribuye una nomenclatura distinta a la prevista en la Resolución.

En su artículo 4, dispone que en cualquiera de los Estados Partes los documentos electrónicos tendrán los mismos efectos jurídicos que los documentos escritos, salvo excepciones contempladas en las legislaciones nacionales. Reconoce la validez de la firma electrónica cuando la misma fuese admitida como válida por las partes que la utilizan o fuese aceptada por la persona a quien fuese opuesto el documento a ella vinculado.

Los Estados Partes asegurarán que no sean negados efectos probatorios a un documento electrónico por el sólo hecho de que éste no esté vinculado a una firma electrónica avanzada, si por algún medio inequívoco se pudiese demostrar su autenticidad e integridad.

Reafirma el principio de libertad de las partes para concertar de común acuerdo las condiciones en que aceptarán las firmas electrónicas, conforme a su legislación nacional, en tanto para aquellos casos en los cuales una de las partes desconozca su firma electrónica, corresponde a la otra parte probar su validez.

A continuación, establece una serie de pautas sobre los proveedores de servicios de acreditación, su sistema de acreditación, de auditoría y control, el reconocimiento de certificados, muy específicos y tecnológicamente orientados a PKI.

Sin embargo en el artículo 7, el tercer párrafo autoriza a los Estados Parte a establecer prescripciones adicionales. Tales prescripciones serán objetivas, transparentes, proporcionadas y no discriminatorias, y sólo podrán hacer referencia a las características específicas de la aplicación de que se trate. Estas

prescripciones no deberán obstaculizar los servicios transfronterizos. (BUGONI, RIVOLTA; 2007: 49)

Marco Legal Argentino de la Firma Digital y el Documento Electrónico

La aparición de Internet y las computadoras ha planteado un interrogante respecto de las normas jurídicas aplicables. Dos corrientes han surgido: una posición "ontológica" que sostiene que el mundo digital es un mundo nuevo que demanda un nuevo derecho, y la corriente "instrumental" que traslada las normas existentes mediante el principio de analogía. (LORENZETTI, 2001: 37). Coincidimos con LORENZETTI al considerar que la posición "ontológica" parece excesiva al sostener que existen dos mundos paralelos: el mundo real y el mundo virtual, y que este no requiere de regulación. También, que la posición "instrumental" podría resultar insuficiente en aquellas situaciones nuevas derivadas del desarrollo tecnológico. Así, creemos que el derecho tradicional es aplicable en cuanto a principios, conflictos y relaciones jurídicas, y que se deberá innovar en los aspectos instrumentales que así lo requieran.

La firma es un medio que la ley reconoce para vincular un documento con su autor. En un sentido amplio, la firma es cualquier método o símbolo utilizado por una persona con la intención de vincularse o autenticar un documento. (LORENZETTI; 2001: 58). Las técnicas que se utilizan para firmar pueden ser variadas: desde el trazo de la mano en un papel (firma manuscrita), la firma manual contenida en un sello, la firma manuscrita digitalizada, una clave compartida (por ejemplo, en los cajeros automáticos de los Bancos), una identificación biométrica o una clave asimétrica reconocida o no en un esquema PKI. Pero cualquiera de estas técnicas serán jurídicamente reconocidas como "firma" de la persona.

Nuestro derecho de fondo, el Código Civil, dispone que la firma sea un requisito para el otorgamiento de instrumentos privados y públicos, como manifestación del consentimiento de la persona con el objeto del acto jurídico. El Código de Vélez, del año 1869, no requiere en su articulado que la firma sea manuscrita, salvo en cuanto al testamento ológrafo. En efecto, el artículo 3639 dispone que:

> *Art. 3.639. El testamento ológrafo para ser válido en cuanto a sus formas, debe ser escrito todo entero, fechado y firmado por la mano misma del testador. La falta de alguna de estas formalidades lo anula en todo su contenido.*

Por otra parte, nuestro Código Civil establece que las formas y solemnidades de los actos jurídicos serán aquellas que se establezcan por las leyes del lugar de celebración.

> *Art. 950. Respecto a las formas y solemnidades de los actos jurídicos, su validez o nulidad será juzgada por las leyes y usos del lugar en que los actos se realizaren.*

A su vez, el Código prevé la existencia de instrumentos públicos y de instrumentos privados. En cada caso, la firma constituye un requisito esencial. La ausencia de firma torna al acto anulable.

> *Art. 988. El instrumento público requiere esencialmente para su validez, que esté firmado por todos los interesados que aparezcan como parte en él. Si alguno o algunos de los cointeresados solidarios o meramente mancomunados no lo firmasen, el acto sería de ningún valor para todos los que lo hubiesen firmado.*
>
> *Art. 989. Son anulables los instrumentos públicos, cuando algunas de las partes que aparecen firmadas en ellos, los arguyesen de falsos en el todo, o en parte principal, o cuando tuviesen enmiendas, palabras entre líneas, borraduras o alteraciones en partes esenciales, como la fecha, nombres, cantidades, cosas, etcétera, no salvadas al fin.*
>
> *Art. 1.012. La firma de las partes es una condición esencial para la existencia de todo acto bajo forma privada. Ella no puede ser reemplazada por signos ni por las iniciales de los nombres o apellidos*

El Código contempla el principio de libertad de las formas para los actos jurídicos celebrados por instrumentos privados.

> *Art. 1.020. Para los actos bajo firma privada no hay forma alguna especial. Las partes pueden formarlos en el idioma y con las solemnidades que juzguen más convenientes.*

El Código Civil prevé el repudio del acto, habilitando al signatario a desconocer el contenido del mismo, mediante los elementos probatorios que considere convenientes, excepto el de testigos.

> *Art. 1.017. El signatario puede, sin embargo, oponerse al contenido del acto, probando que las declaraciones u obligaciones que se encuentran en él, no son las que ha tenido intención de hacer o de contratar. Esta prueba no puede ser hecha con testigos.*

Nuestro país cuenta con un marco normativo completo en materia de transacciones electrónicas [9]. La ley de Firma Digital No. 25.506 reconoce el valor jurídico del documento electrónico, la firma electrónica y la firma digital en todo el territorio nacional. Es una ley que complementa las disposiciones del Código Civil, con el objetivo de facilitar el uso de medios digitales para la realización de transacciones, tanto entre particulares como por parte de los organismos del Estado.

La Ley Nº 25.506 está reglamentada por los Decretos Nº 2628/02 y Nº 724/06, habiendo adquirido plena vigencia desde diciembre de 2002.

La Ley Nº 25.506 establece en su primer capítulo las disposiciones necesarias para otorgar validez jurídica al documento electrónico, a la firma digital y a la firma electrónica. Contiene disposiciones relativas a la consideración de original y a la

[9] Ley Nº 25.506 (B.O. 14/12/2001), el Decreto Nº 2628/02 (B.O. 20/12/2002), el Decreto N° 724/06 modificatorio del Decreto Nº 2628/02 (B.O. 13/06/06) y la Decisión Administrativa de la Jefatura de Gabinete de Ministros N° 6/07 (B.O. 12-02-07)

forma escrita, destacando que un documento electrónico cumple dichos requisitos en la medida que sea accesible para su posterior consulta.

La Ley otorga una fuerza probatoria superior a la firma digital respecto de la firma electrónica. Le asigna dos presunciones iuris tantum, es decir, que admiten prueba en contrario. En efecto, el artículo 7° dispone que un documento firmado digitalmente goza de la presunción de autoría respecto de la persona titular del certificado digital, y por su parte, el artículo 8° establece la presunción de integridad del documento electrónico firmado digitalmente, es decir, que se presume que dicho documento no ha sido alterado.

Sin embargo, debe destacarse que la firma digital de un documento no impide que el mismo sea modificado. Simplemente asegura que, si el documento electrónico firmado digitalmente sufre alguna alteración, esta circunstancia quede en evidencia. Es por ello que el legislador le asigna una presunción de integridad.

Complementariamente, la Ley N° 25.506 contiene disposiciones sobre la calidad de "original" de un documento electrónico en el artículo 11 y sobre la conservación de los documentos digitales en el artículo 12.

En los capítulos siguientes, la Ley crea la Infraestructura de Firma Digital, constituyendo el sistema basado en criptografía asimétrica, con un órgano público que licencia y autoriza a funcionar a las autoridades certificantes emisoras de certificados de firma digital.

Esta Ley reconoce como antecedente el Decreto No. 427 del año 1998, pionero en la región, el cual creaba una Infraestructura de Firma Digital para la Administración Nacional, responde al criterio imperante en la época de su elaboración, 1999 y 2000. En efecto, las normas de ese momento se basaban en criterios tecnológicos determinados. Dicho enfoque ha sido superado con el tiempo, debido a que el incesante avance tecnológico no es acompañado con la misma celeridad en los procesos de aprobación legislativa, con lo cual se hace necesario contar con leyes tecnológicamente neutras, que sobrevivan a los avances de la tecnología. (LORENZETTI; 2001: 45)

Documento electrónico

Los principales obstáculos que presentaba el marco normativo anterior a la Ley N° 25.506 estaban representados por:

a) la exigencia de que los documentos constaran por escrito,
b) la necesidad de que estuvieran firmados, y
c) su carácter de original y la guarda de documentación.

A fin de complementar las disposiciones del Código Civil, la ley de firma digital argentina, aborda en su primer capítulo estos aspectos mencionados.

En efecto, la Ley N° 25.506 incorpora el concepto de documento digital, equiparándolo con el concepto de documento tradicional en soporte papel, aclarando

que el documento electrónico satisface el requerimiento de escritura que los códigos tradicionales incluyen.

Reza la Ley:

> *ARTICULO 6º — 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.*

Además de lo dicho, la Ley contiene disposiciones sobre la calidad de "original" de un documento electrónico en el artículo 11 y sobre la conservación de los documentos digitales en el artículo 12.

> *ARTICULO 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.*

> *ARTICULO 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.*

La Ley Nº 25.506 también incluye un artículo muy interesante referido a la presunción de autoría de los mensajes emitidos por aplicaciones informáticas. En efecto, dispone en el artículo 10 que, salvo prueba en contrario, un documento digital firmado digitalmente por el remitente, y enviado en forma automática por una aplicación informática, se presume que fue remitido por éste.

> *ARTICULO 10. — Remitente. Presunción. Cuando un documento digital sea enviado en forma automática por un dispositivo programado y lleve la firma digital del remitente se presumirá, salvo prueba en contrario, que el documento firmado proviene del remitente.*

Firma Electrónica

Respecto de la firma, la Ley Nº 25.506 incorpora dos conceptos: la firma electrónica y la firma digital. (MASON, 2006: 148). Ambas especies de firma son válidas, de acuerdo con el artículo 1º de la Ley. Más precisamente, existe una amplia gama de alternativas para la firma electrónica, que van desde un simple correo electrónico, el uso de tecnologías de clave pública compartidas (PGP), el uso de palabras clave basadas en criptografía simétrica, hasta el uso de tecnología de clave pública basada en certificados digitales emitidos por una entidad de certificación que no se encuentre licenciada por la autoridad pública.

Una firma digital que utilice criptografía asimétrica y tecnología de clave pública, puede ser considerada como una firma electrónica, tanto como la mera inclusión del nombre como parte del texto de un mensaje de correo electrónico, en la medida que el firmante haya ejecutado o adoptado el símbolo con la intención de firmar, esto es, como declaración de voluntad respecto del contenido del mensaje.

La diferencia entre una firma electrónica y una firma digital, desde el punto de vista jurídico, radica en la carga de la prueba de su validez.

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

Firma Digital

Las leyes entienden por firma digital al mecanismo de autenticación que, basado en criptografía asimétrica, es decir, que usa dos claves, una pública y una privada, permite identificar al firmante y garantizar la integridad del contenido del documento electrónico firmado. Además, para ser considerada legalmente firma digital, ese mecanismo debe haber sido aplicado mediante el uso de un certificado digital emitido por una entidad de certificación acreditaba por el órgano rector del Estado en dicha materia.

Si cumple todos esos requisitos, este mecanismo de autenticación será considerado ante la ley como firma digital, y gozará de dos presunciones asociadas, la presunción de autoría del documento electrónico, y la presunción de integridad de los contenidos del mismo. Sin embargo, estas presunciones son iuris tantum, es decir, admiten prueba en contrario.

Si el mecanismo que aludimos no cumpliera con alguno de los requisitos que la ley exige para considerarlo firma digital, entonces tiene el valor de una firma electrónica, pues ha sido utilizado mediante acuerdo de partes, para identificarse en el entorno digital y para expresar su consentimiento con el contenido del documento electrónico firmado.

La firma digital no implica que el mensaje esté encriptado, es decir, que este no pueda ser leído por otras personas; al igual que cuando se firma un documento en forma manuscrita, este sí puede ser visualizado por otras personas. Tampoco impide que el mensaje sea alterado, no garantiza su inviolabilidad, pero sí da la certeza de que el contenido del mensaje es íntegro o no lo es: permite saber con exactitud si el mensaje es el mismo que fue emitido por el signatario o fue alterado en el camino.

En nuestro derecho positivo, una firma digital es aquella que se basa en certificados digitales emitidos por una autoridad certificante habilitada por la Autoridad de Aplicación de la Ley Nº 25.506.

El artículo 2 define como firma digital al "*resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma. Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.*"

La Ley otorga una fuerza probatoria superior a la firma digital respecto de la firma electrónica. Le asigna dos presunciones iuris tantum, es decir, que admiten prueba en contrario.

En efecto, el artículo 7º dispone que un documento firmado digitalmente goza de la presunción de autoría respecto de la persona titular del certificado digital, y por su parte, el artículo 8º establece la presunción de integridad del documento electrónico firmado digitalmente, es decir, que se presume que dicho documento no ha sido alterado.

Sin embargo, debe destacarse que la firma digital de un documento no impide que el mismo sea modificado. Simplemente asegura que, si el documento electrónico firmado digitalmente sufre alguna alteración, esta circunstancia queda en evidencia. Es por ello que el legislador le asigna una presunción de integridad. (RIVOLTA, 2008: 6)

Marco normativo de la firma digital en las provincias argentinas

Si bien la Ley Nº 25.506 es una ley de alcance federal, pues es complementaria del Código Civil, el último capítulo contiene disposiciones de aplicación administrativa. En efecto, el artículo 47 dispone que el Estado Nacional utilizará las tecnologías y previsiones de la ley en su ámbito interno y en relación con los administrados de acuerdo con las condiciones que se fijen reglamentariamente en cada uno de sus poderes.

Por su parte, el artículo siguiente otorga un plazo de 5 años para la implementación de acciones de gobierno electrónico en el Estado Nacional, dentro de las jurisdicciones y entidades comprendidas en el artículo 8º de la Ley Nº 24.156, promoviendo el uso masivo de la firma digital de tal forma que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a la progresiva despapelización de la Administración Nacional.

Ambos artículos marcaron el comienzo de la introducción por vía legal del gobierno electrónico en la Administración Nacional. Como se advierte, estas primeras disposiciones no son de carácter obligatorio para las jurisdicciones, ya que está sujeta a lo que se disponga reglamentariamente. Sin embargo, son relevantes ya que se trata de las primeras disposiciones de carácter legal referidas a gobierno electrónico. (RIVOLTA; 2008: 7)

Dado que la materia administrativa no ha sido delegada en el Congreso Nacional, las provincias conservan la potestad de regular su propio derecho administrativo, así como los códigos procesales civiles, comerciales, penales, etc. (BUGONI, 2007). En este sentido, y para favorecer la implementación de acciones de gobierno electrónico en todas las jurisdicciones, la misma Ley Nº 25.506 invita a las provincias a adherir a dicha norma. Debe destacarse que tal adhesión se refiere a las disposiciones de carácter administrativo, no a las del capítulo 1 que son de alcance federal pues tratan materias de derecho civil y comercial

Por su parte, el Decreto reglamentario de la Ley de firma digital, aprobado bajo el Nº 2628 en 2002, contiene algunas disposiciones relativas a la Administración Pública Nacional en su Capítulo X, las que podrían considerarse como embrionarias de gobierno electrónico. Según la Carta Iberoamericana de Gobierno Electrónico, el concepto de "gobierno electrónico" alude al uso de las TIC en los órganos de la Administración para mejorar la información y los servicios ofrecidos a los ciudadanos, orientar la eficacia y eficiencia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación de los ciudadanos. (CIGE; 2007: 7)

En efecto, el Decreto Nº 2628/02 dispone en el artículo 42, relativo a la presentación de documentos electrónicos, que los organismos de la Administración Pública Nacional deberán establecer mecanismos que garanticen la opción de remisión, recepción, mantenimiento y publicación de información electrónica, siempre que esto sea aplicable, tanto para la gestión de documentos entre organismos como para con los ciudadanos. Sin embargo, al no tener asociada una sanción para el caso de su no cumplimiento, esta disposición simplemente tiene efecto declarativo, sin que hasta la fecha se haya aplicado en forma sistemática.

Por otra parte, el artículo 43 se refiere a las normas para la elaboración y redacción de la documentación administrativa, y dispone la aplicación alternativa al Decreto Nº 333/85 y sus modificatorios, el cual establece las características de los escritos administrativos en soporte papel. Es decir, con este artículo, se dispone la equivalencia entre el documento electrónico administrativo y el documento administrativo tradicional.

A partir de la invitación de adhesión contenida en el artículo 50 de la Ley Nro. 25.506, numerosas provincias han sancionado leyes en consonancia. En ese marco, la Provincia de San Luis ha aprobado una Ley de Procedimientos Administrativos que admite el uso de medios electrónicos para su tramitación.

La Legislatura de Mendoza ha aprobado la Ley Provincial Nº 7234 que dispone la adhesión de la provincia a la Ley Nacional Nº 25.506 de Firma Digital. La Provincia de Santa Fe también adhirió a la ley nacional mediante la Ley Provincial Nº 12.491. La provincia de Buenos Aires ha adherido a la ley de firma digital mediante la Ley Provincial Nº 13.666, reglamentada por el Decreto Nº 1388 de julio del 2008. Asimismo, han adherido a la mencionada ley nacional las provincias de La Pampa (Ley Nº 2073), Tucumán (Ley Nº 7291), Tierra del Fuego (Ley Nº 633), Jujuy (Ley Nº 5425), Formosa (Ley Nº 1454) y Río Negro (Ley Nº 12.491). Más recientemente, han adherido la provincia de Neuquén (Ley Nº 2578) y el Gobierno de la Ciudad Autónoma de Buenos Aires (Ley Nº 2751). (RIVOLTA, 2008: 7)

V.- FACTORES ORGANIZACIONALES - ADMINISTRATIVOS DE LA INFRAESTRUCTURA DE FIRMA DIGITAL

Desde la perspectiva de la nueva gerencia pública, la incorporación de tecnología es una herramienta que facilita la incorporación de nuevos modos de hacer las cosas. Ayuda a transitar el recorrido desde una concepción tradicional burocrática a una concepción de gerencia pública moderna.

El Informe Gore propuso inventar *"... un gobierno que ponga a la gente en primer lugar"*, mediante la creación de un claro sentido de misión, tomando el timón más que los remos, delegando autoridad, sustituyendo normas y regulaciones por incentivos, formulando presupuestos basados en resultados, exponiendo las operaciones del gobierno a la competencia, buscando soluciones de mercado más que soluciones administrativas, y cuando ello fuese posible, midiendo el éxito de las acciones de gobierno en términos de satisfacción del usuario (GORE, 1993:7).

La reinvención del gobierno forma parte de una corriente de pensamiento y de acción de alcance global. Los reformadores de la nueva gerencia pública se encuentran en la mayoría, si no en todos los niveles de gobierno en naciones tan diversas como el Reino Unido, Suecia, Países Bajos, Canadá, Suiza, Alemania, Italia, Dinamarca, Finlandia, Estados Unidos, Argentina, Brasil, Singapur, Hong Kong, Japón, y tal vez los más conocidos, Nueva Zelanda y Australia.(JONES, 1999:1)

Según JONES, una guía efectiva para la innovación y el cambio organizacional podría estar dada por cinco "R", las cuales suministran un marco para la comprensión de los diversos conceptos que integran la Nueva Gerencia Pública: reestructuración, reingeniería, reinvención, realineación y reconceptualización.

En este sentido, hablar de gobierno electrónico no es solamente transformar los circuitos tradicionales en papel al nuevo soporte digital, sino realizar auténticos cambios que permitan acercar el Estado al ciudadano y gestionar mejor. Esto implica realizar una reingeniería de los procedimientos y flujos de trabajo organizacional, diseños de tareas, mecanismos y estructuras de control. Los que sean superfluos u obsoletos, deberán ser modificados y adecuados para brindar un mejor servicio. Los procesos de reingeniería, acompañados por la reestructuración, se proponen mejorar el desempeño administrativo.

Tal como lo explica Michael HAMMER: *"Es tiempo de dejar de pavimentar el camino de las vacas. En lugar de introducir procesos obsoletos en los sistemas computarizados, deberíamos discontinuarlos y empezar de nuevo. Deberíamos aplicar la reingeniería a nuestras organizaciones, utilizar el poder de la moderna tecnología de la información para rediseñar radicalmente nuestros... procedimientos, de modo de lograr mejoras dramáticas en su desempeño... No podemos lograr nuevos hitos en el desempeño sólo recortando el sobrante o automatizando los procedimientos existentes. Más bien debemos desafiar las premisas tradicionales y cambiar las viejas reglas"* (HAMMER, 1990: 104,107). (RIVOLTA; 2008: 12)

El presente capítulo identifica aquellos organismos de la Administración Nacional que cumplen roles relevantes en materia de firma digital, así como las competencias asignadas.

Organización Funcional de la Infraestructura de Firma Digital

Se han descripto en el capítulo tecnológico los componentes de una PKI: autoridades certificantes, autoridades de registro, usuarios, suscriptores de certificados. En el presente capítulo analizaremos las instituciones que cumplen esos roles en la Administración Nacional.

Las competencias asignadas por la Ley No. 25.506 de firma digital a la Autoridad de Aplicación, la Jefatura de Gabinete de Ministros, fueron concretadas a través de sucesivos decretos que aprobaron las estructuras orgánico-funcionales de dicha jurisdicción.

La Ley, con buen criterio, en ningún momento se refiere a la modalidad organizacional a ser utilizada. El Decreto N° 2628 de diciembre de 2002, reglamentario de la citada ley, creaba el "*Ente Administrador de Firma Digital, dependiente de la Jefatura de Gabinete de Ministros, como órgano técnico, administrativo encargado de otorgar las licencias a los certificadores y de supervisar su actividad, según las exigencias instituidas por el presente decreto y las normas reglamentarias, modificatorias o de aplicación que se dicten en el futuro y de 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.*" (artículo 11)

En los sucesivos artículos, definía las competencias del Ente Administrador, así como los recursos. En el artículo 15, referido a la organización del Ente, otorgaba un plazo de 60 días a partir de la constitución del Directorio, para elevar a consideración del Jefe de Gabinete de Ministros la propuesta de su estructura organizativa y de su reglamento de funcionamiento.

A partir de dicha norma, se nombraron dos directores, pero no se avanzó más en la organización del Ente. Como consecuencia, en noviembre de 2003 se disolvió el Ente Administrador mediante el Decreto N° 1028, y se transfirió a la Oficina Nacional de Tecnologías de Información – ONTI, dependiente de la Subsecretaría de la Gestión Pública, las competencias asignadas al Ente Administrador de Firma Digital.

Con esa medida, quedaron subsumidas las funciones de la Infraestructura de Firma Digital en la ONTI, pero sin que se modificara o adecuara la estructura previa de dicha Oficina Nacional.

Los sucesivos Decretos de estructura tanto de la Subsecretaría de Gestión Pública, como de las posteriores denominaciones como Secretaría de Gabinete y Gestión Pública y de Gestión Pública, y de la Subsecretaría de Tecnologías de

Gestión, creada a partir de diciembre de 2007, no resolvieron esta superposición de funciones y competencias.

En general, el problema que se presentó fue por un lado, la superposición de competencias entre estas tres áreas, por otra parte, dado que la propia ONTI administra una Autoridad Certificante para el Sector Público, el potencial conflicto de interés derivado de los múltiples roles que cumple la ONTI en la práctica.

Aparte de los aspectos formales, no hubo una readecuación funcional de las aperturas inferiores de la ONTI. Ello implicó que no se aumentara la planta de personal, aunque a través del Programa de Modernización del Estado, financiado con fondos del Banco Mundial, se contrataron consultores que realizan las actividades vinculadas a la firma digital.

Competencia de los organismos que ejercen el rol de Autoridad de Aplicación

El tema de firma digital involucra dos funciones principales:

1.- Ejercer el rol de Autoridad de Aplicación de la Infraestructura de Firma Digital de la República Argentina, lo cual implica:

- actuar como Ente Licenciante que emite licencias a los certificadores públicos y privados.
- Regular aspectos vinculados al uso del documento electrónico, la firma electrónica y la firma digital en el ámbito de la APN

2.- Administrar una Autoridad Certificante para la Administración Pública Nacional, emitiendo certificados digitales para funcionarios públicos a ser usados en aplicaciones de gobierno electrónico.

Ambas funciones históricamente han sido desempeñadas por la ONTI, pero en teoría no deberían ser ejercidas por el mismo ente, ya que podría dar lugar a un potencial conflicto de intereses. La ONTI ejerció ambas funciones en un esquema anterior, cuando aún no se había puesto en operación la Infraestructura de Firma Digital prevista por la Ley N° 25.506.

A partir del licenciamiento de las Autoridades Certificantes de AFIP y ANSES, es necesario delimitar claramente las incumbencias para darle a la Infraestructura de Firma Digital una organización que permita gestionar todos los aspectos en forma eficiente. Pero ello encuentra un obstáculo en la normativa de estructura, que asigna las mismas competencias a diferentes órganos, dado que no se han actualizado las aperturas inferiores que asignan funciones a las Direcciones Nacionales y Direcciones simples.

En efecto, si bien en virtud del Decreto N° 1266/08 se asigna la función de autoridad de aplicación de firma digital a la Secretaría de la Gestión Pública, con la

asistencia de la Subsecretaría de Tecnologías de Gestión, al mantenerse vigentes normas anteriores que habían atribuido similar competencia a la ONTI, se produce un solapamiento de funciones entre ellas.

Tal solapamiento podría resolverse mediante la vía interpretativa, aplicando el criterio que atribuye prevalencia a la norma posterior respecto de la previa en el tiempo. Sin embargo, dado que se trata de un tema sujeto a interpretación, sería más conveniente clarificar las competencias para poder así dar una organización acorde con las obligaciones impuestas.

En ese orden de ideas, la creación de la Subsecretaría de Tecnologías de Gestión necesariamente implica una redistribución de competencias, con lo cual se torna necesario analizar detalladamente cada una de las funciones involucradas para definir sus responsables y los recursos necesarios.

Análisis de actividades - Marco normativo

El régimen de firma digital se apoya en una serie de normas que se detallan a continuación:

- Ley N° 25.506 – Crea la Infraestructura de Firma Digital.
- Decreto N° 2628/02 – Reglamenta la Ley N° 25.506.
- Decreto N° 724/06 – Reglamenta la Ley N° 25.506.
- Decisión Administrativa N° 6/07 – Establece los procedimientos para la habilitación de entidades certificantes.
- Resolución Secretaría de Gestión Pública N° 63/07 – Aprueba la Política de Certificación de la Autoridad Certificante Raíz.
- Resolución Secretaría de Gestión Pública N° 64/07 – Establece los procedimientos operativos para la puesta en operación de la Autoridad Certificante Raíz.
- Resolución Secretaría de Gestión Pública N° 62/08 – Asigna a la ONTI la función de emitir el dictamen legal y técnico para el licenciamiento de certificadores, y a la Dirección de Aplicaciones la función de auditoría en dicho proceso.
- Resolución Secretaría de Gestión Pública N° 87/08 – Aprueba el Licenciamiento de la Autoridad Certificante de la ANSES.
- Resolución Secretaría de Gestión Pública N° 88/08 – Aprueba el Licenciamiento de la Autoridad Certificante de AFIP.

Actores previstos en la normativa sustantiva

Las normas sustantivas de firma digital prevén la actividad de las siguientes instancias (BUGONI, RIVOLTA; 2004: 82):

- Autoridad de Aplicación
- Comisión Asesora de Firma Digital
- Ente licenciante
- Entidades de Auditoría
- Certificadores licenciados
- Autoridad Certificante Raíz
- Normas para la despapelización del Estado
- Autoridad Certificante de la ONTI

Organismos involucrados

Por su parte, las normas de estructura, han creado los siguientes organismos a los cuales se les ha asignado funciones relativas a la firma digital, a saber:

- Jefatura de Gabinete de Ministros
- Secretaría de la Gestión Pública de la Jefatura de Gabinete de Ministros
- Subsecretaría de Tecnologías de Gestión de la Jefatura de Gabinete de Ministros
- Oficina Nacional de Tecnologías de Información
- Dirección de Aplicaciones de la ONTI
- Autoridades de Registro remotas: Poderes Judiciales, organismos APN, etc.

Análisis de capacidad institucional

Se han descripto las competencias relacionadas con la Infraestructura de Firma Digital y las unidades a las cuales se les han asignado. A partir de esta información, el análisis se apoyará en el concepto de capacidad de gestión estatal, utilizado en el sistema denominado SADCI – Sistema de Análisis de Capacidad Institucional. Esta metodología de análisis organizacional fue desarrollada por Alain Tobelem para el Banco Mundial y fue empleada en programas y proyectos con financiamiento multilateral con el propósito de prever qué problemas debían resolverse para garantizar su implementación exitosa. De esta metodología se han tomado exclusivamente aquellas causales que afectan la capacidad institucional que tienen relación con el presente trabajo. No se han considerado las causales que involucran variables que no han sido consideradas en la presente investigación, por ejemplo, las referidas a recursos humanos o financieros.

Capacidad estatal es la disponibilidad y aplicación efectiva de los recursos humanos, materiales y tecnológicos que posee el aparato administrativo y productivo del Estado para gestionar la producción de valor público, sorteando las restricciones, condicionamientos y amenazas de su contexto. La capacidad de gestión estatal se manifiesta en el grado en que las organizaciones estatales consiguen resolver las

cuestiones socialmente problematizadas que componen su agenda. (OSZLAK, 2005: 1)

El análisis de capacidad institucional permite contextualizar los factores que se han analizado en el presente trabajo, e intentar responder a la pregunta de investigación respecto de la identificación de algunos factores que estarían rezagando el uso masivo de la firma digital en Argentina, a 10 años de su vigencia.

El SADCI identifica seis causales que podrían afectar la capacidad institucional, a saber:

1. Déficit relacionados con leyes, reglas, normas y "reglas de juego".
2. Déficit relacionados con relaciones interinstitucionales.
3. Déficit relacionados con la estructura organizacional interna y distribución de funciones.
4. Déficit relacionados con la capacidad financiera y física de las agencias ejecutoras.
5. Déficit relacionados con políticas de personal y sistema de recompensas.
6. Déficit relacionados con la capacidad individual de los participantes en las agencias involucradas en el proyecto

De las causales que contempla el SADCI, sólo se utilizarán aquellas que se refieren a las variables analizadas. El presente trabajo no ha centrado su análisis en los recursos, tanto financieros como humanos. Por lo tanto, se aplicarán las tres primeras causales:

1.- Déficit relacionados con leyes, normas y, en general, "reglas de juego":

Esta categoría engloba los problemas que afectan la capacidad de las organizaciones vinculados con impedimentos establecidos en la normativa, tanto por su ausencia como por su imperio. Este déficit se refiere al marco jurídico de la organización, ya sea desde un punto de vista del derecho positivo vigente, el cual puede contener impedimentos o establecer competencias o procedimientos obsoletos, como a las lagunas del derecho que se manifiestan especialmente ante los avances tecnológicos. Dentro de esta categoría entran aquellos factores culturales o pautas de interacción socialmente aceptadas, que constituyen restricciones o condicionamientos para la ejecución de ciertas tareas en la organización.

Siguiendo a OSZLAK, "*en ocasiones estas trabas pueden comprometer la realización de tareas cruciales en la medida en que se ven afectadas por el marco en que se desenvolverán las acciones o las reglas que regirán la actividades de los actores, como en el caso de normas de congelamiento de vacantes que impiden la contratación de personal o subculturas renuentes a la incorporación de innovaciones tecnológicas.*" (OSZLAK, ORELLANA, 1999: 8).

2.- Déficit relacionados con relaciones interinstitucionales:

Esta causal se refiere a la interacción entre distintas organizaciones, situación que puede afectar el desarrollo de las actividades de la unidad de análisis. Dicha causal contempla tanto el caso de competencias superpuestas como de

colaboración interinstitucional. Esta variable intenta identificar los problemas que se derivan de la ausencia de apoyo por parte de otras organizaciones.

3.- Déficit relacionados con la estructura organizacional interna y distribución de funciones:

Esta causal considera que la estructura organizacional interna es un elemento central debido a que establece qué unidades organizativas son responsables de qué actividades para el cumplimiento de los objetivos de la organización. Esta causal intenta identificar los problemas que se derivan de la multiplicidad de áreas intervinientes, o bien de la inexistencia de una definición clara de asignación de responsabilidades. Analiza la distribución de funciones en el plano intra organizacional, incluyendo el grado de formalidad de las distintas áreas operativas dedicadas a las actividades, si el área está contemplada en la estructura funcional, si tiene asignados recursos, etc, intentando reflejar la situación organizativa. (OSZLACK, ORELLANA, 1999: 8)

Déficit de capacidad institucional de la Infraestructura de Firma Digital

1.- Déficit relacionados con las reglas de juego:

El momento político posterior a la sanción de la Ley N° 25.506, cuando se inició el proceso de reglamentación, coincidió con la crisis institucional del país (fines de 2001).

El trámite del Decreto reglamentario, iniciado durante el gobierno de la Alianza, duró hasta diciembre de 2002. El Decreto N° 2628/02 adoptó el criterio de habilitar a la Autoridad de Aplicación a dictar las normas técnicas, a fin de facilitar su actualización permanente. El Decreto no agotaba los aspectos regulatorios vinculados con la firma digital, establecía que la Autoridad de Aplicación debía definir el esquema de licenciamiento, el organismo responsable, designar el personal y las autoridades, aprobar los procedimientos y las normas de auditoría. Esta tarea fue avanzando lentamente, encontrándose hasta la fecha inconclusa.

Recién en el año 2007 se aprobaron las normas técnicas de la Infraestructura de Firma Digital, mediante la Decisión Administrativa N° 6. Seis años después de sancionada la Ley, cinco años después de aprobado su Decreto reglamentario. Estas demoras en la regulación o quizá con mayor propiedad, esta regulación inconclusa[10], constituye un déficit de capacidad institucional.

Quizá podríamos decir que es consecuencia de la principal brecha de capacidad institucional que está dada por la ausencia de un ente específico competente en materia de firma digital. Pero indudablemente, la regulación inconclusa constituye un problema en sí mismo. Este problema afecta notablemente a otras áreas de la administración. En efecto, dado que no se han regulado los aspectos relativos al documento electrónico, por ejemplo, en relación con la

[10] Regulación inconclusa porque aún no se han aprobado diversas normas previstas en la Ley: el sistema de auditoría, los estándares de conservación, etc.

conservación documental, no es posible prescindir por el momento del expediente en papel.

Este déficit de capacidad institucional vinculado con la regulación inconclusa afecta a las políticas de gobierno electrónico. Inclusive, a la propia ley de firma digital en el capítulo referido a la administración nacional, impidiendo el cumplimiento de lo dispuesto por el artículo 48. Dicho artículo establece que el Estado nacional promoverá el uso masivo de la firma digital de tal forma que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a la progresiva despapelización. Fija un plazo máximo de 5 (cinco) años para la aplicación de tecnología de firma digital a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanados de las jurisdicciones y entidades comprendidas en el artículo 8° de la Ley N° 24.156. Dicho plazo se cumplió en diciembre del año 2007.

2.- Déficit relativos a las relaciones interinstitucionales:

Los organismos involucrados en la regulación y el control de los componentes de la Infraestructura de Firma Digital acusan un déficit significativo de capacidad institucional, fundamentalmente en el proceso de configuración del organismo con competencia específica en la materia. El Ente Administrador de Firma Digital, creado mediante el Decreto N° 2628/02, nunca llegó a tener existencia real, a pesar de haber sido designados dos de los tres directores. Nunca llegó a constituirse como tal, ni a tener oficinas o recursos asignados.

A partir de mayo del año 2003, las funciones del Ente Administrador de Firma Digital fueron asignadas a la entonces Subsecretaría de la Gestión Pública, pero al poco tiempo, en noviembre, por otro Decreto, el N° 1028/03, por el cual se disolvió dicho Ente Administrador, regresó sus competencias a la Oficina Nacional de Tecnologías de Información, dependiente de la mencionada Subsecretaría. Esta superposición se ve agravada ya que al mantenerse vigentes las aperturas inferiores anteriores al 2001, que determinan las competencias de las Direcciones simples que integran la ONTI, esto genera una falta de claridad respecto de la responsabilidad para la ejecución de cada una de las acciones.

Esta situación genera, además, un potencial conflicto de intereses pues la ONTI a su vez, administra una Autoridad Certificante para el Sector Público Nacional. Sumado a ello, a partir del año 2007, con la creación de la Subsecretaría de Tecnologías de Gestión dependiente de la Secretaría de la Gestión Pública, se incorpora otro actor al juego de las competencias en firma digital.

3.- Déficit vinculados con los esquemas organizativos y de asignación de funciones:

La regulación inconclusa, sumada a la disolución del Ente Administrador de Firma Digital nunca formado, y a la distribución difusa y superpuesta de

competencias entre distintas áreas de gobierno, en ningún caso dedicadas en forma exclusiva al tema, generaron un déficit organizativo y de distribución de funciones.

Las funciones originalmente asignadas al Ente Administrador de Firma Digital relativas al ejercicio de la regulación administrativa y técnica, de control, fiscalización y licenciamiento de certificadores de firma digital, fueron asignadas en forma superpuesta a distintas áreas: a la Secretaría de la Gestión Pública, a la Subsecretaría de Tecnologías de Gestión, a la ONTI, a la Dirección de Aplicaciones de la ONTI. Como consecuencia, se observa una dispersión de funciones, lo cual sumado a que dichas áreas son responsables de otros temas de igual relevancia, que por ser más urgentes requieren atención más inmediata, ha generado un déficit organizativo importante.

En efecto, al no tener claramente definidas las responsabilidades, ningún área asume como propia la misión de administrar la Infraestructura de Firma Digital. Por el contrario, van cubriendo de manera parcial, los aspectos que surgen como importantes, a medida que se presentan. No ha habido un plan estratégico que señale el rumbo a seguir.

Dicho déficit también fue señalado por la Auditoría General de la Nación en el año 2008, con ocasión de la auditoría realizada a la Infraestructura de Firma Digital. En dicho Informe, respecto a la Organización, la AGN señala que *"las tareas relativas a Firma Digital se desarrollan en el marco del préstamo BIRF 4423-AR como subactividad de Gobierno Electrónico o Digital. La subactividad cuenta con un Coordinador que reporte tanto al responsable técnico del BIRF como a la Directora de Aplicaciones de la ONTI. Tiene a su cargo las áreas no formales Técnica y Licenciamiento. Los responsables son personal contratado por el préstamo. El área Técnica gestiona los certificados digitales para la APN. Concluyendo, la actividad no dispone ni de responsables formales en sus niveles técnicos ni de una organización formal para desempeñarla. También se considera crítico el escaso número de personas con dominio de las tecnologías de encriptación y de sistemas de gestión de Firma Digital."* (AGN, 2008: 55)

En cuanto a los efectos derivados de estos problemas, la AGN advierte *"Estaría en riesgo el soporte técnico a esta actividad, dado que el mercado laboral ofrece mejores condiciones que las pautadas para el personal contratado en el marco del Decreto N° 1184/2."* Sobre los aspectos organizacionales, la Auditoría General de la Nación considera que *"La inexistencia de una estructura formal no permite contar con una organización que pueda cumplir con las altas exigencias de administrar la tecnología de Firma Digital con adecuados estándares de calidad y seguridad."* (AGN, 2008: 55)

En dicho Informe, la AGN también analiza el rol de autoridad de aplicación del régimen de firma digital. Sobre el mismo, la AGN opina que *"La SGP, Autoridad de Aplicación de la Firma Digital, delega en la ONTI las principales funciones técnicas en la materia. La ONTI asume el rol de soporte con servicios de consultoría y asistencia con relación a la s implementaciones en el sector público. Sin embargo, no se ha detectado una actitud rectora para cohesionar en este aspecto a la APN; por ejemplo, no existe normativa para la gestión de técnicas de encriptación y de Firma Digital en las aplicaciones críticas de la APN que las requieren, ni*

procedimientos de control en la administración de claves." En cuanto a los efectos de esta debilidad en el rol de autoridad de aplicación, la AGN advierte que "No contribuye a expandir con mayor celeridad la implementación" de la Infraestructura de Firma Digital. (AGN, 2008: 66)

4.- Déficit ocasionados por la inexistencia o insuficiencia de recursos materiales y humanos:

Aunque el presente trabajo no ha profundizado en los aspectos financieros de la Infraestructura de Firma Digital, pero sí se ha mencionado que las funciones asignadas a la ONTI, la Subsecretaría de Tecnologías de Gestión y la Secretaría de la Gestión Pública, no fueron acompañadas por un refuerzo presupuestal ni tampoco con la adecuación de las aperturas inferiores. Vacantes congeladas, una estructura previa a la sanción de la ley de firma digital, y competencias múltiples, generaron un déficit de recursos materiales y humanos que fue paliado parcialmente por el Proyecto de Modernización del Estado financiado por el Banco Mundial.

Sin embargo, la pérdida de valor de los salarios sumado a la precariedad de los contratos, afectó el desenvolvimiento de la Infraestructura de Firma Digital ya que los técnicos informáticos más calificados se desvincularon de la ONTI. Si bien la Ley y su Decreto reglamentario prevén la posibilidad de cobrar aranceles para operar la Infraestructura de Firma Digital, dicha alternativa no fue aprovechada, debido a la disolución del Ente Administrador, por una parte, y a que los servicios por los cuales se le facultaba cobrar no fueron desarrollados (homologación de software, por ejemplo).

VI.- PERCEPCIONES DE LOS EXPERTOS SOBRE LOS OBSTACULOS PARA EL DESARROLLO DE LA FIRMA DIGITAL

Para la presente investigación, se administró una encuesta a expertos, la cual fue elaborada en base a otra encuesta internacional realizada en 2003 por OASIS. Como parte del trabajo de tesis, en diciembre de 2008 se elaboró una versión del formulario de la encuesta, la cual fue testeada en enero de 2009. En base a los comentarios recibidos, se preparó la versión final del formulario de la encuesta en español, y su correspondiente versión en inglés. También de creó un sitio en Internet en el cual se publicaron ambos formularios, de modo de poder ser accedidos por aquellas personas a las cuales no se les hizo llegar directamente el formulario.

La estrategia de distribución del formulario se apoyó en el uso de Internet. Por un lado, a través del sitio https://sites.google.com/site/mercedesrivolta/, creado especialmente al efecto, en el cual se publicaron los formularios en español e inglés, con una breve descripción del proyecto. Por otra parte, se envió por correo electrónico a todos los referentes en la materia.

El formulario de la encuesta de la investigación se distribuyó por correo electrónico y por la web a partir del 9 de marzo de 2009. Se seleccionaron aquellos grupos referidos a la temática en redes sociales (Facebook y Linkedin). En ese caso, se invitó a completar la encuesta a las siguientes personas:

- Miembros del Cuerpo de Administradores Gubernamentales (20 miembros)
- Miembros de ISOC-Ar, Capitulo Argentino de Internet Society (50 miembros)
- Miembros del Grupo ASI – Agencia de Sistemas de Información de Facebook (17 miembros)
- Miembros del Grupo PKI Public Key Infrastructure de Facebook (117 miembros)
- Miembros del Grupo e-government de Facebook (117 miembros)
- Miembros del Grupo Center for Information Policy and e.-government, de Facebook, University of Maryland – USA (40 miembros)
- Miembros del Grupo e.governemnt for the citizens, de Facebook (87 miembros)
- Miembros del Grupo e-government de Facebook (87 miembros) (académico)
- Miembros del Grupo Gobierno electrónico OEA, de Facebook (45 miembros)
- Miembros del Grupo e-government Argentina de Linkedin (69 miembros)

Complementariamente, para asegurar la obtención de respuestas que abonaran la investigación, se remitió el formulario de la encuesta a las direcciones de mail de reconocidos expertos en el tema, en un total de 60 personas.

Resultados de la Encuesta

Se recibieron 70 respuestas de expertos nacionales y extranjeros. Se recibieron respuestas de Costa Rica, Banco Mundial DC, Australia, Paraguay, Uruguay. Se recibieron respuestas provenientes de expertos de poderes judiciales provinciales (Chubut, Córdoba) y de Capital Federal. Participó el personal de la Infraestructura de Firma Digital de la República Argentina, también el Diputado autor de la ley de firma digital, Lic. Pablo Fontdevila. Pocos participantes del sector privado, pues no se puso énfasis en su distribución en las cámaras del sector. Como Anexo III se adjunta el listado de expertos que completaron la encuesta.

Las encuestas fueron respondidas en su totalidad, salvo las correspondientes a expertos extranjeros que no respondieron el capítulo referido a Argentina. Disponer de formularios en español e inglés fue de gran ayuda para ampliar la muestra.

La primera parte de la encuesta identifica el perfil del encuestado.

La segunda parte, identifica la visión y opinión del encuestado sobre la aplicación de firma digital y los problemas que surgen.

La tercera parte se refiere a la identificación de los factores que pudieran estar rezagando la masificación del uso de la firma digital en Argentina. Este último capítulo es opcional, ya que los expertos extranjeros pueden optar por no contestar.

Por otra parte, esta encuesta reproduce en las dos primeras partes, una encuesta realizada en 2003 a nivel internacional por OASIS, lo cual ha permitido comparar resultados entre aquella encuesta y la que forma parte de la investigación.

Análisis de Resultados

SECCION I – PERFIL DE LA MUESTRA

A.- OCUPACION PRINCIPAL

El perfil profesional vinculado con TIC alcanza el 44%.

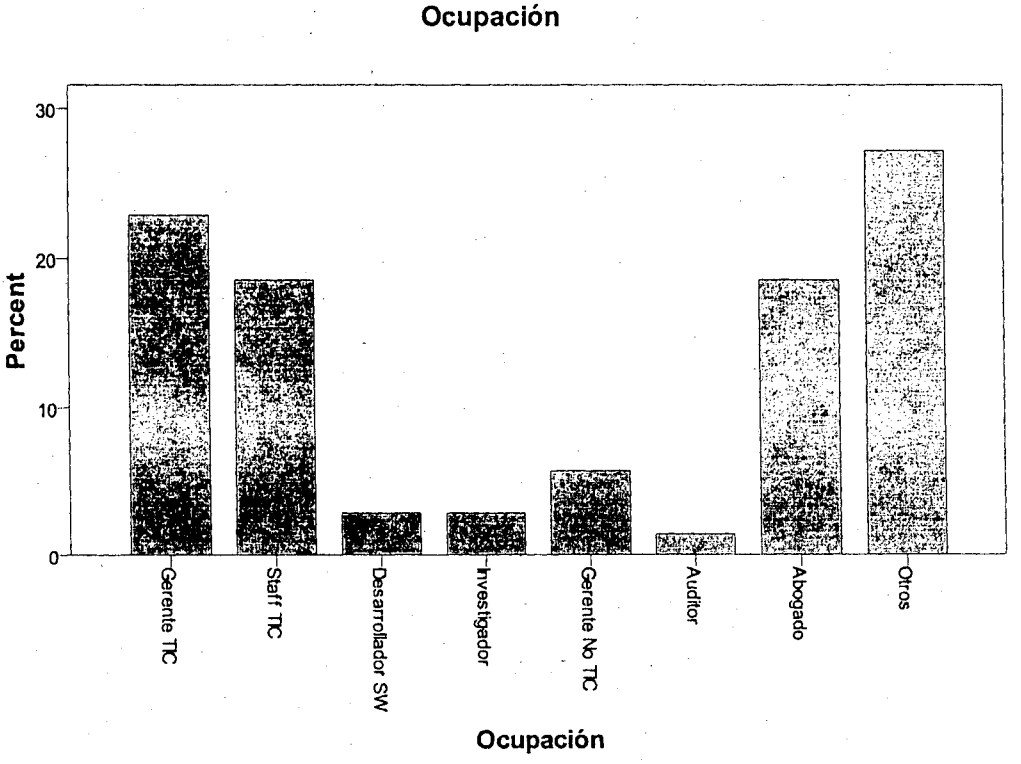
Las ocupaciones principales de los encuestados fueron las de Gerente TIC (22,9%) y en segundo lugar, los abogados y personal de staff TIC, con igual porcentaje (18,6%). Sin embargo, el rubro más amplio fue el de Otros (27,1%), en el cual se incluyen los funcionarios de organismos multilaterales por ejemplo. Los profesionales de auditoría representaron el mínimo de la encuesta (1,4%).

Cuadro de Resultados Encuesta Nº 1: Ocupación

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Gerente TIC	16	22.9	22.9	22.9
	Staff TIC	13	18.6	18.6	41.4
	Desarrollador SW	2	2.9	2.9	44.3
	Investigador	2	2.9	2.9	47.1
	Gerente No TIC	4	5.7	5.7	52.9
	Auditor	1	1.4	1.4	54.3
	Abogado	13	18.6	18.6	72.9
	Otros	19	27.1	27.1	100.0
	Total	70	100.0	100.0	

Fuente: Elaboración propia en base a encuesta a expertos

Gráfico de Resultados Encuesta Nº 1: Ocupación



Fuente: Elaboración propia en base a encuesta a expertos

Comparación con la Encuesta OASIS (2003): el principal perfil profesional mayoritario fue aquel vinculado con TIC; 44% (similar encuesta argentina). (DOYLE, HANNA, 2003: 4)

B.- ANTIGUEDAD EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

Respecto de la experiencia los temas de seguridad y privacidad de la información, el 80% de los encuestados cuenta con más de 5 años de experiencia en el tema.

Cuadro de Resultados Encuesta Nº 2: Antigüedad

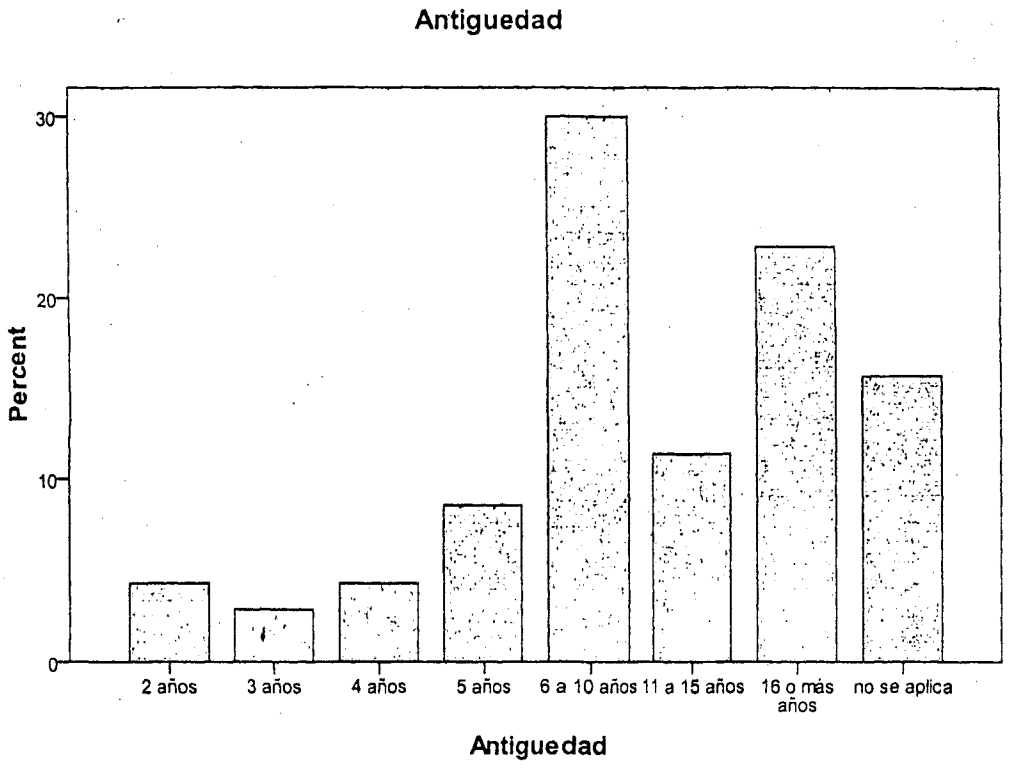
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2 años	3	4.3	4.3	4.3
	3 años	2	2.9	2.9	7.1
	4 años	3	4.3	4.3	11.4
	5 años	6	8.6	8.6	20.0
	6 a 10 años	21	30.0	30.0	50.0
	11 a 15 años	8	11.4	11.4	61.4
	16 o más años	16	22.9	22.9	84.3
	no se aplica	11	15.7	15.7	100.0
	Total	70	100.0	100.0	

Fuente: Elaboración propia en base a encuesta a expertos

El principal grupo fue el de 6 a 10 años de antigüedad (30%), coincidentemente con el surgimiento de la temática en forma masiva a nivel internacional (1999 a 2003) y en lo nacional, con el primer proyecto de Ley presentado en el Congreso (1999) y la aprobación del Decreto No. 2628 de diciembre de 2002, reglamentario de la Ley No. 25.506. El segmento de menor participación fue el correspondiente a una antigüedad de 3 años (2,9%).

Si se considera la antigüedad de los participantes a partir de los 6 años o más, el total asciende al 64,3% del total de la muestra, con lo cual se puede afirmar que la misma es representativa al menos en lo que hace a experiencia en los temas de seguridad y privacidad de la información.

Gráfico de Resultados Encuesta Nº 2: Antigüedad



Fuente: Elaboración propia en base a encuesta a expertos

En la encuesta OASIS 2003, el 75% superaba los 5 años de antigüedad en el tema. (DOYLE, HANNA, 2003: 5)

C.- EXPERIENCIA EN PKI

De las encuestas, el segmento mayoritario ha sido el de aquellos que han desarrollado software de PKI (57,1%), junto con el segmento que ha usado PKI (57,1%). El de menor relevancia en cuanto a experiencia con PKI ha sido el segmento de los que han considerado utilizar PKI (31,4%), lo cual implica que el 68,6% no ha considerado su uso. En cuanto a los que tienen una experiencia apoyada en la lectura, asciende al 55,7%. Estos resultados nos dan cuenta de la representatividad de la muestra en cuanto a su relación con la temática PKI.

- Ha leído sobre PKI: 55,7%
- Ha considerado utilizar PKI: 31,4%
- Ha usado PKI: 57,1%
- Ha ayudado a desarrollar PKI: 41,4%
- Ha desarrollado software vinculado a PKI : 57,1%

La encuesta OASIS 2003 fue respondida por un 90% de expertos con experiencia en el desarrollo de PKI. (DOYLE, HANNA, 2003: 6)

D.- SECTOR O INDUSTRIA DEL EMPLEADOR

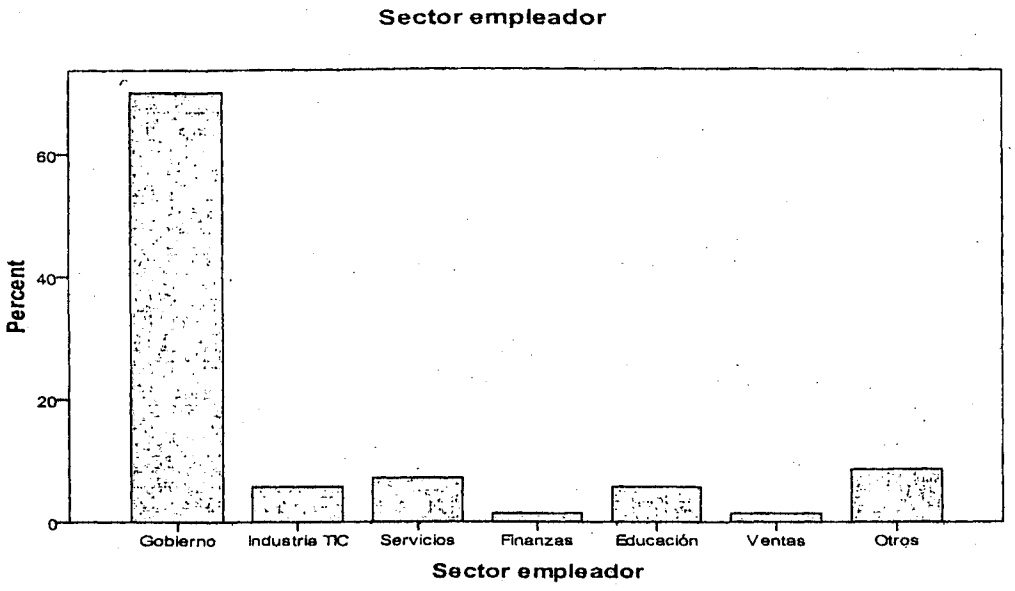
La encuesta fue respondida mayoritariamente por personas pertenecientes al sector público (70%), seguido por el sector servicios (7,1%) y los de Educación e Industria TIC (5,7% cada uno), siendo los de menor representatividad los sectores de Finanzas y Ventas (1,4% cada uno).

Cuadro de Resultados Encuesta Nº 3: Sector Empleador

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Gobierno	49	70.0	70.0	70.0
	Industria TIC	4	5.7	5.7	75.7
	Servicios	5	7.1	7.1	82.9
	Finanzas	1	1.4	1.4	84.3
	Educación	4	5.7	5.7	90.0
	Ventas	1	1.4	1.4	91.4
	Otros	6	8.6	8.6	100.0
	Total	70	100.0	100.0	

Fuente: Elaboración propia en base a encuesta a expertos

Gráfico de Resultados Encuesta Nº 3: Sector Empleador



Fuente: Elaboración propia en base a encuesta a expertos

Este ítem muestra resultados significativamente diferentes con la encuesta OASIS 2003, en la cual, el 30% de los encuestados pertenecía al sector gobierno, mientras que el 28% provenían del sector industria TICs. (DOYLE, HANNA, 2003: 6)

E.- TAMAÑO DEL EMPLEADOR (cantidad de empleados)

Con respecto a esta variable, los resultados no son demasiado confiables pues se tomaron distintos criterios para la selección del tamaño del empleador en aquellos casos de pertenencia a organismos del Estado. Algunos encuestados contestaron tomando como base la cantidad de personas en sus unidades, otros hicieron lo propio en relación a la administración como conjunto.

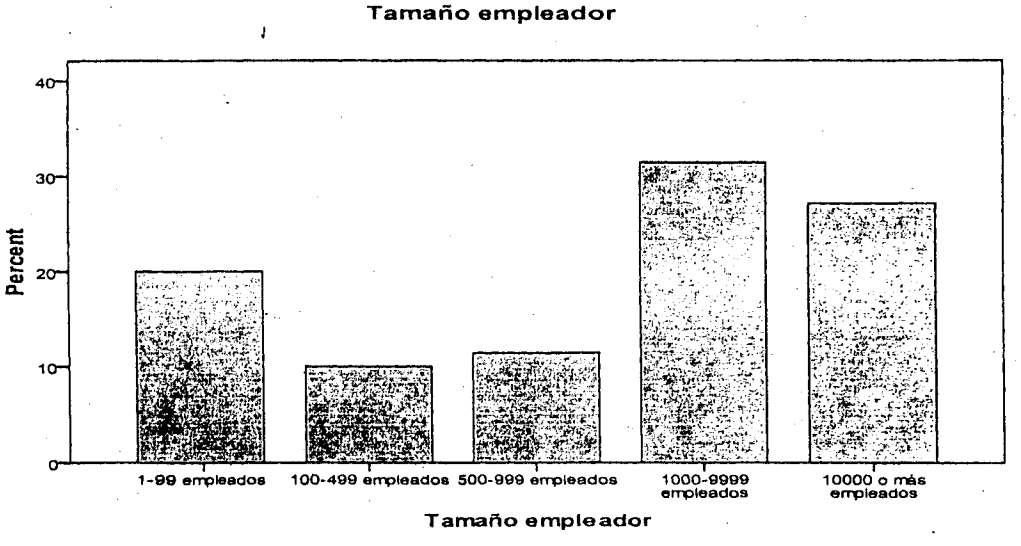
El 58% de encuestados pertenece a organizaciones de más de 1000 empleados.

Cuadro de Resultados Encuesta Nº 4: Tamaño Empleador

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-99 empleados	14	20.0	20.0	20.0
	100-499 empleados	7	10.0	10.0	30.0
	500-999 empleados	8	11.4	11.4	41.4
	1000-9999 empleados	22	31.4	31.4	72.9
	10000 o más empleados	19	27.1	27.1	100.0
	Total	70	100.0	100.0	

Fuente: Elaboración propia en base a encuesta a expertos

Gráfico de Resultados Encuesta Nº 4: Tamaño Empleador



Fuente: Elaboración propia en base a encuesta a expertos

La encuesta OASIS 2003 muestra un resultado similar: alrededor del 60% pertenece a organizaciones de más de 1000 empleados. (DOYLE, HANNA, 2003: 8)

F.- REGION DE TRABAJO PRINCIPAL

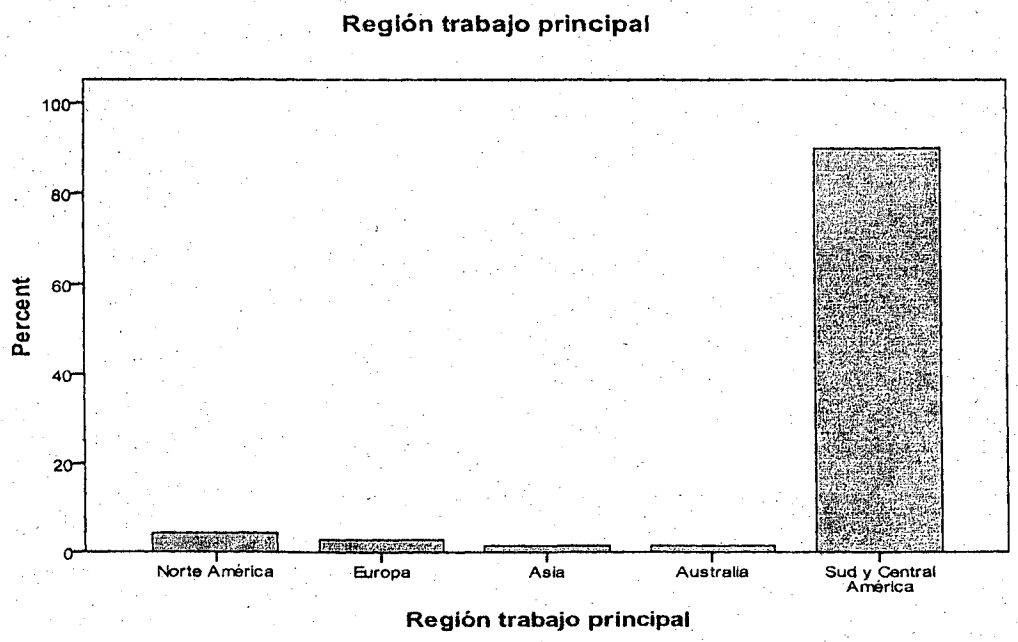
El 90% de los participantes de la encuesta pertenecen a América del Sur o Central, apenas el 4,3% a América del Norte, un 2,9% a Europa, y el 1,4% a Australia y Asia, respectivamente. Lo interesante de la encuesta es que ha logrado respuestas en varios continentes.

Cuadro de Resultados Encuesta Nº 5: Región de Trabajo Principal

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Norte América	3	4.3	4.3	4.3
	Europa	2	2.9	2.9	7.1
	Asia	1	1.4	1.4	8.6
	Australia	1	1.4	1.4	10.0
	Sud y Central América	63	90.0	90.0	100.0
	Total	70	100.0	100.0	

Fuente: Elaboración propia en base a encuesta a expertos

Gráfico de Resultados Encuesta Nº 5: Región de Trabajo Principal



Fuente: Elaboración propia en base a encuesta a expertos

La encuesta de OASIS 2003 obviamente tiene un perfil geográfico diferente: el 60% de los encuestados pertenece a América del Norte. (DOYLE, HANNA, 2003: 7)

G.- ALCANCES DE SU INTERES POR PKI

El segmento de quienes poseen un interés en PKI que excede a su propio país es el principal (41,4%), seguido del grupo cuyo interés excede su propia

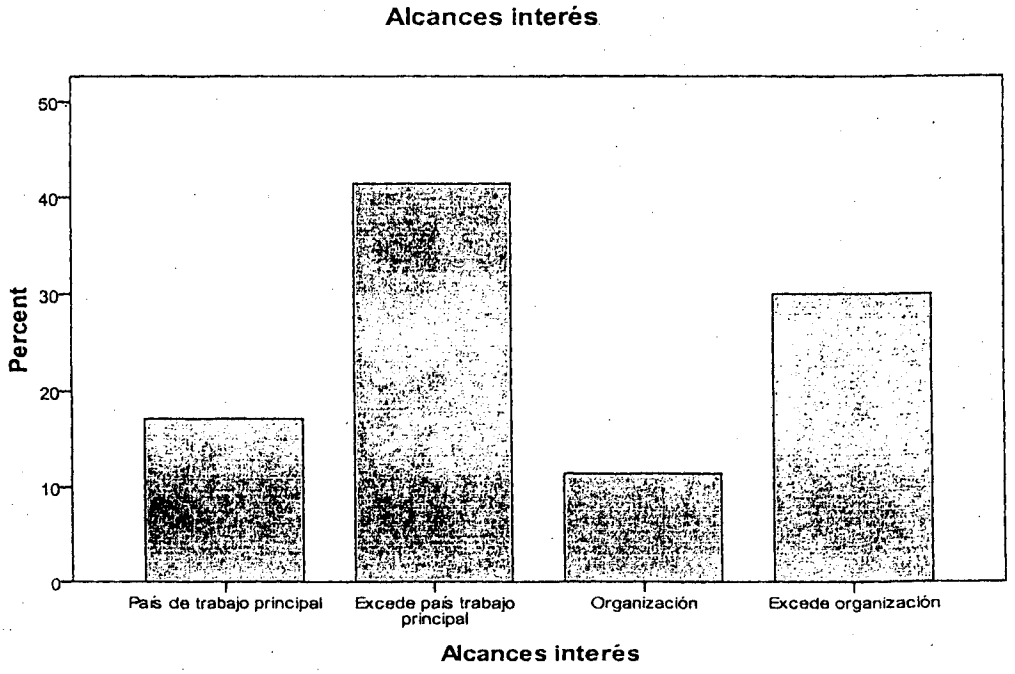
organización (30%). El segmento menos representativo es aquel que manifiesta un interés limitado a su organización (11,4%).

Cuadro de Resultados Encuesta Nº 6: Alcances Interés

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	País de trabajo principal	12	17.1	17.1	17.1
	Excede país trabajo principal	29	41.4	41.4	58.6
	Organización	8	11.4	11.4	70.0
	Excede organización	21	30.0	30.0	100.0
	Total	70	100.0	100.0	

Fuente: Elaboración propia en base a encuesta a expertos

Gráfico de Resultados Encuesta Nº 6: Alcances Interés



Fuente: Elaboración propia en base a encuesta a expertos

La encuesta OASIS 2003 muestra que una sustancial mayoría de los participantes tienen un interés que se extiende más allá de su país de trabajo (77%), mientras que un 84% expresó que su interés excede su propia organización. (DOYLE, HANNA, 2003: 8)

SECCION II.- VISION Y OPINIONES

Los encuestados respondieron voluntariamente, con lo cual probablemente no sean representativos de todos los invitados a participar de la encuesta, ni mucho menos, del público en general, ya que la muestra se obtuvo de grupos de expertos. Esto implica que los encuestados poseen un alto nivel de experiencia y conocimientos sobre el tema. Son profesionales que han estudiado y utilizan la herramienta de alguna manera. El perfil de la muestra de OASIS 2003 es similar. (DOYLE, HANNA, 2003: 8)

A.- APLICACIONES PKI

Los participantes de la encuesta fueron invitados a considerar diversas aplicaciones según su orden de importancia (Más importante, Importante y No importante) Tuvieron la opción de agregar otras aplicaciones y su grado de relevancia.

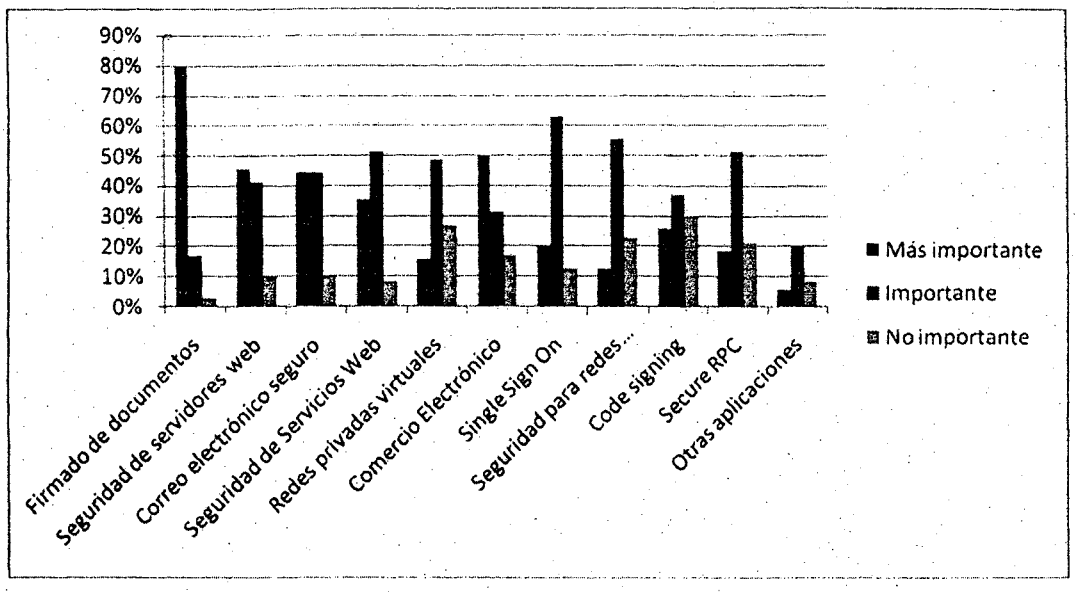
En cuanto a las aplicaciones de la firma digital, un 80% de encuestados afirmó como la más importante la de firmado de documentos, seguida de la aplicación para comercio electrónico (50%) y la de seguridad de servidores web (45.7%). Dentro de la categoría de importantes, se mencionó en primer lugar el single sign on (62,9%) seguido de la seguridad para redes inalámbricas (55,7%), la seguridad de servicios web (51,4%), y las redes privadas virtuales (48,6%).

Cuadro de Resultados Encuesta Nº 7: Aplicaciones PKI

Aplicaciones	Más importante	Importante	No importante
Firmado de documentos	80%	17,1%	2,9%
Seguridad de servidores web	45,7%	41,4%	10%
Correo electrónico seguro	44,3%	44,3%	10%
Seguridad de Servicios Web	35,7%	51,4%	8,6%
Redes privadas virtuales	15,7%	48,6%	27,1%
Comercio Electrónico	50%	31,4%	17,1%
Single Sign On	20%	62,9%	12,9%
Seguridad para redes inalámbricas LAN	12,9%	55,7%	22,9%
Code signing	25,7%	37,1%	30%
Secure RPC	18,6%	51,4%	21,4%
Otras aplicaciones	5,7%	20%	8,6%

Fuente: Elaboración propia en base a encuesta a expertos

Gráfico de Resultados Encuesta Nº 7: Aplicaciones PKI



Fuente: Elaboración propia en base a encuesta a expertos

En la encuesta OASIS 2003, todas las aplicaciones, excepto Secure RPC, fueron consideradas como importantes al menos, por más del 50% de los encuestados. Fue común que los participantes señalaran varias aplicaciones importantes, pero, a diferencia de la encuesta argentina, ninguna fue considerada como la más importante por la mayoría. Esto indica que PKI es verdaderamente una tecnología horizontal que permite varias aplicaciones. (DOYLE, HANNA, 2003: 11)

B.- OBSTACULOS PARA EL DESARROLLO Y USO DE PKI

Se presentó a los encuestados una lista de posibles obstáculos para su consideración según el orden de importancia (Obstáculo Máximo, Obstáculo Mínimo, No es un Obstáculo). Se permitió a los encuestados agregar obstáculos en "Otros".

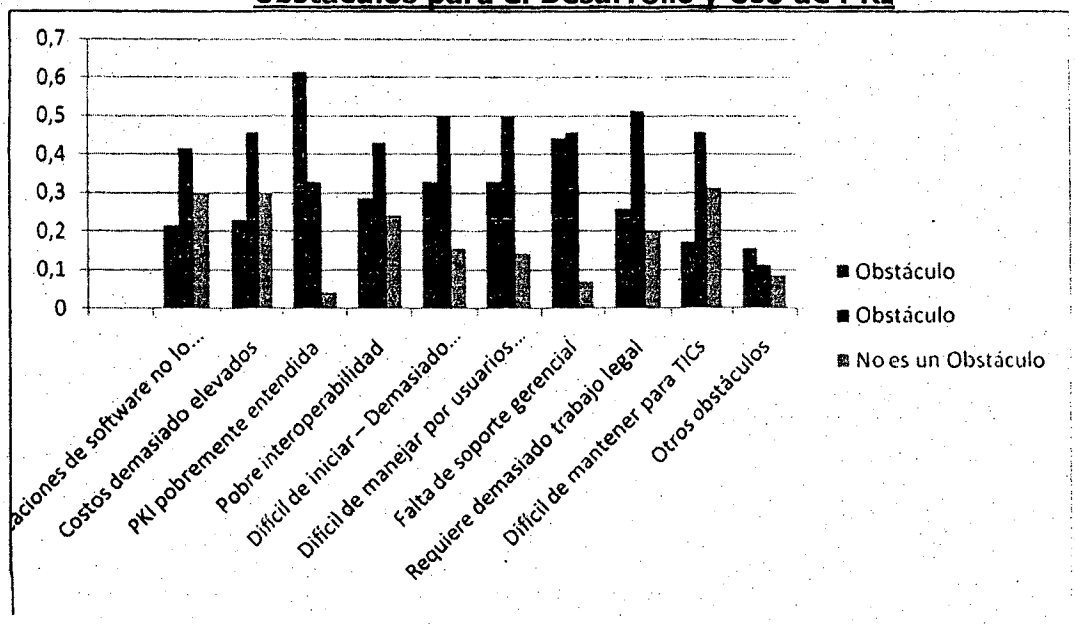
En términos generales, los resultados mostraron que el principal obstáculo es que la dificultad de ser entendida la temática de la firma digital (61,4%). El otro obstáculo máximo identificado por los expertos fue la falta de soporte gerencial (44,3%). Como obstáculos mínimos se identificaron primero el abundante trabajo legal requerido (51,4%) seguido de la complejidad y la dificultad de uso por los usuarios finales (50% cada una). Ninguna de las variables identificadas fue considerada mayoritariamente como que no constituye un obstáculo.

Cuadro de Resultados Encuesta Nº 8: Obstáculos para el Desarrollo y Uso de PKI

Obstáculo	Obstáculo Máximo	Obstáculo Mínimo	No es un Obstáculo
Las aplicaciones de software no lo soportan	21,4%	41,4%	30%
Costos demasiado elevados	22,9%	45,7%	30%
PKI pobremente entendida	61,4%	32,9%	4,3%
Pobre interoperabilidad	28,6%	42,9%	24,3%
Difícil de iniciar – Demasiado compleja	32,9%	50%	15,7%
Difícil de manejar por usuarios finales	32,9%	50%	14,3%
Falta de soporte gerencial	44,3%	45,7%	7,1%
Requiere demasiado trabajo legal	25,7%	51,4%	20%
Difícil de mantener para TICs	17,1%	45,7%	31,4%
Otros obstáculos	15,7%	11,4%	8,6%

Fuente: Elaboración propia en base a encuesta a expertos

Gráfico de Resultados Encuesta Nº 8: Obstáculos para el Desarrollo y Uso de PKI



Fuente: Elaboración propia en base a encuesta a expertos

Los 5 principales obstáculos identificados por los encuestados fueron:

1.- PKI pobremente entendida (61%)
2.- Falta de soporte gerencial (44,3%)
3.- Difícil de iniciar - demasiado compleja (32,9%)
4.- Difícil de manejar por usuarios finales (32,9%)
5.- Pobre interoperabilidad (28,2%)

Estos resultados difieren de los de la Encuesta OASIS 2003 (DOYLE, HANNA, 2003: 12), que identificaba los siguientes obstáculos principales:

1.- Aplicaciones de Software no lo soportan (54%)
2.- Costos demasiado altos (53%)
3.- PKI pobremente entendida (47%)
4.- Pobre interoperabilidad (46%)
5.- Difícil de iniciar- demasiado compleja (46%)

SECCION III.- MOTIVOS DEL ESCASO USO MASIVO DE LA FIRMA DIGITAL EN ARGENTINA

La encuesta desarrollada para esta investigación, agrega al modelo de OASIS 2003, una sección específica aplicable a la PKI argentina. Respecto de los factores que explican el escaso uso masivo de la firma digital en Argentina, los resultados muestran que los expertos perciben que la inmadurez del mercado (64,3%) y la escasa difusión (61,4%) son los que poseen mayor incidencia, seguido de las escasas aplicaciones (50%). Por su parte, la insuficiente conectividad (55,7%) y la inmadurez de los estándares tecnológicos son los factores que son percibidos como de mínima incidencia, seguido por los del ente rector no exclusivo (41,4%) y la inadecuada normativa (40%).

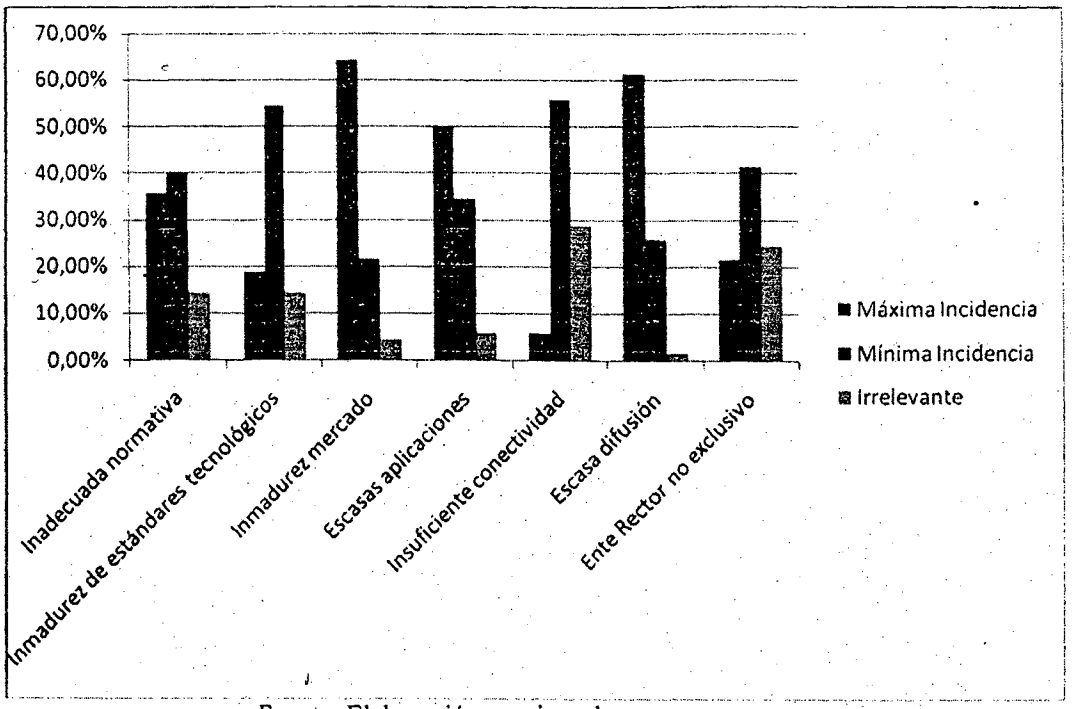
En síntesis, los expertos explican el escaso uso de la firma digital en Argentina más como un problema del mercado y de la pobre difusión, seguido de un problema estructural referido tanto a la inmadurez de los estándares, como a lo institucional (normas y ente rector). Ninguno de los factores de la encuesta fue mayoritariamente considerado irrelevante.

Cuadro de Resultados Encuesta Nº 9: Factores del Escaso Uso Masivo

Factores del escaso uso masivo	Máxima Incidencia	Mínima Incidencia	Irrelevante
Inadecuada normativa	35,7%	40%	14,3%
Inmadurez de estándares tecnológicos	18,6%	54,3%	14,3%
Inmadurez mercado	64,3%	21,4%	4,3%
Escasas aplicaciones	50%	34,3%	5,7%
Insuficiente conectividad	5,7%	55,7%	28,6%
Escasa difusión	61,4%	25,7%	1,4%
Ente Rector no exclusivo	21,4%	41,4%	24,3%
Otros factores (enumerar y ponderar)	25,7%	4,3%	1,4%

Fuente: Elaboración propia en base a encuesta a expertos

Gráfico de Resultados Encuesta Nº 9: Factores del Escaso Uso Masivo



Fuente: Elaboración propia en base a encuesta a expertos

COMPARACION CON RESULTADOS ENCUESTA OASIS 2003

Como resultado de la encuesta realizada en 2003, OASIS concluye que "Hasta el momento, PKI no ha alcanzado todo su potencial. PKI puede utilizarse para autenticar personas, superando la necesidad de recordar docenas de pins y passwords. Puede usarse para asegurar transacciones comerciales y proteger la privacidad de correos electrónicos y conversaciones telefónicas. Pero una cantidad de barreras, incluyendo la escacez de aplicaciones, alto costo, pobre entendimiento de PKI y problemas de interoperabilidad, han contribuido al uso limitado de PKI." (OASIS; 2004: 3)

Entre los principales factores que explican el escaso desarrollo de la PKI, podemos comparar los resultados en el cuadro siguiente:

Encuesta OASIS 2003	Encuesta PKI Argentina 2009
1.- Aplicaciones de Software no lo soportan (54%)	1.- PKI pobremente entendida (61%)
2.- Costos demasiado altos (53%)	2.- Falta de soporte gerencial (44,3%)
3.- PKI pobremente entendida (47%)	3.- Difícil de iniciar - demasiado compleja (32,9%)
4.- Pobre interoperabilidad (46%)	4.- Difícil de manejar por usuarios finales (32,9%)

5.- Difícil de iniciar- demasiado compleja (46%)	5.- Pobre interoperabilidad (28,2%)

Los factores vinculados con el desarrollo de software y el alto costo, presentes en la encuesta del 2003, no aparecen como relevantes en la del 2009. Quizá sea por el desarrollo tecnológico, que en general tiende a bajar los precios. Los factores que se mantienen, aunque con distinta ponderación, son los vinculados con la complejidad de la PKI: difíciles de implementar, difíciles de entender. Aparece también el factor interoperabilidad en ambas, aunque con ubicación diferente en cuanto a su incidencia. El factor novedoso en la encuesta desarrollada por nosotros para el presente trabajo es el referido a la falta de soporte gerencial.

En síntesis, podemos afirmar que el resultado de la encuesta base de esta tesis no difiere grandemente de los resultados de la encuesta internacional de 2003, a pesar del tiempo transcurrido, que en materia de tecnologías tiene un impacto muy alto, pareciera ser que la problemática del escaso desarrollo de la firma digital es percibida por los expertos de manera similar, lo cual nos permitiría afirmar que los factores que impiden su desarrollo son estructurales.

VII.- FACTORES QUE EXPLICARIAN EL ESCASO DESARROLLO DE LA FIRMA DIGITAL

En Capítulos anteriores de la presente investigación, se analizaron los componentes de la Infraestructura de Firma Digital, describiendo, para su mejor comprensión, los factores tecnológicos, jurídicos y organizacionales - administrativos que la integran. El capítulo precedente, presentó las percepciones de los expertos sobre los obstáculos que pudieran haber afectado la masividad de uso de la firma digital en Argentina, obtenidas a partir de una encuesta que se desarrolló como parte de esta Tesis.

Este capítulo del trabajo de investigación, analiza la incidencia de los factores tecnológicos, normativos y organizacionales - administrativos en el escaso desarrollo del uso masivo de la firma digital en Argentina. Se hace referencia previamente al escenario político que, entendemos, afectó directamente el desarrollo de esta iniciativa, debido a que en pleno proceso de reglamentación de la Ley N° 25.506 se produjo la crisis económico-social-institucional de diciembre de 2001 en Argentina.

El contexto político administrativo general

Quizá sea necesario en este punto hacer referencia al contexto político del momento en el cual, habiéndose aprobado la ley de firma digital, se inicia su reglamentación y su institucionalización. La Ley No. 25.506 fue sancionada a mediados del año 2001. Inmediatamente, el Secretario para la Modernización del Estado de la Jefatura de Gabinete de Ministros, Dr. Marcos Makón, encomendó a la suscripta la elaboración del decreto reglamentario. A tal fin, se convocó a una comisión técnica redactora integrada por destacados expertos en la materia. El Anteproyecto de Decreto reglamentario fue circulado a una lista ampliada de expertos, recibiéndose comentarios y sugerencias, por correo electrónico o a partir de entrevistas. En diciembre de 2001 estaba listo el Anteproyecto de Decreto, y se había iniciado el expediente para su aprobación.

En ese momento, se produjo una importante crisis institucional profundizada por la renuncia del Vicepresidente en el marco de una crisis económica severa. El escenario social mostraba elevadas tasas de desempleo y subocupación, con una imagen negativa generalizada del gobierno por parte de la opinión pública.

En octubre de 2001, el gobierno perdió abultadamente las elecciones legislativas y en diciembre de 2001 se llegó al epicentro de la crisis: la reducción en la valoración del crédito de Argentina, el incremento del riego país y la estampida bancaria se enlazaron con la decisión de restringir los depósitos bancarios y las transferencias al exterior, medida que se efectivizó en forma paralela a la decisión del FMI de eliminar un desembolso de $1.300 millones. La restricción bancaria, conocida como "corralito", acrecentó la incertidumbre y la movilización, a la que después de tal medida se incorporaron los sectores medios, prefigurándose una

situación de inestabilidad en todos los planos. La realización de una nueva huelga general, los saqueos, las movilizaciones masivas pidiendo "que se vayan todos", dieron lugar a la renuncia del presidente De la Rúa y su gabinete. Esos días marcaron un hito en la historia política y social de la Argentina: la masiva movilización popular exigía cambios radicales en la propia institucionalidad gubernamental y, naturalmente, en las orientaciones estratégicas de las políticas públicas. (OSZLAK, 2005: 10)

Con la asunción de la administración Duhalde, luego de la declaración del default sobre la deuda y el abandono de la Convertibilidad, se adoptó un régimen de emergencia pública y reforma del sistema cambiario que dispuso la emergencia social, económica, administrativa, financiera y cambiaria. El peso se devaluó, creando condiciones muy favorables a las exportaciones argentinas. La negociación con organismos internacionales de crédito, el restablecimiento de la confianza interna y en el exterior, la renegociación de la deuda externa pública con los acreedores privados en cesación de pagos, la renegociación de los contratos con las privatizadas, los aumentos en las tarifas de los servicios y la crítica situación social interna fueron algunos de los principales temas de la agenda pública del gobierno de Duhalde y de quien sería su sucesor, Néstor Kirchner. (OSZLAK, 2005: 11)

A partir del año 2003 se recuperó la normalidad institucional, sin embargo, lentos fueron los avances de la Infraestructura de Firma Digital. Como se verá más adelante, puede afirmarse que nuestra Infraestructura de Firma Digital aún presenta una institucionalización inconclusa. A lo largo de la presente tesis se han analizado los distintos aspectos que integran una PKI, a fin de encontrar los motivos específicos que pudieron dar lugar al escaso desarrollo de la firma digital en Argentina.

Sin embargo, y sin ánimo de efectuar un análisis detallado que excede largamente los objetivos de la tesis, en relación a la contextualización teórica desde la perspectiva de la ciencia administrativa, cabe preguntarse si la institucionalización inconclusa de la firma digital en Argentina es un fenómeno exclusivo de ella, o si por el contrario, es una característica compartida con otras áreas de la administración nacional.

Las reformas administrativas en democracia

A partir de la recuperación de la democracia en Argentina, se han producido grandes transformaciones tecnológicas, económicas, estatales y políticas. SCHWEINHEIM sostiene que "*Estos cambios estructurales, como es sabido, se han caracterizado por la consolidación de un capitalismo global asociado a la revolución tecnológica de las últimas cinco décadas, combinada con profundas transformaciones en el rol y configuración de los Estados Nacionales, tanto en los países del capitalismo avanzado, como los ex estados socialistas y los países del Tercer Mundo, incluido América Latina.*" Destaca el impacto que ha tenido sobre la administración pública, los modelos de gestión y de políticas públicas esta "*reconfiguración de la matriz de intervención, tamaño y morfología del Estado*" (SCHWEINHEIM, 2007: 1)

En relación con las reformas de los 80 y los 90, SCHWEINHEIM destaca su déficit institucional administrativo. Menciona que *"Estas reformas económicas y estatales no estuvieron asociadas a la construcción de una administración pública republicana. Las políticas que buscaron promover tal diseño institucional fueron escasas, descoordinadas, carecieron de continuidad, no tuvieron apoyo de los gobiernos y partidos políticos y se caracterizaron por graves fallas de diseño en el sentido del modelo administrativo republicano. Entre ellas cabe mencionar los intentos por la construcción de un cuerpo de servicio civil de excelencia al estilo francés en 1985, la reforma de los sistemas de administración financiera y de los organismos de control de 1993, y la reforma parcial del sistema de personal público de 1991."*(SCHWEINHEIM: 2003, 7)

Desde fines de los años 70 y aún hasta el presente, el principal enfoque de reforma administrativa ha sido el enfoque de sistemas (SCHWEINHEIM, 2008: 2), a partir de la premisa de que la gestión pública puede ser entendida como un conjunto de sistemas integrados, y cada uno de ellos, como un conjunto de procesos, actividades y tareas orientados a producir ciertos resultados y garantizar funciones estatales básicas. En la Administración Nacional argentina, se han implementado distintos sistemas que constituyeron el eje de la reforma administrativa en los 90. Sin embargo, los escasos resultados obtenidos medidos en relación a las capacidades de gestión pública, han demostrado la limitación del enfoque sistémico y la necesidad de incluir en los procesos de reforma la perspectiva institucional. (SCHWEINHEIM, 2009: 4, 5)

A partir de los 90 y hasta el año 2001, la administración nacional fue objeto de sucesivos intentos de reforma. A pesar de que fueron encaradas sucesivas reformas administrativas, con su correspondiente financiamiento, *"la evidencia práctica y la evaluación fundada de los funcionarios públicos, los expertos, los cuadros políticos superiores o intermedios que lideraron tales cambios y los expertos internacionales de la banca multilateral que financió en gran medida los mismos, es que resta aún un importante camino por recorrer. No sólo muchos de los cambios impulsados tuvieron escasos avances, sino que ha habido retrocesos notorios en sistemas que se suponía consolidados en el sector público nacional"*(SCHWEINHEIM, 2008: 1)

SCHWEINHEIM explica el déficit institucional administrativo a partir de *"la ausencia de reglas de juego y de instituciones para la organización y funcionamiento de la administración pública de naturaleza republicana"*, lo cual trajo como consecuencia o fue consecuencia de un tipo de institucionalidad administrativa asociada con la democracia delegativa, que se apoya en el principio de discrecionalidad. (SCHWEINHEIM: 2003, 9)

Resulta interesante analizar la paradoja de que, a pesar de haberse implementado sucesivas reformas y sistemas administrativos con el objetivo de mejorar la capacidad de gestión pública, basadas en los principios de gestión por resultados, inspiradas en el marco teórico de la Nueva Gerencia Pública, al menos nominalmente, los resultados alcanzados fueron escasos. Para SCHWEINHEIM, esta

paradoja está asociada a dos cuestiones: *"En primer lugar, a una desarticulación y una superposición de esfuerzos que ha conducido a escasos logros y a un desaprovechamiento de recursos e información de gestión. En segundo lugar, a una débil propensión institucional a la gestión y al control por resultados."* (SCHWEINHEIM: 2008, 24)

SCHWEINHEIM explica esta paradoja como consecuencia de las condiciones institucionales. En efecto, si bien los objetivos de las sucesivas reformas apuntaban a mejorar la capacidad de los gobiernos mediante el enfoque de sistemas, con su correspondiente planificación y asignación, medición y control de recursos, las condiciones institucionales no favorecieron su adecuada implantación y desarrollo. (SCHWEINHEIM, 2008: 7).

Como se advierte, la escasa capacidad institucional de la administración nacional, a pesar de los esfuerzos de las reformas administrativas, es una característica general. En ese marco, la institucionalización inconclusa de la Infraestructura de Firma Digital es una manifestación más del fenómeno general, es decir, no escapa a las condiciones imperantes en la Administración Pública en su conjunto.

Factores que explican el escaso desarrollo de la firma digital

A continuación de presentan las conclusiones que intentan explicar el escaso desarrollo de la firma digital en Argentina a partir del análisis de los tres factores que la integran: el jurídico, el tecnológico y el organizacional administrativo. Se presentan las conclusiones teóricas y los resultados de la encuesta a expertos.

Incidencia de los factores jurídicos

Menciona LORENZETTI que las leyes deben basarse en principios generales y reglas indeterminadas, que no estén orientadas a una u otra tecnología. Ya antes de la sanción de la Ley N° 25.506, LORENZETTI planteaba que *"Esta relación entre firma y criptografía es un error desde el punto de vista legislativo. La firma electrónica encontrará muchas técnicas y, a medida que estas cambien, caerán las leyes que se basan en una asimilación tan dura y rígida, desconociendo la relatividad histórica de estos procesos"*. (LORENZETTI; 2001: 60)

La Infraestructura de Firma Digital en su dimensión jurídica presenta numerosos problemas. En primer lugar, si bien existe una ley y sus decretos reglamentarios, no se ha completado la regulación prevista en dichas normas. En efecto, el Decreto N° 2628/02 dispone que la Autoridad de Aplicación deberá regular los siguientes aspectos:

a) normas y los procedimientos técnicos para la generación, comunicación, archivo y conservación del documento digital o electrónico, según lo previsto en los artículos 11 y 12 de la Ley N° 25.506. (Artículo 4)

b) Los estándares tecnológicos y de seguridad aplicables en consonancia con estándares internacionales. (Artículo 6)

c) Los procedimientos de firma y verificación en consonancia con los estándares tecnológicos definidos conforme el inciso precedente.

d) Las condiciones mínimas de emisión de certificados digitales.

e) Los casos en los cuales deben revocarse los certificados digitales.

f) Los datos considerados públicos contenidos en los certificados digitales.

g) Los mecanismos que garantizarán la validez y autoría de las listas de certificados revocados.

h) La información que los certificadores licenciados deberán publicar por internet.

i) La información que los certificadores licenciados deberán publicar en el Boletín Oficial.

j) 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.

k) El sistema de auditoría, incluyendo las modalidades de difusión de los informes de auditoría y los requisitos de habilitación para efectuar auditorías.

l) Las normas y procedimientos para la homologación de los dispositivos de creación y verificación de firmas digitales.

m) El procedimiento de instrucción sumarial y la gradación de sanciones previstas en la Ley N° 25.506, en virtud de reincidencia y/u oportunidad.

n) Los procedimientos aplicables para el reconocimiento de certificados extranjeros.

o) 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.

p) Los niveles de licenciamiento.

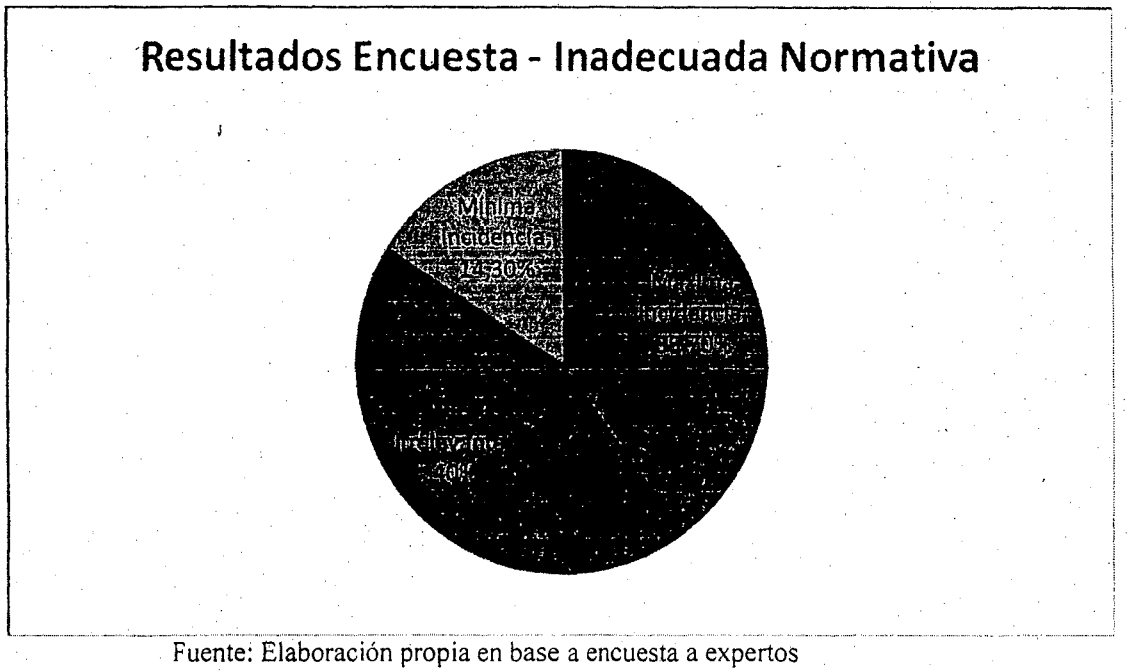
q) Reglamentar el uso y los alcances de los certificados de firma digital emitidos por los Registros Públicos de Contratos.

r) Las condiciones de prestación de otros servicios en relación con la firma digital y otros temas cubiertos en la ley.

Dicha regulación aún no ha sido abordada, en parte por la falta de claridad respecto de quién es el órgano responsable de llevarla a cabo, y en parte, porque no se ha dotado de recursos suficientes. Dilución de la responsabilidad, escasez de recursos, ausencia de liderazgo y no ser el principal objetivo de la organización, han dado por resultado que el marco normativo de la firma digital aún se encuentre inconcluso.

La dimensión jurídica de la Infraestructura de Firma Digital fue contemplada en la encuesta, como uno de los factores que explicarían su escaso uso masivo. Se identificó la variable como "inadecuada normativa", y obtuvo resultados más o menos parejos en cuanto a los que consideraban que tenían máxima incidencia (35.7%) y mínima incidencia (40%). Para el 14 % de los encuestados, la normativa es irrelevante para explicar el escaso desarrollo de la firma digital en Argentina.

Gráfico Nº 10 – Resultados Encuesta



Fuente: Elaboración propia en base a encuesta a expertos

Incidencia de los factores tecnológicos

Esta tesis ha abordado brevemente algunos aspectos tecnológicos básicos involucrados en la implementación de una Infraestructura de Firma Digital. No se han considerado múltiples aspectos técnicos, tal como los estándares de certificados X509, los estándares que se aplican a las listas de certificados, ni los aspectos técnicos del equipamiento o software necesarios, tampoco se analizaron los relativos a la capacidad de conectividad requerida para soportar aplicaciones con firma digital, ni los requerimientos vinculados con las medidas de seguridad informática.

A pesar de ello, la enumeración de los puntos tratados habla por sí misma de la gran complejidad inherente a la firma digital.

En síntesis, se han identificado los siguientes obstáculos tecnológicos para el uso masivo de la firma digital:

- Gran complejidad de implementación.
- Alto costo en dinero, recursos humanos y tiempo.
- Pocas aplicaciones lo usan.
- Difícil de entender para usuarios no expertos.
- Valor probatorio débil.
- Presenta problemas para conservar documentos y acceder a ellos en el mediano plazo.
- Obstaculiza el comercio electrónico entre partes localizadas remotamente en distintas jurisdicciones.
- Requiere presencia física para identificar personas siempre, de lo contrario no tiene valor.
- Requiere presentación de papeles para acreditar personería ante la autoridad de registro, pero no da certeza de la personería.....
- Posee debilidades intrínsecas en la administración de certificados.
- Presenta debilidades intrínsecas en la administración de listas de certificados.
- Posee debilidades intrínsecas para el almacenamiento de la clave privada (en definitiva, todo sigue dependiendo de una password....) passwords not dead!
- No aprovecha sinergia con otras implementaciones masivas exitosas (banca electrónica, medios de pago electrónicos, clave única de identificación tributaria.....)
- Escasa interoperabilidad debido a inmadurez de los estándares.

La evaluación de experiencias de PKI basada en certificados X.509 revela un grado de complejidad tecnológica muy alto, un despliegue y evolución lentos, caros y numerosas deficiencias técnicas y legales, tales como las relativas a la conservación de documentos electrónicos firmados digitalmente.

Más aún, los comentarios generales acerca del marco de seguridad y confianza que PKI brinda son exageradas, tal como vimos en relación por ejemplo, al

tema de conservación de documentos digitales firmados digitalmente. Además de las limitaciones de responsabilidad que las autoridades de certificación incluyen en sus contratos, de cuya lectura se desprende que en realidad es casi nada lo que garantizan.

Otros enfoques alternativos para autenticación parecen ser más adecuados como medios para satisfacer las necesidades que presenta el comercio y el gobierno electrónicos. Por una parte, las aplicaciones informáticas masivas en general utilizan mecanismos de autenticación más sencillos, basados en criptografía simétrica, esto es, claves compartidas. Por ejemplo, la operación en cajeros automáticos. Si la aplicación informática requiere mecanismos de alta seguridad para la autenticación del usuario, en general se utilizan tecnologías biométricas. En los últimos años la biometría ha tomado un impulso importante. Actualmente, existen tecnologías biométricas para el reconocimiento de las huellas dactilares, para el reconocimiento facial, para el reconocimiento de voz, del iris, del ADN, multibiometrías, etc.

Estas tecnologías biométricas se usan no solamente para el desarrollo de políticas públicas vinculadas con la seguridad, sino también para la identificación de personas. Actualmente, los pasaportes incluyen biometría y están desarrollándose pasaportes electrónicos que cuentan con dispositivos que albergan información de la persona (huellas dactilares, foto, datos personales). En la medida que estos documentos electrónicos sean adoptados en forma masiva para la identificación de las personas, si contienen dispositivos electrónicos que las identifique en el medio electrónico, no será necesario contar con una firma digital para tal fin. Por el contrario, la firma digital podrá ser usada de forma voluntaria como mecanismo de expresión del consentimiento por aquellas personas que así lo establezcan, pero no se espera un uso masivo.

Ya en el año 2001 CLARKE entendía que las tecnologías de clave pública en general parten de asumir condiciones del mundo real que no son razonables. Expresaba la necesidad urgente de avanzar en implementaciones concretas que contemplen enfoques de autenticación alternativos, para poder evaluar si éstos proveen una base adecuada para el comercio electrónico. (CLARKE; 2001: Conclusions)

Transcurridos nueve años desde ese momento, podemos afirmar que se ha avanzado mucho en la materia, y que las aplicaciones que utilizan enfoques alternativos de autenticación han sido exitosas, pues se utilizan masivamente y no han generado repudios de transacciones.

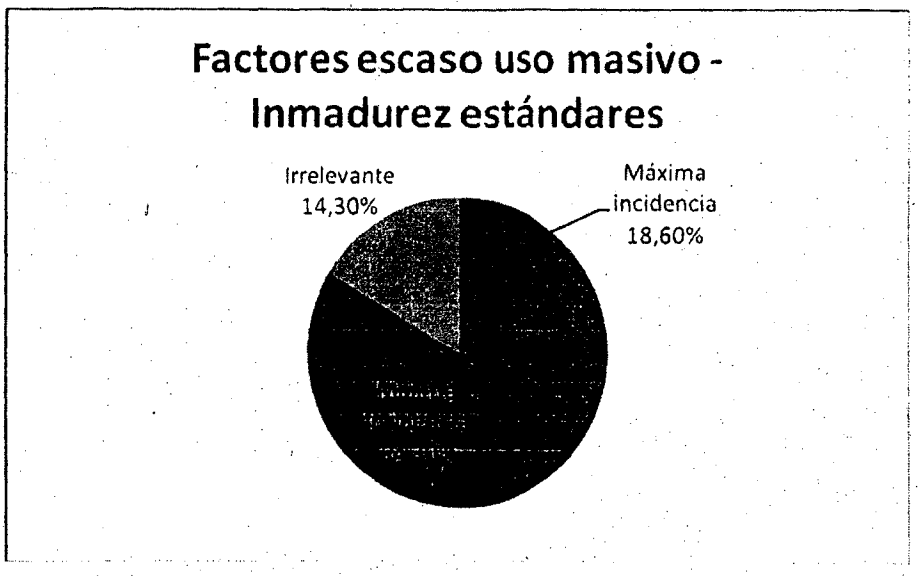
Un estudio realizado en Europa, muestra que desde la perspectiva económica, la difusión de PKI en el mercado europeo ha sido notablemente inferior a las expectativas. (GASSON et all, 2005: 59).

Los aspectos tecnológicos fueron considerados en la encuesta que se realizó a expertos para evaluar los posibles factores que podrían explicar el escaso uso masivo de la firma digital. Se identificaron las siguientes variables tecnológicas: inmadurez

de estándares tecnológicos, inmadurez del mercado, escasas aplicaciones e insuficiente conectividad.

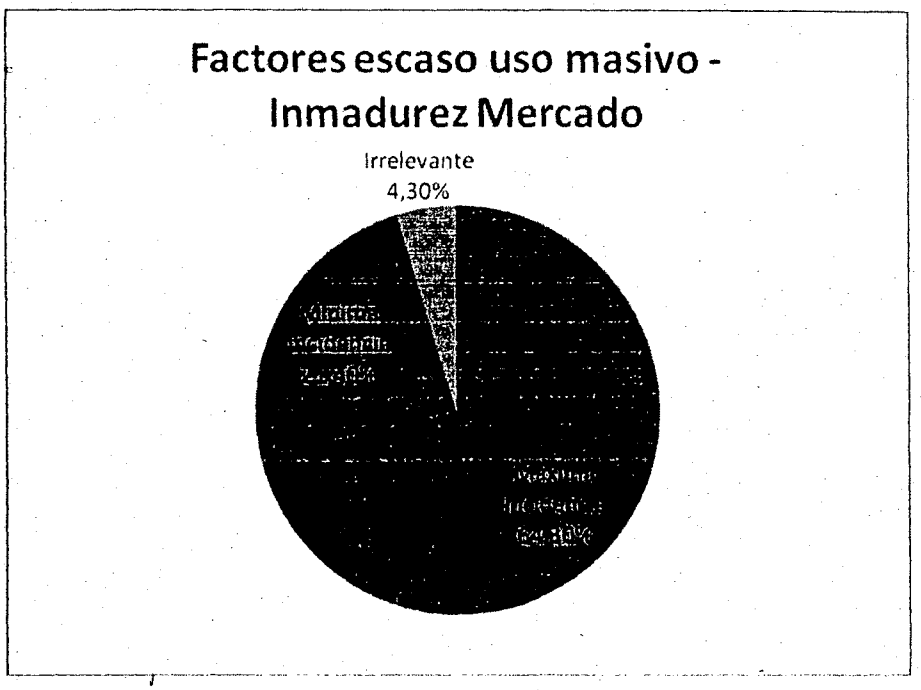
Los resultados obtenidos muestran que la variable que se considera más importante es la de *inmadurez del mercado*, el 64,3% de los encuestados le otorgó máxima incidencia. La menos importante fue la de *escasa conectividad* que fue considerada como irrelevante por el 28,6% de los encuestados y como de mínima incidencia por el 55,7%. La *inmadurez de estándares tecnológicos* fue considerada como de mínima incidencia por el 54,3% y la *escasez de aplicaciones*, como de máxima incidencia por el 50% de los encuestados.

Gráfico Nº 11 – Resultados Encuesta



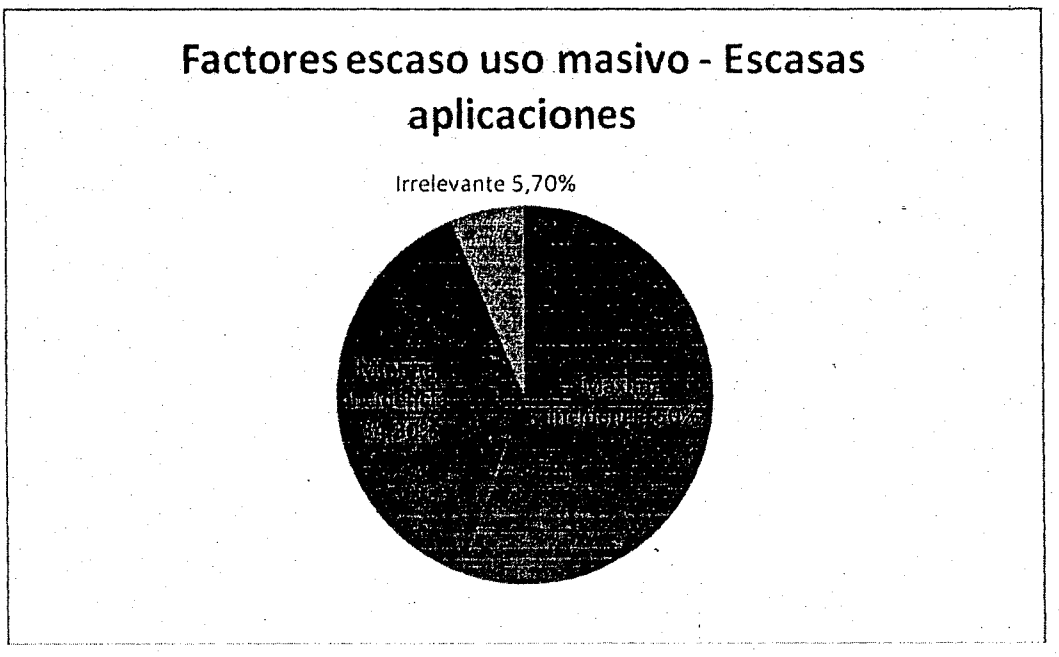
Fuente: Elaboración propia en base a encuesta a expertos

Gráfico Nº 12 – Resultados Encuesta



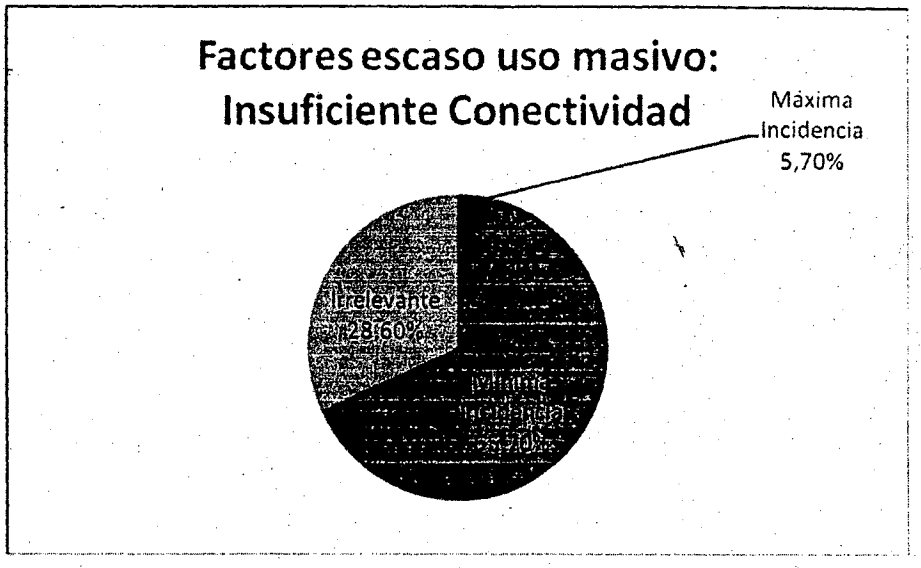
Fuente: Elaboración propia en base a encuesta a expertos

Gráfico Nº 13 – Resultados Encuesta



Fuente: Elaboración propia en base a encuesta a expertos

Gráfico Nº 14 – Resultados Encuesta



Fuente: Elaboración propia en base a encuesta a expertos

Incidencia de los factores organizacionales administrativos

En el capítulo referido a los factores organizacionales administrativos de la Infraestructura de Firma Digital se identificaron las múltiples normas que otorgan competencia a distintas áreas de la administración sobre el tema. Asimismo, se analizaron los aspectos administrativos mediante la metodología de Alain TOBELEM, el SADCI.

Déficit de capacidad institucional de la Infraestructura de Firma Digital

A continuación se sintetizarán los principales déficit de capacidad institucional detectados, y su impacto en la encuesta realizada a los expertos.

1. Déficit relacionados con las reglas de juego:

En la investigación, se identificaron los siguientes déficit de capacidad institucional de la IFD relacionados con las reglas de juego:

- La IFD fue afectada por la crisis político-económica- institucional de diciembre de 2001 en pleno proceso de regulación.
- Regulación inconclusa: falta definir reglas respecto de conservación de documentos electrónicos, procedimientos de auditoría, estándares tecnológicos, etc.
- Sistema de auditoría ausente: no se han aprobado los procedimientos y documentos para la precalificación de entidades de auditoría.

- Inflación normativa respecto de la asignación de competencias como Autoridad de Aplicación de la firma digital

2. **Déficit relativos a las relaciones interinstitucionales:**

Los organismos involucrados en la regulación y el control de los componentes de la Infraestructura de Firma Digital acusan un déficit significativo de capacidad institucional, fundamentalmente en el proceso de configuración del organismo con competencia específica en la materia.

Por otra parte, la regulación inconclusa y la institucionalización inconclusa han generado una pérdida de liderazgo a nivel nacional, ya que muchas provincias han ido aprobando leyes de firma digital que en muchos casos no respetan el esquema instaurado por la Ley No. 25.506, como en el caso de la provincia de Buenos Aires, pero que encuentran su justificación debido a la tardanza de la administración nacional de poner en marcha la Infraestructura de Firma Digital. Sintéticamente, los principales déficit relativos a las relaciones institucionales serían:

- No existe un organismo responsable exclusivo y excluyente para ejercer el rol de Autoridad de Aplicación.
- Potencial conflicto de interés en la ONTI al ejercer simultáneamente el rol de Autoridad de Aplicación real, Autoridad Certificante para el Sector Público y organismo auditor.
- Proliferación de leyes provinciales sobre firma digital con esquemas diversos al de la ley nacional.
- Ausencia de liderazgo sostenido en el tiempo de la Autoridad de Aplicación a nivel nacional.

3. **Déficit vinculados con los esquemas organizativos y de asignación de funciones:**

La regulación inconclusa, sumada a la disolución del Ente Administrador de Firma Digital nunca formado, y a la distribución difusa y superpuesta de competencias entre distintas áreas de gobierno, en ningún caso dedicadas en forma exclusiva al tema, explican el déficit en la organización y en la distribución de funciones.

Los principales aspectos detectados relacionados con el esquema organizativo y de asignación de funciones son:

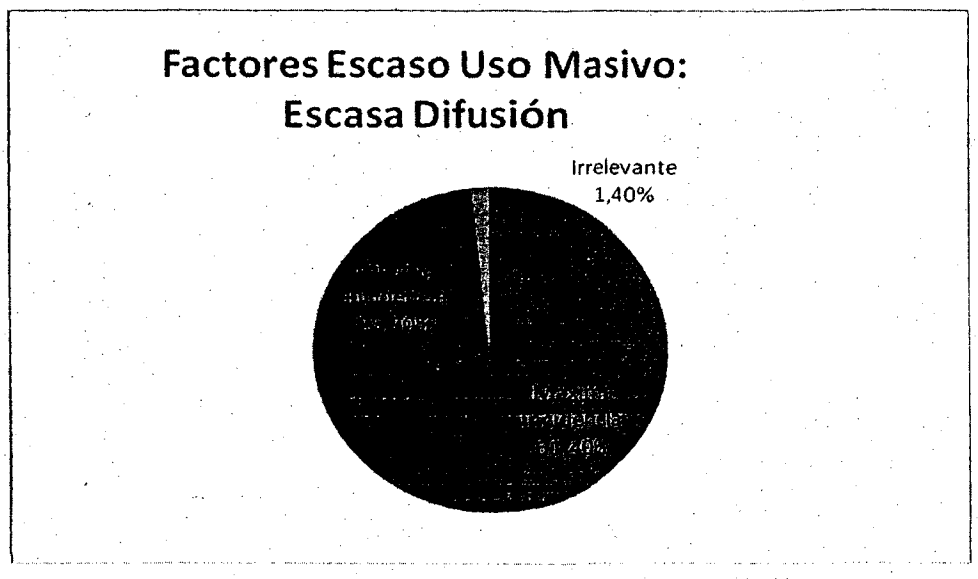
- Inexistencia de un órgano rector que ejerza en forma exclusiva el rol de Autoridad de Aplicación de la Infraestructura de Firma Digital.
- Proliferación de normas de estructura que diluyen la responsabilidad en la ejecución de las actividades de firma digital.
- Consecuentemente, inexistencia de recursos adecuados para el ejercicio del rol de Autoridad de Aplicación

- Conflicto de intereses en cabeza de la ONTI por el triple rol que cumple en los hechos: Autoridad de Aplicación real, Autoridad Certificante del Sector Público y organismo auditor de firma digital.

La Encuesta contempló los aspectos institucionales, en el apartado jurídico hemos presentado los resultados vinculados con la variable normativa, y en este presentaremos los resultados obtenidos para las variables "ente rector no exclusivo" y "escasa difusión". Con referencia a la ausencia de un ente rector exclusivo, los encuestados no lo consideraron un factor de máxima incidencia para explicar el escaso uso masivo de la firma digital. En efecto, la distribución es bastante pareja entre quienes lo consideran un factor de máxima incidencia (21.4%), aquellos para los que es un factor de mínima incidencia (41,4%) y los que lo consideran totalmente irrelevante (24.3%).

Por el contrario, los aspectos vinculados con la escasa difusión son considerados como de máxima incidencia por el 61,4% de los encuestados, y el 25,7% le asigna una mínima incidencia. Solamente el 1, 4% de las respuestas considera que es un factor irrelevante.

Gráfico Nº 15 – Resultados Encuesta



Fuente: Elaboración propia en base a encuesta a expertos

Gráfico Nº 16 – Resultados Encuesta

Fuente: Elaboración propia en base a encuesta a expertos

La Infraestructura de Firma Digital como componente del proyecto de gobierno digital

Cerrando el capítulo de factores, se advierte que la Argentina si bien ha superado en algunos aspectos relevantes la crisis del 2001, aún tiene un amplio camino por recorrer. Los gobiernos posteriores al 2001 han impulsado políticas referidas a paliar los efectos más problemáticos de la crisis institucional, política y económica. En efecto, se reestructuró la deuda pública, se salió del default, se normalizó la actividad bancaria, en materia económica. En lo institucional, se sucedieron elecciones libres que retomaron la continuidad institucional vulnerada. En lo social, y quizá sea el aspecto más complejo, se pusieron en marcha numerosos planes sociales, se brindó articulación a los movimientos sociales, incorporándolos a la vida institucional y económica, se reabrieron fábricas, se disminuyó el desempleo, se nacionalizó el sistema de seguridad social, volcando una fuerte cantidad de recursos al mercado interno y a la realización de políticas públicas efectivas, como el subsidio por hijo. Como consecuencia, el país mostró índices de crecimiento impresionantes y una mejora en la calidad de vida de la gente perceptible a simple vista.

Sin embargo, no hubo políticas específicas orientadas al mejoramiento de la administración nacional. Todas las medidas de políticas sustantiva no contaron con el apoyo de una administración pública que pudiera facilitar su instrumentación. No hubo una política de reforma administrativa explícita y generalizada que acompañara los esfuerzos de los gobiernos en mejorar los servicios del Estado. Se apoyó más bien en una metodología de transferencia directa de recursos, sin la mediación de las estructuras burocráticas. En este contexto, la Infraestructura de Firma Digital no fue una excepción.

En tal sentido, compartimos con OSZLAK la opinión de que *"los distintos gobiernos, incluido el actual, han intentado con variado éxito superar los efectos más graves de esa crisis y, con tal propósito, han ensayado diversas soluciones que, por ahora, no incluyen una seria reforma del estado orientada al fortalecimiento de su capacidad de gestión. La administración del Presidente Kirchner ha logrado resultados destacables en la renegociación de la deuda externa, el manejo de las finanzas públicas y la implementación de políticas sociales de emergencia. Pero no se ha planteado con igual grado de iniciativa y creatividad la tarea de avanzar en las reformas estatales de segunda generación pendientes."* (OSZLAK, 2005: 33)

A fin de contextualizar a la Infraestructura de Firma Digital como proyecto vinculado a la reforma administrativa, es útil el análisis del grado de éxito de las políticas de reforma del Estado realizado por OSZLAK, en el cual se señalan elementos clave. Destaca que *"el éxito de las reformas e innovaciones "hacia dentro" depende, esencialmente, de la dinámica que establezcan quienes tienen la responsabilidad de conducir el aparato estatal y sus funcionarios permanentes."* (OSZLAK, 2003: 11)

Además de estos funcionarios, participan los siguientes actores externos:

- los organismos multilaterales o agencias bilaterales de cooperación, que aportan financiamiento para las reformas y, no pocas veces, orientaciones más o menos precisas sobre la modalidad y alcances que deben tener las políticas e instrumentos de reforma empleados; y

- los proveedores de servicios (incluyendo consultoría), que realizan diagnósticos y proporcionan insumos para innovar la gestión (v.g., modelos organizativos, equipamiento informático, relevamientos geo-referenciales, asesoramiento jurídico, reingenierías de procesos, manuales de operación, etc.).

En el caso de la Infraestructura de Firma Digital, el elenco de funcionarios políticos y permanentes fue variado, no lográndose en ningún momento que el tema fuera central en la Agenda política. Si bien existieron los actores secundarios representados por organismos multilaterales, en este caso, el Banco Mundial a través del Proyecto de Modernización del Estado, y también los proveedores de servicios de certificación, como Certisur, filial argentina de Verising, con representación en la Comisión Asesora de Firma Digital y como autores del proyecto de la Diputada Puiggross, la Infraestructura de Firma Digital careció de un líder político que tomara la iniciativa necesaria para ponerla en marcha en el Poder Ejecutivo. En el Poder Legislativo, el Diputado (MC) Pablo Fontdevila (PJ) lideró el tema, logrando en poco tiempo la sanción de la ley de firma digital después de un excelente trabajo de construcción de consenso entre los distintos proyectos presentados. Los proyectos de ley presentados fueron varios, por lo cual el trabajo de coordinación realizado por el Ing. Christian Jensen, asesor del Diputado Fontdevila, fue clave para la unificación de los proyectos derivado en su posterior sanción.

En 1999 se había presentado un proyecto de ley elaborado por la entonces Secretaría de Función Pública, fruto del trabajo del Subcomité de Criptografía y Firma Digital que funcionaba en el Banco Central y que estaba integrado entre otros por el Dr. Hugo Scolnik (experto internacional en criptografía) y por la Dra. Patricia Prandini (Directora Nacional de Integración Tecnológica de la ex Secretaría de la Función Pública). Dicho proyecto de ley se elaboró a partir de la experiencia de la Infraestructura de Firma Digital para el Sector Público Nacional creada por el Decreto N° 427 de 1998, pionero en la materia a nivel internacional.

Luego del cambio de gobierno, en el año 2000 se conformó una Comisión Redactora en el Ministerio de Justicia, integrada por reconocidos profesionales, el Dr. Horacio Granero (Director de la carrera de postgrado de Derecho de la Alta Tecnología de la Universidad Católica Argentina), el Dr. Daniel Altmark (Director de la carrera de especialización de Derecho Informático de la Universidad de Buenos Aires), el Dr. Damián Loreti (asesor del Senador Pedro Del Piero), la Dra. Mercedes Rivolta (Administradora Gubernamental), la Cdora. Patricia Prandini (Directora Nacional de Integración Tecnológica), la Dra. Mercedes Velazquez, el Dr. Miguel Sama y el Subsecretario de Justicia, Dr. Carlos Balbín.

Este proyecto se unificó con el presentado por el Diputado Pablo Antonio Fontdevila (PJ), quien desde la presidencia de la Comisión de Informática y Comunicaciones, impulsó el tratamiento del proyecto. En dicha comisión se formó un grupo de expertos que asesoraban a los legisladores y se analizaron los distintos proyectos presentados, para elaborar una única versión consensuada. Es así que el grupo se integró por el Ing. Cristian Jensen (asesor del Diputado Fontdevila), por el Dr. Damián Loreti, por la Dra. Rivolta, por el Dr. Hugo Scolnik y el Lic. Armando Carratalá (asesores de la Diputada Puigross), entre otros asesores de los diputados que habían presentados sendos proyectos de ley (Diputado Corchuelo Blasco, Diputado Atanasof, Diputada Camaño, Diputado Cardesa).

Finalmente, gracias al liderazgo del Diputado Fontdevila, se logró consensuar un único proyecto de ley sobre firma digital, el cual fue sancionado a mediados de 2001. Mientras tanto, en el ámbito de la entonces Secretaría para la Modernización del Estado de la Jefatura de Gabinete de Ministros, comandada por el Dr. Marcos Makón, se trabajaba en la redacción del decreto reglamentario de la ley, con el objetivo de poner en marcha la Infraestructura de Firma Digital lo más rápido posible. Lamentablemente el alejamiento del Dr. Makón, previo a la crisis del 2001, sumado a dicho evento, dejó sin liderazgo político a esta iniciativa en el ámbito de la administración nacional.

Señala OSZLAK que en los casos de innovación en la gestión administrativa está presente la incorporación de las tecnologías de comunicación e información, que pueden o no implicar un cambio en los procedimientos. Las reformas administrativas "internas" se refieren *"a las dimensiones y variables asociadas a la organización y funcionamiento de la burocracia: su marco normativo, su estructura organizativa, su dotación de personal y de recursos materiales, sus procesos y procedimientos de gestión, la capacidad de sus agentes y el comportamiento de los mismos en la producción de los bienes, servicios y regulaciones a su cargo."* (OSZLAK, 2003:11)

Estas reformas representan un intento del gobierno para mejorar la capacidad del aparato estatal a fin de poder implementar las políticas sustantivas por las cuales han sido elegidos. El propósito de un nuevo elenco de gobierno puede verse obstaculizado por las resistencias de la administración, que percibe todo cambio como una amenaza al statu quo. Señala OSZLAC que *"las innovaciones tecnológicas no operan si no son incorporadas a la cultura de la administración. Esto implica un cambio profundo en la disposición de los servidores públicos a funcionar bajo reglas de juego diferentes, lo cual se verifica cuando ese personal ha conseguido incorporar las nuevas reglas y su fundamento axiológico o moral a su conciencia, a sus percepciones, actitudes y comportamientos. Debe existir entonces un proceso previo de "naturalización" de esas innovaciones en las manifestaciones de conducta de cada agente, para que pueda producirse una real institucionalización de las reformas"*. (OSZLAK, 2003: 11)

Esta explicación que ensaya OSZLAK es aplicable al caso en estudio. En efecto, uno de los obstáculos que se han detectado para el desarrollo de la Infraestructura de Firma Digital es la carencia de una estructura organizacional específica. En un primer momento se crea un Ente Administrador que no logra constituirse, y posteriormente, se disuelve dicho Ente y se transfieren las competencias a la ONTI. Dicha transferencia generó más dificultades que resultados. Una posible explicación radica en que la cultura de la ONTI estaba fuertemente impregnada por su rol en el anterior régimen de firma digital. No advirtió el cambio que implicaba la nueva ley, en la medida que ampliaba los alcances de la firma digital a todas las actividades, además de las del sector público nacional.

En efecto, analizando las actividades que desarrollan actualmente, se advierte que en gran medida son las mismas que se realizaban en 1999 con el régimen de firma digital para el sector público. El Decreto Nro. 427 de abril de 1998, regulaba el uso de documentos electrónicos en la Administración Nacional, equiparando el requisito de la firma ológrafa con una firma digital y creaba una Infraestructura de Firma Digital para el Sector Público Nacional. A partir de esta experiencia, que se desarrolló en la entonces Secretaría de la Función Pública de la Jefatura de Gabinete de Ministros, se puso en operación una Autoridad Certificante Raíz, se licenció una Autoridad Certificante de la Oficina Nacional de Tecnologías de Información - ONTI, se desarrolló un software de autoridad certificante de libre disponibilidad que se entregó gratuitamente a distintos organismos públicos, nacionales, provinciales, Poderes Judiciales y Universidades, se montó un Laboratorio de Firma Digital, se levantó en Internet una página web con información y se publicó un newsletter que se mantiene en Internet hasta la fecha.

Durante el período de existencia del Ente Administrador, nada se hizo. La ONTI continuó sus actividades normales sin alterar su rutina. Cuando se le transfieren las competencias a la ONTI, la organización no se adaptó al nuevo escenario, y por el contrario, la cultura organizacional afectó las posibilidades de innovación de manera conservadora, esto es, manteniendo las antiguas rutinas. Esta característica cultural de la organización, reactiva a los cambios, conservadora de las viejas tareas, se vio agravada por la discontinuidad política.

En este aspecto, una alternativa seria tendría que considerar la creación de un órgano independiente conformado con personal seleccionado por concurso, de

modo de poder instalar una nueva cultura que se identifique con el rol de autoridad de aplicación de la firma digital con alcance nacional. (OSZLAK, 2003: 12)

El mismo OSZLAK menciona que la introducción de la firma digital para la tramitación de expedientes fue uno de los aspectos que los informes de gestión destacados por la Subsecretaría de la Gestión Pública. Sin embargo, se pregunta cuál es el grado de implementación concreto de dicha medida. Esta observación agudísima de OSZLAK realizada en 2003, sin mayores elementos que su vasta experiencia, es totalmente cierta aún ahora en 2010.

Si bien recién a partir de 2010 desde la Subsecretaría de Tecnologías de Gestión de la Jefatura de Gabinete de Ministros se impulsa el uso generalizado para toda la Administración Nacional del sistema de gestión documental Com-Doc, y del sistema de administración de recursos humanos, SAHRA, lo cierto es que al día de hoy no existe un sistema masivo de tramitación de expedientes en formato electrónico, con firma digital o sin firma digital. Sencillamente, la Administración Nacional, salvo contadas excepciones, se sigue moviendo al ritmo del expediente en papel. *"Para un observador externo, el desafío es poder estimar el grado en que estos aparentes resultados se tradujeron en reales innovaciones."* (OSZLAK, 2003: 14).

Señala OSZLAK: *"Las consultas que he realizado al respecto me permiten sostener que la implantación efectiva de estas reformas prácticamente no tuvo lugar. La mayoría de las iniciativas nacieron en los comienzos de la Presidencia De la Rúa, a fines de 1999, a instancias del Vicepresidente Carlos Alvarez, bajo cuya jurisdicción se hallaba la Secretaría de Modernización del Estado. El impulso que cobró la reforma estatal en esa época se fue debilitando luego de la renuncia de Alvarez en 2000 y especialmente, después de la crisis producida a fines de 2001. De manera que durante la transición del Presidente Duhalde poco pudo hacerse para mantener la continuidad del esfuerzo de reforma, de modo que las actividades realizadas por la Subsecretaría de la Gestión Pública - desde su jerarquía secundaria-, fueron adquiriendo un carácter esencialmente formal. Esta conclusión se compadece con la interpretación más pesimista que he ofrecido al referirme a las dificultades de la reforma e innovación en el aparato estatal argentino."* (OSZLAK, 2003: 15)

Finalmente, OSZLAK esboza un diagnóstico del estado de avance del gobierno electrónico[11], que si bien es un concepto más amplio que el de la firma digital, tiene a la Infraestructura de Firma Digital como uno de sus componentes. Interesa conocer cuál es su percepción de la ONTI, ya que dicha organización es la que actualmente ha vuelto a concentrar las competencias sobre firma digital, aunque formalmente figuren asociadas a la figura del Secretario de la Gestión Pública.

[11] Este trabajo adopta la definición de "gobierno electrónico", como sinónimo de "administración electrónica", contenida en la Carta Iberoamericana de Gobierno Electrónico de 2007. La Carta de Pucón entiende por tal al "uso de las TIC en los órganos de la Administración para mejorar la información y los servicios ofrecidos a los ciudadanos, orientar la eficacia y eficiencia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación de los ciudadanos."

En 2003, OSZLAK presenta al caso del gobierno digital como un caso paradigmático de fracaso. Destaca el rol fundamental que tienen las tecnologías de comunicación e información en las reformas internas de la administración. Respecto de la ONTI, órgano rector en la materia, opina que *"frente a la importante misión que debería haber cumplido, los factores propios de la actual crisis, sumados a las fallas acumuladas en la gestión de tecnologías informáticas en la Administración Pública, configuran hoy un escenario limitado por:*

- *Discontinuidad de personas y de políticas*
- *Falta de recursos materiales*
- *Carencia de instrumentos que permitan coordinar el conocimiento localizado en un sistema distribuido y resguardar la memoria institucional.*
- *Dificultades de aplicación de políticas diseñadas e implementadas de manera centralizada.*
- *Compartimentación de las áreas.*
- *Falta de inserción y legitimidad de la ONTI como área coordinadora y rectora".* (OSZLAK; 2003:16)

Según OSZLAK *"este diagnóstico refleja el resultado de una sucesión incoherente de iniciativas, impulsadas por los gobiernos argentinos de los últimos años, que se embarcaron en alrededor de 30 programas diferentes -la mayoría de ellos con múltiples objetivos- tendientes a emplear tecnologías de información en el manejo de la administración pública y la provisión de servicios públicos."* (OSZLAK; 2003: 16)

Continúa OSZLAK explicando que *"tal como surge de un informe de evaluación externa no publicado, hay muy poco para mostrar como resultados de estos esfuerzos y recursos aplicados. La administración pública argentina no ha alcanzado siquiera los estándares mínimos de funcionalidad que típicamente se atribuyen a gobiernos digitales. Existen evidencias de muy serias deficiencias en el modo de abordaje de esta experiencia, en su implementación y en su efectividad."* (OSZLAK; 2003: 17)

Se podrían aplicar a la Infraestructura de Firma Digital las conclusiones preliminares que aporta OSZLAK referidas a las políticas orientadas a TICs, caracterizadas como *"excesivamente ambiciosas, de muy "alto vuelo" y poco aterrizadas. Casi sin excepción, los resultados fueron significativamente menores que lo que indicaban las expectativas iniciales. La mayoría de las ellas enfrenta problemas o se han suspendido. Sin duda, la crisis económica ha influido financieramente sobre estos programas, pero es muy probable que muchas de estas iniciativas se hubieran debilitado o trabado de todos modos. No hubieron evaluaciones realistas respecto a inversiones y costos operativos, ni capacidad institucional de implementación, ni desarrollo de usuarios, ni cooperación y coordinación entre partes interesadas."* (OSZLAK; 2003: 18)

En similar línea de pensamiento, el diagnóstico que precede al Proyecto de Macroestructura del Estado realizado por la Jefatura de Gabinete de Ministros en 2001 señalaba que *"... las capacidades institucionales públicas para desempeñar las funciones emergentes del nuevo modo de relacionamiento entre el entorno externo, el gobierno y la sociedad, muestran un atraso relativo. Es decir, todavía no se cristaliza un conjunto coherente y suficiente de instituciones con reglas transparentes*

de funcionamiento". En particular, destaca la falta de sincronía entre las reformas institucionales y económicas y la modernización del Estado. (JGM; 2001: 3)

Es notable como este diagnóstico efectuado en 2001, previo a la crisis, en el mencionado estudio es totalmente aplicable a la situación de la Infraestructura de Firma Digital en 2010. En efecto, el documento expresa que *"Cuando se encararon cambios organizativos con escasa claridad de las respectivas misiones de política pública y sin un desarrollo de instrumentos efectivos, ellas fueron inoperantes y, peor aún, generaron expectativas que fueron rápidamente frustradas. Por otro lado, la aplicación de instrumentos modernos de gestión sobre una organización del sector público caracterizada por redundancias innecesarias, vacíos y desajustes encuentra límites para su consolidación más temprano que tarde".* (JGM; 2001: 4)

OSZLAK menciona los problemas comunes que padecieron las implementaciones de programas de innovación con componentes tecnológicos, entre los que destaca la falta de previsión de costos, la superposición de programas, la ausencia de mecanismos de coordinación implícitos, la desfinanciación y limitada implementación, la carencia de controles de efectividad. Otra característica negativa observada es la desvinculación entre los objetivos planteados, generalmente con sentido, y la estrategia utilizada para concretarlos.

En ese orden, OSZLAK destaca que *"se presume que algunos programas específicos de las organizaciones estatales involucradas se orientaron más a hacerse de recursos que a comprometerse con resultados. Invariablemente, sus objetivos son deseables y tienen sentido, pero raramente han sido "desempacados" operativamente para convertirlos en programas de acción efectiva. La fijación de metas específicas, o sea, resultados y no insumos, es algo casi ausente en los programas gubernamentales, de modo que la responsabilización es casi inexistente. Además, la presencia de cotos cerrados en la conformación de los programas conspira contra su efectividad."* (OSZLAK, 2003: 18)

En el mismo trabajo, OSZLAK menciona los déficit de capacidad institucional para la implementación de tales programas, debido a la ausencia de:

- Un plan de implantación y reglas claras para la toma de decisiones;
- Un presupuesto realista;
- Ajustes requeridos para mejorar la capacidad de implementación;
- Responsabilización de los directivos en términos de resultados;
- Una concepción operativa, más que puramente conceptual;
- Incentivos al desempeño;
- Una orientación a resultados más que al control de recursos;
- Un mecanismo de realimentación para reasignar recursos en función del desempeño efectivo.

La investigación realizada en el presente trabajo corrobora la validez de estas reflexiones en relación con la Infraestructura de Firma Digital.

VIII.- CONCLUSIONES

Reflexiones finales

A modo de cierre, o mejor, de apertura al debate sobre la firma digital en Argentina, se puede decir que se han encontrado razones tecnológicas, jurídicas y administrativas que explican el escaso uso en estos 10 años de existencia.

Las **razones tecnológicas** que hasta el momento no encuentran respuesta, giran en torno a la accesibilidad posterior de los documentos electrónicos. En un contexto en el cual el permanente cambio tecnológico torna obsoletas aplicaciones que hasta hace un año eran lo último, es necesario garantizar el acceso permanente a los documentos electrónicos. Un contrato firmado hoy, debe ser conservado en formato electrónico en perfecto estado para su posterior consulta por ejemplo, dentro de 15 años. Un expediente administrativo en formato electrónico, debe poder ser leído por los organismos de control varios años después de su archivo.

Para ello, es necesario actualizar el formato periódicamente, para mantenerlo accesible. En esa transformación, el documento electrónico cambia, y se pierde así la posibilidad de verificar su integridad aún si ha sido firmado digitalmente. En otras palabras, debido a los constantes cambios tecnológicos y a la necesidad de mantener accesible los datos del documento digital, la firma digital no permite verificar la integridad del documento pasado cierto tiempo.

Si a esta cuestión se le agrega la inmadurez de los estándares sobre firma digital, selección de números primos, dispositivos criptográficos, documentos electrónicos, y conservación, es claro que la firma digital más que una solución se ha constituido en un obstáculo en sí misma para el desarrollo del gobierno electrónico.

En cuanto a las **razones de orden jurídico** que explican el escaso uso de la firma digital en Argentina, la misma Ley Nº 25.506 admite dos tipos de firmas en formato electrónico: la firma electrónica y la firma digital. Además, otorga valor legal al documento electrónico, habilitando de esta manera todo tipo de transacción digital. En efecto, se ha visto que el esquema de autenticación apoyado exclusivamente en la firma digital, fue la primera aproximación que desde el campo del derecho, se presentó para resolver el tema de la validez legal de las transacciones realizadas en formato electrónico.

Si bien las primeras normas a nivel internacional fueron explícitas en cuanto a la necesidad de contar con infraestructuras de firma digital para reemplazar el requisito de la firma manuscrita en actos jurídicos, prontamente fueron superadas por las nuevas corrientes que propiciaban legislaciones "tecnológicamente neutras". La evolución internacional posterior tiende a reconocer ampliamente distintos tipos de firmas electrónicas, coherentemente con las disposiciones tradicionales de derecho civil.

En este sentido, esta tendencia internacional superadora de la firma digital, se enmarca en el tradicional principio de libertad de las partes para establecer los mecanismos de autenticación en el otorgamiento de un acto jurídico. En esencia, la vigencia del principio del derecho de que los contratos son ley entre las partes, ya vigente en el derecho romano *"pacta sunt servanda"*, y reconocido en nuestro

Código Civil en el artículo 1197[12]. Y el reconocimiento que la Ley Nº 25.506 da al documento electrónico en su artículo 6 y a la firma electrónica y la firma digital. Respecto de las formalidades, se aplica la normativa de fondo, y el propio Código Civil establece cuáles son las formalidades requeridas para el otorgamiento de actos jurídicos.[13]

La Convención de UNCITRAL sobre comunicaciones electrónicas en contratos internacionales, a partir del principio del equivalente funcional, admite el uso de variadas técnicas de autenticación electrónica. En cuanto a las razones jurídicas, es posible afirmar que la evolución del derecho ha superado la visión inicial proclive a admitir solamente las firmas digitales. En ese sentido, el panorama jurídico es lo suficientemente amplio como para dar validez a cualquier método de autenticación electrónica que esté acordado entre las partes o cuyo procedimiento cuente con algún marco procedimental. Así se admiten las claves simétricas, tecnologías biométricas, firmas digitales emitidas por certificadores no licenciados, todas ellas con el valor jurídico de una firma electrónica susceptible de dar por satisfecho el requisito legal de "firma" como expresión del consentimiento de la persona.

Debido a estas cuestiones, al profundo impacto que el uso de las comunicaciones móviles produce en las configuraciones sociales, y a estas nuevas perspectivas dimensionales de tiempo y espacio, es muy importante el rol del derecho en este punto. En efecto, es necesario que las normas que aprueban los países respondan a esquemas internacionales, es decir, abreven en fuentes comunitarias o tratados internacionales que fijen criterios mínimos comunes, con un enfoque tecnológicamente neutro que las dote de la capacidad de mantener su vigencia a pesar del constante avance tecnológico (LORENZETTI, 2001: 45). (RIVOLTA; 2008: 26).

Con relación a las **razones organizacionales administrativas** que explican el limitado desarrollo de la firma digital en Argentina, se ha analizado la escasa institucionalización de la Infraestructura de Firma Digital en nuestro país. A partir del análisis de las competencias asignadas por la normativa de fondo (Ley Nº 25.506, Decreto Nº 2628/02 y normas complementarias) y de la normativa que sucesivamente asignó dichas competencias a distintas unidades de la Administración Nacional, cabe señalar que no existe un órgano con competencia específica exclusiva, que tampoco cuenta con una asignación exclusiva de recursos, y que el proceso de institucionalización de dicha Infraestructura está inconcluso.

Las razones que pudieran explicar esta institucionalización inconclusa no difieren de las que se mencionan respecto de otras áreas de la administración nacional para la época. En efecto, sin que estas conclusiones pretendan abarcar un tema tan amplio como la contextualización teórica de las administraciones públicas

---

[12] Código Civil Argentino: Art. 1.197. Las convenciones hechas en los contratos forman para las partes una regla a la cual deben someterse como a la ley misma.

[13] Código Civil Argentino: Art 974.Cuando por este código, o por las leyes especiales no se designe forma para algún acto jurídico, los interesados pueden usar de las formas que juzgaren convenientes.

latinoamericanas, entendemos que, además de los aspectos específicos que se han mencionado referidos a la tecnología, el derecho y la administración, la institucionalización inconclusa de la firma digital en Argentina no es ajena a la escasa institucionalización de otras áreas de la administración nacional.

Líneas de investigación futura

En el desarrollo del presente trabajo, a medida que avanzabamos en uno u otro aspecto, se iban abriendo múltiples materias que podrían haber sido analizadas. En ese sentido, se podrían profundizar los análisis de los factores tecnológicos, incluyendo los aspectos no considerados en el presente estudio, los factores jurídicos, incluyendo las regulaciones internacionales y las de las provincias argentinas, y en cuanto a los factores organizacionales-administrativos, se podría contemplar el relevamiento y análisis de los recursos humanos y de los financieros.

Otro aspecto que sería útil analizar es el vinculado con el uso efectivo de la firma digital en las aplicaciones de gobierno electrónico, es decir, cuántas trámites electrónicos actualmente vigentes usan firma digital y para qué.

En otro sentido, se podrían plantear líneas de investigación relativas a los aspectos económicos vinculados con el uso de la firma digital. Cuál es el costo de su operación para las empresas, cuál sería el costo para el usuario, cuál es el costo para la instalación de una autoridad certificante y para la administración de la misma, etc.

Líneas de Acción Sugeridas

En un contexto de crecimiento económico y disminución de la pobreza como el que impera en nuestro país, urge la necesidad de dotar al Estado de un aparato estatal que permita consolidar estas políticas. Para ello, coincidimos con SCHWEINHEIM en el diagnóstico y en la propuesta referidas a la necesidad de contar con estructuras gubernamentales que permitan gestionar los nuevos problemas del desarrollo humano, dentro de los cuales las políticas de inclusión digital, acceso a la sociedad de la información e innovación requieren de una infraestructura tecnológica de la administración ágil y eficiente, de la cual forma parte la Infraestructura de Firma Digital. (SCHWEINHEIM, 2010: 23)

A tal fin, entendemos que resulta conveniente fortalecer la capacidad de la Infraestructura de Firma Digital mediante su completa institucionalización, dotándola de una estructura propia, una burocracia profesional que pueda desplegar una carrera administrativa y ser evaluada por resultados concretos de gestión, y por supuesto, de los recursos económicos y tecnológicos necesarios para el cabal cumplimiento de sus funciones.

Pero también la investigación nos ha conducido a una visión general crítica sobre el potencial de la firma digital. Pareciera ser que el futuro no traerá más desarrollo de la firma digital como herramienta de autenticación electrónica, sino que han aparecido otras tecnologías que brindan seguridad y confianza similares, como

la biometría, la criptografía simétrica, la explosiva expansión de la telefonía celular, etc.

En ese sentido, estamos convencidos que nuestro país debería adherir a la Convención de Naciones Unidas sobre Comunicaciones Electrónicas, la cual le permitiría ampliar el marco de validez de las transacciones electrónicas por fuera de las fronteras nacionales, y además, privilegiaría el uso de mecanismos de autenticación digital más sencillos que la firma digital.

La presente tesis aspira a constituir un aporte para la discusión que permita comprender el escaso grado de institucionalización que alcanzó la Infraestructura de Firma Digital en Argentina en sus 10 años de vida, y proponer medidas que promuevan el desarrollo del gobierno y comercio electrónicos y la inclusión digital masiva para su uso.

IX.- BIBLIOGRAFÍA

Se señala a continuación la bibliografía consultada, tanto la referida a los aspectos sustantivos de la investigación como la que versa sobre las cuestiones metodológicas.

ADAMS, C., JUST, M. (2004): **"PKI: ten years later"**, University of Ottawa, 3er. Annual PKI R&D Workshop, NIST, Abril 2004, Gaithersburg, MD., USA. Disponible en Internet en http://middleware.internet2.edu/pki04/proceedings/pki_ten_years.pdf. Accedido Mayo 2010.

AUDITORÍA GENERAL DE LA NACIÓN (2008): Informe de Auditoría sobre la Infraestructura de Firma Digital, 2008. Disponible en Internet en http://www.agn.gov.ar/informes/informesPDF2008/2008_152.PDF. Accedido noviembre 2009.

BUGONI, M. y RIVOLTA, M. (2007): **"e-autenticación. Firma Digital y Firma Electrónica. Panorama en la República Argentina"**, Observatorio de Políticas Públicas de la Jefatura de Gabinete de Ministros, Buenos Aires, Septiembre 2007.

BURR, W., POLK, T. Y DODSON, D. (2006): **"Electronic Authentication Guideline"**, NIST Special Publication 800-63, Versión 1.0.2, National Institute of Standards and Technology, US Department of Commerce, Abril 2006. Disponible en Internet en http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf. Accedido Mayo 2010.

CLAD (1999), **"Una nueva gestión pública para América Latina"**, disponible en Internet en http://unpan1.un.org/intradoc/groups/public/documents/CLAD/UNPAN000161.pdf Accedido Julio 2010

CLAD (CENTRO LATINOAMERICANO DE ADMINISTRACION PARA EL DESARROLLO) (2007): "Carta Iberoamericana de Gobierno Electrónico", Pucón, Chile, 2007. Disponible en Internet en http://www.clad.org/documentos/declaraciones/cartagobelec.pdf. Accedido Mayo 2010.

CLARKE, R. (2001): **"The re-invention of Public Key Infrastructure"**, Australian National University, 2001. Disponible en internet en http://www.rogerclarke.com/EC/PKIReinv.html. Accedido Mayo 2010.

COMMISION OF THE EUROPEAN COMMUNITIES (2006): **"Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures"**, Bruselas, 2006. Disponible en internet en http://ec.europa.eu/information_society/eeurope/i2010/docs/single_info_space/com_electronic_signatures_report_en.pdf. Accedido Mayo 2010.

COSENTINO, G.: "**Aplicación de la firma digital en el ámbito de la Justicia**", Foro Patagónico de los Superiores Tribunales de Justicia, accesible en Internet en http://www.sup-trib-delsur.gov.ar/ForoPatagonico/DoctrinaJuridicaPatagonica0.htm. Accedido Julio 2010.

DOYLE, P., HANNA, S. (2003): **"Analysis of June 2003 Survey on Obstacles to PKI Deployment and Usage"**, informe del OASIS PKI Technical Committee, v1.0, 8 August 2003. Disponible en Internet en http://www.oasis-open.org/committees/pki/pkiobstaclesjune2003surveyreport.pdf. Accedido Mayo 2010.

ELLISON, C., SCHNEIER, B. (2000): "**Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure**", Computer Security Journal, vol.XVI, no.1, 2000.

FISCHER-DIESKAU, S., WILKE, D. (2006): **"Electronically signed documents: legal requirements and measures for their long-term conservation"**, Digital Evidence Journal, Vol. 3 number one, London, UK, 2006.

GASSON, M.; MEINTS, M.; WARWICK, K. (2005): **"D3.2: A study on PKI and biometrics"**, FIDIS Consortium (Future of Identity in the Information society), Julio 2005, European Union. Disponible en Internet en http://fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.2.study_on_PKI_and_biometrics.pdf. Accedido Mayo 2010.

GUTMANN, P. (2002): **"PKI: It's Not Dead, Just Resting"**, IEEE Computer, August 2002; Disponible en internet en: http://www.cs.auckland.ac.nz/~pgut001/pubs/notdead.pdf. Accedido Mayo 2010.

HAMMER, M. (1990): **"Reengineering Work: Don't Automate, Obliterate"**, en Harvard Business Review (July-August), 1990, p. 104-112. Disponible en Internet en http://www3.uma.pt/filipejmsousa/ge/Hammer,%201990.pdf. Accedido Mayo 2010.

HANNA, S. (2003): **"Analysis of August 2003 Follow-up Survey on Obstacles to PKI Deployment and Usage"**, Octubre 2003, OASIS. Disponible en Internet en http://www.oasis-open.org/committees/pki/pkiobstaclesjune2003surveyreport.pdf. Accedido Mayo 2010.

HEADY, F. : **"Administración Pública. Una perspectiva comparada"**, Méjico, FCE. Estudio Introductorio de Víctor Alarcón Olguín y Capítulo II – Enfoque Comparativo.

JEFATURA DE GABINETE DE MINISTROS (2001), **"Proyecto de Macroestructura para el Poder Ejecutivo Nacional"**, Secretaría para la Modernización del Estado, Octubre 2001.

JONES, L. (2000): "**Learning from experience with New Public Management**", International Public Management Journal, disponible en internet en http://www.ipmn.net/content/view/45/32/. Accedido Julio 2010.

JONES, L. y THOMPSON, A. (1999): **"Un modelo para la nueva gerencia pública: lecciones de la reforma de los sectores público y privado"**, Revista del CLAD Reforma y Democracia Nro. 15, Octubre 1999, Caracas.

KUHN, R.; HU, V.; POLK, T. y CHAN, S. (2001): **"Introduction to Public Key Technology and the Federal PKI Infraestructure"**, National Institute of Standards and Technology, NIST, USA, Febrero 2001. Disponible en Internet en http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf. Accedido Mayo 2010.

KLIKSBERG, B. (2000): **"Una nueva gerencia pública para la modernización del Estado y afrontar los desafíos de la integración".** 2000. Disponible en Internet en http://www.pnfa.org/lecturas/Gerencia%20Publica%20Nuevos%20Desafios.doc. Accedido septiembre 2009.

KOORN, R. (2002): **"Auditing and Certification of a Public Key Infraestructure"**, *Information Systems Control Journal*, Volume 5, 2002, disponible en Internet en http://www.isaca.org/Content/ContentGroups/Bookstore6/Study_aid_corrections/v5-02p28-31.pdf. Accedido Mayo 2010.

LORENZETTI, R. (2001): **"Comercio Electrónico. Documento, firma digital, contratos, daños, defensa del consumidor"**, Cap.I, p. 52, Editorial Abeledo Perrot, Buenos Aires, mayo 2001.

MALDONADO, T. (1998): **"Crítica de la razón informática",** Ed. Paidós, 1998.

MARTA, W., PRANDINI, P. y RIVOLTA, M. (2003): **"Análisis Legislación Actual y Mejores Prácticas Internacionales sobre PKI",** Instituto Dominicano de las Telecomunicaciones Indotel, República Dominicana, 2003. Disponible en internet en http://www.indotel.gob.do/component/option,com_docman/task,doc_view/gid,190/out.html Accedido en julio 2010.

MARRADI, A. y otros (2007): **"Metodología de las Ciencias Sociales"**, Buenos Aires, Emecé, 2007.

MASON, S. (2006): **"Electronic Signatures in Practice"** Journal of High Technology Law, Volume 6, Number 2, 148 – 164. J. High Tech L. 148 Disponible en Internet en http://www.jhtl.org/docs/pdf/Mason.pdf. Accedido Julio 2010.

MOLLOY, S. (1995): **"The Effects of Information Technology on Strategic Decision Making"**, Journal of Management Studies 32:3, May 1995: 283-311.

MULLER, P. (2006): **"Las políticas públicas"**, Edit. Externado de Colombia, 2ª edición, 2006.

NAVARRO ISLA, J. (compilador) (2005): **"Tecnologías de la Información y de las Comunicaciones: aspectos legales"**, Editorial Porrúa México, 2005.

OASIS (2004): **"PKI Action Plan"**, Disponible en internet en http://www.oasis-open.org/committees/pki/pkiactionplan.pdf. Accedido Agosto 2010.

OECD (2007) ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT **"OECD Recomendation on Electronic Authentication and OECD Guidance for Electronic Authentication"**, 2007. Disponible en Internet en http://www.oecd.org/dataoecd/32/45/38921342.pdf. Accedido Mayo 2010.

OSZLAK, O. (1980): **"Estado, planificación y burocracia: los "procesos de implementación" de políticas públicas en algunas experiencias latinoamericanas"**, Revista de Administración Pública. Publicación Conmemorativa del 25 aniversario del INAP, México, 1955-1980, Número Especial, Méjico DF, 1980.

OSZLAK, O. y ORELLANA, E. (1999), **"El análisis de la capacidad institucional: aplicación de la metodología SADCI"**, 1999, Biblioteca Virtual TOP, Disponible en Internet en http://www.top.org.ar/Documentos/ . Accedido Septiembre 2009.

OSZLAK, O.; MALVICINO, G.; HINTZE, J.; GRAZIANO, R. (2001): **"Nuevos modelos institucionales para la gestión pública: experiencias comparadas y aplicaciones potenciales al caso argentino"**. Programa de Modernización del Estado, Jefatura de Gabinete de Ministros, Buenos Aires, Marzo 2001.

OSZLAK, O. (2003), **"Escasez de recursos o escasez de innovación?: la reforma estatal argentina en las últimas dos décadas"**, Ponencia presentada en el VIII Congreso Internacional del CLAD sobre la Reforma del Estado y de la Administración Pública, Panamá, 28-31 Oct. 2003. Disponible en Internet en http://unpan1.un.org/intradoc/groups/public/documents/CLAD/clad0047320.pdf. Accedido junio 2010.

OSZLAK, O. (2005): **"Políticas sectoriales, transformación estatal y gobernabilidad en la Argentina: de Menem a Kirchner"**, ponencia presentada en el X Congreso Internacional del CLAD sobre la Reforma del Estado y de la Administración Pública, Santiago, Chile, 18 - 21 Oct. 2005. Disponible en Internet en http://www.iij.derecho.ucr.ac.cr/archivos/documentacion/inv%20otras%20entidades/CLAD/CLAD%20X/documentos/oszlakos.pdf. Accedido Julio 2010.

PANEBIANCO, A. (1991): **"Comparación y explicación"**, en SARTORI, Giovani et al, "La comparación en las ciencias sociales", Alianza Editorial, Madrid, 1991.

PEREZ SEDEÑO, E. (2008): ***"Ciencia y Tecnología en sociedades auténticamente democráticas"***, CIENCIA, TECNOLOGIA Y SOCIEDAD – Ponencias del Seminario realizado en Agosto 2008 organizado por el Centro Cultural de España, Montevideo, Septiembre 2008. Pág. 10-35

REYES KRAFT, A. A. (2005): ***"El derecho como impulsor del comercio electrónico en Méjico"***, en "Tecnologías de la Información y de las Comunicaciones: Aspectos Legales", Coordinado por Jorge Navarro Isla, Editorial Porrúa, Méjico, 2005.

RIVOLTA, M. y PRANDINI, P. (2002), **"Argentine Public Key Infrastructure Development – a comparative study of PKI experiences in Latin America"**, Abril 2002, Internet Society.

RIVOLTA, M. y SCHAPPER, P. (2004): "**Authentication & Digital Signatures in E-Law and Security - A Guide for Legislators and Managers**", Diciembre 2004, Procurement Harmonization Project of The Asian Development Bank, The Inter-American Development Bank and The World Bank. Disponible en internet en http://idbdocs.iadb.org/wsdocs/getdocument.aspx?docnum=645472
Accedido Mayo 2010.

RIVOLTA, M., SCHAPPER, P. y LEIPOLD, K. (2005): **"Authentication: International Scope and Non Discrimination in Government Commerce vs. PKI"**, e-Signature Law Journal, Vol. 2 number 2, London, UK, 2005.

RIVOLTA, M., SCHAPPER, P. y VEIGA MALTA, J. (2006): **"Risk and Law in Authentication"**, Digital Evidence Journal, Vol 3 number 1, London, UK, 2006.

RIVOLTA, M. y SLUCKI, D. (2004): **"e-compras públicas en Argentina"**, Revista Gobierno Digital, Buenos Aires, Octubre 2004, disponible en línea en http://www.gobiernodigital.org.ar/archivos/15-Panorama%20de%20Arg%20(64-77).pdf

RIVOLTA, M. (2007): **"Medios de prueba electrónicos: estado de avance en la legislación argentina"**, ponencia presentada en el IV Congreso de Administración Pública, Buenos Aires, Agosto 2007. Disponible en Internet en www.aaeap.org.ar/ponencias/congreso4/.../**Rivolta**,%20Mercedes.doc. Accedida marzo 2010

RIVOLTA, M. y FRAGA, P. (2007): **"Valor legal de las transacciones digitales: firma digital, firma electrónica y documento electrónico"**, Buenos Aires, elDial, Agosto 2007.

RIVOLTA, M. y SA ZEICHEN, G. (2007): **"El correo electrónico. Algunas notas acerca de su valor probatorio y su acreditación en juicio a propósito de un fallo"**, Buenos Aires, El Dial, Julio 2007. Disponible en línea en http://www.eldial.com/eldialexpress/tcd.asp?vengode=fr&id_publicar=&fecha_publicar=11/07/2007&numero_edicion=2321&titulo_rojo=Jurisprudencia%20-%20Comentario%20a%20Fallo&id=3016

RIVOLTA, M. y FRAGA, P. (2008): **Capítulo Argentino para el libro "International Electronic Evidence** (British Institute of International and Comparative Law, 2008) *1002pp* ISBN 978-1-905221-29-5, compilador Dr. Stephen Mason, London, UK.

RIVOLTA, M. (2008): **"Leyes de 3ª generación: hacia el pleno reconocimiento del derecho a la administración electrónica"**. Ponencia presentada en el XIII Congreso del CLAD para la reforma del Estado y de la Administración, Buenos Aires, noviembre 2008.

RODRIGUEZ GUSTA, A. L.: **"La comparación de casos y el estudio de la gerencia pública: cronología de un trabajo de campo"**, Centro de Estudios en Desarrollo y Territorio, Escuela de Política y Gobierno, Universidad Nacional de San Martín, Argentina.

RODRIGUEZ GUSTA, A. L., Ph D: ***"La transversalización de género en Chile: la "división digital" entre las burocracias expertas y los espacios deliberativos"***. CIENCIA, TECNOLOGIA Y SOCIEDAD – Ponencias del Seminario realizado en Agosto 2008 organizado por el Centro Cultural de España, Montevideo, Septiembre 2008.

SARTORI, G. (1991): **"Comparación y método comparativo"**, en "La comparación en las ciencias sociales" Madrid, Alianza, 1991.

SCHMUKLER, R. (2002): **"Public Administration Theory as Musical Theory"**, Administrative Theory and Praxis, Vol. 24, N° 3, 2002.

SCHWEINHEIM, G.F.F. (2003):**¿Podría una institucionalidad administrativa republicana contribuir a la transición política después de una crisis? Lecciones de la República Argentina"**, Revista del CLAD Reforma y Democracia, N° 27, Octubre 2003, Caracas. Disponible en Internet en http://www.clad.org/portal/publicaciones-del-clad/revista-clad-reforma-democracia/articulos/027-octubre-2003/0047121. Accedido Abril 2010.

SCHWEINHEIM, G.F.F. (2007): **"Reivindicación del populismo, demandas republicanas y construcción institucional del Estado"**, Ponencia presentada en el IV Congreso Argentino de Administración Pública "Sociedad, Gobierno y Administración", Buenos Aires, Agosto 2007. Disponible en Internet en http://www.asociacionag.org.ar/congreso-de-administracion-publica/cuarto-congreso/paneles-y-ponencias4/. Accedido Mayo 2010.

SCHWEINHEIM, G.F.F. (2008): **"La institucionalización de sistemas administrativos y el incremento de la capacidad de gobierno democrático"**, XIII Congreso Internacional del CLAD sobre la Reforma del Estado y de la Administración Pública, Buenos Aires, Argentina, Noviembre 2008. Disponible en Internet en http://www.mp.gov.br/hotsites/seges/clad/documentos/schweinh.pdf. Accedido Abril 2010.

SCHWEINHEIM, G.F.F. (2009): **"Desafíos provinciales en materia de gestión pública: aprendizajes a partir de la experiencia nacional"**, Ponencia presentada en el V Congreso Argentino de Administración Pública "Sociedad, Gobierno y Administración", San Juan, mayo 2009. Disponible en Internet en http://www.congresoap.gov.ar/sitio/docs/ponencias/S/Schweinheim.pdf. Accedido Mayo 2010.

SCHWEINHEIM, G.F.F. (2010): **"Estado, Administración y Desarrollo. Contribución a un paradigma de investigación y políticas estatales para un nuevo desarrollo en América Latina"**, Revista Aportes, Buenos Aires, 2010. En prensa.

SINGH, S. (2000): **"Los códigos secretos. El arte y la ciencia de la criptografía, desde el antiguo Egipto a la era de Internet"**, Editorial Debate, Madrid, 2000.

TELLEZ VALDÉS, J. (2004): **"Derecho Informático"**, Ed. Mc.Graw Hill, 3ª edición, México, 2004.

THOENING, J-C. (2006): **"El rescate de la publicness en los estudios de la organización"**, Revista Gestión y Política Pública, Volumen XV, Número 2, II semestre 2006.

TEMBOURY REDONDO, M; FERRARI, A. (2006), **"La Sociedad de la Información en la Argentina. Presente y Perspectivas 2004 – 2006"**, Fundación Telefónica, Buenos Aires.

UNCITRAL (1999): **"Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al derecho interno 1996"**, Naciones Unidas, Nueva York 1999. Disponible en Internet en http://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf. Accedida Julio 2010.

UNCITRAL (2001): **"Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno 2001"**, Naciones Unidas, Nueva Cork, 2002. Disponible en Internet en http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf. Accedida Julio 2010.

UNCITRAL (2006): **"Informe sobre Revisión de la Ley Modelo de Contratación Pública de Bienes, Obras y Servicios"**, fruto del 10º Período de sesiones, Grupo de Trabajo I, Naciones Unidas, Viena, Septiembre 2006. Disponible en línea en http://daccessdds.un.org/doc/UNDOC/LTD/V06/550/91/PDF/V0655091.pdf?OpenElement. Accedido Julio 2010.

UNCITRAL (2007): **"Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en Contratos Internacionales"**, Naciones Unidas, Nueva York, 2007. Accedido Junio 2010. Disponible en Internet en http://www.uncitral.org/pdf/spanish/texts/electcom/06-57455_Ebook.pdf

UNCITRAL (2009): **"Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica"**, Naciones Unidas, Viena, 2009. Disponible en Internet en http://www.uncitral.org/pdf/spanish/publications/sales_publications/Promoting_confidenceS.pdf. Accedido Mayo 2010.

WEBER, M.: **"Economía y Sociedad. Esbozo de sociología comprensiva"**, 1ª edición 1922, Méjico, FCE, Tomo II, páginas 730-738.

ANEXO I - ASPECTOS METODOLOGICOS

En un primer momento se consideró la posibilidad de realizar un estudio comparado de distintas PKI. Finalmente, se llegó a la conclusión que dada su extrema complejidad se dificultaba la alternativa del caso comparado. Se determinó realizar un estudio de caso sobre la PKI argentina, pero que en realidad en cierta manera es un caso comparado con su antecedente inmediato argentino, la PKI del sector público. En cierta medida, he confirmado adecuadamente el enfoque a partir de SARTORI, en el sentido de que el caso elegido "resulta útil para generar hipótesis o porque es crucial a la hora de confirmar o no confirmar una teoría" (SARTORI, 45). Este caso entiendo que cumple ambos aspectos, ya que permitirá elaborar una hipótesis en relación con el uso de la firma digital, cuyos problemas se han presentado en otros países, y con la encuesta se intentará verificar las hipótesis.

El caso elegido, la PKI argentina, es implícitamente comparativo, por una parte, con su antecesora de 1998, y por la otra, en los distintos aspectos que se abordan para describir acabadamente los componentes de una PKI, se hace referencia a las normas jurídicas y tecnológicas internacionales. A su vez, se analizan antecedentes internacionales que intentan dar respuesta al estancamiento de la firma digital en Europa y el mundo, con lo cual de alguna manera si bien no se ha hecho explícitamente un estudio profundo comparado sobre las experiencias de cada país sobre firma digital, sí se han tomado las conclusiones de estudios comparados sobre la misma pregunta que nos formulamos, pero aplicada a otras realidades.

En este sentido, la investigación ha intentado hacer una comparación que permita asimilar y diferenciar en los límites (SARTORI, 35). Esto es, entre "entidades que poseen atributos en parte compartidos (similares) y en parte no compartidos (y declarados no comparables)" (SARTORI, 35). La comparación entre entidades dentro del país (cross country) será en relación con la PKI del Sector Público antecesora de la PKI nacional argentina, y la comparación entre países será multi-nivel, sin considerar las características internas de cada país, sino los resultados de estudios sobre los factores que pudieran representar un obstáculo para el desarrollo de la firma digital en forma global.

Dada la complejidad de la unidad de análisis, el esquema de investigación propuesto podría ser considerado como de "triangulación metodológica", con un enfoque cualitativo para el análisis de las variables (aspectos normativos, tecnológicos y gerenciales), y un enfoque cuantitativo para medir los resultados de la encuesta a expertos. (MARRADI, 45)

En cuanto a los alcances de la indagación sobre los factores, el trabajo ha intentado respetar el requisito básico de toda investigación: el que los conceptos, las variables, sean definidos con suficiente claridad para permitir que la investigación progrese (MERTON 1949) (MARRADI, 51). Esto es muy importante, pues el análisis de estas nuevas figuras vinculadas al gobierno electrónico, en general se realiza sólo desde una perspectiva. Los tecnólogos abordan los aspectos informáticos, los abogados, los jurídicos. Existe escaso desarrollo teórico desde la ciencia de la administración. La presente investigación ha abordado los tres factores que integran

una Infraestructura de Firma Digital, lo cual representa el elemento novedoso, a fin de brindar un panorama amplio sobre la problemática.

Aspectos teóricos sobre gerencia pública

La investigación incorporó un factor adicional vinculado con aspectos de gerencia pública, denominados "factores organizacionales administrativos". Este factor se desarrolló debido a la insuficiencia de los factores normativos y tecnológicos para explicar el escaso desarrollo de la firma digital. Identificado como un factor relevante, vinculado con los aspectos organizacionales propios de una PKI, por una parte, y adicionalmente, abordando los aspectos organizacionales del órgano rector público. En tal sentido, la investigación intenta brindar un aporte novedoso con el fin de contextualizar a dicha organización pública, la Autoridad de Aplicación de Firma Digital, dentro del marco teórico de administración pública, desde la perspectiva de un sistema técnico administrativo.

Se analizó la jurisdicción responsable, a fin de poder identificar las principales características estructurales, relacionando con los modelos burocráticos señalados por HEADY (básicamente, la estructura organizativa y la asignación de funciones). En particular, las pautas de conducta por las cuales las burocracias se desvían del logro de sus objetivos legítimos, a fin de dar cuenta de los posibles factores que pudieran tener relevancia para explicar la demora de la masificación de la firma digital. Para formular el análisis de capacidad de gestión, se utilizó el sistema denominado SADCI – Sistema de Análisis de Capacidad Institucional. Esta metodología de análisis organizacional fue desarrollada por Alain Tobelem para el Banco Mundial.

Para el desarrollo de las hipótesis, se relevaron el marco regulatorio, los aspectos tecnológicos involucrados, los estándares de autenticación electrónica internacionalmente vigentes, así como los aspectos organizacionales contextualizados dentro de la teoría de administración pública.

Se describieron los elementos que componen una infraestructura de firma digital, a los fines de poder clarificar el objeto sobre el cual versa la investigación.

También, se hizo un repaso sobre los principales conceptos jurídicos involucrados en el tema, con similar propósito.

Como el uso de la firma digital es un componente presente en transacciones electrónicas globalizadas, se presentaron los principales enfoques internacionales.

Adicionalmente con la búsqueda por Internet de material sobre el tema, referido a estudios sobre infraestructuras de firma digital, de reconocidos expertos, se administró una encuesta, referida a los obstáculos para la masificación de la firma digital, que se describe más adelante.

Por último, el trabajo intentó interrelacionar las variables entre sí a fin de lograr la verificación o refutación de cada una de las hipótesis.

Recorte del objeto o problema de investigación.

La presente investigación se propuso identificar algunos factores que estarían rezagando el uso masivo de la firma digital en la Argentina, de acuerdo con la percepción de expertos en el tema.

La unidad de análisis del proyecto de investigación es la Infraestructura de Firma Digital de la República Argentina. Una infraestructura de firma digital es el conjunto de hardware, software, normas, personas y procesos que interactúan para conformar un sistema de autenticación electrónica específico, en un país determinado.

La presente investigación se propuso realizar un estudio de caso referido a la firma digital en la República Argentina, dentro del período comprendido desde 1997, momento en el cual nace la primera norma argentina en la materia, hasta noviembre de 2009.

Planteo de los objetivos del trabajo

Objetivo General

El **objetivo general** de la investigación es indagar la incidencia de los factores tecnológicos, normativos y organizacionales de la Infraestructura de Firma Digital Argentina en el escaso desarrollo de su uso masivo.

Objetivos específicos

Son **objetivos específicos**:

a.- Identificar y describir los **factores tecnológicos** inherentes a la firma digital:

a.1.- Presentar en forma breve y accesible los conceptos de criptografía simétrica y asimétrica y tecnología de clave pública, subyacentes en la firma digital.

a.2.- Describir sencillamente el proceso de firma digital de un documento electrónico.

a.3.- Identificar y describir en forma accesible los principales componentes técnicos de una Infraestructura de Firma Digital: Autoridades de Certificación, Autoridades de Registro, certificados digitales, listas de certificados, etc.

a.4.- Identificar los principales usos de la tecnología de clave pública: confidencialidad, seguridad, autenticación, conservación de documentos.

a.5.- Describir mecanismos de autenticación en entornos electrónicos alternativos.

b.- Identificar y describir los **factores normativos** vinculados a la firma digital:

b.1.- A nivel Nacional:

b.1.1.- Relevar el marco jurídico de la firma digital, esto es, las leyes, decretos y resoluciones que regulan el uso de la firma digital en nuestro país, así como las normas que otorgan competencia a los órganos públicos en materia de firma digital. Comprende tanto la regulación de carácter nacional como las regulaciones provinciales, identificando los alcances respectivos.

b.1.2.- Explicar brevemente el concepto de documento electrónico y firma electrónica y su virtualidad jurídica en el derecho argentino.

b.1.3.- Identificar las presunciones legales asociadas a la firma digital y a la firma electrónica presentes en la normativa argentina.

b.2.- A nivel Internacional: relevar el marco normativo internacional: Antecedentes de organismos multilaterales: UNCITRAL, Bancos Multilaterales de Desarrollo (Banco Mundial, Banco Interamericano de Desarrollo, Banco de Desarrollo Asiático). Detectar normas supranacionales, acuerdos regionales, esquemas de reconocimiento de certificados digitales entre países, si existieren.

c.- Identificar y describir los **factores organizacionales** relacionados con la firma digital:

c.1.- Identificar y describir los componentes específicos de una Infraestructura de Firma Digital: Autoridad Certificante Raíz, Entidades de Certificación, Autoridades de Registro, usuarios, terceros, entidades de auditoría.

c.2.- Identificar las organizaciones públicas de la Administración Nacional que cumplen roles relevantes en materia de firma digital.

c.3.- Analizar la evolución de la estructura orgánico funcional de la autoridad de aplicación de firma digital en la Argentina.

d.- Analizar la **incidencia de los factores** tecnológicos, normativos y organizacionales en el escaso desarrollo del uso masivo de la firma digital.

d.1.- Describir la posible incidencia de cada uno de los distintos factores en el escaso desarrollo del uso masivo de la firma digital.

d.2.- Obtener datos cuantitativos que permitan medir la incidencia de los distintos factores a partir de una encuesta a expertos en el tema.

Obtención de datos

Bibliografía e Internet

Se utilizaron múltiples fuentes de información para el desarrollo de la investigación. Se recopiló material bibliográfico (ver el Capítulo Bibliografía), así como material obtenido en Internet en sitios especializados.

Además de la información mencionada, se realizó una encuesta a expertos a fin de obtener datos medibles que permitieran dar cuenta de los posibles factores que estarían rezagando el uso masivo de la firma digital en Argentina. El envío y recepción del formulario de la encuesta se efectuó mediante correo electrónico.

Encuesta

La encuesta de la investigación se hizo a partir de otra, previa, de carácter internacional realizada en el año 2003 relativa a los obstáculos para la implementación de una Infraestructura de Firma Digital. Dicha encuesta fue realizada por el Comité Técnico de la Sección PKI de OASIS.

La Sección Infraestructura Firma Digital – PKI por sus siglas en inglés- de OASIS fue creada en 1999 para apoyar las iniciativas tendientes a desarrollar PKI basadas en estándares interoperables, como fundamento para transacciones seguras en aplicaciones de comercio electrónico. Sus miembros pertenecen a empresas, organismos del Estado, Universidades, y despliegan su actividad de manera colaborativa en un ambiente neutral, con el propósito de incrementar los conocimientos sobre PKI e iniciar estudios y proyectos que demuestren el valor de una PKI interoperable y de las soluciones basadas en PKI.

OASIS (Organization for the Advancement of Structured Information Standards) es una organizacion sin fines de lucro que impulsa el desarrollo, convergencia y adopción de estándares abiertos para la sociedad global de la información. Fundada en 1993, OASIS cuenta con más de 5000 participantes que representan más de 600 organizaciones y miembros individuales en 100 países.

La encuesta realizada por OASIS se administró desde su página web, orientada al público en general, logró una muestra de 217 respuestas. Los resultados de la encuesta resultaron altamente esclarecedores respecto de los obstáculos que los usuarios consideran que impiden el desarrollo de PKI.

La idea fue reproducir esta encuesta de OASIS, con un agregado específico para el caso argentino, de modo de poder realizar comparaciones entre ambos resultados. La encuesta argentina se distribuyó por correo electrónico, entre las personas del sector público y privado que están trabajando en el tema de gobierno digital, comercio electrónico y firma digital. Asimismo, se circuló entre expertos internacionales que podían o no completar la sección especifica del caso argentino. Se distribuyeron versiones en español e inglés.

La encuesta no es totalmente cerrada, enumera una cantidad de motivos que podrían ser considerados obstáculos, pero incluye un ítem "otros" en el cual el encuestado puede incluir otros aspectos que no hayan sido considerados.

Se adjunta el formulario de la encuesta realizada como Anexo II.

ANEXO II - FORMULARIO DE LA ENCUESTA

"OBSTACULOS PARA EL DESARROLLO DE LA INFRAESTRUCTURA DE FIRMA DIGITAL - PKI - ARGENTINA"

La presente encuesta forma parte del trabajo de investigación de la AG Dra. Mercedes Rivolta para la Maestría en Administración Pública de la Facultad de Ciencias Económicas de la Universidad de Buenos Aires. La investigación se propone identificar los factores que estarían rezagando el uso masivo de la firma digital en Argentina, según la percepción de los expertos.

Se basa en la encuesta "Obstáculos para el Desarrollo de la PKI" que fue realizada en el año 2003 por OASIS (Organization for the Advancement of Structured Information Standards). OASIS es una organización sin fines de lucro que impulsa el desarrollo, convergencia y adopción de estándares abiertos para la sociedad global de la información. Fundada en 1993, OASIS cuenta con más de 5000 participantes que representan más de 600 organizaciones y miembros individuales en 100 países.

La idea es reproducir la misma encuesta para poder así tener una base de comparación con los resultados obtenidos en 2003, y agregando un capitulo específico para el caso argentino, que permita contextualizar la investigación.

Esta encuesta es confidencial y anónima. Es corta, no le llevará más de 20 minutos para ser completada. En general, es de multiple choice, pero admite texto explicativo. La 3ª sección de la encuesta (no prevista en la encuesta realizada por OASIS) se refiere al caso argentino. Para poder ser considerada, la encuesta debe ser completada en su totalidad.

La encuesta se enviará y recibirá por mail a la siguiente dirección: mercedesrivolta@yahoo.com.ar.

Será de gran ayuda que los expertos que hayan recibido la encuesta la circulen entre sus colegas, a fin de aumentar la muestra y lograr resultados más significativos.

Se asegura la confidencialidad de la encuesta. Los datos obtenidos se presentarán en forma agregada. El mail de contacto de los expertos que participen se conservará para invitarlos a participar en futuras actualizaciones de la encuesta, pero en forma totalmente independiente del formulario de la encuesta.

PARTICIPANTES DE LA ENCUESTA

La muestra de la presente encuesta incluye a toda persona que tenga alguna opinión en el tema, pero fundamentalmente, a quienes estén involucrados, tengan algún grado de expertise o experiencia en el área. En consecuencia, esta encuesta se focalizará en gerentes, funcionarios, personal y expertos en Tecnología de la Información y Comunicaciones (TIC) que hayan trabajado o estén considerando hacerlo en el futuro, en proyectos de PKI, gobierno electrónico, justicia electrónica, parlamento electrónico, comercio electrónico, compras electrónicas, autenticación

electrónica o similares. La muestra también intentará comprender a vendedores, proveedores, gerentes, expertos y personal de empresas de tecnología, así como abogados o consultores que hayan trabajado o realizado observaciones en dichas áreas.

FORMULARIO DE LA ENCUESTA
"OBSTACULOS PARA EL DESARROLLO DE LA INFRAESTRUCTURA DE FIRMA DIGITAL - PKI - ARGENTINA"

Por favor, completar marcando con una X en el casillero correspondiente. En las opciones "Otros" se podrá incluir texto explicativo.

SECCION I – PERFIL DE LA MUESTRA

A.- OCUPACION PRINCIPAL

Por favor, marque el casillero correspondiente a su función laboral principal.

- □ Gerente TIC
- □ Staff TIC
- □ Desarrollador de software
- □ Desarrollador de producto
- □ Investigador
- □ Gerente no TIC
- □ Auditor
- □ Abogado
- □ Otros

B.- ANTIGUEDAD EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

Por favor, marcar los años de experiencia en aspectos de seguridad y privacidad de la información.

- □ 1
- □ 2
- □ 3
- □ 4
- □ 5
- □ 6 a 10
- □ 11 a 15
- □ 16 o más
- □ No se aplica

C.- EXPERIENCIA EN PKI

Por favor, marque todas las categorías que se apliquen en su caso.

- □ Ha leído sobre PKI

- ☐ Ha considerado utilizar PKI
- ☐ Ha usado PKI
- ☐ Ha ayudado a desarrollar PKI
- ☐ Ha desarrollado software vinculado a PKI

D.- SECTOR O INDUSTRIA DEL EMPLEADOR

- ☐ Gobierno
- ☐ Industria (vinculada con TICs)
- ☐ Otros servicios
- ☐ Finanzas
- ☐ Educación
- ☐ Salud
- ☐ Ventas
- ☐ Industria (no vinculada con TICs)
- ☐ Otros

E.- TAMAÑO DEL EMPLEADOR (cantidad de empleados)

- ☐ 1 – 99
- ☐ 100 – 499
- ☐ 500 – 999
- ☐ 1000 – 9999
- ☐ 10000 o más

F.- REGION DE TRABAJO PRINCIPAL

Por favor, indique con una X la región en la cual desempeña su trabajo principal. Además, en "País" complete el país.

- ☐ Norte América
- ☐ Europa
- ☐ Asia
- ☐ Australia
- ☐ Sud y Central América
- ☐ Africa

País:

G.- ALCANCES DE SU INTERES POR PKI

Por favor, marque con una X en los casilleros correspondientes.

- ☐ Su interés se circunscribe a su país de trabajo principal.

- □ Su interés se extiende más allá de su país de trabajo principal.
- □ Su interés se circunscribe a su organización.
- □ Su interés se extiende más allá de su organización.

SECCION II.- VISION Y OPINIONES

A.- APLICACIONES PKI

Por favor, indique con una X en el casillero correspondiente, su opinión sobre las siguientes aplicaciones de PKI. En el casillero "Otros" podrá incluir otras aplicaciones no contempladas en la presente encuesta.

Aplicaciones	Más importante	Importante	No importante
Firmado de documentos			
Seguridad de servidores web			
Correo electrónico seguro			
Seguridad de Servicios Web			
Redes privadas virtuales			
Comercio Electrónico			
Single Sign On			
Seguridad para redes inalámbricas LAN			
Code signing			
Secure RPC			
Otras aplicaciones			

B.- OBSTACULOS PARA EL DESARROLLO Y USO DE PKI

Por favor, identifique y priorice los obstáculos para el desarrollo y uso de PKI. Este es el corazón de la encuesta! Complete con una X los casilleros correspondientes, según la valoración que Ud. asigne a cada obstáculo. Si considera necesario incluir otros obstáculos no incluidos en la encuesta, por favor especifique y detalle los mismos brevemente con texto en "Otros obstáculos".

Obstáculo	Obstáculo Máximo	Obstáculo Mínimo	No es un Obstáculo
Las aplicaciones de software no lo soportan			
Costos demasiado elevados			
PKI pobremente entendida			
Pobre interoperabilidad			
Difícil de iniciar – Demasiado compleja			

Difícil de manejar por usuarios finales			
Falta de soporte gerencial			
Requiere demasiado trabajo legal			
Difícil de mantener para TICs			
Otros obstáculos			

SECCION III.- MOTIVOS DEL ESCASO USO MASIVO DE LA FIRMA DIGITAL EN ARGENTINA

Por favor, identifique y priorice los factores que explican el escaso uso masivo de la firma digital en Argentina. Complete con una X los casilleros correspondientes, según la valoración que Ud. asigne a cada factor. Si considera necesario incluir otros factores no incluidos en la encuesta, por favor especifique y detalle los mismos brevemente con texto en "Otros factores".

Factores del escaso uso masivo	Máxima Incidencia	Mínima Incidencia	Irrelevante
Inadecuada normativa			
Inmadurez de estándares tecnológicos			
Inmadurez del mercado			
Escasas aplicaciones			
Insuficiente conectividad			
Escasa difusión			
Ente rector no exclusivo			
Otros factores (enumerar y ponderar)			

Muchas gracias por su tiempo y colaboración con esta encuesta!

Por favor remitir por correo electrónico a Mercedes Rivolta, mercedesrivolta@yahoo.com.ar

ANEXO III – PARTICIPANTES DE LA ENCUESTA

	Encuestado	Perfil
1	AAshish	Australia
2	Abalo Laforgia, Mónica	Presidente Isoc-Ar
3		
4	Anónimo	Ministerio Defensa - Informática
5	Ballart, Alicia	Administradora Gubernamental
6	Barthsh	
7	Belcastro, Susana	
8	Biaggio, Alejandro	Poder Judicial Chubut – Informática
9	Boccardo, Roberto	Banco de la Provincia de Buenos Aires, Informática
10	Capua, Luis	Anses
11	Caputi, Beatriz	PKI Argentina
12	Cofiño, Rodrigo	USA
13	Cosentino, Guillermo	Poder Judicial Chubut
14	Daoud	
15	Del Barco, José Luis	Universidad Litoral – Sistemas – Red Interconexión Universitaria
16	Díaz, Javier	Vicedecano Facultad Informática Universidad Nacional de La Plata
17	Dopazo, Fernando	Asesor Subsecretaría Tecnologías de Gestión
18	Duarte, Fernando	Administrador Gubernamental
19	Enciso, Natalia	Abogada experta TICs – Paraguay
20	Fernández Landoni, Jorge	Administrador Gubernamental
21	Fontdevila, Pablo	Gerente Sistemas Anses, Diputado Nacional MC autor ley firma digital
22	Fores	Fores – Poderes Judiciales
23	Franchino, Juan	Gerente Agencia Sistemas Información CABA, ex Subsecretario de Tecnologías de Información Nación
24	Franco	
25	Franco, Gastón	Coordinador ArCert – ONTI
26	Gómez, Nicolás	Oficina Anticorrupción – Argentina
27	González, Hugo	Administrador Gubernamental
28	Granero, Horacio	Director Carrera Derecho Alta Tecnología – UCA –
29	Guaglianone, Norberto	PKI argentina – ONTI
30	Guini, Leonor	PKI argentina – ONTI
31	Haddad, Sergio	ONTI
32	Herrera, Rafael	PKI argentina – ONTI
33	Jensen, Christian	Anses – ex asesor Diputado Fontdevila, coordinador del proyecto de ley de firma digital.
34	Julián	
35	Leipold, Knut	Banco Mundial, DC. Experto en contrataciones electrónicas
36	LaSerna, Diego	Director Sistemas Poder Judicial Córdoba

37	Rodríguez, Lionel	
38	Liserre, Fernando	ONTI
39	Mason, Stephen	Abogado especialista TICs, Editor revista firma electrónica, Londres, Gran Bretaña
40	Martino, Antonio	Abogado experto tecnologías. Italia
41	Melhman, Gabriel	Director Sistemas, Corte Suprema de Justicia de la Nacion – Consejo de la Magistratura
42	Rivolta, Mercedes	Administradora Gubernamental
43	Messano, Oscar	CABASE, Argentina
44	Molina Quiroga, Eduardo	Poder Judicial CABA
45	Otamendi, José María	Asesor Subsecretaría Tecnologías de Gestión
46	Pereira, Gustavo	
47	Poggi, Eduardo	AFIP
48	Prandini, Patricia	Directora Aplicaciones – ONTI
49	Prince, Alejandro	Presidente Prince and Cooke
50	Pujol, Gabriel	ONTI
51	Ramos, Silvia	Secretaría Gestión Pública – Proy. Modernización del Estado (Informática)
52	Romanos, Pablo	Experto seguridad informática
53	Roncoroni,	
54	Sa, Gustavo	Ministerio Público Fiscal CABA
55	Schapper, Paul	Universidad Curtin, Western Australia
56	Slucki, Diego	Economista de Gobierno - Ministerio de Justicia, Seguridad y Derechos Humanos
57	Solís	
58	Soriano, José	Agencia de Sistemas de Información – CABA
59	Souto, Jorge	Director del INDEC
60	Srur, Jorge	Especialista en gobierno electrónico – BID DC – USA
61	Tanuz, Rita	Administradora Gubernamental
62	Tate, Carlos	Corte Suprema de Justicia de la Nación, Seguridad informática
63	Thienemann, Jonathan	IBM
64	Valenti, Edmundo	Cabase – Argentina
65	Vallina, María	Administradora Gubernamental
66	Vazquez	
67	Veiga Malta, Joao	Especialista compras electrónicas, Banco Mundial, DC – USA
68	Velazquez, Gastón	Ecuador
69	Velázquez, Mercedes	Abogada especialista TICs
70	Vilches, César	Perú