VI CONGRESO ARGENTINO DE ADMINISTRACION PUBLICA

PANEL: "ADMINISTRACIÓN ELECTRÓNICA, INCLUSIÓN DIGITAL Y DERECHO"

COORDINADOR: Gabriel Casal - Jefe de Asesores Subsecretaría de Tecnologías de Gestión, Jefatura de Gabinete de Ministros de la Nación

PONENCIA: "Firma digital: instrumento para el desarrollo del gobierno electrónico"

Autora: Mercedes Rivolta
Administradora Gubernamental, Asesora del Subsecretario de Tecnologías de Gestión, Jefatura de Gabinete de Ministros de la Nación

Tabla de contenido

I.- INTRODUCCION

Los sistemas jurídicos nacionales han reconocido la validez de la firma electrónica, la firma digital y el documento electrónico. Estas normas constituyen el marco normativo básico para el gobierno electrónico. En la región se han adoptado, en general, esquemas basados en Infraestructuras de Clave Pública. Una Infraestructura de Firma Digital presenta tres componentes fundamentales: los técnicos vinculados con la tecnología de

clave pública, los jurídicos relacionados con el marco legal que habilita las transacciones electrónicas, y el tercer factor, el organizacional, que tiene que ver con los aspectos de gerencia pública aplicables a la institucionalización de estos organismos técnico administrativos.

Sin embargo, a 10 años de su reconocimiento, no se ha masificado el uso de la firma digital. La ponencia intenta responder al interrogante respecto de los motivos que pudieran explicar el escaso desarrollo de la firma digital en estos 10 años de vigencia. Fueron motivos tecnológicos asociados a la ausencia de estándares? Quizá una inadecuada normativa, o inconclusa? O se podría pensar que la organización funcional del organismo rector fue causante de esta demora? A fin de responder a estas cuestiones, se ha planteado una investigación que innova en el enfoque sobre el tema, al considerar simultáneamente los aspectos tecnológicos, jurídicos y organizacionales involucrados en la PKI argentina. La ponencia expone las conclusiones del estudio, y presenta los resultados de una encuesta que se realizó en el año 2009 a expertos acerca de los obstáculos para el desarrollo de la firma digital, basada en otra encuesta internacional formulada en 2003, a fin de poder comparar resultados.

Argentina fue pionero en firma digital. 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 no alcanzó gran masividad. Este trabajo presentará los factores que pudieran explicar los motivos de este estancamiento, según la opinión de expertos.

En 2008 realizamos un trabajo de investigación para la tesis de Maestría en Administración Pública de la Universidad de Buenos Aires, abordando el tema de la firma digital en la República Argentina desde tres perspectivas: la tecnológica, la jurídica y la organizacional-administrativa. Como parte de esa investigación, se administró una encuesta a expertos para identificar los posibles motivos que podrían incidir en el escaso uso de la firma digital. Esta ponencia expone los resultados de dicha encuesta.

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 Gabinete de la Jefatura de Gabinete de Ministros de la Nación.

Relevancia de la Investigación

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.

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).

El presente trabajo se ha apoyado en una encuesta internacional realizada por OASIS[1] 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. A tal fin, se administró una encuesta similar con el agregado de la situación en Argentina, cuyos resultados son presentados en la presente ponencia.

Por otra parte, se apoyó en una vasta exploración ya realizada previamente a fin de delinear tres enfoques sobre la unidad de análisis, la cual permitió identificar a priori tres posibles factores que podrían incidir en el escaso uso masivo de la firma digital:

- Factores tecnológicos.
- Factores normativos.
- Factores organizacionales – administrativos

El derecho acompaña la evolución tecnológica

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

[1] 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.

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[2] fueron aprobando leyes que complementan sus ordenamientos jurídicos vigentes y reconocen el

[2] 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

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.

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

---

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)).

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.

II.- 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. 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 tres autoridades certificantes de los organismos de recaudación tributaria y de seguridad social (AFIP y ANSES) y la Autoridad Certificante para la Administración Pública de la ONTI, y se encuentran en proceso de licenciamiento tres solicitudes del sector privado.

III.- ANALISIS DE LAS COMPLEJIDADES DE LA FIRMA DIGITAL

La extensión de la ponencia no permite entrar en detalle de los aspectos tecnológicos involucrados, pero es necesario clarificar algunos conceptos esenciales a fin de poder plantear la problemática.

Qué es una Infraestructura de Firma Digital

Una Infraestructura de Firma Digital, o PKI por sus siglas en inglés (Public Key Infraestructure) 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"* (KNOOR; 2000:1). 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.

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.

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.

Qué es una firma 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.

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 más claro.

Los estándares se refieren, entre otros, a los siguientes componentes:

- 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.

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.

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).

Se han identificado los siguientes aspectos que representan complejidades para el uso de la firma digital:

- **Relativas a la implementación de PKI**

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 (200 personas, de las cuales, el 95% tenían experiencia en el desarrollo de software para PKI) quienes identificaron los obstáculos específicos según su propio criterio. (DOYLE, HANNA; 2003)

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

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

- **Relativas a la interoperabilidad. Cross certificación, estructuras jerárquicas, acuerdos de reconocimiento.**

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

- 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....)

- **Relativas a la conservación de documentos**

Se han identificado los siguientes riesgos del uso de firma digital para conservación documental.

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 daría 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.

- **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. Qué ocurre con aquellas operaciones en las que las partes se encuentran en distintos países? 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.
- Mediante el reconocimiento formulado por una autoridad de certificación nacional.

Un **problema sustancial** se presenta con el requisito de presencia física para la emisión del certificado.

IV.- ENCUESTA A EXPERTOS

Se realizó una encuesta a expertos durante 2009, basada en una encuesta realizada por OASIS en 2003, con un agregado especìfico sobre la situación argentina. 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.

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 MC 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.

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.

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%).

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

VER CUADRO Nº 1 – OCUPACIÓN ENCUESTADOS
VER GRAFICO Nº 1 – OCUPACIÓN ENCUESTADOS

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.

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.

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

VER CUADRO Nº 2 – ANTIGÜEDAD EN EL TEMA DE ENCUESTADOS
VER GRAFICO Nº 2 – ANTIGÜEDAD EN EL TEMA DE ENCUESTADOS

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).

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)

VER CUADRO Nº 3 – SECTOR EMPLEADOR ENCUESTADOS
VER GRAFICO Nº 3 – SECTOR EMPLEADOR ENCUESTADOS

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.

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

VER CUADRO Nº 4 – TAMAÑO EMPLEADOR ENCUESTADOS
VER GRAFICO Nº 4 – TAMAÑO EMPLEADOR ENCUESTADOS

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.

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)

VER CUADRO Nº 5 – REGION DE TRABAJO PRINCIPAL
VER GRAFICO Nº 5 – REGION DE TRABAJO PRINCIPAL

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%).

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)

VER CUADRO Nº 6 – ALCANCES INTERES POR PKI
VER GRAFICO Nº 5 – ALCANCES INTERES POR PKI

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%).

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%

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.

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%

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 Encueta 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 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.

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%

V.- CONCLUSIONES

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 escasez de aplicaciones, alto costo, pobre entendimiento de PKI y problemas de interoperabilidad, han contribuido al uso limitado de PKI." (OASIS; 2004: 3). Similar conclusión se deriva de los resultados de la encuesta administrada en Argentina.

Adicionalmente, podemos citar las conclusiones referidas a la incidencia de los factores jurídicos, tecnológicos y organizacionales en la escasa masividad de la firma digital. Con relación a los factores jurídicos, compartimos la opinión de LORENZETTI sobre la neutralidad tecnológica de las leyes, es decir, que 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 Nº 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)

Si bien la Ley Nº 25.506 es producto de un determinado momento histórico, y de una experiencia pionera en la Administración Nacional, incluye también figuras más modernas como la validez jurídica del documento digital y la firma electrónica. De todas maneras, sería conveniente analizar la factibilidad de adecuar el marco legal a las nuevas tendencias internacionales, que son decididamente tecnológicamente neutras. Además, la actual reglamentación de la mencionada ley se encuentra inconclusa, quizá como consecuencia de lo dicho anteriormente.

En cuanto a los factores organizacionales, se aplican las restricciones propias de cualquier sistema técnico administrativo, es decir, cuál forma organizativa ideal debería adoptar un área del estado con funciones rectoras en materia tecnológica. La ciencia de la administración aún no ha podido dar una respuesta a esta cuestión. Pareciera ser que ni el esquema tradicional burocrático weberiano ni la nueva gerencia pública han dado respuesta a esta cuestión.

Respecto de los factores tecnológicos, se han mencionado algunos obstáculos para la masificación de la firma digital, tales como la inmadurez de estándares, la escasez de aplicaciones, la inmadurez del mercado, entre otros. Además, la aparición permanente de nuevas tecnologías que permiten autenticar a las personas en entornos digitales con igual grado de certeza. 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.

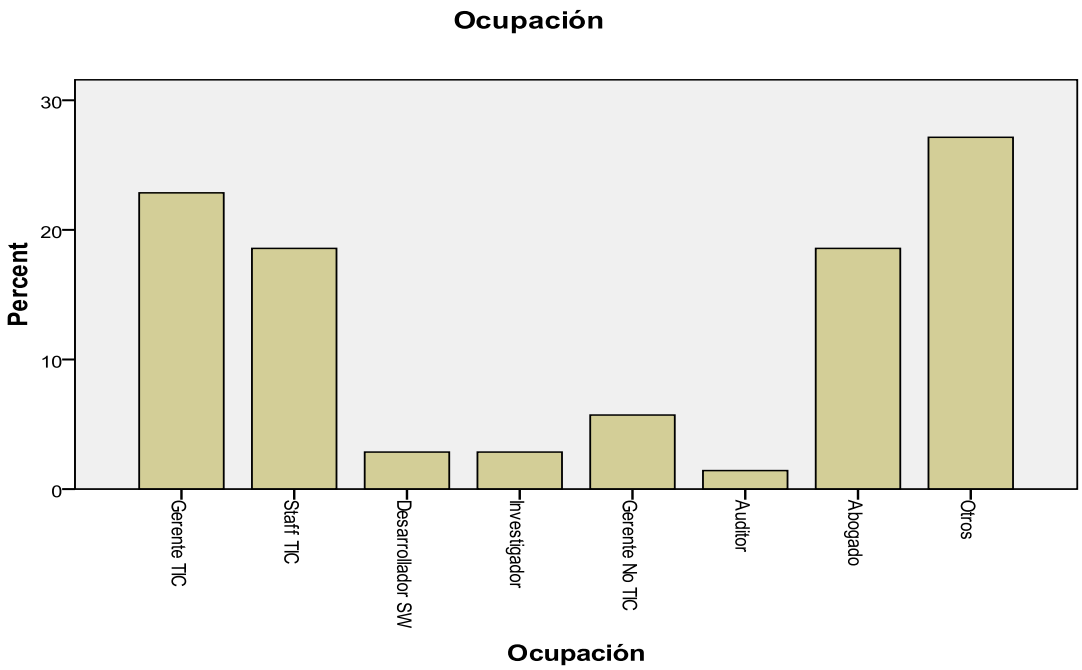
Estas tecnologías biométricas se aplican actualmente en políticas públicas vinculadas con la seguridad, el transporte fronterizo, y fundamentalmente, para la identificación de personas. Actualmente, los pasaportes incluyen biometría y están desarrollándose pasaportes electrónicos que cuentan con dispositivos 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 les permita identificarse 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.

VII.- CUADROS

CUADRO Nº 1 – OCUPACIÓN ENCUESTADOS

		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	

GRAFICO Nº 1.- OCUPACION ENCUESTADOS

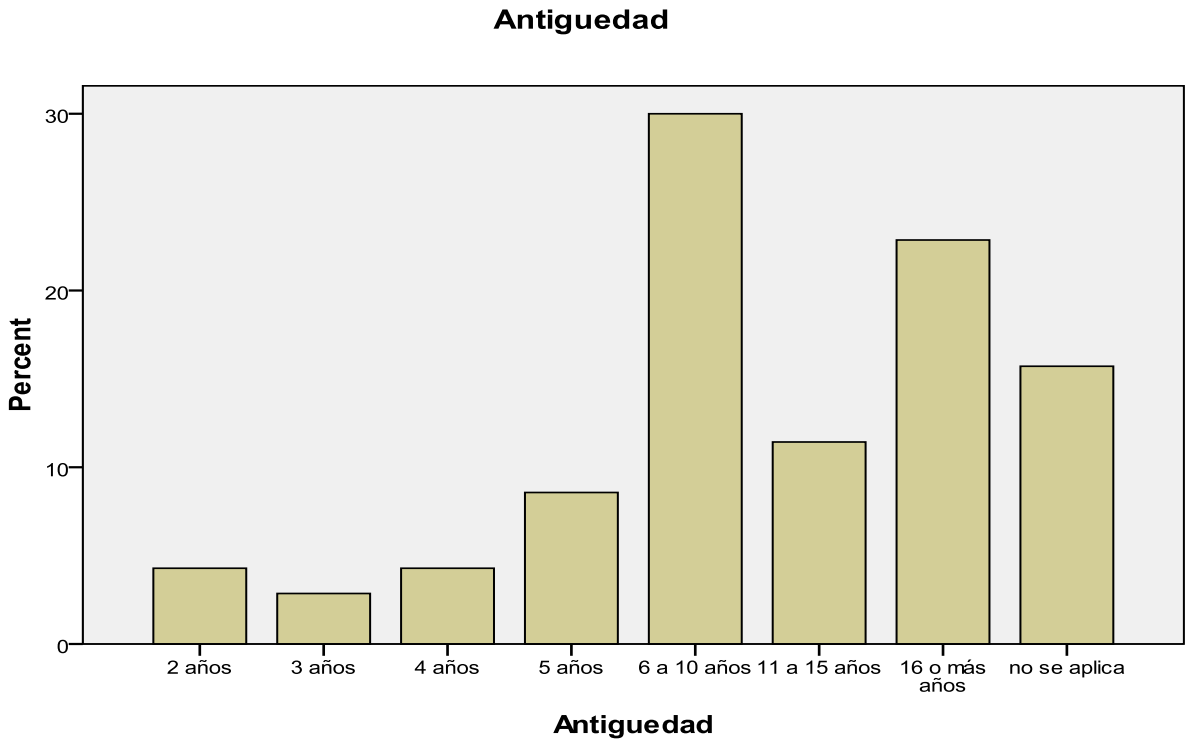


CUADRO Nº 2: ANTIGÜEDAD EN EL TEMA DE ENCUESTADOS

		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	

GRAFICO Nº 2: ANTIGÜEDAD EN EL TEMA DE ENCUESTADOS

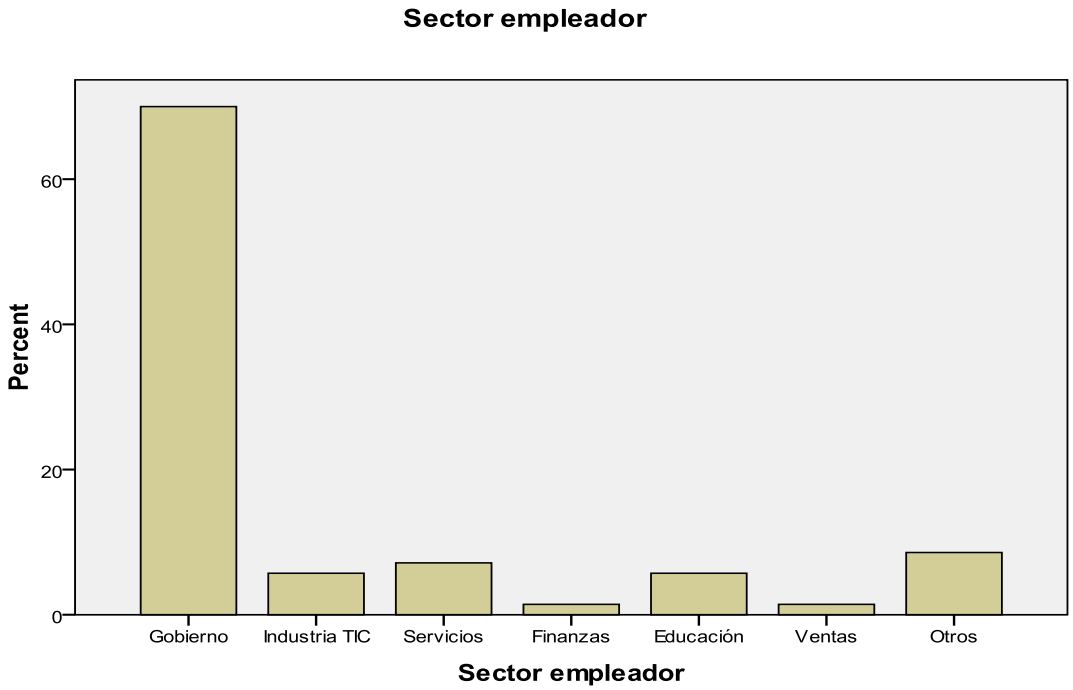


CUADRO Nº 3: SECTOR EMPLEADOR DE ENCUESTADOS

		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	

GRAFICO Nº 3: SECTOR EMPLEADOR ENCUESTADOS



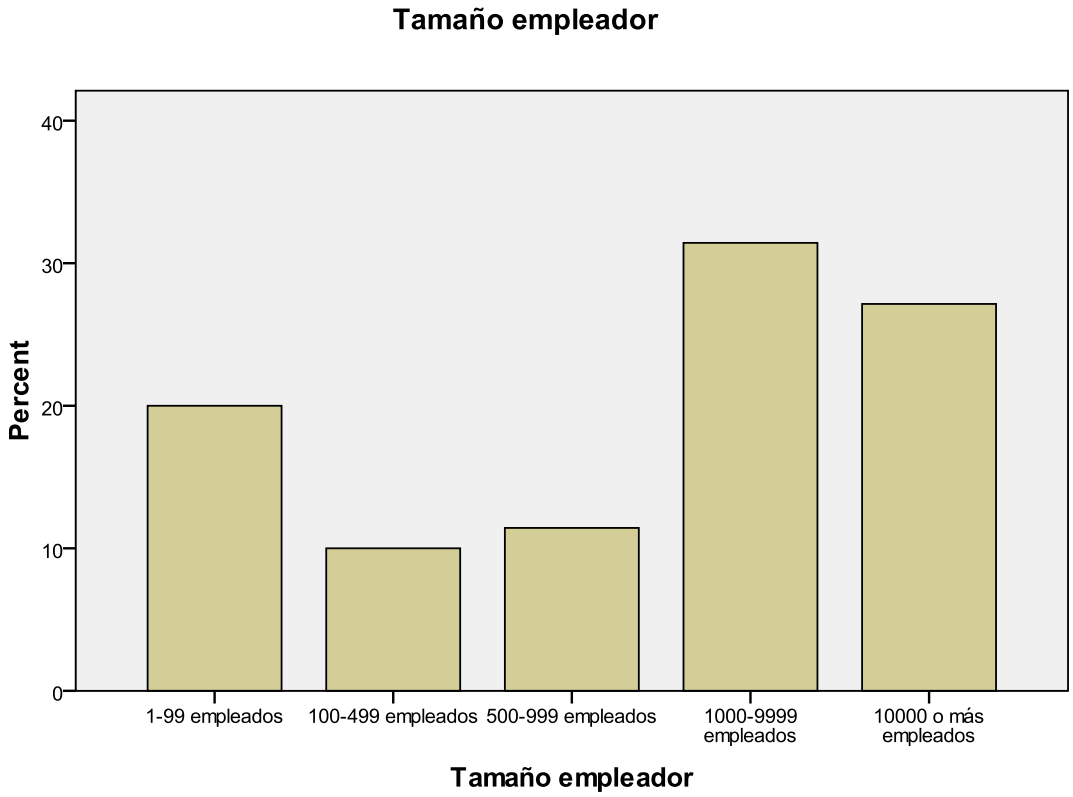
CUADRO Nº 4: TAMAÑO EMPLEADOR DE ENCUESTADOS

	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	

GRAFICO Nº 4: TAMAÑO EMPLEADOR

ENCUESTADOS

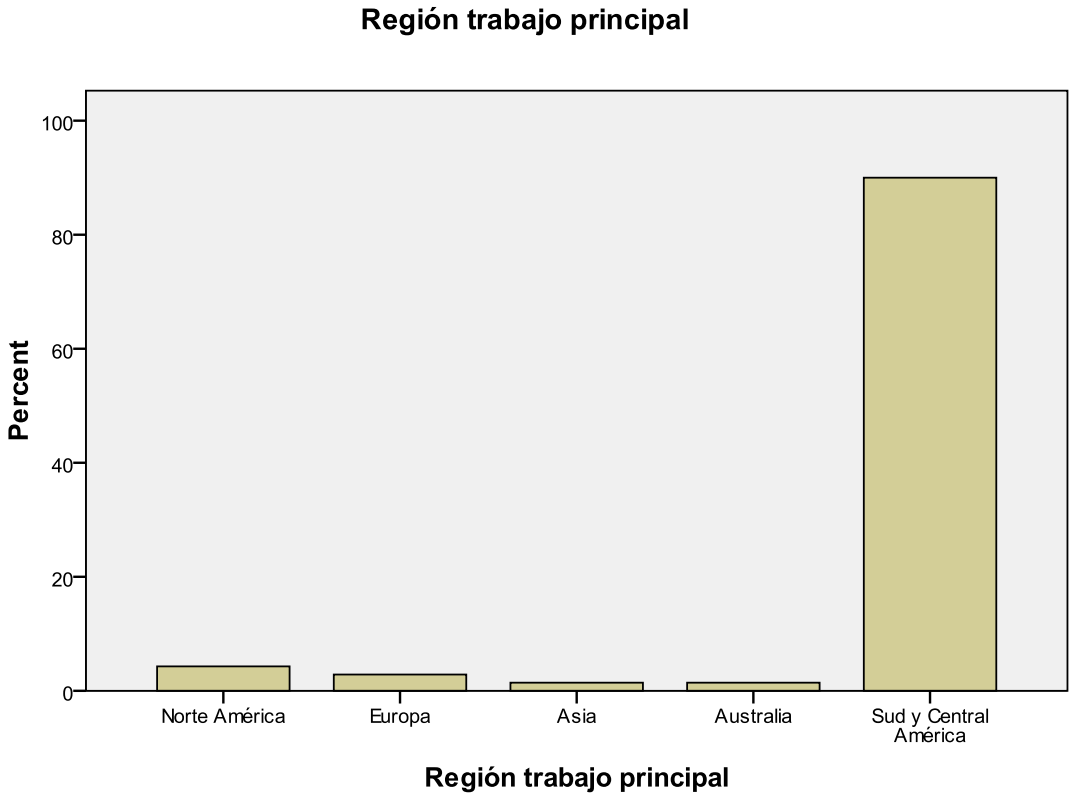


CUADRO Nº 5: REGIÓN TRABAJO PRINCIPAL DE ENCUESTADOS

		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	

GRAFICO Nº 5: REGION DE TRABAJO PRINCIPAL

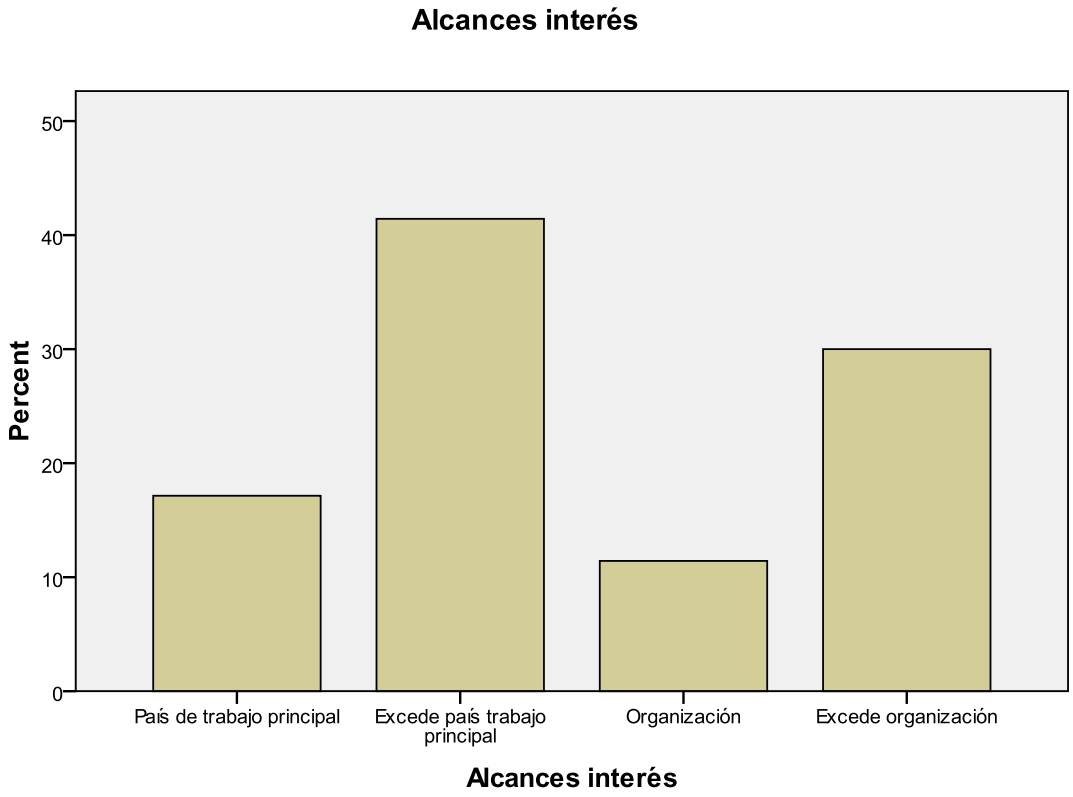


CUADRO Nº 6: ALCANCES INTERÉS EN PKI

		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	

GRAFICO Nº 6: ALCANCES INTERES EN PKI



VIII.- BIBLIOGRAFIA

ADAMS, C., JUST, M.: **"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.

BUGONI, M. y RIVOLTA, M. **"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.

COMMISION OF THE EUROPEAN COMMUNITIES: "**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.
DOYLE, P., HANNA, S.: **"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 julio 2010.
HANNA, Steve: **"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.
KLIKSBERG, Bernardo: **"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.docAccedido septiembre 2009.

KOORN, Ronald: **"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, Ricardo L., **"Comercio Electrónico. Documento, firma digital, contratos, daños, defensa del consumidor"**, Cap.I, p. 52, Editorial Abeledo Perrot, Buenos Aires, mayo 2001.
OASIS: "PKI Action Plan", 2004. Disponible en internet en http://www.oasis-open.org/committees/pki/pkiactionplan.pdf. Accedido Agosto 2010.
OSZLAK, Oscar; MALVICINO, Guillermo; HINTZE, Jorge; GRAZIANO, Ricardo, **"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.
RIVOLTA, Mercedes y SCHAPPER, Paul: "**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 2011.
RIVOLTA, Mercedes: **"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. Disponible en Internet en http://www.planejamento.gov.br/hotsites/seges/clad/documentos/rivolta.pdf. Accedido Septiembre 2009.
UNCITRAL, **"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 2011.