La firma digital en la Argentina.
Responsabilidad legal de los certificadores licenciados: el cumplimiento según estándares

Por Horacio R. Granero

Fecha: 05-02-2004

1. Nociones previas de firma digital:

A modo meramente esquemático y aclaratorio del procedimiento de firma digital adoptado por nuestro país, consideramos conveniente aclarar previamente algunos puntos esenciales:

a. ¿Qué es la firma digital ?

La firma digital es un conjunto de datos asociados a un mensaje digital e incorporados a éste por un programa de computación desarrollado al efecto, que permite garantizar la identidad del firmante y la integridad del documento firmado. A tal fin se utiliza una tecnología denominada "criptografía de clave pública" (también conocida por su sigla en inglés PKI) que es un sistema de alta seguridad informática basada en el empleo de funciones algorítmicas para generar dos "claves" o “llaves” diferentes pero matemáticamente relacionadas entre sí.

La criptografía es la rama de las matemáticas aplicadas que se ocupa de codificar mensajes, transformándolos en forma aparentemente ininteligible con la posibilidad de devolverlos a su forma original mediante la aplicación de un sistema idóneo a tal fin.

En el caso de la aplicación a la firma digital, una vez preparado el documento que desea firmar el programa informático -usando criptografía de clave pública- genera mediante una función matemática, una huella digital ("hash function"), que es una versión comprimida del mensaje. Dicho digesto se encripta con la clave privada y su resultado es lo que llamamos firma digital, que se enviará adjunta al mensaje original.

Una de esas claves -la privada- sirve para crear una firma digital, y la otra -la pública- se aplica para verificar la autenticidad de la firma, y para ello se requiere, la obtención de un certificado digital de parte de un Certificador Licencido el Certificado digital, previa acreditación por parte del interesado de su identidad y –en su caso- la calidad en que la pide (profesional, cliente de un banco, etc.) ante la Autoridad de Registro, entidad que autorizará la emisión del certificado y velará por la vigencia del mismo.

b. ¿Cómo se firma digitalmente ?

La respuesta varía según se trate de la firma de un correo electrónico o de otro tipo de documento electrónico:

1. Correos electrónicos: Una vez obtenido el certificado digital se lo ingresa al programa de correo electrónico que se utilice. Dicho programa genera el par de claves criptográficas únicas, (la clave privada y la clave pública) El remitente prepara el mensaje que desea enviar firmado y activa la opción de firma digital del programa de correo electrónico. Al firmar el correo electrónico, el remitente envía la firma digital y el mensaje (codificado o no) al receptor y éste luego verifica la firma digital del remitente utilizando la clave pública incluida en el certificado digital que "viajó" con el correo.

2. Documentos electrónicos: Para firmar un documento electrónico el firmante debe utilizar un programa adecuado para el almacenamiento de la información digital segura (por ejemplo la extensión .pdf del Acrobat), que se encuentre habilitado para incluir certificados digitales. El sistema obtiene un digesto de mensaje, único y exclusivo al contenido del documento, utilizando tecnología de criptografía de clave pública. Al aplicar su clave privada a dicho digesto, el programa lo transformará en una firma digital. De esta forma se puede firmar desde un contrato (que se remitirá a la otra parte por vía electrónica para que lo signe de la misma manera) hasta una historia clínica que puede ser de esta forma almacenada en forma segura, o el video de una audiencia judicial o un archivo de audio.

c. ¿Qué diferencia hay entre una firma digital y una firma electrónica?

Si bien tecnológicamente son generadas exactamente igual, y con los mismos estándares de calidad –a partir de un cerificado digital-, la diferencia es meramente legal, dado que la firma digital debe haber sido originada de un certificado emitido por una autoridad certificante habilitada, el que –a su vez- debe estar vigente temporalmente. En caso contrario la firma vale exclusivamente como firma electrónica y, en caso de ser repudiada corresponde al emisor acreditar su validez..

d. ¿Dónde residen la clave pública y la privada?

Cuando se crea el par de claves, cada una de ellas es en realidad una muy larga secuencia de números que en el futuro se empleará para firmar o verificar la autoría e integridad de los mensajes. Recordemos que la clave privada se utilizará para firmar mientras que la clave pública servirá para la verificación de las firmas.

El almacenamiento de la clave privada requiere de un adecuado nivel de seguridad debido a que no debe ser conocida ni utilizada por nadie, excepto por su titular (quien la generó). Por ello se la encripta y protege mediante una contraseña y se la guarda en un disco, diskette o, idealmente, en una tarjeta inteligente (smart card) debiendo permanecer bajo el exclusivo control de su propietario siendo este el único capaz de tener acceso a ella.

La clave pública, en cambio es la que permite que un tercero verifique el origen de la firma y la no alteración del documento y se encuentra incluida en el certificado digital,

que contiene además datos identificatorios del titular de dicho certificado, fecha de expedición del mismo, vigencia, etc.

e. Regulación normativa:

En la Argentina, la regulación de la firma digital se remonta a noviembre de 2001, cuando fue promulgada la Ley 25.506 de Firma Digital reglamentada por el Decreto Reglamentario 2628/2002 (BO 20/12/02)

El Decreto 1628/2003 del 6/11/2003 (BO 10/11/2003), posteriomente, disolvió el Ente Administrador de Firma Digital (creado por el art. 11 del Dec. 2628/2002) y reconoció a la Oficina Nacional de Tecnología de la Información (ONTI) como Autoridad Certificante para el Sector Público Nacional y encargada de definir las normas y procedimientos reglamentarios del régimen de firma digital , definió que la Comisión Asesora actuará en el ámbito de la Subsecretaría de la Gestión Pública de la Jefatura de Gabinete de Ministros (art. 3º)

El Decreto Reglamentario estableció los recaudos para obtener una licencia de provisión de servicios de certificación (art. 24), que no podrá exceder de 5 años, (si bien admite que pueden ser renovadas indefinidamente), y exige al certificador contar con seguros vigentes acordes con las responsabilidades asumidas (art. 30) dado que el Estado en su calidad de ente administrador de la Infraestructura de Firma Digital no asume responsabilidades por los actos cometidos por los certificadores (art. 25). Los certificadores están autorizados a utilizar los servicios de infraestructura tecnológicos prestados por un tercero (art. 33). Se faculta a la Autoridad de Aplicación a "elaborar y firmar acuerdos de reciprocidad con gobiernos de países extranjeros, a fin de otorgar validez, en sus respectivos territorios, a los certificados digitales emitidos por certificadores de ambos países, en tanto se verifique el cumplimiento de las condiciones establecidas por la Ley N° 25.506 y su reglamentación para los certificados emitidos por certificadores nacionales" (art. 28)

Los proveedores de servicios de certificación pueden delegar en Autoridades de Registro las funciones de validación de identidad, y otros datos de los suscriptores de certificados y de registro de las presentaciones, y trámites que les sean formuladas bajo la responsabilidad del Certificador Licenciado (art. 35) Dichas Autoridades están igualmente autorizadas para el archivo y la conservación de toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el certificador licenciado, el cumplimiento de las normas y recaudos establecidos para la protección de datos personales.

Con fecha 30 de diciembre de 2003 la ONTI dio a conocer públicamente el proyecto de las normas y procedimientos reglamentarios para el otorgamiento de licencias habilitantes para acreditar a los certificadores de firma digital, los que se encuentran aún a estudio. [2]

Hasta tanto se aprueben dicha regulaciones, la validez legal de los documentos digitales firmados de acuerdo con la tecnología prevista en la Ley de Firma Digital y reglamentación accesoria se supliría con la redacción de convenios particulares que den

a la firma electrónica la presunción de autoría e integridad que posee la firma digital (arts. 5, 6 y 7 Ley 25.506), siempre que se cumpla con los estándares tecnológicos necesarios.

2. El tema de la responsabilidad de los Certificadores Licenciados

a. Responsabilidad objetiva o subjetiva

Para el otorgamiento de la firma digital, como vimos, es necesaria la concesión previa de una licencia por parte de la ONTI , dependiente de la Subsecretaría de la Gestión Pública, y se exige el cumplimiento de una serie de requisitos mínimos esenciales, una responsabilidad estructural, distinta de la responsabilidad funcional general derivada de sus actos frente a los titulares de los certificados y los terceros, conforme lo previsto en la Ley de Firma Digital (LFD), del Decreto Reglamentario y de la normativa dictada en consecuencia.

Ello genera de parte de los Certificadores Licenciados (CL) una responsabilidad especial derivada de sus actos frente a suscriptores y terceros usuarios y se plantea la cuestión si la misma debe tratarse de una responsabilidad objetiva –prefijada- o subjetiva -basada en la demostración de su eventual negligencia-

Con respecto a la responsabilidad objetiva la doctrina ha alegado, en contra de la misma, su carácter estrictamente excepcional (actuaciones altamente peligrosas, como en el caso de la aviación. por ejemplo) y el desaliento que genera en quienes desean actuar como certificadores, lo que obliga a su limitación cuantitativa, y se ha propuesto en algunos casos la responsabilidad de la autoridad pública de certificación como responsable de la habilitación [3]. Ello que no ocurre en nuestro país, dado que el artículo 31 del Decreto Reglamentario 2628/02, de la ley de Firma Digital determina que “en ningún caso, la responsabilidad que pueda emanar de una certificación efectuada por un certificador licenciado, público o privado, comprometerá la responsabilidad pecuniaria del Estado en su calidad de Ente Administrador de la Infraestructura de Firma Digital”, razón por la cual el Estado, como responsable de la habilitación de las CA no responderá eventualmente ante reclamo de terceros que pudieren verse perjudicados por aquellos.

La responsabilidad subjetiva, en cambio, fue la adoptada por la Directiva de la Comunidad Europea, que dispone en su artículo 6.1 que los proveedores de certificación responden de la exactitud de la información contenida en el certificado reconocido y de que el titular identificado en el certificado tiene la clave privada correspondiente, y adecuada, sin pronunciarse respecto de la naturaleza de la responsabilidad, pero al final indica que la misma se dará “salvo que el proveedor de servicios de certificación demuestre que no ha actuado con negligencia”, lo que permite concluir que la Directiva opta por la responsabilidad con culpa [4].

La ley 25.506 de Firma Digital (LFD) adoptó el mismo criterio, estableciendo que la relación del certificador con el titular del certificado se rige por el contrato que celebren entre ellos (art. 37) , pero, a su vez le reconoce a aquel que “es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de ésta, por

los errores u omisiones que presenten los certificados digitales que expida... y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá al prestador del servicio demostrar que actuó con la debida diligencia".

De tal forma, si el CL no ha sido negligente, el tercero usuario que ha confiado en el certificado erróneo no podrá actuar contra ella sino contra el suscriptor o asumir finalmente su error, dado que –como vimos- no existe responsabilidad del Estado.

El art. 37 del Proyecto de Disposición de la ONTI sobre marco normativo aplicable al otorgamiento y revocación de las licencias de firma digital, por su parte, adopta igualmente la responsabilidad objetiva de los CL y establece que

"Los certificadores licenciados responderán por los daños y perjuicios causados en el ejercicio de sus actividades, cuando actúen negligentemente o bien incurran en incumplimiento de sus obligaciones respecto de solicitantes, titulares y terceros usuarios de los certificados digitales por ellos emitidos o demás servicios de firma digital provistos".

La LFD, permite, además, la limitación de la responsabilidad en dos normas . En el artículo 37 LFD la dispone "en función de la clase de certificados que emitan conforme la política de certificación licenciada o bien conforme a las condiciones establecidas en el art. 39 de la ley 25.506" . En el mencionado art. 39 LFD, por su parte, permite la limitación de la responsabilidad a los CL en los siguientes casos

Uso del certificado no expresamente previstos en las condiciones de emisión,

Por la restricción de su uso que surge del mismo certificado

Por las inexactitudes que surgen del certificado por información dada por el titular

El Proyecto de Disposición, a su vez, impone la necesidad de que el CA cuente con un seguro de responsabilidad -art. 22- por un monto de $ 3.000.000.

Si bien tanto la ley como el decreto de firma digital y el Proyecto adoptaron correctamente la responsabilidad subjetiva del CL –debe probarse la culpa-, uno de los problemas a nuestro entender que ha quedado insoluto radica en la dificultad de probar su debida diligencia (en los términos del artículo 37 LFD, dado que su responsabilidad es potencialmente alta e imprevisible por el indefinido número de operaciones a las que puede referirse un mismo certificado, lo cual, aparte de incrementar costos y no incentivar transacciones, puede acabar siendo contrario a los fines del sistema de certificados, por lo que es válida la auto-limitación, siempre que le misma sea concreta y definida.

Consideramos que dicha demostración de la "debida diligencia" se cumpliría con la acreditación del cumplimiento de los standards de calidad fijados por las partes, la administración y el uso internacionalmente admitido.

b. El cumplimiento de los standars como parámetro de buen cumplimiento

Los juristas norteamericanos llaman "on standard" al cumplimiento correcto de una obligación, "out of standard" al incorrecto, y "over standard" al que no solamente cumplió, sino que ha previsto aún más de lo que correspondía para el desarrollo de su actuar. El ejemplo clásico ha sido el del contrato de seguro de incendio, donde la aseguradora obliga a colocar extintores de tantos kilos como resguardo mínimo para el pago de la póliza en caso de siniestro (es el standard), aún cuando muy probablemente el asegurado no pueda hacer mucho con ellos. Pero si no los coloca y ocurre el siniestro, la compañía seguramente no pagará (demostrará que el asegurado estaba out standard). Ahora bien, el asegurado –para cubrirse- puedo contratar un helicóptero hidrante dando vueltas sobre el bien asegurado (será, posiblemente una previsión over standard), pero en caso de siniestro, la aseguradora pagará igual la póliza como si sólo hubiera colocado los extintores requeridos.

En el Proyecto de Código Único de Código Civil de 1998 se había establecido que el standard de diligencia debía ser "adecuado a las circunstancias de personas, de tiempo y de lugar" (art. 1603 del Proyecto de Unificación del Código Civil), lo que implica que para su determinación —entre otras circunstancias— debe tenerse en cuenta que el deudor no puede estar obligado sino a la diligencia razonable, conforme a los alcances de la relación jurídica apreciada según la ya invocada directiva de buena fe.

Así, la jurisprudencia ha determinado, por ejemplo:

El incendio, por sí mismo, en principio no constituye caso fortuito (CNCiv., Sala D, JA, 1962-IV-180) y, por aplicación de las reglas generales, quien lo invoca debe demostrar su carácter imprevisible e irresistible, el hecho de un tercero constituye caso fortuito si confluyen los requisitos de irresistibilidad e imprevisibilidad (CNCom., Sala E, LL, 1981-B-523; CCiv. y Com. San Isidro, Sala II, DJ, 1989-I-182).

En el caso del hurto -apoderamiento ilegítimo de cosa mueble ajena (art. 162 , Cód. Pen.)- no es eximente si ha resultado posible en virtud de la negligencia del deudor en la guarda de la cosa hurtada y no es considerado caso fortuito (CNCom., Sala A, LL, 114-224; id., Sala B, JA, 14-1972-162; LL, 1987-E-39; id., Sala C, LL, Rep. XXXIX-A-I), pero constituye caso fortuito si el deudor adoptó las diligencias adecuadas (CNCom., Sala A., LL, 142-315).

En caso de robo, es decir, de apoderamiento ilegítimo de cosa mueble ajena con fuerza en las cosas o con violencia física en las personas (art. 164 , Cód. Pen.), se ha decidido —en materia del contrato de garaje— que no constituye caso fortuito si no fueron tomadas las medidas tendientes a prevenirlo (CNCom., Sala D, LL, 1987-E-19; id., Sala E, LL, 1987-D-147).

En el caso, por ejemplo de la responabilidad de los bancos por robos en las cajas de seguridad ha sido resuelto en la jurisprudencia norteamericana ("Morgan vs. Citizens' Bank of Spring Hope", 190 N.C. 209, 129 S.E. 585 [1925], "Henderick vs. Uptown Safe Deposit Co.", 159 N.E. 2d 58) e italiana (Corte di Cassazione, 27/7/1976, nro. 2981, Giur. Civile, 1976, I, 1763)— que el banco no es una compañía de seguros, por lo cual, hacerlo soportar el daño del cliente a pesar de la ocurrencia de un caso fortuito, en los hechos, lo convertiría gratuitamente en una aseguradora sin póliza que, además,

violaría flagrantemente la ley 20091 que regula la actividad de las compañías del sector. En una sentencia se consideró que no es invocable como caso fortuito por las "significativas deficiencias que padecieron el sistema de seguridad y el sistema de alarma", y porque "sería muy fácil hacer un boquete en la pared" (CNCom., Sala D, ED, 156-511, votos de los Dres. Rotman y Cuartero, respectivamente); de la sentencia de primera instancia resulta que la pericia de ingeniería determinó que "la calidad del hormigón, según se observó en el lugar del hecho, es de baja resistencia, ya que se observa numerosa porosidad, bajo porcentaje de arena gruesa, y que al golpearse entre trozos se deshace". En otro caso (CNCom., Sala C, ED, 2/10/1995, fallo 46.685) también se aceptó que el caso fortuito en sentido lato ("una causa a él no imputable") libera al banco, pero se consideró que tampoco era invocable, porque el banco permitió la entrada sin control a la bóveda, y por la falibilidad del sistema resultante de la posibilidad de que un empleado infiel obtuviera copia de las llaves de la caja de seguridad que se entregan al cliente, de que las cajas pudieran ser abiertas con llaves diversas a la original o sus copias, y del incumplimiento de las normas respecto de las llaves en desuso. Un criterio contrario fue sostenido en un fallo (CNCom., Sala B, ED, 152-534) en el que se afirmó que el robo no sería invocable por el banco, porque "para sustraer los valores al peligro de tal evento está destinada la caja de seguridad".[5]

En cuanto al tema de la responsabilidad en el manejo de una empresa, se ha resuelto que "los miembros del Consejo Administrativo son responsables pero no en función a la dirección de una sociedad complicada ni por cuestiones financieras, etc, son responsables porque no cuidaron el maíz ajeno como cuidan el propio. No es necesario tomar como estandard al "buen administrador" basta con referirnos al "buen chacarero". (C. Civ. y Com. Mar del Plata, sala 1ª, 8/10/1996, - Navarro, Lucas Martín v. Betriu, Antonio y otros s/ Daños y perjuicios).BA B1351487."

Y en cuanto a la posibilidad sancionatoria de los organismos de control, se dispuso que "la ley 24.065 -marco regulatorio del servicio público de electricidad-, crea el Ente Regulador (art. 54), y le otorga las facultades necesarias para el cumplimiento de los objetivos fijados en su art. 2º de raigambre constitucional -art. 42 C.N.- A su vez, el art. 27 preceptúa que "los transportistas y los distribuidores efectuarán el mantenimiento de sus instalaciones en forma de asegurar un servicio adecuado a los usuarios". La reglamentación de la ley, agrega que dicho standard se mide según el grado de cumplimiento a "las normas de calidad de servicio que se definan en el contrato de concesión específico y a las que a tales efectos establezca el Ente Nacional Regulador de la Electricidad" (art. 27, dec. 1398/92). ("Edesur S.A. c/ Resolución 14/93 -ENRE- (expte. Nº 119/93)" Sala II 03/02/98 Citar: elDial - AH1E1D elDial.com - Editorial Albrematica).

Dicho esto, se puede concluir que en ciertos casos la responsabilidad se basa en el cumplimiento de parámetros bien definidos –que se pueden considerar objetivos- tanto por el uso común como por las propias partes.

c. Los standards aplicables en la firma digital.

Los standards técnicos para el reconocimiento de certeza de los diversos componentes de la firma digital ya se encuentran definidos y pueden ser considerados como universales.

Dichos standars han sido volcados en un interesante trabajo de la Universidad Católica de Lovaina solicitado por la Comisión Europea de Sociedad de la Información de la CE, efectuado por el Centro Interdisciplinario de Derecho y Tecnología de la Información de setiembre de 2003 a cargo de Jos Dumortierdnde se exponen los aspectos legales y del mercado de la aplicación de la Directiva 1999/93/EC y aplicaciones práctica de la firma digital en los países miembros de la Comunidad [6] . En las Recomendaciones sobre "estandarización" (ver 5.5.2) hace suya la decisión de la la Comunidad Europea (CE) del 14 de julio de 2003 de "acoger los números de referencia de las norma que gozan de reconocimiento general para productos de firma electrónica" (CWA 14167-1 de marzo de 2003 Security requirements for trustworthy systems managing certificates for electronic signatures Part 1: System Security Requirements y CWA 14167-2 de marzo de 2002 Security requirements for trustworthy systems managing certificates for electronic signatures Part 2: criptographic module for CSP signing operations – Protection Profile (MCSO-PP) y CWA 14169 (marzo de 2002) secure signature-creation devices) considerados conformes con los requisitos de los Anexos Iif y III de la Directiva 1999/93/CE sobre firma digital. [7]

En los Anexos del Proyecto de Disposición del ONTI se establecen diversos parámetros de evaluación, adaptados en su gran mayoría a las estandarización mundial antes mencionada:

Para las políticas de certificación :

1. ANSI [8] X9.79-1 - Part 1: PKI Practices and Policy Framework

2. RFC 2527 - Certificate Policy and Certification Practices Framework

3. RFC 3039 - Qualified Certificates Profile

4. RFC 3280 - Certificate and Certificate Revocation List (CRL) Profile

5. RFC 3279 - Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile: El documento RFC2527 (Infraestructura de Llave Pública, Política de Certificados y marco de Trabajo de la Certificación) presenta un esqueleto para asistir a los que escriben la política de certificación o las prácticas de certificación para las autoridades de certificación y PKIs. Provee una lista comprensiva de tópicos que potencialmente (a discreción de los escritores) necesitan ser cubiertas en una Política de Certificación (CP) o Práctica de Certificación (CPS). Su propósito es establecer una clara relación entre la Política de Certificación (CP) y las Prácticas de Certificación (CPS), CP y presentar un perfil para asistir a los escritores en sus tareas. Identifica los elementos que deben ser considerados durante la formulación, pero el propósito es que no se definan CPs o CPSs particulares, para cada PSC o PKI. El rango de aplicación de este documento está limitado a la discusión de contenidos de la Política de Certificación (como se define en la X.509). El documento presenta las siguientes definiciones:

a. Política de certificación (Certificate policy, CP): Conjunto de reglas que indican la aplicabilidad de un certificado en una comunidad y/o clase de aplicación con requerimientos de seguridad comunes.

b. Trayectoria o camino de certificación (Certificate path): Es una secuencia ordenada de certificados con los cuales, en conjunto con una clave pública del objeto inicial en la ruta o trayectoria (path), se puede proceder a obtener el objeto final en la ruta o trayectoria (path).

c. Declaración de prácticas de Certificación (Certification practice statement, CPS): Es una declaración de las prácticas que la autoridad certificadora emplea para la emisión de certificados.

d. Campos del certificado (Certificate fields): En la X.509 existen los siguientes campos para soportar las políticas de certificación:

d.1 Políticas de certificación (Certificate Policies extension). Esta extensión tiene dos variantes, críticas y no críticas.

d.2 Mapeo de la política (Policy mappings extension). Puede ser utilizado únicamente en los certificados de las PSC. Permite indicar si ciertas políticas en su propio dominio pueden ser consideradas equivalentes a otras políticas en el dominio de la PSC usuaria.

d.3 Restricciones de la política (Policy Contrains Extension). Soporta dos características opcionales. La primera habilita a la PSC para requerir de una política de certificación explícita que debe estar presente en todos los caminos de certificación subsecuentes cuando el certificado abandona el dominio de confianza. La segunda característica opcional es habilitar a la PSC a desactivar el mapeo de la política, con lo cual la PSC evita que una PSC de mayor jerarquía imponga su dominio de confianza a una PSC usuaria.

d.4 Calificadores de Política (Policy Qualifiers): Permite la utilización de políticas estandarizadas (o definida por parámetros), punteros a sitios donde se publican la CPS, etc.

Para la evaluación de la estructura y de los contenido de los certificados, CRL y datos de verificación :

1. Perfil Mínimo de Certificados y Lista de Certificados Revocados

2. ISO/IEC 9594-8 - Information technology Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks. (Information technology – Open systems interconnection – the directory atttribute certificate framework) Esta recomendación plantea algunos requerimientos de seguridad en las áreas de autenticación y otros servicios de seguridad a través de la provisión de un conjunto de marcos de trabajo sobre los cuales pueden basarse los servicios completos. Específicamente define marcos de trabajo para certificados de llave pública, certificación de atributos y servicios de autenticación. Incluye definiciones de los objetos de información para una PKI, incluyendo certificados de llave pública y listas de revocación de certificados (CRL). Igualmente hace entrega de un marco de trabajo para

el manejo de los atributos de un certificado el cual provee fundamentos sobre los cuales la Infraestructura de Gestión de Privilegios puede ser construida junto con la lista de revocación de atributos de los certificados (ACRL). El estándar no incluye elementos tales como protocolos de gestión de llaves y certificados, protocolos operacionales.

3. RFC 3039 - Qualified Certificates Profile

4. RFC 3280 - Certificate and Certificate Revocation List (CRL) Profile

5. RFC 3279 - Algorithms and Identifiers for the Certificate and Certificate Revocation (CRL) Profile

Como parámetros de evaluación de las políticas de seguridad:

1. ISO/IEC IRAM 17799 - Information Technologies - Code of practice for information security management

2. ANSI X9.79-1 - Part 1: PKI Practices and Policy Framework

Para la evaluación del repositorio de información :

1. RFC 2510 - Certificate Management Protocols

2. RFC 2511 - Internet X.509 Certificate Request Message Format

3. RFC 2585 - Operational Protocols - FTP and HTTP

4. RFC 2797 - Certificate Management Messages over CMS

5. ISO/IEC 9594-1 - Information technology - Open Systems Interconnection - The directory: overview of concepts, models, and services.

6. ISO/IEC 9594-1 - Information technology - Open Systems Interconnection - The directory: Models.

7. RFC 3377 - Lightweight Directory Access Protocol (v3) - Technical Specification

Para el ambiente de control, evaluación de personal, plan de seguridad, análisis de riesgos, plan de continuidad del negocio y ambiente de control

1. ISO/IEC 17799 - Information Technologies - Code of practice for information security management

Para la evaluación del ciclo de vida de las claves criptográficas del certificador y de los certificados

1. ANSI X9.79-1 - Part 1: PKI Practices and Policy Framework

2. FIP 140-2 – Security Requirements for Cryptographic Modules.

Dichos standars son una guía segura de cumplimiento de los recaudos mínimos exigidos al CA para el otorgamiento de certificados digitales dentro la normativa de la ley 25.506 y sus accesorias y de la habilitación correspondiente.

En tal sentido, consideramos conveniente reformar el artículo 37 del proyecto de Disposición, ampliándolo de la siguiente manera:

"Los certificadores licenciados responderán por los daños y perjuicios causados en el ejercicio de sus actividades, cuando actúen negligentemente o bien incurran en incumplimiento de sus obligaciones respecto de solicitantes, titulares y terceros usuarios de los certificados digitales por ellos emitidos o demás servicios de firma digital provistos. Sólo podrán establecer límites a dicha responsabilidad en función de la clase de certificados que emitan conforme a la política de certificación licenciada o bien conforme a las condiciones establecidas en el art. 39 de la ley 25.506.

La acreditación de la debida diligencia exigida en el art. 37 de la ley 25.506 podrá realizarse con la demostración por parte de los certificadores licenciados del cumplimiento de los stándares técnicos vigentes al momento de imputar el damnificado al certificador licenciado el daño que considera que éste le ha causado"

---

[1] El autor es abogado, Doctor en Ciencias Jurídicas, socio de Allende & Brea y Director de la Carrera de Posgrado de Derecho de la Alta Tecnología (UCA). Participó en la redacción de la ley de firma digital y en el decreto reglamentario.

[2] Ver http://www.pki.gov.ar/images/stories/documents/20031230_Disposicion_de_Licenciamiento_v1.1.doc

http://www.pki.gov.ar/images/stories/documents/20031230_Procedimiento_de_Licenciamiento_v1.1.doc http://www.pki.gov.ar/images/stories/documents/20031230_Politica_de_Certificacion_Modelo_v1.1.doc y http://www.pki.gov.ar/images/stories/documents/20031230_Perfil_de_Certificados_y_CRL_v1.1.doc

[3] Martínez Nadal, Apol-lonia, "Comercio electrónico digital y autoridades de certificación", 2da. ed. 2000, pág. 284

[4] Martínez Nadal, A., op cit pág. 285

[5] Brizzio, Claudia "Contrato de servicio de Cajas de Seguridad" en Instituciones de Derecho Moderno, dirigido por Alterini, y otros, Lexis-Nexis Abeledo Perrot (Citar: Lexis Nº 1014/007430)

[6] Ver http://europa.eu.int/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf

[7] Ver versiones de los textos mencionados en http://europa.eu.int/eur-lex/

[8] El proyecto enviado por la ONTI indica erróneamente ANS y no ANSI (American National Secure Institute), por un error meramente tipográfico. Ver http://www.pki.gov.ar/