Especialización en Medicina Legal

Trabajo Final de Especialización

Autor: Lucas Landolfi

DESCRIPCIÓN DE LA NORMATIVA QUE REGULA LA UTILIZACIÓN DE LA FIRMA DIGITAL EN EL ÁREA DE LA SALUD EN ARGENTINA

2016

Citar como: Landolfi, L. (2016). Descripción de la normativa que regula la utilización de la firma digital en el área de la salud en Argentina. [Trabajo Final de Especialización, Universidad ISALUD]. RID ISALUD.

Agradecimientos

A Cecilia, Ignacio y Luciano por recorrer juntos el camino de la vida

A mi amigo Diego Duarte por su colaboración para el desarrollo de este trabajo

A mis Maestros por la generosidad en su Enseñanza

Indice

1. Introducción 2

2. Planteamiento del tema / problema 4
   1. Objetivos Generales 4
   2. Objetivos Específicos 4

3. Marco Teórico 5

   1. Ley ejercicio de la medicina 6
   2. Decreto 427/98 6
   3. Ley de Firma Digital. 2001 6
   4. Código de Etica para el Equipo de Salud de la AMA 8
   5. Ley 26.529: Derechos del Paciente, Historia Clínica y Consentimiento Informado 8
   6. Disposición 927/ 2014 8
   7. Código Civil Argentino de 1871 (derogado en Agosto de 2015) 10
   8. Modificación del Código Civil Argentino vigente desde Agosto de 2015 11
   9. Legislación vigente en provincia testigo: San Luis 11
   10. Legislación del Mercosur 13

4. Desarrollo 15

   1. Aspectos técnicos de la Firma Digital 16
   2. Análisis del desarrollo de la Firma Digital de acuerdo al marco legal en Argentina. 19
   3. Situación en otros Países y en el ámbito del Mercosur 21
   4. Utilización de la Firma Digital en Argentina 22
   5. Caso de Receta Electrónica (con FD) en España 26

5. Resultados 27
6. Conclusiones 28
7. Referencias 29
8. Abreviaturas 31

1. Introducción

Durante más de tres mil años, los humanos vivimos anotando en minerales, maderas, cueros o papel, signos o formas que nos permitieran interpretar en forma más o menos indubitable las ideas o conceptos que quisiéramos comunicar.
Para que esas manifestaciones perduraran en el tiempo fue necesario que el medio utilizado asegurara mediante su alteración (por ejemplo: la escritura, que altera el papel) el reconocimiento de tales signos.
Cuando esos actos debían contener algún tipo de compromiso o acuerdo entre las partes involucradas fue necesario que el medio utilizado tuviere tres características, a saber:

1. Que su duración material fuese superior al tiempo por el que se establecía el acuerdo a efectos de su posterior constatación en caso de dudas.
2. Que permitiere detectar las manifestaciones de su alteración como por ejemplo "borrados" y "agregados" posteriores a la confección del "original".
3. Que reconociere el "no repudio" o desconocimiento de la conformidad otorgada, lo que se logra con la inclusión de algún elemento que modificando el medio, permitiere identificar sin duda a las personas que hubieran intervenido en el acto mediante la incorporación de su firma o impresión digital.

Es así que se desarrolla el concepto de Firma, que de acuerdo al diccionario de la Real Academia Española se define como: "Nombre y apellido, o título, de una persona que esta pone con rúbrica al pie de un documento escrito de mano propia o ajena, para darle autenticidad, para expresar que se aprueba su contenido, o para obligarse en lo que en él se dice...". Siendo la Rúbrica "el rasgo o conjunto de rasgos de figura determinada, que como parte de la firma cada cual pone después de su nombre o título. A veces pónese la rúbrica sola, esto es, sin que vaya precedido del nombre o título de la persona que rubrica..."[1].

Con la utilización del papel como medio, surgen los "originales" y las "copias" de los documentos y con el descubrimiento del papel carbónico surgen los duplicados", "triplicados", etc., todos ellos identificatorios del orden de prelación del papel en el proceso de copia. En los últimos veinte años, la tecnología nos permitió o nos obligó a otras formas de comunicación. Estas nuevas formas implican nuevas formas de pensar o de comunicarse en forma escrita. Por ello ya no tenemos solamente el papel, sino que podemos comunicarnos a través de otros métodos como por ejemplo mediante la utilización de archivos electrónicos. Para ello fue necesario el desarrollo de sistemas como el binario donde se piensa cómo escribir a través de un sistema lógico de ceros y unos.

Quiere decir que ya no resulta tan sencillo leer con letras y palabras. Ya no nos habla más el texto de manera directa. Ahora contamos con medios magnéticos que van a ser interpretados con ayuda de la tecnología.[2]

Actualmente contamos con un entorno tecnológico favorable que permite viabilizar escenarios importantes de las Tecnologías de Informática y Comunicación (TIC) al servicio de la salud.

Una de las herramientas tecnológicas desarrolladas en los últimos años es la Firma Digital que es el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control.
Su utilización podría lograr entre otras cosas la reducción de la burocracia y tiempo sin dejar de lado la confiabilidad de los documentos médicos optimizando los recursos en salud y potencialmente mejorar la calidad de la atención médica.
Sin embargo, la utilización de la firma digital en Argentina es limitada no así el uso de historia clínica informatizada o incluso recetas electrónicas aunque en la mayoría de los casos con firma manuscrita.

El objetivo de este trabajo es describir la legislación actual acerca de la Firma Digital tanto nacional como regional y sus cambios en el nuevo Código Civil para poder tener herramientas sólidas para promover o no su utilización en el ámbito de la salud.

2. PLANTEAMIENTO DEL PROBLEMA

¿Cómo regula la legislación la utilización de la firma digital?
¿Qué cambios se producen a partir del nuevo Código Civil en el tema?
¿Cómo se legisla en otros países sobre la firma digital?
¿Sería de utilidad la firma digital en el área de Salud?

1. Objetivo General

Describir la legislación regional y nacional actual sobre la firma digital, sus cambios en el nuevo Código Civil y su utilización en el área de la salud en Argentina

2. Objetivos Específicos

1. Describir la metodología para la utilización de la firma digital
2. Describir la legislación vigente en Argentina con respecto al uso de la firma digital
3. Analizar la legislación vigente en otros países de la región y del mundo
4 Explorar la posible utilización de la firma digital en Argentina
5 Identificar un caso de utilización de Firma Digital en el área de Salud en España

3. Marco Teórico

En este trabajo se discutirán las leyes, decretos y reglamentos relacionados con el marco legal de la Firma Digital.

1. Ley ejercicio de la medicina
2. Decreto 427/98
3. Ley de Firma Digital. 2001
4. Ley 26.529: Derechos del Paciente, Historia Clínica y Consentimiento Informado. 2009
5. Código de Ética para el Equipo de Salud de la AMA
6. Disposición 927/ 2014
7. Código Civil Argentino de 1871 (derogado en Agosto de 2015)
8. Modificación del Código Civil Argentino vigente desde Agosto de 2015
9. Legislación vigente en provincia testigo: San Luis
10. Mercosur

3.1- Ley Nº 17.132. "Ejercicio de la Medicina, Odontología y Actividades de Colaboración"[3]. Enero de 1967.

Esta ley, en el inciso 7º de su artículo 19 determina que los profesionales que ejerzan la medicina están obligados a prescribir o certificar en formularios que deberán llevar impresos en castellano su nombre, apellido, profesión, número de matrícula, domicilio y número telefónico cuando corresponda. Respecto de las prescripciones y/o recetas establece que deberán ser manuscritas, formuladas en castellano, fechadas y firmadas. A su vez, y a título de excepción, la Secretaría de Estado de Salud Pública puede autorizar el uso de formularios directamente impresos solamente para regímenes dietéticos o para indicaciones previas a procedimientos de diagnóstico.

Se realizó una modificación a este inciso 7º en mayo de 2008: "Redactar las prescripciones o certificados en forma manuscrita con letra claramente legible o por medios electrónicos o mecanografiados, los que deberán ser formulados en castellano, fechados y con la firma debidamente aclarada, especificando domicilio, teléfono, especialidad y matrícula profesional. Los que fueren redactados electrónicamente y mantenidos únicamente en ese soporte, deberán adecuarse a la ley 25.506, de firma digital."

3.2- Decreto 427/98:[4]

En el año 1998 a través del decreto 427/98 se autoriza la utilización de la firma digital en la instrumentación de los actos internos del Sector Público Nacional, otorgándole los mismos efectos que la firma ológrafa y estableciendo las bases para la creación de la Infraestructura de Firma Digital para el Sector Público Nacional.

3.3- Ley Nacional de Firma Digital[5]; Ley 25.506 y su Decreto Reglamentario Nº 2628/02[6]. Promulgada de Hecho: Diciembre 11 de 2001.

En su artículo 2º menciona: "Se entiende por 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."
En su artículo 3º sobre el requerimiento de firma menciona que cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital.
Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia.

Este artículo se complementa con el artículo 4° que habla de Exclusiones:
"Las disposiciones de esta ley no son aplicables:
a) A las disposiciones por causa de muerte;
b) A los actos jurídicos del derecho de familia;
c) A los actos personalísimos en general;
d) A los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes."

Artículo 5º — Firma electrónica. Se entiende por 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.

Artículo 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.

Artículo 7º — Presunción de autoría. Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma.

Artículo 8º — Presunción de integridad. Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma.

Artículo 9º — Validez. Una firma digital es válida si cumple con los siguientes 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, según el artículo 16 de la presente, por un certificador licenciado.

Artículo 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.

Artículo 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.

Artículo 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.

3.4 Código de Ética para el Equipo de Salud. AMA 2001.

En su artículo 185 menciona que: "En caso de computarización de la Historia Clínica deberán implementarse sistemas de seguridad suficientes para asegurar la inalterabilidad de los datos y evitar el accionar de violadores de información reservada[7]."

3.5 Ley 26.529 "Derechos del paciente, historia clínica y consentimiento informado"[8]

En su artículo 13 sobre Historia Clínica informatizada menciona que el contenido de la historia clínica puede confeccionarse en soporte magnético siempre que se arbitren todos los medios que aseguren la preservación de su integridad, autenticidad, inalterabilidad, perdurabilidad y recuperabilidad de los datos contenidos en la misma en tiempo y forma. A tal fin, debe adoptarse el uso de accesos restringidos con claves de identificación, medios no reescribibles de almacenamiento, control de modificación de campos o cualquier otra técnica idónea para asegurar su integridad.
Por otro lado, en su Reglamentación aclara que la historia clínica informatizada deberá adaptarse a lo prescripto por la Ley N° 25.506, sus complementarias y modificatorias.

3.6 Decisión Administrativa N° 927/14[9]

Considerando que la Ley N° 25.506 de Firma Digital, reconoce la eficacia jurídica del documento electrónico, la firma electrónica y la firma digital, estableciendo las características de la Infraestructura de Firma Digital de la República Argentina. En su inciso h) del artículo 30 de la mencionada ley asigna a la autoridad de aplicación la función de otorgar o revocar las licencias a los certificadores y supervisar su actividad, según las exigencias instituidas por la reglamentación.

La Decisión Administrativa N° 927 del 30 de octubre de 2014, establece las pautas técnicas complementarias del marco normativo de firma digital, aplicables al otorgamiento y revocación de licencias a los certificadores que así lo soliciten.
Se dispone que se apruebe el "Manual de Procedimientos" Versión 2.0 de la Autoridad Certificante de la Oficina Nacional de Tecnologías de Información (AC ONTI). Dicho Manual[10] detalla los requerimientos operativos del Ciclo del Certificado que en el punto 4 se comentan en forma resumida:
4- Ciclo del Certificado: requerimientos operativos

4.1. - Solicitud de certificado.
Las solicitudes sólo podrán ser iniciadas por el solicitante, en el caso de certificados de personas físicas, por el representante legal o apoderado con poder suficiente a dichos efectos, o por el Responsable del Servicio, aplicación o sitio web, autorizado a tal fin, en el caso de personas jurídicas.
Dicho solicitante debe presentar la documentación prevista en los apartados 3.2.2. - Autenticación de la identidad de Personas Jurídicas Públicas o Privadas y 3.2.3. - Autenticación de la identidad de Personas Físicas, así como la constancia de C.U.I.T. o C.U.I.L. Deberá también demostrar la pertenencia a la comunidad de suscriptores prevista en el apartado 1.3.3. Suscriptores de certificados.

Los pasos para realizar la solicitud son los siguientes:
a) Ingresar al sitio web del Certificador https://pki.jgm.gob.ar/app/ seleccionando el enlace a la aplicación de solicitud de emisión de certificados.
b) Completar la solicitud de certificado con los datos requeridos de acuerdo al tipo de certificado, seleccionando la AR que le corresponde.
c) Aceptar el Acuerdo con Suscriptores en el que se hace referencia a la Política Única de Certificación que respalda la emisión del certificado.
d) Enviar su solicitud a la AC ONTI e imprimirla.
e) Presentarse ante la AR correspondiente para realizar la identificación personal y la verificación de la documentación requerida en cada caso.
Una vez ingresados sus datos y como paso previo a la generación del par de claves, seleccionará el nivel de seguridad del certificado requerido (alto o normal).

4.2. - Procesamiento de la solicitud del certificado.
El procesamiento de la solicitud finaliza con su aceptación o rechazo por parte de la AR.
La AR efectúa los siguientes pasos:
• Verifica la existencia de la solicitud en la aplicación del Certificador.
• Valida la identidad del solicitante o su representante autorizado mediante la verificación de la documentación requerida.
• Verifica la titularidad de la solicitud mediante el control de la nota de solicitud del certificado.
• Requiere al solicitante o su representante autorizado la firma de la nota de solicitud en su presencia.
• Resguarda toda la documentación respaldatoria del proceso de validación por el término de DIEZ (10) años a partir de la fecha de vencimiento o revocación del certificado.

4.3. - Emisión del certificado.
Cumplidos los recaudos del proceso de validación de identidad y otros datos del solicitante, de acuerdo con esta Política Única de Certificación y una vez aprobada la solicitud de certificado por la AR, la AC ONTI emite el certificado firmándolo digitalmente y lo pone a disposición del suscriptor.

4.5. - Uso del par de claves y del certificado.

4.5.1. - Uso de la clave privada y del certificado por parte del suscriptor. Según lo establecido en la Ley N° 25.506, en su artículo 25, el suscriptor debe:

a) Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;
b) Utilizar UN (1) dispositivo de creación de firma digital técnicamente confiable;
c) Solicitar la revocación de su certificado al Certificador ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;
d) Informar sin demora al Certificador el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.

4.5.2. - Uso de la clave pública y del certificado por parte de Terceros Usuarios. Los Terceros Usuarios deben:
a) Conocer los alcances de la presente Política Única de Certificación.
b) Verificar la validez del certificado digital.

4.9.1. – Revocación de Certificados: Causas de revocación.
El Certificador procederá a revocar los certificados digitales que hubiera emitido en los siguientes casos:
• A solicitud del titular del certificado digital o del responsable autorizado para el caso de certificados de Personas Jurídicas o Aplicación.
• Si determinara que el certificado fue emitido en base a información falsa, que al momento de la emisión hubiera sido objeto de verificación.
• Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.
• Por Resolución Judicial.
• Por Resolución de la Autoridad de Aplicación.
• Por fallecimiento del titular.
• Por declaración judicial de ausencia con presunción de fallecimiento del titular.
• Por declaración judicial de incapacidad del titular.
• Si se determina que la información contenida en el certificado ha dejado de ser válida.
• Cuando la clave privada asociada al certificado, o el medio en que se encuentre almacenada, se encuentren comprometidos o corran peligro de estarlo.
• Ante incumplimiento por parte del suscriptor de las obligaciones establecidas en el Acuerdo con Suscriptores.
• Si se determina que el certificado no fue emitido de acuerdo a los lineamientos de la Política Única de Certificación, del Manual de Procedimientos, de la Ley N° 25.506, el Decreto Reglamentario N° 2628/02 y demás normativa sobre firma digital.
• Por revocación de su propio certificado digital.
El Certificador, de corresponder, revocará el certificado en un plazo no superior a las VEINTICUATRO (24) horas de recibido el requerimiento de revocación.
Los suscriptores serán notificados en sus respectivas direcciones de correo electrónico o en la aplicación del Certificador, del cumplimiento del proceso de revocación.

3.7- Código Civil Argentino de 1871 (derogado en Agosto de 2015)[11]

El Código Civil en vigencia desde 1871, redactado por el Doctor Dalmacio Vélez Sarsfield menciona en su Art 1012 que: "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."

3.8- Código Civil y Comercial Argentino (Vigente desde Agosto de 2015)[12]

En su artículo 288 sobre Firma enuncia: "Firma. La firma prueba la autoría de la declaración de voluntad expresada en el texto al cual corresponde. Debe consistir en el nombre del firmante o en un signo. En los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho si se utiliza una firma digital, que asegure indubitablemente la autoría e integridad del instrumento".

3.9- Legislaciones vigentes en provincia testigo: San Luis

Ley Nº V-0591-2007: "Adhesión a la Ley Nacional Nº 25.506 – Firma Digital."[13]

La Provincia de San Luis aprobó la Ley Provincial adhiriendo a la Ley 25.506. Legislando los siguientes puntos:

Artículo 1º: La Provincia de San Luis, adhiere a la Ley Nacional Nº 25.506 - Firma Digital

Artículo 2º: Las disposiciones de la presente Ley serán de aplicación en el ámbito del sector privado así como en toda la jurisdicción del sector público provincial, el cual comprende los Municipios, la Administración Centralizada y Descentralizada, los Organismos de la Constitución, los Entes Autárquicos y todo otro Ente en que el Estado Provincial o sus organismos descentralizados tengan participación suficiente para la formación de sus decisiones. Su aplicación incluye al Poder Ejecutivo, al Poder Legislativo y al Poder Judicial.

Artículo 8º: A los efectos de la aplicación de la presente Ley, el gobierno reconocerá como Certificador Licenciado a aquéllos que contando con la aprobación nacional se avengan a encuadrarse en la normativa que regula la infraestructura de Firma Digital de la Provincia de San Luis.

Artículo 14º: La Autoridad de Aplicación bregará por el fiel respeto de los principios relativos a la protección de los datos personales en un todo de acuerdo con lo normado por la Ley Nacional Nº 25.326.

Por su parte el Decreto Reglamentario Nº 428-MP-2008 [14] en su capítulo primero se refiere al Ámbito de Aplicación:

Artículo 1º.- Esta reglamentación tiene por objeto regular el empleo de la firma digital a los efectos de su plena eficacia jurídica tanto en el ámbito público como en el privado.-

Artículo 2º.- Las disposiciones del presente Decreto, en virtud del alcance previsto por la Ley de Firma Digital de la Provincia Nº V-0591-2007, serán de aplicación en toda la jurisdicción del Sector Público Provincial. Este comprende a la administración centralizada y descentralizada, los organismos de la Constitución Provincial, los Entes Autárquicos, los bancos y entidades financieras oficiales y todo otro ente en que el Estado Provincial o sus organismos descentralizados tengan participación suficiente para la formación de sus decisiones. Asimismo, su aplicación, alcanza a los actos del Poder Legislativo y del Poder Judicial. El Sector Privado podrá utilizar la infraestructura de firma digital en las relaciones de las personas físicas y/o personas jurídicas entre sí y/o con el Estado Provincial y sus distintos Poderes.

Artículo 7º.- Se entiende por "firma digital" al resultado de una transformación de un documento digital empleando una criptografía asimétrica y un digesto seguro, de forma tal que una persona que posea el documento digital inicial y la clave pública del firmante pueda determinar con certeza lo siguiente: 1) si la transformación se llevó a cabo utilizando la clave privada que corresponde a la clave pública del firmante, lo que impide su repudio; 2) si el documento digital ha sido modificado desde que se efectuó la transformación, de manera tal de garantizar con esta comprobación la integridad del documento. Todo lo cual conlleva a garantizar las características de "no repudio" y la "integridad" del documento que son requisitos de la firma digital.

Artículo 8º.- Por "criptografía asimétrica" se entiende al algoritmo que utiliza por un lado, una clave privada que es utilizada para firmar digitalmente y por otro su correspondiente clave pública para verificar esa firma digital. A efectos de este Decreto, se entiende que la criptografía asimétrica deberá ser técnicamente confiable.

Artículo 9º.- La función de "digesto seguro" es una función matemática que transforma un documento digital en una secuencia de bits de longitud fija, llamada como tal, de forma que se obtiene la misma secuencia de bits de longitud fija cada vez que se calcula esta función respecto del mismo documento digital.

Artículo 10º.- Por "Infraestructura de Firma Digital" se entiende al conjunto integrado por las leyes, decretos y normativa legal complementaria que regulen la firma digital, las obligaciones y deberes de todas aquellas instituciones, organismos y personas que formen parte del circuito de la firma digital tales como la Autoridad de Aplicación, el Ente Licenciante, los Certificadores Licenciados, las Autoridades de Registro, así como también, a los estándares tecnológicos, los procedimientos de seguridad, el hardware, el software, las redes, los bancos de datos y la infraestructura física de alojamiento, que permitan la utilización de la firma digital en condiciones de seguridad e integridad.

Artículo 11º: La Universidad de La Punta será la Autoridad de Aplicación de la Ley Nº V-0591-2007 y del presente decreto reglamentario. Como tal, se encuentra facultada para dictar los manuales de procedimiento del Ente Licenciante, de los Certificadores Licenciados y las normas de auditoría. Queda bajo su competencia la generación de la política de certificación. Asimismo fijará los estándares tecnológicos aplicables a las claves conteniendo el último estado del arte. Se encuentra facultada para realizar todas las diligencias necesarias para adquirir, administrar y mantener la Infraestructura de Firma Digital de la Provincia lo que involucra el espacio físico que responda a las normas

nacionales e internacionales, el hardware y el software de base, los dispositivos criptográficos y de seguridad, el diseño lógico y físico de la infraestructura y todo cuanto fuese necesario para la generación y mantenimiento de aquélla. Llevará a cabo las auditorías de acuerdo a lo dispuesto en el Capítulo V y resolverá todas aquellas contingencias respecto a la Infraestructura de Firma Digital.

3.10- Legislación en el Mercosur[15]. Resolución 37/2006.

Esta Resolución define en sus considerandos a que para la seguridad y confianza en los documentos electrónicos se requieren firmas electrónicas y servicios conexos; que las firmas electrónicas avanzadas, basadas en un certificado reconocido, permiten lograr un mayor nivel de seguridad y que debido a la asimetría en los marcos jurídicos nacionales sobre la materia, es necesario adoptar normas comunes de acuerdo a los estándares internacionales a fin de promover un entendimiento tecnológico entre las respectivas estructuras legales y técnicas de los Estados Partes.
Por otro lado se menciona que el desarrollo de la firma electrónica avanzada en los Estados Partes no restringirá las actividades relacionadas a la emisión de certificados digitales vinculados a firmas electrónicas, que tendrán sus efectos jurídicos limitados a la autonomía de la voluntad de las partes que confían en dichas tecnologías o no se oponen a su utilización.
En base a estos considerando el Grupo Mercado Común define en su artículo 3° que se entenderá por:

1. "Firma electrónica" a los datos en forma electrónica anexos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados por el firmante como medio de identificación

2. "Firma electrónica avanzada": la firma electrónica que cumple los requisitos siguientes:
a) requerir información de exclusivo conocimiento del firmante, permitiendo su identificación unívoca
b) ser creada por medios que el firmante pueda mantener bajo su exclusivo control;
c) ser susceptible de verificación por terceros;
d) estar vinculada a estos datos de tal modo que cualquier alteración subsiguiente en los mismos sea detectable; y
e) haber sido creada utilizando un dispositivo de creación de firma técnicamente seguro y confiable y estar basada en un certificado reconocido y válido al momento de la firma.

3. "Firma digital": utilizada indistintamente con "firma electrónica avanzada" a los efectos de la presente Resolución.

Con el objetivo de alcanzar el reconocimiento mutuo de las firmas electrónicas avanzadas y de los certificados digitales, el artículo 5° de esta Resolución define que los Estados Partes podrán celebrar, entre sí, acuerdos de reconocimiento mutuo. A tales efectos, el GMC aprobará las Directrices para la celebración de dichos acuerdos. Dichas Directrices reflejarán el estado de la materia al momento de su aprobación y podrán ser actualizadas

a propuesta del SGT N° 13, de manera de acompañar la evolución de las tecnologías a ellas relacionadas.
A través de los Acuerdos de Reconocimiento Mutuo se otorgará a las firmas electrónicas avanzadas, que cumplan con las condiciones dispuestas en ellos, el mismo valor jurídico y probatorio que el otorgado a las firmas manuscritas.
Los Estados Partes reconocerán la autenticidad e integridad de un documento electrónico firmado con una firma electrónica avanzada, admitiéndola como prueba documental en procesos judiciales, conforme lo que se disponga en los Acuerdos de Reconocimiento Mutuo. Los Estados Partes indicarán, en el ámbito del SGT N° 13, cuáles serán los organismos competentes habilitados para suscribir Acuerdos de Reconocimiento Mutuo.

En el artículo 7° los Estados Partes asegurarán la creación de un sistema adecuado de acreditación y control de los prestadores de servicios de certificación que emitan certificados reconocidos que permitan la verificación de firmas electrónicas avanzadas, establecidos en sus respectivos territorios.

En su artículo 8° sobre Responsabilidades esta Resolución menciona que los Estados Partes asegurarán como mínimo que un prestador de servicios de certificación acreditado en los términos del artículo 7, sea responsable por los daños y perjuicios causados a cualquier persona física o jurídica que confíe razonablemente en el certificado digital por él emitido, en lo que respecta a:

a) la inclusión de todos los campos y datos requeridos por las respectivas Infraestructuras nacionales para el certificado reconocido y a la exactitud de los mismos, al momento de su emisión.
b) que al momento de emisión de un certificado reconocido por parte del prestador de servicios de certificación acreditado, la firma en él identificada obedece a los datos de creación de firma correspondientes a los datos de verificación incluidos en el certificado reconocido del prestador, con el objeto de asegurar la cadena de confianza.
c) los errores u omisiones que presenten los certificados reconocidos que emitan, o por la inobservancia de los procedimientos de certificación establecidos a partir de los Acuerdos de Reconocimiento Mutuo.
d) el registro en tiempo y forma de la revocación de los certificados reconocidos que haya emitido, cuando así correspondiere.

Corresponde al prestador de servicios de certificación acreditado demostrar que no actuó ni con culpa ni con dolo. Esta Resolución se deberá incorporar la presente Resolución a sus ordenamientos jurídicos nacionales como lo indica el artículo 10°.

4- Desarrollo

Es indiscutible que en el transcurso de las últimas tres décadas asistimos a un proceso de grandes cambios a nivel tecnológico y que, como todo cambio, genera una crisis en los conceptos con los que tradicionalmente nos manejamos. Así, sucede por caso con el concepto de firma que se ha modificado, de la misma manera que lo han hecho otros tales como el comercio y la educación.

Esta "crisis" puede ser tomada como una oportunidad para un cambio positivo que nos permita mejorar las situaciones que diariamente se plantean.
Actualmente las nuevas tecnologías de la información y comunicación (TIC), proveen una serie de herramientas que agilizan la vida diaria. Sin embargo, para que dichas herramientas puedan ser utilizadas en toda su potencialidad, es necesaria la reinterpretación de varios conceptos jurídicos. En muchos casos ello no implica que tales conceptos cambien radicalmente, sino que sean adaptados a la hora actual.
Por ello, acciones tales como la emisión de una prescripción médica puede verse facilitada con la utilización de herramientas informáticas.

4.1 Aspectos técnicos de la Firma Digital.

A diferencia de la firma manuscrita, que es un trazo sobre un papel, la firma digital consiste en el agregado de un apéndice al texto original, siendo este apéndice, en definitiva, la firma digital; al conjunto formado por el documento original más la firma digital se lo denominará mensaje. Este apéndice o firma digital es el resultado de un cálculo que se realiza sobre la cadena binaria del texto original. En este cálculo están involucrados el documento mismo y una clave privada (que, generalmente, pertenece al sistema de clave pública-privada o sistema asimétrico) la cual es conocida sólo por el emisor o autor del mensaje, lo que da como resultado que para cada mensaje se obtenga una firma distinta, es decir, a diferencia de la firma tradicional, la firma digital cambia cada vez con cada mensaje, porque la cadena binaria de cada documento será distinta de acuerdo a su contenido.
A través de este sistema podemos garantizar completamente las siguientes propiedades de la firma tradicional:

Quien firma reconoce el contenido del documento, que no puede modificarse con posterioridad (integridad).
Quien lo recibe verifica con certeza que el documento procede del firmante. No es posible modificar la firma (autenticidad).

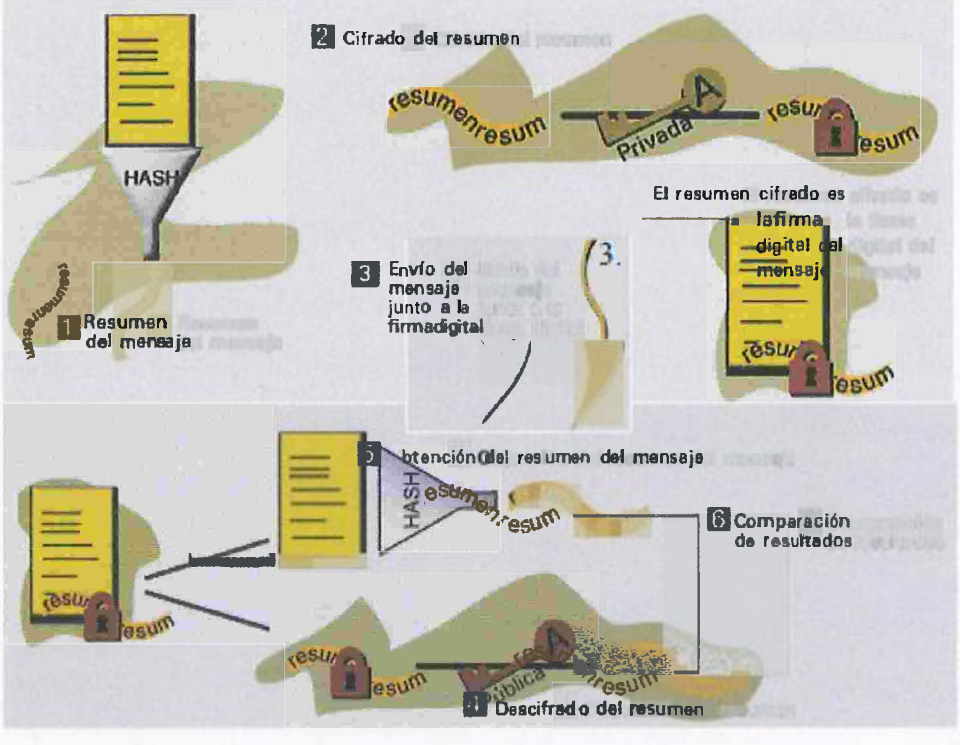
El documento firmado tiene fuerza legal. Nadie puede desconocer haber firmado un documento ante la evidencia de la firma (no repudio).
El concepto de criptografía de clave pública fue introducido por Whitfield Diffie y Martin Hellman a fin de solucionar la distribución de claves secretas de los sistemas tradicionales, mediante un canal inseguro. Este sistema utiliza dos claves diferentes: una para cifrar y otra para descifrar. Una es la clave pública, que efectivamente se publica y puede ser conocida por cualquier persona; otra, denominada clave privada, se mantiene en absoluto secreto ya que no existe motivo para que nadie más que el autor necesite conocerla y aquí es donde reside la seguridad del sistema.
Ambas claves son generadas al mismo tiempo con un algoritmo matemático y guardan una relación tal entre ellas que algo que es encriptado con la privada, solo puede ser desencriptado por la clave pública.

El principal inconveniente de los algoritmos de clave pública es su lentitud que, además, crece con el tamaño del mensaje a cifrar. Para evitar este problema, la firma digital hace uso de funciones hash. Una función hash es una operación que se realiza sobre un conjunto de datos de cualquier tamaño de tal forma que se obtiene como resultado otro conjunto de datos, en ocasiones denominado resumen de los datos originales, de tamaño fijo e independiente al tamaño original que además, tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es prácticamente imposible encontrar dos mensajes distintos que tengan un resumen hash idéntico.

El método más simple de firma digital consiste en crear un hash de la información enviada y cifrarlo con nuestra cave privada (de nuestro par de claves de la criptografía asimétrica) para que cualquiera con nuestra clave pública pueda ver el hash real y verificar que el contenido del archivo es el que hemos mandado nosotros.

Resumiendo, la clave privada es imprescindible para descifrar criptogramas y para firmar digitalmente, mientras que la clave pública debe usarse para encriptar mensajes dirigidos al propietario de la clave privada y para verificar su firma.
Si bien no se trata de un tema estrictamente técnico, es conveniente aclarar que en tiempo de generación de cada par de claves, pública y privada, podría intervenir otra clave que es la de la Autoridad Certificante, que provee la garantía de autenticidad del par de claves generadas, así como también, su pertenencia a la persona cuya propiedad se atribuye.

Figura. Construcción de la Firma Digital



Este esquema se utiliza en intercambios entre entidades cuando se trata de transferencias electrónicas de dinero, órdenes de pago, etc. donde es indispensable que las transacciones cumplan con los requisitos de seguridad enunciados anteriormente (integridad, autenticidad, no repudio del origen, imposibilidad de suplantación, auditabilidad y acuerdo de claves secretas), pero no se satisface el concepto de confidencialidad de la información (secreto).

Como vemos, la firma digital es mucho más que ingresar una clave identificatoria. La firma del profesional debe estar certificada por un certificador licenciado. Los certificadores licenciados son por ahora en su mayoría entes públicos (si bien la ley también permite

certificar a entes privados) autorizados por la Oficina Nacional de Tecnologías de la Información (ONTI) para emitir certificados digitales. Un certificado digital no es más que un documento electrónico firmado digitalmente por el certificador licenciado donde consta la Clave Pública y los datos del usuario al que hace referencia. El proceso consiste básicamente en las generaciones de dos claves, una Pública y otra Privada, ligadas entre sí matemáticamente mediante la aplicación de algoritmos técnicamente confiables. La Clave Pública es de libre distribución y debe estar en disponibilidad de todo aquel que quiera verificar que la firma digital generada con la clave privada se corresponde con dicha clave pública. Se garantiza así que la firma es de quien dice ser y que lo que firmó no ha sido alterado. La Clave Privada es de conocimiento exclusivo del usuario y debe ser resguardada con el máximo nivel de seguridad para evitar su uso por personas no autorizadas.

De esta forma, el autor del documento electrónico procede a codificarlo (encriptarlo), luego lo remite a su destinatario quien no podrá transformar el documento en legible si no posee la clave pública del remitente. Sólo si posee dicha clave pública el destinatario podrá "decodificar" el mensaje y hacerlo nuevamente legible, ya que sólo la clave pública del transmisor es capaz de decodificar el documento cifrado con la clave privada. Dicho en otras palabras, la clave privada funciona como una llave que cierra el documento que sólo puede ser abierto por otra llave, la clave pública. Al haber control externo de la firma, este sistema permite escapar al control de los "Super Usuarios"- los responsables de sistemas-, de las distintas Instituciones. Son todavía muy pocos los profesionales de la salud que han certificado su firma de esta forma ya que las entidades que controlan la matrícula (ej: Colegios Médicos) no se han constituido como certificadores licenciados pudiendo hacerlo, según el artículo 18 de la Ley. Hasta el momento ningún certificador privado se ha acreditado para operar como Certificador Licenciado, por lo cual no es posible para un particular obtener un certificado de firma digital. Esto por el momento está privando a la comunidad médica del vehículo más fácil y accesible para validar su firma digital.

Lo concreto es que todavía los médicos y profesionales de la salud no tienen a quien recurrir para para obtener un certificado digital y deben contentarse sólo con la firma electrónica, que también es aceptada por la ley pero que no brinda la seguridad de la firma digital. Los únicos avances en este sentido provienen de la administración pública, siendo los primeros certificadores licenciados la AFIP y el ANSES (Marzo de 2009). Sin embargo, el proceso de obtención del certificado digital – que no sería demasiado complicado- está limitado a funcionarios y agentes de la administración pública.
La misma Autoridad Certificante de la Oficina Nacional de Tecnologías de la Información (ONTI) emite certificados de identificación personal en forma gratuita, si bien los mismos también están limitados a empleados estatales y, en el caso del resto de los ciudadanos a la protección de las comunicaciones por correo electrónico, no validando la identidad de la persona sino tan sólo verificando la existencia y disponibilidad de dicha cuenta[16]. En todos los casos, para obtener un certificado digital se deberá comprobar la identidad, bien directamente o por medio de entidades colaboradoras. Recién ahí el certificador licenciado creará con los dispositivos técnicos adecuados el par de claves pública y privada y generará el certificado digital correspondiente a esas claves, entregándole al profesional el certificado, ya sea en un medio magnético o directamente en formato de archivo[17].

4.2 Análisis del desarrollo de la Firma Digital de acuerdo al marco legal

Si bien es cierto que la Ley 17.132 en su artículo 19 inc. 7), respecto de las obligaciones de los profesionales de la medicina, expresa que deberán prescribir o certificar en formularios previamente impresos y que las prescripciones y/o recetas deberán ser "manuscritas", formuladas en castellano, fechadas y firmadas, no es menos cierto que la interpretación de dicha cláusula debe hacerse de manera contextual, y de acuerdo al "espíritu del legislador".

Por ello debemos analizar el contexto de la sanción de la Ley 17.132:
Más precisamente, esta ley fue sancionada y promulgada el 24/01/1967, siendo publicada en el Boletín Oficial de la República Argentina pocos días después, un 31/01/1967. Ello demuestra que la noción o avizoramiento de nuestras modernas técnicas de expresión eran, claro está, desconocidas por el legislador, o se encontraban en una etapa tan incipiente que es posible que no pudiera siquiera prever el actual desarrollo tecnológico. Puede interpretarse que lo que el legislador pretendió fue brindar indicios que aseguraran la atribución de autoría del instrumento. A su vez, pareciera que el carácter de "manuscrito" estuviera destinado a los fines probatorios más que a los constitutivos del documento escrito.

Cabe tener en cuenta que esta ley es de fines de la década del ´60, de manera que la expresión "manuscrito" no debería tomarse de manera literal pues si bien hace referencia a la forma más común de prescribir, se supone que su objetivo fundamental es que sea el "profesional" quien confeccione la receta.
Se podría afirmar que al momento de la sanción de la Ley 25.649, 35 años después de la Ley 17.132 estarían implícitamente reconociendo otras formas de prescripción, y de allí que expresamente requiera la mención de "puño y letra" del profesional médico en los supuestos excepcionales previstos.

4.2.1Cambios en el Código Civil vigente desde 2015

En el Código Civil de 1871 en su Art 1012 desarrollado más arriba suscribe que "...la Firma no puede ser reemplazada por signos ni por las iniciales de los nombres o apellidos." Por lo tanto, la firma digital no podía asumir el valor de instrumento privado ya que sería requisito ineludible la firma ológrafa .
Sin embargo, este texto de hace 145 años no contemplaba la evolución tecnológica de estas últimas décadas. Con la entrada en vigencia de la Ley 25.506 se incorpora el concepto de Firma electrónica y Firma Digital para que el nuevo Código Civil deje definitivamente plasmada la ausencia de diferencias entre firma y firma digital.

La redacción del artículo 288 del nuevo CC y C es similar a la del art. 266 del Proyecto de 1998. El CC trataba la firma de los instrumentos privados en el art. 1012, aunque proporcionaba una definición en las notas a los arts. 916 y 3639. En la primera nota al art. 916, Vélez —con cita de Savigny— decía que "la firma establece que el acto expresa el pensamiento y la voluntad del que lo firma". Bien se ha dicho que la firma "es el

testimonio de la voluntad de la parte, el sello de verdad del acto. Solo la firma obliga, pues la mera presencia de una persona en el acto, y aún su intervención en él, no bastan para obligarla válidamente" . La trascendencia jurídica de la firma es bien conocida porque opera como requisito esencial para la existencia de todo acto bajo forma privada, a tal punto que se ha considerado - con razón- que resulta técnicamente erróneo calificar como instrumentos privados a aquellos que no se encuentran firmados. En la nota al art. 3639, por su parte, Vélez explicaba que "la firma no es la simple escritura que una persona hace de su nombre o apellido; es el nombre escrito de una manera particular, según el modo habitual seguido por la persona en diversos actos sometidos a esta formalidad.

La firma se caracteriza por ser ológrafa y por la exclusividad del trazo. Existe amplia libertad de elección y las personas pueden adoptar cualquier grafía para firmar; la prueba está en que en la gran mayoría de los casos son ilegibles. Su esencia e importancia radica en que constituye la expresión o manifestación habitual de la individualidad de quien la estampa y debe estar puesta con el fin de expresar voluntad de adhesión al texto en el que la misma se inserta .

El nuevo CC y C establece que el requisito de la firma queda satisfecho si se utiliza la FD en los términos que establece la Ley 25.506 que además en su art 3° equipara el valor de esta clase de firma a la dela firma manuscrita, incluso en lo vinculado a los efectos debidos a su omisión .

4.3 Situación en otros Países[18] en el ámbito del Mercosur

Firma Digital en Alemania

En Alemania la firma digital es un sello integrado en datos digitales, creado con una clave privada que permite identificar al propietario de la firma y comprobar que los datos no han sido alterados.

Firma Digital en Naciones Unidas

En las Naciones Unidas una firma digital o numérica es un valor numérico que se consigna en un mensaje de datos y que, gracias al empleo de un procedimiento matemático conocido y vinculado a la clave criptográfica privada del originante, logra identificar que dicho valor se ha obtenido exclusivamente con la clave privada de iniciador del mensaje.

Firma Digital en los Estados Unidos

Podemos observar la sanción de diferentes leyes relativas a la firma digital, para la creación de una infraestructura de firma digital que asegure la integridad y autenticidad de las transacciones efectuadas en el ámbito gubernamental y en su relación con el sector privado:

Proyecto "Gatekeeper": Prevé la creación de una autoridad pública que administre dicha infraestructura y acredite a los certificadores de clave pública;
Resolución de la FDA (Administración de Alimentos y Medicamentos - "Food and Drug Administration") reconociendo la validez de la utilización de la firma electrónica como equivalente a la firma manuscrita;
Iniciativa del Departamento de Salud proponiendo la utilización de la firma digital en la transmisión electrónica de datos en su jurisdicción

Firma Digital en el ámbito del Mercosur

Tal cual se detalló en el Resolución 37/2006 del Mercosur se define a la firma electrónica avanzada con las características de "Firma digital":
a) requerir información de exclusivo conocimiento del firmante, permitiendo su identificación unívoca;
b) ser creada por medios que el firmante pueda mantener bajo su exclusivo control;
c) ser susceptible de verificación por terceros;
d) estar vinculada a estos datos de tal modo que cualquier alteración subsiguiente en los mismos sea detectable;
e) haber sido creada utilizando un dispositivo de creación de firma técnicamente seguro y confiable y estar basada en un certificado reconocido y válido al momento de la firma.
Como también deja aclarado que la FD puede ser utilizada indistintamente con "firma electrónica avanzada" a los efectos de la presente Resolución.

4.4 Utilización de la Firma Digital en Argentina

4.4.1 Situación en Provincia Testigo - San Luis

La legislación vigente en la Provincia de San Luis adhiere a la Ley Nacional 25.506 de FD. Tiene aplicación en el sector público y privado, no obstante en su reglamentación solo abarca al sector público sin puntualizar demasiado sobre el sector privado.
Define como dato interesante que la Universidad de La Punta será la Autoridad de Aplicación encargada de adquirir, administrar y mantener la Infraestructura de FD de la Provincia de San Luis. A la vez, prevé que llevará a cabo las auditorías que exijan la Ley Nº V-0591-2007 y su decreto reglamentario.

4.4.2 Posibilidad de Implementación de la FD en Argentina: Dos Casos

Antes de desarrollar estos dos casos que nos orientarán al estado actual del desarrollo de los instrumentos digitales en el área de salud de la República Argentina conviene recordar que más allá de mejorar la atención de los pacientes y reducir la carga de trabajo burocrático a los médicos es importante que como se está manejando información personal muy sensible que queda almacenada en bases de datos informáticas, el paciente tiene el derecho a que se garantice para sus datos personales la normativa de protección de datos[19].

4.4.2.1Proyecto de Implementación en el Hospital Italiano de Buenos Aires [20]

El Hospital Italiano de Buenos Aires tomó la iniciativa de crear su propia infraestructura PKI por intermedio de un desarrollo "in house" que posibilita llevar adelante todo el proceso de creación y administración de claves públicas y privadas. El sistema de información de nuestra institución, registra todos los eventos médicos que genera el proceso de atención. Basado en un sistema de registro electrónico, el medico registra en la HCE web determinados ítems médicos que agrupamos de la siguiente forma:

- Problemas médicos.
- Evoluciones Médicas.
- Estudios solicitados.
- Observaciones clínicas
- Prescripción Farmacológica.
- Fecha y Hora

Todos estos conceptos agrupados representan un evento médico o consulta médica, todo los datos médicos que un profesional registra en el acto de atención, se registra dentro de estos ítems que representan el evento en salud o la consulta médica propiamente dicha. Una vez terminada la consulta, el medico firma digitalmente el evento médico y se almacena en un repositorio seguro. Toman la decisión de almacenar dichos eventos con el estándar propuesto por HL7 en su "Clinical Document Architecture" (CDA) y así generar un repositorio de eventos clínicos firmados (y no las bases analíticas transaccionales). El

proceso de firma digital consiste en reunir la información médica ingresada, y se construye un archivo XML.
El XML es un estándar en crecimiento utilizado principalmente en los entornos Web, desarrollando en los últimos tiempos un estándar que ayuda a generar seguridad en el entorno. La seguridad en XML combina algoritmos criptográficos con tecnología XML brindando un entorno seguro tanto para los usuarios como para las aplicaciones. La firma digital de archivos XML es un estándar de seguridad recientemente implementado por el consorcio W3C [21]

El proyecto, incluye como objetivo principal, generar los mecanismos de seguridad necesarios para operar y mantener un sistema de registro médico descentralizado, teniendo presente que la seguridad de la información médica se basa en cinco aspectos fundamentales:
· La privacidad: hace referencia a que la información médica no pueda se accedida por un tercero que no esté relacionado al proceso de atención.
· Evitar el Repudio: Hace referencia a la autoría del documento, sólo el poseedor de la firma digital es el responsable por los datos generados y guardados.
· Autenticidad: Se refiere al carácter de auténtico del documento, es decir que sea el original.
· La integridad: Relacionado con el anterior, se refiere al contenido de la información médica impidiendo que sea alterado de su registro original.
· La cronología o temporalidad: Relacionada directamente con la integridad, permite tener registro de la fecha y hora de la creación de la información original, dando así a los datos una secuencia temporal.

Queda claro que la FD es un certificado que se otorga para firmar determinada cuestión en determinado ámbito y funciona invirtiendo la carga de la prueba siendo imposible negar su legitimidad, porque se asume que el único conocedor de la clave es el profesional que tiene habilitada la firma digital[22].

A fin de garantizar su integridad y autenticidad, un documento digital debe cumplir con tres características principales:

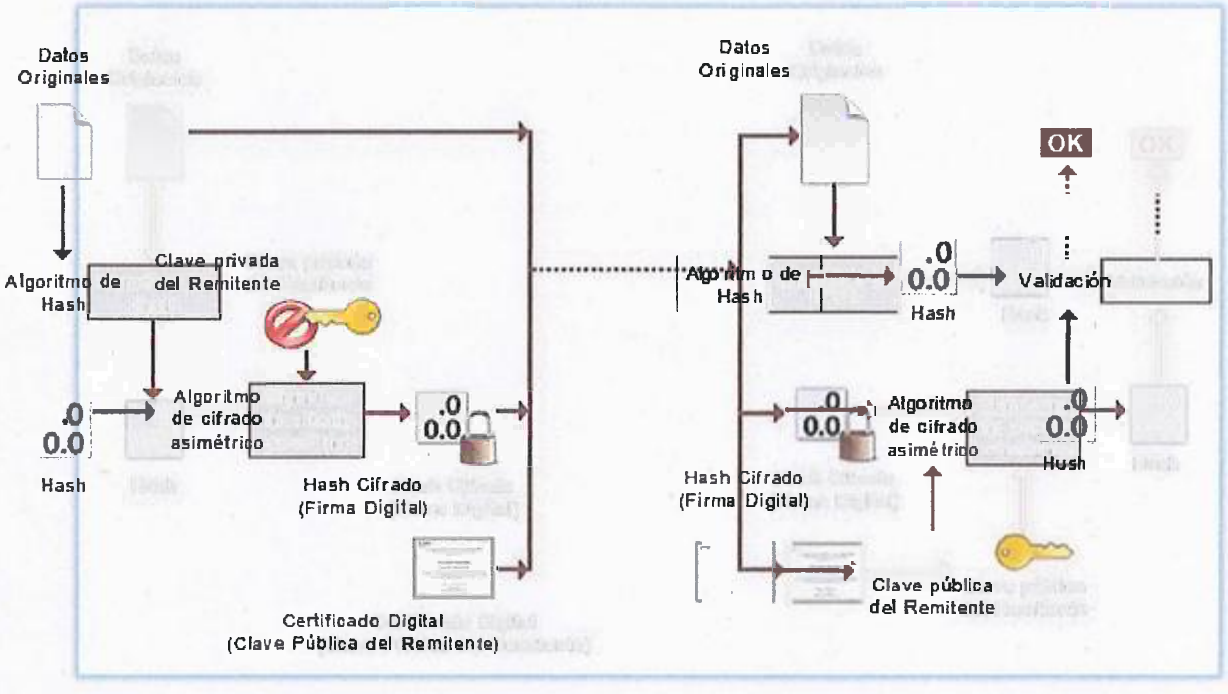
- Poseer un hash, para garantizar la integridad del documento. Se trata de un identificador corto y único, una cadena de dígitos, generado luego de aplicar una fórmula matemática a un documento o secuencia de texto, únicamente correspondiente con el original e irreversible.
- Haber sido firmado con un sistema de claves privada y pública, para garantizar su autoría.
- Y poseer un servicio de Time Stamping, para darle temporalidad al documento.

Con el agregado de la Firma Electrónica/Digital provista por el e-token y de un servicio de Time Stamping (también firmado), permitirá crear un registro fiable y único de los actos médicos. En nuestro proyecto, las claves pública y privada de una persona son almacenadas en un E-Token. El E-Token es un componente electrónico con interfaz USB (Universal Serial Bus), similar a un dispositivo de memoria tipo flash (pendrive), pero a diferencia de éste, posee un microchip que tiene la capacidad de almacenar y procesar algoritmos criptográficos.

El time stamping de documentos es uno de los procesos más complejos y problemáticos en la implementación de firma digital de documentos médicos. El momento exacto cuando ocurrió la carga primaria de la información es una de las variantes más importantes ya que se debe determinar en forma segura la existencia del documento médico en un determinado momento en el tiempo.

En consulta personal a uno de los autores de la publicación, Dr Adrián Gómez, nos comenta que a través de este sistema informatizado se ha logrado resolver el manejo interno de la información médica, el pedido de estudios sin embargo, cuando se requiere trabajar con terceros como una mandataria de fármacos se encuentran con limitaciones legales, de contrato que no han permitido implementar la FD para operaciones fuera de su circuito interno[23].

Figura del Circuito de la FD.



4.4.2.2 Caso de Receta Electrónica de PAMI

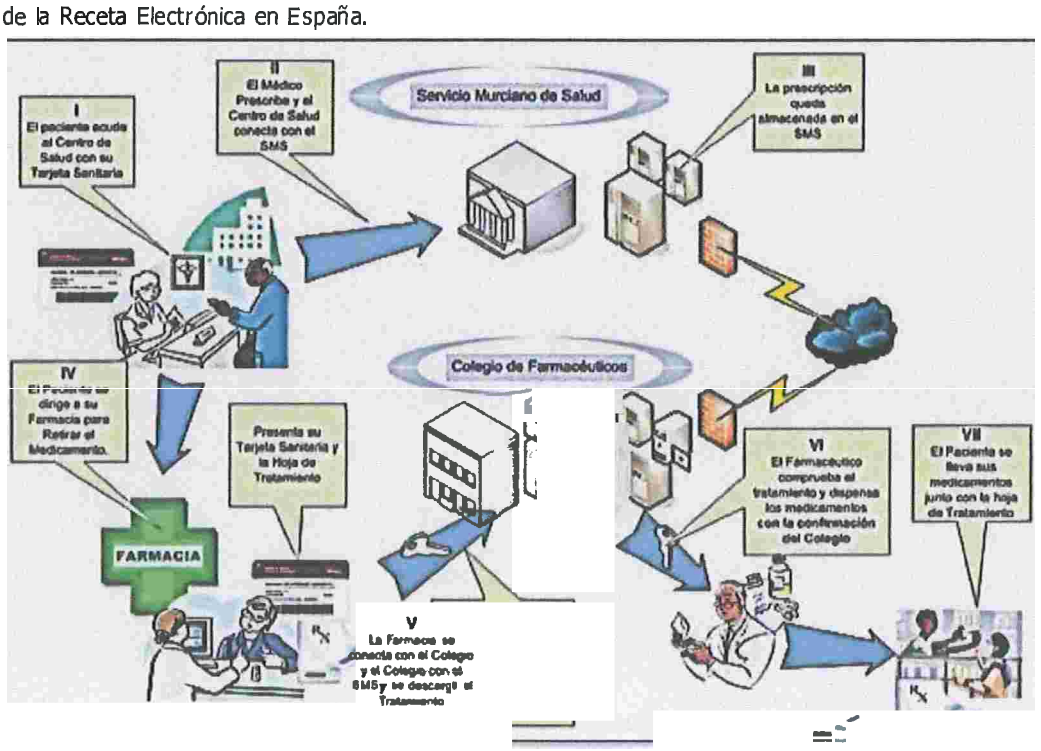
La posibilidad de utilizar los recursos informáticos disponibles minimiza las posibilidades de error. Así lo afirman algunos autores al decir que"... la informatización de la prescripción médica evita las principales causas de error médico a la hora de prescribir y/o hacer indicaciones, ya que evita básicamente el trabajo mecánico de la transcripción de datos por parte de médicos, enfermeras y farmacéuticos, eliminando las discrepancias existentes entre la interpretación y la transcripción de datos"
Por lo que se puede decir que: "sin duda la receta electrónica proporcionaría seguridad y garantías al paciente, elevando asimismo la calidad y accesibilidad de los servicios de

salud" (El código de barras permite la captura y procesamiento de la información de un modo mucho más ágil y seguro, que el tipeo manual. Su aplicación por ejemplo en las Farmacias significaría un paso previo importante a la receta firmada digitalmente y en línea.)
Con la finalidad de reducir la carga administrativa para el profesional médico y asistirlo en el adecuado seguimiento sobre la historia diagnóstica y farmacológica del paciente se desarrolló la emisión computarizada de recetas.
Desde el año 2010 entra en vigencia un nuevo recetario de PAMI el cual coexiste con los actuales. Dichas recetas deben validarse on line bajo el mismo procedimiento que se usa actualmente para las prescripciones ambulatorias de PAMI y bajo los mismos parámetros de cobertura (la Norma de Dispensación es la misma que para los recetarios actuales).
Con respecto a los datos contenidos en esta nueva receta electrónica cabe aclarar que la prescripción del médico está hecha por computadora (no manuscrita) pero sí debe estar en original y manuscrita la firma y sello del profesional prescriptor. Los datos faltantes como cantidad entregada, porcentajes de descuento, importes totales y unitarios e importes a cargo de la entidad y del afiliado deben constar en la copia del ticket fiscal o comprobante de venta, el cual es obligatorio que se adjunte a la receta.
La firma y los datos del que retira los medicamentos deben constar tanto al dorso de la receta como en la copia del ticket. La firma y sello del profesional farmacéutico debe constar al dorso de la receta. La presentación física de estas recetas se realiza en los mismos lotes que las recetas ambulatorias y bajo las normas y cronograma de presentación vigente.
Sin embargo, en la provincia de Buenos Aires la Ley 10.606 en su artículo 36 enuncia que: "No despachará recetas que no estén prescriptas de puño y letra del profesional, las que deberán ser confeccionadas con letra legible, y firmadas por el mismo con la aclaración de nombres, apellido y matrícula". Por lo tanto el farmacéutico que pueda recibir una receta de este tipo queda expuesto frente al paciente y frente a la norma que rige la práctica profesional
Es importante destacar que el artículo 6º de la ley 25.506 ha dicho que: "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 la escritura.". Este texto otorga aval normativo-legal a la utilización de la receta confeccionada con soporte electrónico y/o digital[24].

4.5Caso de Receta Electrónica en España

Resulta útil citar el ejemplo de la receta electrónica en España, donde la firma será estampada personalmente una vez cumplimentados los datos de consignación obligatoria y la prescripción objeto de la receta. En las recetas electrónicas se requerirá la firma electrónica, que deberá producirse conforme con los criterios establecidos[25] por la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos. Los tratamientos prescritos al paciente en receta médica electrónica podrán ser dispensados en cualquier oficina de farmacia del territorio nacional (España) o en botiquines dependientes de las mismas, así como en los servicios de farmacia de los centros de salud y de las estructuras de atención primaria (ambulatorios y centros de salud). Para garantizar esto, el Ministerio de Sanidad, Política Social e Igualdad facilitará el acceso al resto de Administraciones sanitarias (incluidas las mutualidades de funcionarios), a sus sistemas electrónicos con el objeto de que se tenga un único identificador para todos los medicamentos y productos sanitarios (códigos de identificación, formas farmacéuticas, vías y unidades de dosificación, contenido de los envases comerciales etc.). Las recetas médicas electrónicas de cada una de las Administraciones sanitarias deberán necesariamente incorporar el código identificador unívoco de usuarios del Sistema Nacional de Salud y, con carácter exclusivo, el código de identificación del medicamento o del producto sanitario y del resto de parámetros de definición del tratamiento prescrito, que figuren en el Nomenclátor oficial de productos farmacéuticos del Sistema Nacional de Salud.

Figura. Circuito de la Receta Electrónica en España.



5. Resultados

Se desarrolló el estado del arte en relación a la legislación que permite la implementación de la FD en Argentina y el Mercosur.

Figura. Descripción de Leyes que regulan la Firma Digital.

Ley de Firma Digital. 2001

Ley ejercicio de la medicina	**Decreto 427/98**	**Disposición 927/ 2014**
Ley 26.529: Derechos del Paciente, Historia Clínica y Consentimiento Informado.	**Código Civil Argentino de 1871**	**Código Civil Argentino vigente desde 2015**
Legislación del Mercosur	**Código de Etica para el Equipo de Salud de la AMA**	**Legislación vigente en provincia testigo: San Luis**

El nuevo Código Civil y Comercial puesto en vigencia en 2015 supera las dificultades planteadas con respecto al texto anterior en donde solo se hablaba de firma manuscrita. Esto se logra fundamentándose en la Ley 25.506 de Firma Digital en donde se equipara en términos legales a la firma ológrafa con la FD (con las excepciones correspondientes ya descriptas).
Por otro lado, este trabajo logra explicar dos ejemplos reales que demuestran acabadamente que existe un contexto favorable en cuanto a los aspectos técnicos e infraestructura requeridos para la implementación de la FD en el ámbito de la salud; a saber, Historia Clínica Electrónica en el Hospital Italiano (aunque existen numerosos centros que ya la implementaron) y Receta Electrónica en PAMI.
En otros países cercanos culturalmente como España se pudo poner en práctica la Receta Electrónica (con FD) en el ámbito público logrando disminuir la carga burocrática para los médicos.
Es importante señalar que, a diferencia de la firma autógrafa, todas las firmas digitales generadas por una persona son diferentes entre sí. En otras palabras la firma digital cambia con cada documento firmado. Por otra parte, si dos personas firman un mismo documento, también se producen dos diferentes documentos firmados, ya que la clave privada utilizada es diferente.

6. Conclusiones

El marco legal que abarca la FD en nuestro medio cuenta con amplia normativa que a lo largo de los años se fue adaptando a los cambios tecnológicos que se han suscitado en las últimas décadas. En el contexto legal se ha buscado otorgar a la FD un alto valor de integridad y autenticidad que la dejan en un lugar de similar jerarquía a la Firma Ológrafa; incluso con algunas características de inviolabilidad de los certificados digitales que acompañan que la convierten en un recurso interesante, aunque poco explotado en el ámbito de la medicina local. De esta manera, la FD cumple con la Ley 26.529 garantizando la integridad de la HC electrónica.

De acuerdo a la descripción de las leyes vigentes y la implementación de la FD en nuestro medio con relativo éxito (no se usa para recetas aún) considero que no habría obstáculos legales para la implementación de la FD de manera ampliada, incluso para su aplicación en la confección de recetas médicas, pedidos de estudios y análisis con formato electrónico con FD.

La FD mejora la confiabilidad de la prescripción ya sea por dificultad para falsificar o por desaparición del error de interpretación de la letra del médico; y finalmente mejorando el control de los organismos de salud en el gasto en medicamentos sin perjudicar el abastecimiento de los pacientes.

El uso sistematizado de la FD podría resultar en una disminución en la carga burocrática durante la consulta médica y evitar numerosas consultas presenciales con pacientes que sólo requieren recetas de medicamentos crónicos, formularios de auditoría, etc. Sin embargo, se deberá reevaluar esta situación luego de implementada la FD para saber si realmente estos cambios terminarán favoreciendo a los pacientes. Además, deberemos observar los costos reales que su implementación pueda ocasionar.

Por último, más allá de todas estas consideraciones, el avance tecnológico y la telemedicina tarde o temprano llegarán a nuestro ámbito y se instalarán. Será tarea de los médicos conocer de antemano la legislación vigente y las implicancias que esta puede tener en nuestro trabajo diario para ser observadores cercanos de la calidad de atención que el sistema de salud dará a nuestros pacientes.

7. Referencias

[1] Diccionario de la Real Academia Española 2015. Definición de Firma. http://dle.rae.es/

[2] Guini G; Besana G. " La integridad, autenticidad y legalidad de los documenteos digitales". 2° Congreso Metropolitano de Ciencias Económicas, 2007. Area: documento digital. http://www.ele-ve.com.ar/documentos/artdemos/guinibesana.pdf

[3] Ley 17.132. InfoLEG, base de datos del Centro de Documentación e Información, Ministerio de Economía y Finanzas Públicas http://www.infoleg.gov.ar/infolegInternet/verNorma.do?id=19429

[4] Decreto 427/98: InfoLEG, base de datos del Centro de Documentación e Información, Ministerio de Economía y Finanzas Públicas. http://www.infoleg.gov.ar/infolegInternet/anexos/50000-54999/50410/norma.htm

[5] Ley de Firma Digital. InfoLEG, base de datos del Centro de Documentación e Información, Ministerio de Economía y Finanzas Públicas. http://infoleg.mecon.gov.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

[6] Decreto 2628/02. Reglamentación de la Ley de Firma Digital. http://infoleg.mecon.gov.ar/infolegInternet/anexos/80000-84999/80733/norma.htm

[7] Asociación Médica Argentina. Código de Ética para el Equipo de Salud. 2001. Capítulo 11 (De la Historia Clínica), pág 49. http://www.fmed.uba.ar/depto/medlegnew/CODIGOS/Codigo%20de%20Etica,%20AMA%202001.pdf

[8] Ley 26.529. InfoLEG, Base de datos del Centro de Documentación e Información, Ministerio de Economía y Finanzas Públicas. http://www.infoleg.gov.ar/infolegInternet/anexos/160000-164999/160432/norma.htm

[9] Disposición 927/2014. InfoLEG, Base de datos del Centro de Documentación e Información, Ministerio de Economía y Finanzas Públicas. http://www.infoleg.gob.ar/infolegInternet/anexos/235000-239999/237642/norma.htm

[10] Disposición 6/2015. InfoLEG, Base de Datos del Centro de Documentación e Información, Ministerio de Economía y Finanzas Públicas. http://infoleg.mecon.gov.ar/infolegInternet/anexos/250000-254999/251024/norma.htm

[11] Ley N°340. Código Civil Argentino 1871. D. Velez Sarsfield. http://docs.argentina.justia.com/federales/codigos/codigo-civil-apr-8-2010.pdf

[12] Código Civil y Comercial de la Nación. Ley 26.994 http://www.infoleg.gob.ar/infolegInternet/verNorma.do?id=235975

[13] Ley Nº V-0591-2007: "Adhesión a la Ley Nacional Nº 25.506 – Firma Digital. Cámara de Diputados de San Luis. http://www.diputadossanluis.gov.ar/diputadosasp/paginas/NormaDetalle.asp?NormaID=259

[14] DECRETO Nº 428-MP-2008. San Luis. http://www.diputadossanluis.gov.ar/diputadosasp/paginas/NormaDetalle.asp?NormaID=259

[15] Grupo Mercado Común Reconocimiento de la eficacia jurídica del documento electrónico, la firma electrónica y la firma electrónica avanzada en el ámbito del Mercosur. Resolución 37/2006. http://www.infojus.gob.ar/37-internacional-reconocimiento-eficacia-juridica-documento-electronico-firma-electronica-firma-electronica-avanzada-ambito-mercosur-rmr20060000037-2006-07-18/123456789-0abc-de7-3000-06002rserced

[16] ONTI: Oficina Nacional de Tecnologías de la Información. Página oficial de la Autoridad Certificante de ONTI: www.ca.pki.gov.ar

[17] Vítolo F. Aspectos médico- legales de la historia clínica electrónica. Biblioteca Virtual Noble. 2009. http://www.nobleseguros.com/ARTICULOS NOBLE/39.pdf

[18] XVIII Jornadas Nacionales de Derecho Civil, Comisión N° 7, "Derecho Internacional Privado. La jurisdicción internacional en el comercio electrónico."2001

[19] Ley 25.326. Año 2000. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales. http://infoleg.mecon.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

[20] Gómez Adrián. Desarrollo de un sistema digital para la firma de registros médicos. Conference: 2do Congreso de Tecnologías de la Información en Salud, Chile 2006

[21] Gonzalez Bernaldo de Quiros, F., et al. *Migración a plataforma web de una Historia Clínica Electrónica*. in *CBIS'2004 - IX Congresso Brasileiro de Informática em Saúde*. 2004. Ribeirao Preto-SP. Brasil.

[22] VIII Jornadas de Informática Médica del Hospital Italiano de Buenos Aires 2013. http://www.hospitalitaliano.org.ar/infomed/index.php?contenido=ver curso.php&id curso=15652#.Vg3xM9IrJdg

[23] Entrevista Dr Adrián Gómez, 2015. Departamento de Información Hospitalaria, Hospital Italiano, Buenos Aires, Argentina

[24] Qué es y cómo funciona la receta médica electrónica oficial del Sistema Nacional de Salud. 2011. Consumoteca. http://www.consumoteca.com/bienestar-y-salud/medicamentos/que-es-y-como-funciona-la-receta-medica-electronica-oficial-del-sistema-nacional-de-salud/

[25] Real Decreto 1718/2010, sobre receta médica y órdenes de dispensación. España https://www.boe.es/diario boe/txt.php?id=BOE-A-2011-1013

8. Abreviaturas

AR: Autoridad de Registro

Art: Artículo

CC: Código Civil

CC y C: Código Civil y Comercial

CDA: Clinical Document Architecture

FD: Firma Digital

FE: Firma Electrónica

GMC: Grupo Mercado Común

HCE: Historia Clínica Electrónica

ONTI: Oficina Nacional de Tecnologías de la Información

PAMI: Programa de Atención Médica Integral)

TIC: Tecnologías de la Información y Comunicación