Oftalmología Clínica y Experimental

Publicación científica del Consejo Argentino de Oftalmología • ISSN 1851-2658 • Volumen 8 • Suplemento 2015

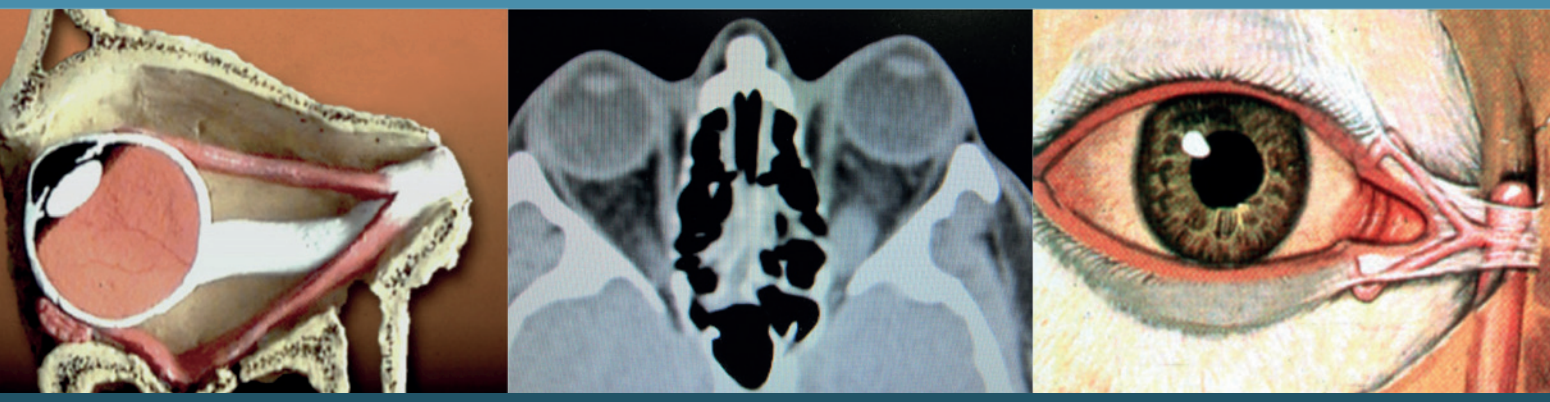
Historia clínica computarizada y firma digital: su implementación práctica

Por Julio A. Ramos

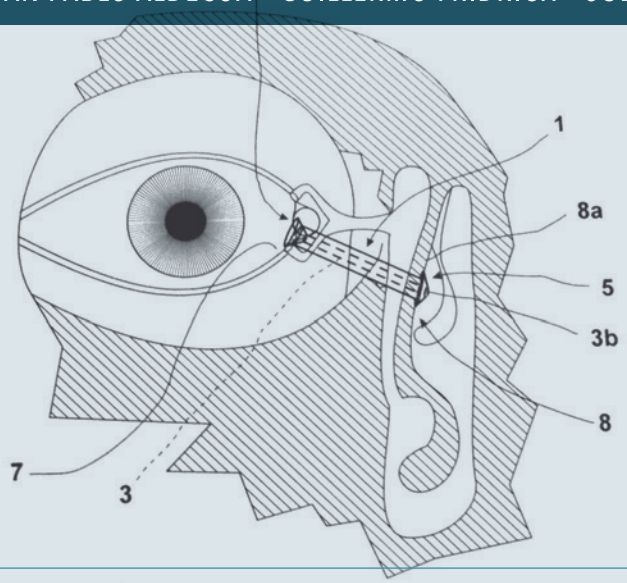
OCE 8.S

OCULOPRÁCTICA

Conceptos y Herramientas en Plástica Ocular



DIRECTORES: JUAN PABLO ALDECOA – GUILLERMO FRIDRICH – JULIA CASALE



SÁBADO 29 DE AGOSTO DE 2015

8:30 A 17:30 HS

Sede del Consejo Argentino de Oftalmología
Tte. Gral. Perón 1479 PB. CABA

Auspicia

CAO | Consejo Argentino de Oftalmología

Publicación científica del Consejo Argentino de Oftalmología ISSN 1851-2658

Oftalmología Clínica y Experimental

Volumen 8 Suplemento 2015

Sumario

Equipo

Oftalmología Clínica y Experimental

La publicación **Oftalmología Clínica y Experimental** tiene una frecuencia trimestral (cuatro números por año). El objetivo es brindar acceso a material científico en español, en portugués y en inglés. Contiene trabajos originales de investigación clínico-quirúrgica y básica, comunicaciones breves, informe de casos y series, revisiones sistemáticas, apuntes en medicina basada en la evidencia, bioestadística y prevención de la ceguera, comentarios de resúmenes destacados para la práctica oftalmológica presentados en congresos y reuniones de la especialidad y referencias a publicaciones de otras revistas. Se estimula el envío de correspondencia para la sección de cartas de lectores abierta a todos los profesionales que deseen expresar sus comentarios sobre los trabajos publicados y observaciones preliminares importantes para la práctica oftalmológica. Los trabajos recibidos son evaluados por profesionales con conocimiento del tema tratado de acuerdo con normas internacionales. La revista cuenta con un sistema de autoevaluación para contabilizar créditos de educación permanente. Los artículos podrán ser localizados e identificados a través de los buscadores usuales de la web abierta y bases de datos regionales.
El Comité Editorial de la revista adhiere a los principios establecidos por el Internacional Committee of Medical Journal Editors y se ajusta a los principios de la Declaración de Helsinki y a los principios de cuidados de animales para experimentación de la Association for Research in Vision and Ophthalmology (ARVO).

CAO

Domicilio editorial: Consejo Argentino de Oftalmología, Tte. Gral. J. D. Perón 1479, PB, 1037AAO Buenos Aires, Argentina - Teléfono: (54-11) 4374-5400 líneas rotativas.

Correspondencia al editor: secretaria@oftalmologos.org.ar

Las instrucciones para los autores se encuentran al final de la publicación.

Historia clínica computarizada y firma digital: su implementación práctica

Julio A. Ramos

Profesor consulto de Oftalmología de la Universidad de Buenos Aires.

Correspondencia:
Prof. Adj. Dr. Julio A. Ramos
Avenida N. de la Riestra 5644
1439 Buenos Aires
drjamos@gmail.com

Oftalmol Clin Exp (ISSN 1851-2658)
2015; 8(S): 1-20.

Resumen

Objetivos: Comprender los requerimientos legales que se le exigen a una historia clínica computarizada. Conocer qué valor tiene y cómo se obtiene un certificado de identificación digital. Saber qué se entiende por infraestructura de firma digital (PKI, por sus siglas en inglés), cómo se firma digitalmente un documento y cuáles son los beneficios que un profesional puede obtener en su consultorio debido a la aplicación de estas tecnologías.
Palabras clave: prescripción electrónica, autoridad certificante, clasificación internacional de enfermedades, clave privada, clave pública, certificado digital, farmacoobservancia, firma digital, historia clínica computarizada, infraestructura de firma digital (PKI).

Introducción

1. Historia clínica computarizada

"No guardes nunca en la cabeza aquello que te quepa en un bolsillo".
Albert Einstein

El objetivo fundamental de la labor médica es aliviar y consolar a sus pacientes. Con este propósito se debe en primer lugar averiguar cuál es el problema que lo aqueja, basándose en su sintomatología, en sus antecedentes y en su conocimiento, para luego desarrollar hipótesis diagnósticas y corroborarlas con el examen clínico.

A tal efecto se hace necesario registrar y conservar todo un conjunto de datos que sirven para evaluar y controlar la exactitud de las hipótesis diagnósticas y la evolución del enfermo.

Si bien el objetivo primario de confeccionar una historia clínica (HC) debería ser ayudar al paciente, la trascendencia médicolegal que ha adquirido últimamente ha llevado a pensar —tal como lo manifiesta el Dr. Lassisuk[1]— que "podríamos decir que la historia clínica constituye el testigo escrito del hacer o no hacer del galeno".

Un concepto al que no siempre se le da la importancia que merece es que la historia clínica debería registrarse con la idea de que se realiza para que otro la pueda leer. Esto tiene significativas implicancias acerca de la prolijidad, el orden y la claridad con la que debería ser hecha.

Debe tenerse en cuenta que la HC computarizada, como la convencional en papel, no debe ser un registro de lo que es cierto acerca del paciente, sino de lo que **se pensó, dijo o hizo** acerca de él. La fidelidad es, por lo tanto, un criterio de diseño fundamental[2].

Sin dejar de tener en cuenta las exigencias que la legislación impone a las historias clínicas, cuando se realizan en la forma escrita convencional presentan numerosos inconvenientes entre los que pueden citarse:

- Crecimiento continuo del volumen almacenado.
- Necesidad de disponer de un volumen cada vez mayor de espacio físico.
- Inevitable alteración en el orden preestablecido de almacenamiento de los documentos originales.
- Peligro de deterioro o pérdida de los datos con el transcurso del tiempo.
- Dificultades en la legibilidad de los datos escritos.

Con el propósito de solucionar estos inconvenientes se ha considerado viable cada vez más la digitalización de los datos y los registros de los pacientes en los últimos años gracias al desarrollo de la tecnología.

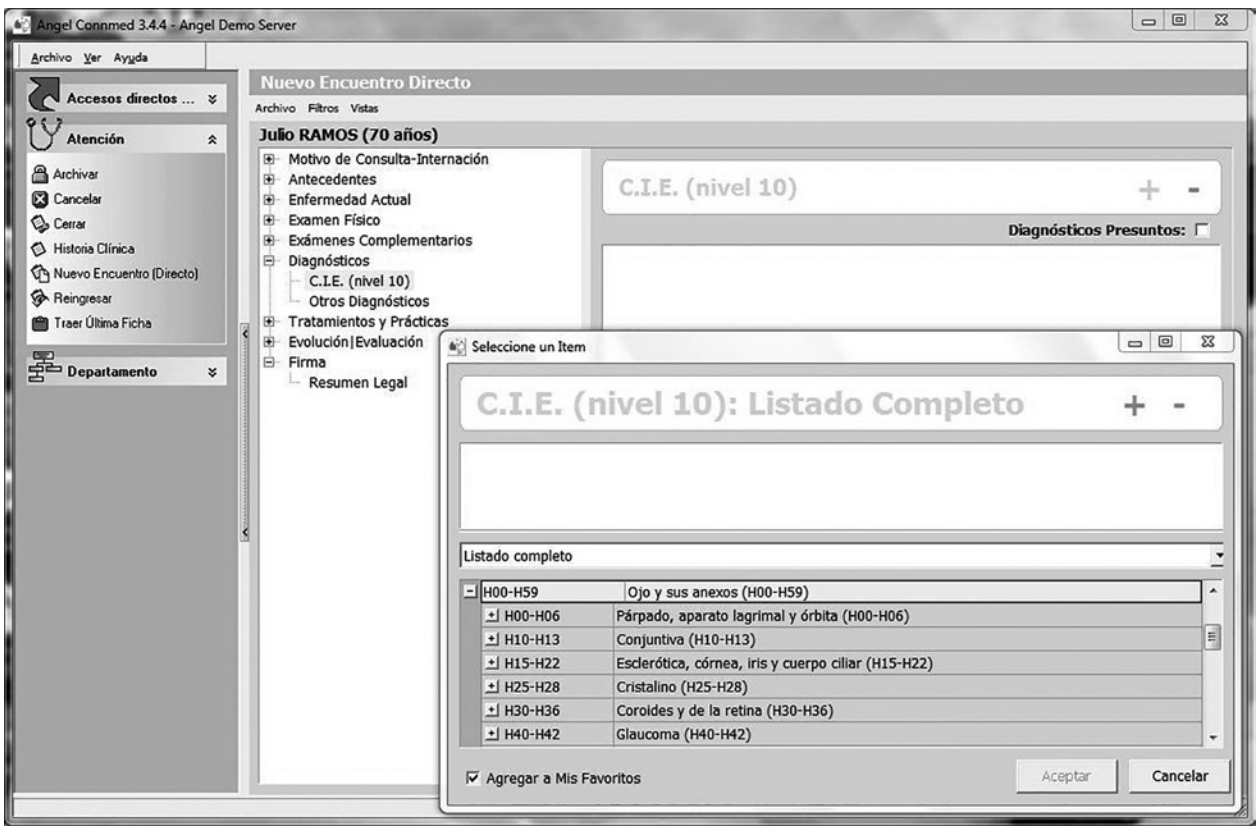


Figura 1.

El tema de la HC computarizada ha preocupado desde hace años a legisladores y legistas hasta el punto en que Juan Carlos do Pico insistió que para que ésta sea aceptada deberían garantizarse ciertos aspectos jurídicos[3].

Así como con los años se han fijado criterios a aplicar para conceder autenticidad a una HC manuscrita, consideramos también que de admitirse o adoptarse como sistema a utilizar la confección de las HC mediante la computadora será menester garantizar también, desde el punto de vista legal, ciertos aspectos básicos de lógica jurídica, tales como:

- Inviolabilidad de los datos
- Posibilidad de recuperar esos archivos
- Perdurabilidad de la información
- Garantía sobre la posibilidad de inspección por parte de la justicia
- Seguro en la remisión de información a un tribunal que solicite una historia clínica
- Recaudos para su posible secuestro judicial
- Posibilidad de actuación de los organismos estatales de control de salubridad o de ética profesional, etc.

Teniendo en cuenta la complejidad que supone el cumplimiento de estos requisitos y considerando las ventajas que la digitalización lleva implícitas, hay en la Argentina empresas de software que han trabajado sobre este tema.

Si bien el logro de una HC fácil de usar y sencilla es una meta a la que se aspira, ya es posible comenzar a utilizarla en diferentes especialidades como en oftalmología.

Con el intento de cumplir con la Ley 26.529 acerca de la historia clínica, la firma Ángel puso a disposición de los colegas un sistema que cumple con todos los requisitos legales, incluyendo el otorgamiento de certificados de identificación expedidos por una autoridad certificante y los instrumentos de software para confeccionar una firma digital[4].

Si bien los que estén interesados pueden obtener mas información en http://www.proyectoangel.net/, en la figura 1 se ofrece una pantalla del módulo de oftalmología.

En esta pantalla se puede observar cómo el programa facilita la ubicación del diagnóstico correcto utilizando la Clasificación Internacional de Enfermedades (CIE) nivel 10.

Nótese que estas historias clínicas por su carácter comercial* incluyen también otras especialidades. Esta particularidad las hace más complejas y en algunos casos más difíciles de usar.

El desarrollo del *software* de base de datos ha alcanzado un grado tal que actualmente es posible desarrollar historias clínicas que se adapten a la forma de trabajo de cada médico oftalmólogo.

Si bien solucionan en gran parte las dificultades que presentan las historias sobre papel, persisten algunos aspectos relacionados con la inviolabilidad que no están del todo resueltos.

Si es que un tribunal solicita determinada HC, es posible realizar —como se explicará más adelante— un informe firmado digitalmente que sea auténtico e inmodificable y que contenga los datos del paciente y los del firmante incluyendo la hora en que ese documento fue emitido.

2. El certificado digital

El certificado digital es un documento firmado digitalmente por una persona o entidad denominada autoridad certificante (AC), mediante el cual se atestigua que una clave pública pertenece a un determinado individuo o entidad. En general, contiene la identidad de la persona (nombre), su clave pública y el nombre de la AC.

Un certificado se considera parte de su identidad digital como usuario de una red o de internet.

Para obtener un certificado de identificación, de acuerdo con la importancia de la cuestión a considerar, éste puede obtenerse de una autoridad certificante.

Estas AC o certificadores son las terceras partes confiables que dan fe de la veracidad de la información incluida en los certificados que emiten.

El uso de certificados de empresas internacionales muy conocidas, como Verisign[5], Trust Network, Thawte[6], Geotrust[7], PGP Corporation[8], etc., podría justificarse cuando la importancia de la cuestión haga necesario difundirlas a un gran número de personas, pues es muy probable que algunos de estos certificados estén en poder del

* Si bien la descarga del programa es gratuita se cobra el soporte técnico y el asesoramiento en su uso.

receptor. Estos son emitidos por sitios de internet y entidades bancarias.

Es de hacer notar —y esto es de sumo valor para el médico que trabaja en su consultorio— que también es posible que uno mismo realice su propio certificado de identificación siguiendo los lineamientos detallados en este trabajo.

Existen programas que permiten:

- Crear un certificado autofirmado (*a "self-signed" certificate*).
- Crear un certificado que le permita generar certificaciones a terceros (*certificate authority [CA]*).
- Solicitar un certificado a una autoridad certificante (AC).
- Ver y evaluar certificados recibidos por otros.

Un certificado que emite una AC es una confirmación de su identidad y contiene información para proteger sus datos o establecer conexiones de red seguras.

Se denominan *certificate store* al área de almacenamiento del sistema donde se mantienen los certificados.

Los sistemas operativos tales como Mac OS X o Windows contienen programas especiales que permiten crear listas de certificados confiables y listas de certificados revocados.

Existen diferentes tipos de certificado digital en función de la información que contiene cada uno y a nombre de quién se emite el certificado:

- **Certificado personal:** acredita la identidad del titular.
- **Certificado de pertenencia a empresa:** además de la identidad del titular acredita su vinculación con la entidad para la que trabaja.
- **Certificado de representante:** además de la pertenencia a una empresa acredita también los poderes de representación que el titular tiene sobre ella.
- **Certificado de persona jurídica:** identifica una empresa o sociedad como tal a la hora de realizar trámites ante administraciones o instituciones.
- **Certificado de atributo:** permite identificar una cualidad, estado o situación. Este tipo de certificado va asociado con el certificado personal (por ejemplo: médico, director, casado, apoderado, etc.).

Además, existen otros tipos de certificado digital utilizados en entornos más técnicos:

- **Certificado de servidor seguro:** utilizado en los servidores web que quieren proteger ante terceros el intercambio de información con los usuarios.
- **Certificado de firma de código:** garantiza la autoría y la no modificación del código de aplicaciones informáticas.

3. La firma digital

Es una forma de asegurar la integridad y el origen de los datos.

Provee una fuerte evidencia de que los datos no han sido alterados desde que fueron firmados y confirma la identidad de la persona que los firmó. Esto hace posible la integridad y la aceptación de la validez, elementos que son esenciales no solo para las transacciones comerciales sino también para las legales.

Las firmas digitales se usan típicamente cuando los datos se distribuyen como texto simple o encriptados. En estos casos, mientras que la sensibilidad del mensaje en sí mismo no justifica que se encripte, podría haber una razón imperiosa para asegurarse de que los datos están en su forma original y no han sido modificados por ningún impostor debido a que en un ambiente empresario con sistemas de computación en red, un texto puede ser leído o alterado por cualquiera que tenga acceso a ella.

La firma digital otorga al documento las siguientes características:

- **Autenticidad**: atribuye el documento únicamente a su autor de forma fidedigna, a fin de poder identificarlo.
- **Integridad**: pone en evidencia su eventual alteración luego de que fue firmado.
- **Exclusividad**: garantiza que la firma se encuentra bajo el absoluto y exclusivo control del firmante.
- **Responsabilidad**: garantiza que el emisor no pueda negar o desentender su autoría o existencia y sea susceptible de su verificación ante terceros.

La firma digital es un código informático que permite determinar la autenticidad de un documento electrónico y su integridad. Está constituida por un pequeño sistema que puede hacer tanto legible o ilegible un documento o archivo digital[9].

La firma digital hace referencia, en la transmisión de mensajes y en la gestión de documentos electrónicos, a un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento[10].

En función del tipo de firma puede, además, asegurar la integridad del documento o mensaje.

Las aplicaciones posibles son numerosas[11] entre ellas pueden citarse:

- Publicación de información segura en la red
- Consulta de información personal a través de internet
- Notificaciones oficiales
- Remisión de información vía correo electrónico
- Compras electrónicas
- Inscripción y tramites en línea
- Notificaciones judiciales
- Expedientes digitales
- Comunicación entre dependencias administrativas
- Voto electrónico
- Autenticación de certificados médicos e historias clínicas

A los efectos de comprender su funcionamiento resulta conveniente tener una idea, aunque sea somera, acerca de la forma como se genera una firma digital.

En primer lugar debe aplicarse al documento original un algoritmo matemático denominado función *hash* con el que se procede a su encriptación. Funciona en una sola dirección, es decir, no es posible calcular —a partir del valor resumen— los datos originales. Cuando la entrada es un documento, el resultado de la función es un número que identifica inequívocamente al texto.

A continuación debe aplicarse, empleando una clave privada, el algoritmo de firma al documento anterior con lo que se genera la así llamada firma digital.

El *software* de firma digital debe además efectuar varias validaciones, entre las cuales podemos mencionar:

- Vigencia del certificado digital del firmante,
- Revocación del certificado digital del firmante (puede ser por OCSP o CRL),
- Inclusión de sello de tiempo.

Online certificate status protocol (OCSP)

Es un método para determinar el estado de revocación de un certificado digital X.509 usando otros medios que no sean el uso de CRL (listas de revocación de certificados). Este protocolo se describe en el registro de estándares de internet.

Los mensajes OCSP se codifican en ASN.1 y habitualmente se transmiten sobre el protocolo HTTP. La naturaleza de las peticiones y respuestas de OCSP hace que a los servidores OCSP se les conozca como *OCSP responders.*

Ventajas sobre las CRL

OCSP fue creado para solventar ciertas deficiencias de las CRL. Cuando se despliega una infraestructura de clave pública (PKI) es preferible la validación de los certificados mediante OCSP sobre el uso de CRL por varias razones:

- OCSP puede proporcionar una información más adecuada y reciente del estado de revocación de un certificado.
- OCSP elimina la necesidad de que los clientes tengan que obtener y procesar las CRL, ahorrando de este modo tráfico de red y procesamiento por parte del cliente.
- El contenido de las CRL puede considerarse información sensible, por ejemplo la lista de morosos de un banco.
- Un *OCSP responder* puede implementar mecanismos de tarificación para pasarle el coste de la validación de las transacciones al vendedor, más bien que al cliente.
- OCSP soporta el encadenamiento de confianza de las peticiones OCSP entre los *responders*. Esto permite que los clientes se comuniquen con un *responder* de confianza para lanzar una petición a una autoridad de certificación alternativa dentro de la misma PKI.

Una consulta sobre el estado de un certificado sobre una CRL se debe recorrer completamente de manera secuencial para determinar si es válido o no.

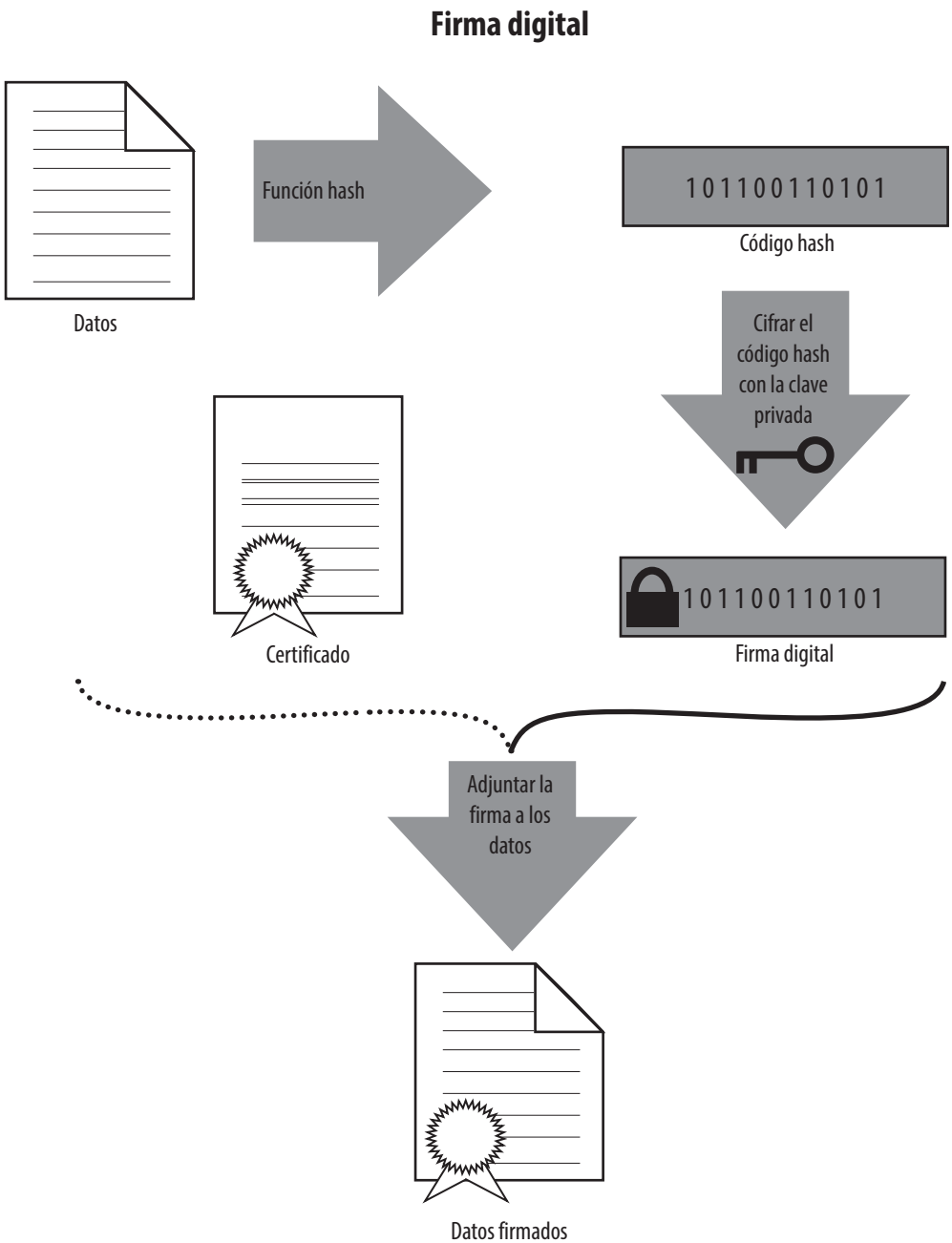
Un *OCSP responder* usa un motor de base de datos para verificar el estado del certificado solicitado con todas las ventajas y estructura para facilitar las consultas. Esto se manifiesta aún más cuando el tamaño de la CRL es muy grande.

Infraestructura de firma digital (PKI)

Se define infraestructura de firma digital o infraestructura de claves públicas (PKI) al conjunto de normas jurídicas, *hardware*, *software*, bases de datos, redes, estándares tecnológicos, personal calificado y procedimientos de seguridad que permiten que distintas entidades (individuos u organizaciones) se identifiquen entre sí de manera segura al realizar transacciones en redes, especialmente en internet, permitiendo además dotar de auditoría e integridad a los documentos digitales mediante el uso de certificados digitales (figs. 2 y 3).

Es importante tener en cuenta algunas consideraciones que realiza la Subsecretaría de la Gestión Pública de la Argentina para los usuarios de estos certificados:

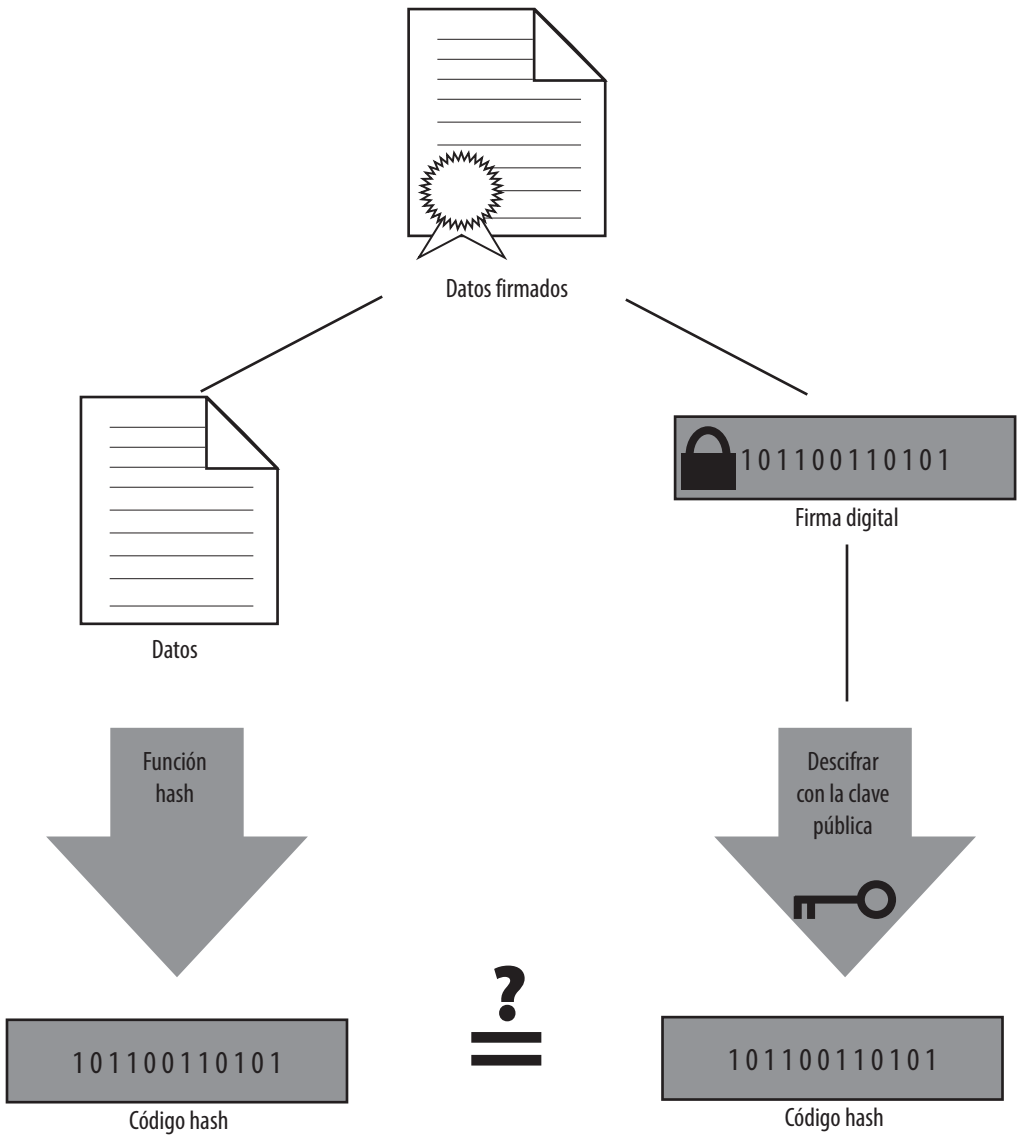
- La clave privada se genera, almacena y utiliza en la estación de trabajo del usuario.



- Se debe proteger la clave privada; para esto se pueden usar contraseñas.
- La firma digital se realiza también en la estación de trabajo, NO en los servidores.
- La autoridad certificante NO posee copia de la clave privada, por lo tanto no puede restaurarla si se pierde.
- El certificador NO interviene en las comunicaciones entre las partes.
- No es necesario un certificado por cada documento que se firme digitalmente.

La firma electrónica, como la firma hológrafa (autógrafa, manuscrita), puede vincularse a un documento para identificar al autor, para señalar conformidad (o disconformidad) con el contenido, para indicar que se ha leído y en su defecto mostrar el tipo de firma y garantizar que no se pueda modificar su contenido.

Comprobación de una firma



Si los códigos hash coinciden la firma es válida

Los términos de firma digital y firma electrónica se utilizan con frecuencia como sinónimos, pero este uso en realidad es incorrecto.

Mientras que *firma digital* hace referencia a una serie de métodos criptográficos, *firma electrónica* es un término de naturaleza fundamentalmente legal y más amplio desde un punto de vista técnico, ya que puede contemplar métodos no criptográficos.

Un ejemplo claro de la importancia de esta distinción es el uso por la Comisión Europea. En el desarrollo de la directiva europea 1999/93/CE que establece un marco europeo común para la firma electrónica, empezó utilizando el término *firma digital* en el primer borrador, pero finalmente acabó utilizando el término *firma electrónica* para desacoplar la regulación legal de este tipo de firma de la tecnología utilizada en su implementación.

En los Estados Unidos la National ePrescribing Patient Safety Initiative (NEPSI)[12] se desarrolló en respuesta al creciente número de errores médicos que plagan el sistema de salud. Esta coalición está formada por compañías tecnológicas, prestadores de servicios de salud y farmacéuticas que están dedicadas a influir positivamente en el proceso de la prescripción a través de la implementación de la prescripción electrónica (ePrescribing).

NEPSI trabaja sobre estos principios ofreciendo a cada médico en forma gratuita lo necesario para prescribir en América del Norte.

Si bien la prescripción digital y su envío a la correspondiente farmacia es de uso corriente en los Estados Unidos, se ha despertado una nueva inquietud para poder controlar en forma más efectiva la prescripción de sustancias controladas. Estas son drogas u otros componentes que tienen un potencial de abuso y dependencia física o psicológica. Incluyen a los opiáceos, los estimulantes, los depresores, los alucinógenos, los esteroides anabólicos y las drogas que son inmediatos precursores de estas sustancias.

Estas regulaciones se agregan y no reemplazan a las reglas preexistentes. Otorgan a los farmacéuticos, hospitales y médicos la oportunidad de usar la tecnología moderna para controlar la prescripción de elementos controlados, reducir el papeleo y evitar la falsificación de las recetas. Tienen también el potencial de reducir los errores en la prescripción causados por la ilegibilidad de las recetas manuscritas y los consiguientes malentendidos.

Una ventaja adicional es que resultaría posible incorporar estas prescripciones en las historias clínicas mejorando su eficiencia y reduciendo potencialmente el tiempo que los pacientes deben esperar para que estas recetas sean completadas.

Desarrollo en la Argentina

Se está extendiendo el uso de la firma digital como una solución para dar cumplimiento a las exigencias legales. La posibilidad de poder acreditar en forma fehaciente la autoría y la integridad de documentos enviados por vía electrónica es ya una realidad accesible en nuestro país.

La Ley 25.506 sancionada el 14 de diciembre del 2001 reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en el artículo 2:

"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".

Y en su artículo 3 dice:

"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 establecer la obligación de firmar o prescribe consecuencias por su ausencia".

Esta revolución es de magnitud comparable a la aparición de la imprenta, ya que podría permitir en poco tiempo la total despapelización del Estado[13] y con ello, una solución al atolladero en que se encuentra hoy, por ejemplo, el sistema judicial, del que no podrá salir si continúa sometido a tecnologías del siglo pasado, la tecnología del papel y los expedientes cosidos o abrochados.

Objetivo de la firma digital de la Subsecretaría de la Gestión Pública

Este es un servicio abierto a la comunidad de internet para todas aquellas personas que deseen contar con un certificado digital o certificado de clave pública para firmar experimentalmente sus correos electrónicos.

Téngase en cuenta que esta autoridad certificante emite certificados de correo electrónico, por lo cual únicamente verificará la existencia y disponibilidad de la dirección de correo electrónico desde la cual se efectuó la solicitud, pero en ningún caso verificará la identidad de quien lo solicita.

El equipo de firma digital de la Subsecretaría de la Gestión Pública espera impulsar de esta forma el uso de la firma digital en nuestro país estableciendo un punto de partida que permita motivar el cambio tecnológico-cultural que esta tecnología implica.

La firma digital se instala en la Justicia argentina

A los efectos de comprender la trascendencia de estas modificaciones en el Poder Judicial argentino, resulta de interés transcribir casi textualmente las explicaciones que sobre el tema da el director de la Oficina Nacional de Tecnologías de Información (ONTI), Carlos Achiary:

"La inserción de la 'firma digital' en el ámbito judicial constituye un importante paso que promete dejar atrás demoras en tramitaciones ante la Justicia, acelerar los tiempos procesales, brindar un resguardo adecuado de la información y hasta cambiar la forma en que se realizan las notificaciones en la Justicia.

Así, la Procuración General de la Nación implementó la firma digital como 'prueba piloto' para sustituir los oficios entre todos los fiscales federales del interior del país. Es decir, 350 fiscalías nacionales y federales.

También cuentan con este mecanismo magistrados y funcionarios a cargo de juzgados del país.

Mientras se estima que un caso de 300 cuerpos entra en un DVD, los esfuerzos en la digitalización se traducen hoy en 391.049 carillas y casi 2000 cuerpos de expedientes.

En Salta analizan que las pruebas que conforman expedientes judiciales tales como imagen, video, sonido e incluso hasta huellas dactilares se digitalicen a partir de este año. En Mendoza se usa el correo electrónico para las órdenes de allanamiento contando con firma digital.

También se lo utiliza para pedir antecedentes penales, enviar notificaciones, para el dictado de sentencias de ejecución, entre otros ejemplos dependiendo de la jurisdicción.

Hacia esos objetivos se perfila su adopción que entró de lleno en la 'administración' judicial y que apunta a llegar a instalarse a la hora de llevar adelante juicios e incluso, avanza entre los distintos organismos del sector público.

En esta línea, la Administración Federal de Ingresos Públicos (AFIP) y la Administración Nacional de la Seguridad Social (ANSES) fueron de los primeros en solicitar licencias para poder otorgar certificados de este tipo.

En este contexto, la firma digital hoy representa una nueva metodología que se implementa en la Justicia 'para poder validar a un firmante y verificar la integridad del documento que acompaña', explicó Carlos Achiary, director de la Oficina Nacional de Tecnologías de Información (ONTI).

A la vista, este dispositivo se representa por una extensa e indescifrable cadena de caracteres que constituye un número, el cual es el resultado de un procedimiento matemático aplicado a un documento. Por lo tanto, no resulta inteligible como una firma escaneada.

Una ventaja fundamental que se desprende de la implementación de la firma digital tiene que ver con el mecanismo de notificaciones. Con sólo usar la notificación electrónica se reducirían a la mitad la duración de los juicios, aseguró Achiary.

La incorporación de la firma digital en la administración de Justicia es un paso importante cuando se trata de digitalizar los expedientes y comenzar a prescindir del soporte papel.

Este primer paso, que viene de parte del nuevo marco normativo sobre firma digital, ya viene avanzando en varias provincias del país para lo cual fue necesario formular reformas a los códigos de procedimiento.

No obstante, la cuota pendiente es la modificación a nivel nacional. "Para que la información que se brinda tenga validez en la Justicia tendría que modificarse el Código Procesal, que sólo admite hasta el momento un sistema en soporte papel", remarca el experto[14].

Otras iniciativas nacionales

Proyecto FARO (Fármaco Observancia)[15]

En nuestro país existe un proyecto de ley sobre la trazabilidad de medicamentos que tiene por objeto establecer un sistema de rastreo que asegure el control y seguimiento de especialidades medicinales o farmacéuticas desde la producción o importación del producto hasta su adquisición por parte del consumidor. Este proyecto espera su sanción de la Cámara de Diputados y Senadores.

Material y métodos

Explicadas las características y funcionamiento de los certificados y de la firma digital detallaremos los procedimientos implementados para confeccionar una firma digital. Esta implica un compromiso legal que afirma su acuerdo con los documentos oficiales que se ajustan a la norma PDF verificada por Adobe Systems Incorporated.

Esta firma incluye su nombre, su dirección de correo electrónico, información acerca de su organización, la fecha y el motivo por el cual el documento fue firmado digitalmente.

Implementación

A los fines de su implementación se utilizó: sistema operativo Microsoft Windows 7 y Adobe Acrobat DC, versión 2015.

Procedimiento

Se describirá un método que incluirá dentro de la firma una imagen de su firma holográfica.

En el apéndice se encuentran gráficos que pueden ser de ayuda al seguir los pasos.

1. Es necesario escanear su firma digital y guardarla en la computadora en formato PDF. Asegúrese al cortar el gráfico que incluya solamente el espacio de su firma. Para lograr mejores resultados use un marcador de trazos sólidos y haga su firma algo más grande que lo normal.
2. Una vez que su firma se encuentre guardada en su disco rígido, abra el programa Adobe Acrobat. Luego despliegue el menú *Edición* y seleccione *Preferencias*.
3. Dentro del recuadro Preferencias, seleccione *Firmas y* haga clic en "*Más...*" para abrir el recuadro de diálogo *Creación y aspecto.* Debajo, en el campo *Aspectos,* seleccione *Nuevo* y en el campo de título asígnele a su firma un nombre.
4. En la sección de configuración, seleccione el botón de *Gráfico importado* y el ahora disponible botón de *Archivo* hasta localizar el archivo con la firma digitalizada en formato PDF.
5. Observe que su firma manuscrita es parte de la firma digital.
6. Para afinar la apariencia de su firma digital puede seleccionar algunos de los recuadros de la sección *Configurar texto* o cambiar las opciones bajo *Prioridades de texto*. Si desea una firma manuscrita solamente quítele el tilde a todos los recuadros en la sección *Configurar texto*.
7. Cuando esté satisfecho con el resultado, haga clic en *OK* para guardar el aspecto de la firma y *OK* nuevamente para salir de las Preferencias de Adobe.

Tenga en cuenta que con el Adobe Reader es posible firmar documentos con la firma digital únicamente si esta opción fue habilitada en el documento Acrobat original, pero no puede crear nuevas apariencias para su firma que contengan imágenes.

Su firma está ahora lista para firmar en forma digital.

Identificación digital

Para hacer que la firma sea legalmente válida también necesita un certificado o identificación

digital. Para obtenerla, el procedimiento es el que sigue:

Abra con el Adobe Acrobat el documento que quiere firmar para hacerlo válido legalmente y elija: Herramientas > Certificados > *Certificar* > *Arrastrar nuevo rectángulo de firma*.

Aparecerá entonces el rectángulo de diálogo *Agregar un ID digital*.

Elija *Un ID digital nuevo...*; *Siguiente* y luego seleccione *Nuevo archivo de ID...* .

Clic en *Siguiente* y llene los campos con su información.

Nótese que se requieren: el nombre, la unidad organizativa, el nombre de la organización, la dirección de correo electrónico, el país o región, el *Algoritmo de clave* y *Usar ID digital*.

Al hacer clic en *Siguiente* > aparecerá el cuadro de diálogo que deberá completarse.

Es necesario ahora elegir una ubicación en el disco rígido (Mis Documentos o cualquier otra carpeta) y guardar el documento que contendrá lo que constituye la ID digital con su correspondiente clave.

Discusión

Como es posible deducir de la bibliografía consultada, el tema en estudio es sumamente amplio y abarca numerosos aspectos.

En forma de resumen podemos concluir que:

- En general, para que la *historia clínica electrónica (HCE)* cumpla con todos los requisitos legales que se le exigen, necesita ser implementada a través de una empresa de informática especializada y lleva implícita una serie de costos que dificultan su acceso a consultorios privados.
- Si bien hay sistemas que se ofrecen en forma gratuita, su soporte de funcionamiento debe realizarse a través de un contrato pago.
- Para que estas historias clínicas sean útiles deben adecuarse a la forma de trabajo de cada uno, personalización que incluye un costo adicional.
- Se considera que puede resultar muy conveniente por la eficiencia lograda en el manejo de la información para organizaciones con varios profesionales que atienden gran cantidad de pacientes.
- La posibilidad de que un profesional pueda convertirse en autoridad certificante raíz y firmar digitalmente un certificado que podrá ser enviado en forma digital junto con el documento y de esa manera tener la misma validez que un manuscrito firmado, es realmente un valioso cambio de paradigmas.
- Se ha demostrado en el acápite *Implementación* de este trabajo que este procedimiento está al alcance de cualquier colega que lo quiera efectuar.
- De esta manera estaría en condiciones de firmar digitalmente con el consiguiente reconocimiento de su validez: certificados, historias clínicas, presupuestos, consentimientos informados, etc.

Conclusiones

La realización de este trabajo ha permitido:

1. Analizar las características, ventajas e inconvenientes de la historia clínica electrónica (HCE).
2. Estudiar las propiedades, funcionamiento y ventajas de la firma digital.
3. Implementar un procedimiento de firma digital de bajo costo que se encuentre al alcance de un médico oftalmólogo y que pueda ser utilizado en su consultorio.

Glosario

Abstract Syntax Notation One (ASN.1) (*notación sintáctica abstracta 1*): es una norma para representar datos independientemente de la computadora que se esté usando y sus formas de representación internas.

Clave pública: se entiende así una llave o par de llaves usada en la creación de una firma digital. Pública significa que la o las llaves se usan para verificar la firma digital. Esta llave pública está disponible para cualquiera que reciba un documento firmado digitalmente por quien es el poseedor de las dos claves.

CRL: lista de revocación de certificados.

HTTP o hypertext transfer protocol (*protocolo de transferencia de hipertexto*): es el protocolo

usado en cada transacción de la *world wide web* y define la sintaxis y la semántica que utilizan los elementos de *software* de la arquitectura web (clientes, servidores, proxies) para comunicarse.

Public key infrastructure (PKI): significa una estructura bajo la cual una autoridad de certificación verifica la identidad de los solicitantes; emite, renueva o revoca los certificados digitales; mantiene un registro público de las claves y mantiene una lista de los certificados actualizados y revocados.

Online certificate status protocol (OCSP): es un método para determinar el estado de revocación de un certificado digital X.509 usando otros medios que no sea el CRL (listas de revocación de certificados).

X.509: En criptografía, X.509 es un estándar para infraestructuras de claves públicas (en inglés, *Public Key Infrastructure* o PKI). X.509 especifica, entre otras cosas, formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación.

Apéndice

Procedimiento a usar por el firmante

Firma de ejemplo escaneada en formato PDF (fig. 4).

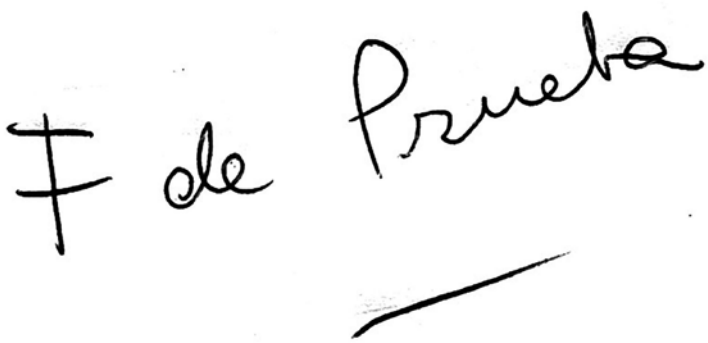


Figura 4.

Acrobat Preference Security (fig. 5).

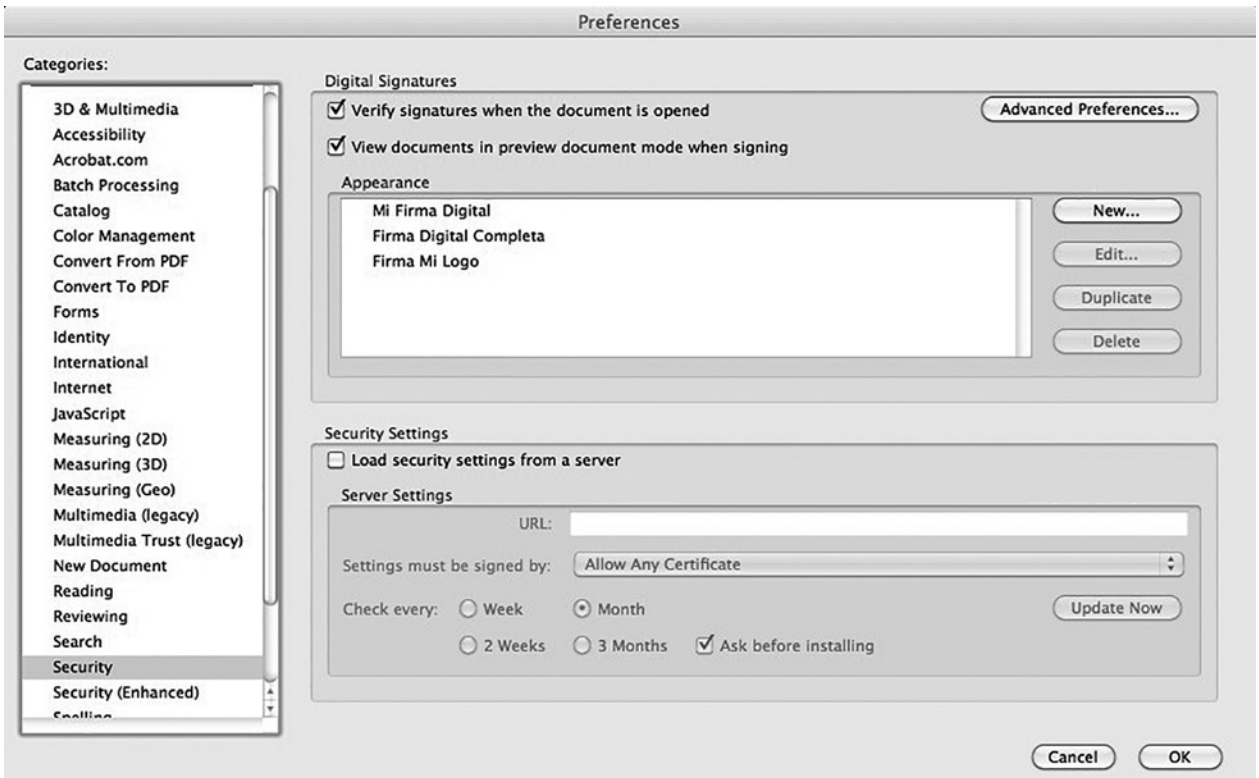


Figura 5.

Creación y otorgamiento de un nombre a la nueva firma (fig. 6).

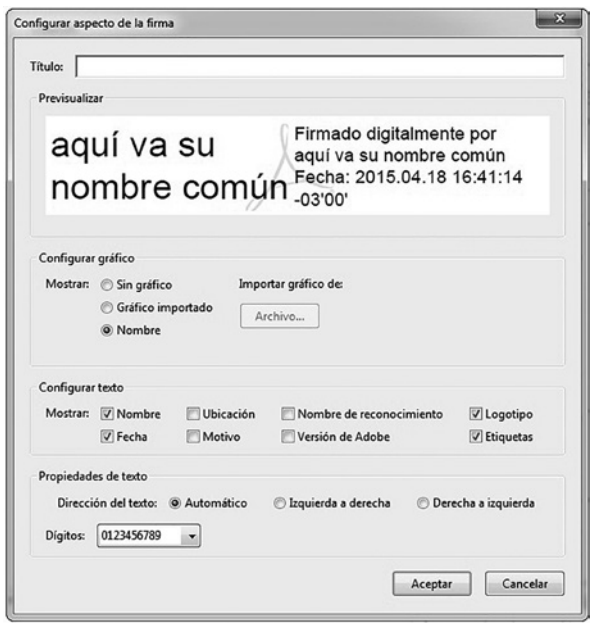


Figura 6.

Téngase en cuenta que el *nombre común* se refiere al nombre único con que el usuario es conocido en la red a la que pertenece.

Una vez abierto con el Adobe Acrobat el documento que uno quiere firmar debe elegirse: *Herramientas* > *Certificados* > *Firmar digitalmente* (fig. 7 y 8).

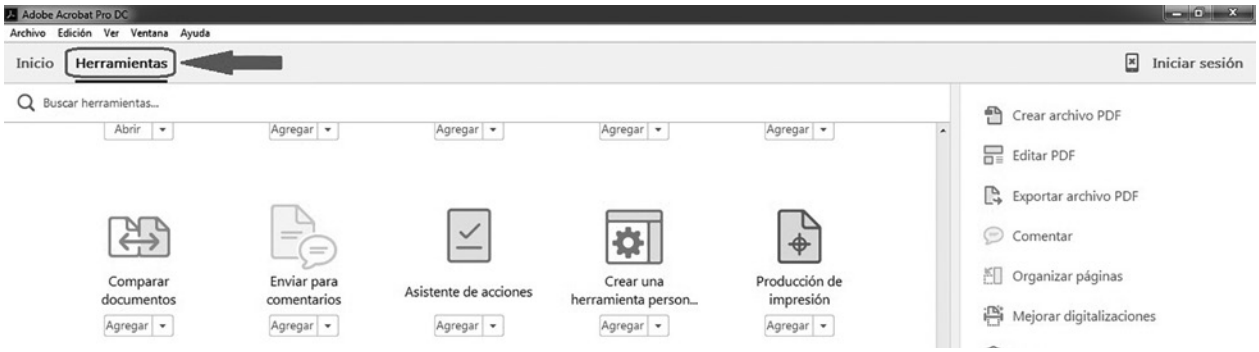


Figura 7.

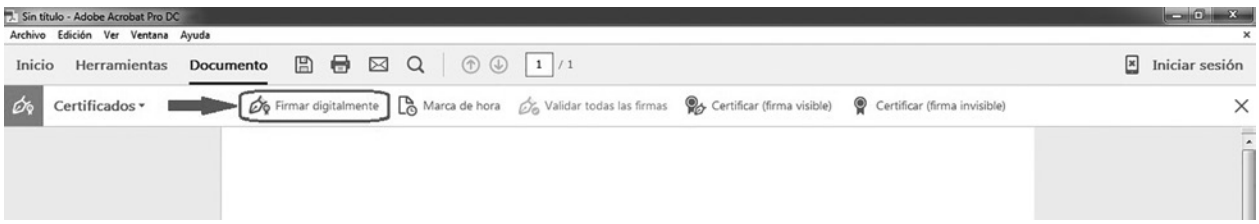


Figura 8.

Acrobat le solicitará que dibuje un rectángulo haciendo clic con el mouse y arrastrando el cursor hasta el extremo opuesto donde desee ubicar su firma.

Aparecerá entonces el rectángulo de diálogo *Agregar un ID digital*.

Elija *Un ID digital nuevo*.

Clic en *Siguiente* > *Nuevo archivo de ID digitales...* > *Siguiente* y llene los campos con su información.

Nótese que se requieren: el nombre, la unidad organizativa, el nombre de la organización, la dirección de correo electrónico, el país o región, el *Algoritmo de clave* y *Usar ID digital para* (fig. 9).

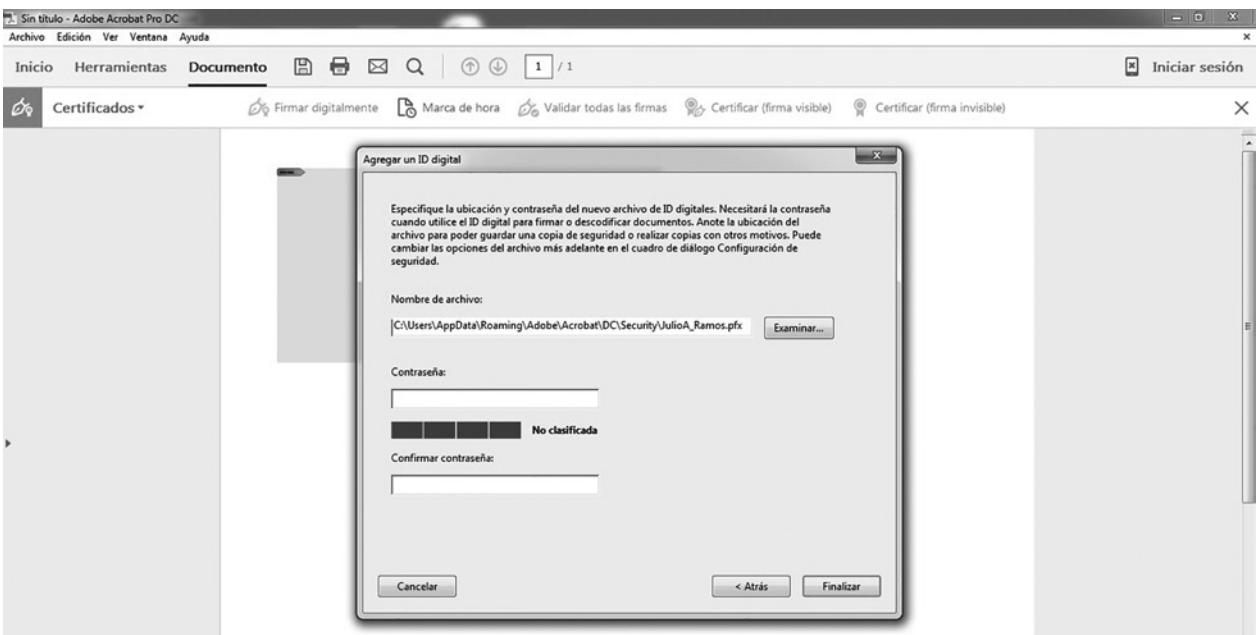


Figura 9.

Al hacer click en *Siguiente* > aparecerá (fig. 10):

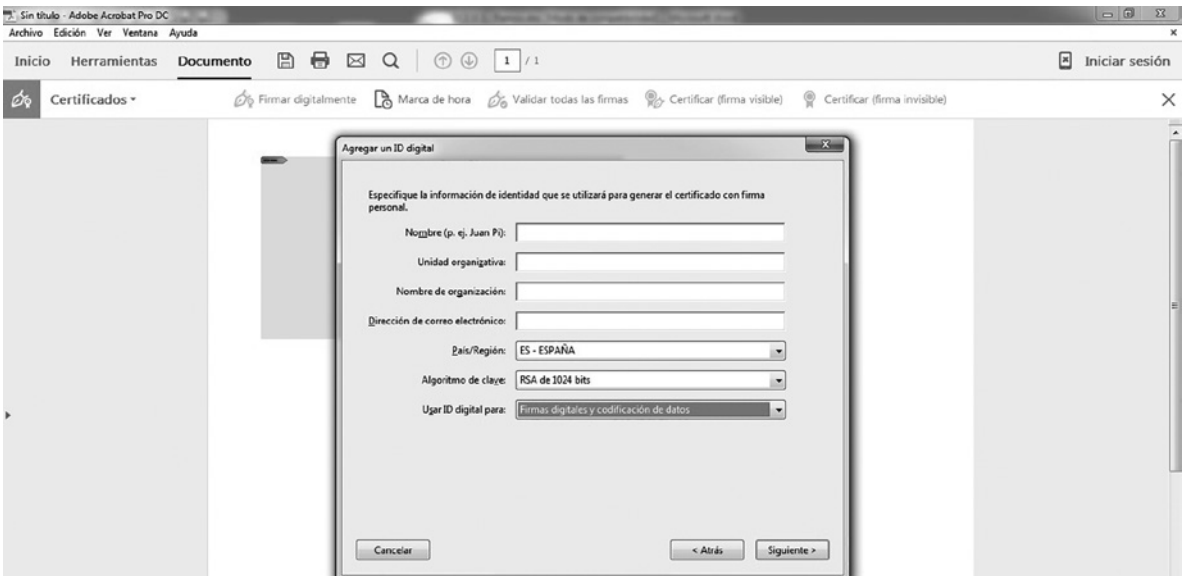


Figura10.

Es necesario ahora elegir una ubicación en el disco rígido y guardar el documento que contendrá lo que constituye la CLAVE PRIVADA con su correspondiente *contraseña*.

Haga clic en *Finalizar* para guardar su identificación digital (CLAVE PÚBLICA) y se puede volver al documento inicial que se pretendía firmar para seleccionar dentro del Acrobat el diálogo de *Firmar documento* donde se puede ahora seleccionar su ID desde el menú que dice *Firmar como*.

Debajo del campo *Firmar como*, escriba su contraseña y seleccione la *Identificación digital*. Usted va a notar que la firma digital que se ve por defecto muestra una firma de texto simple con el característico logo del Acrobat debajo. Esta es la apariencia estándar. Se puede cambiar a la apariencia deseada —una con la firma manual digitalizada u otra— eligiendo el nombre dado oportunamente del menú de *Apariencia.*

Al hacer clic en el botón para firmar digitalmente el documento se le sugerirá guardar el archivo (fig. 11).

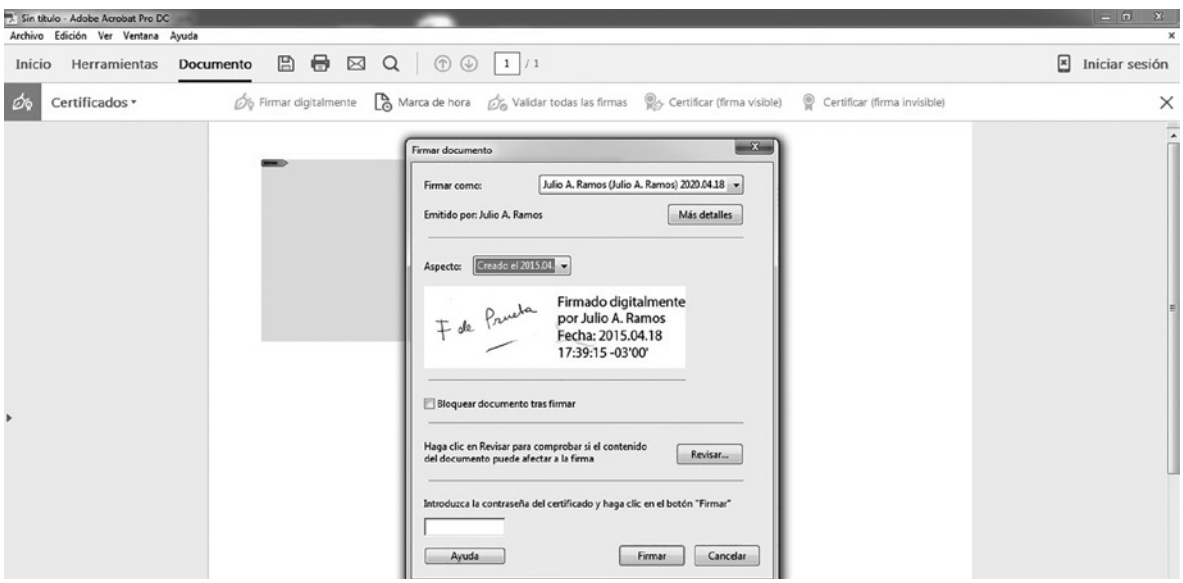


Figura 11.

Ud. tendrá ahora un documento que ha sido firmado oficial y digitalmente con su firma manuscrita y que es legal desde todo punto de vista (fig. 12).

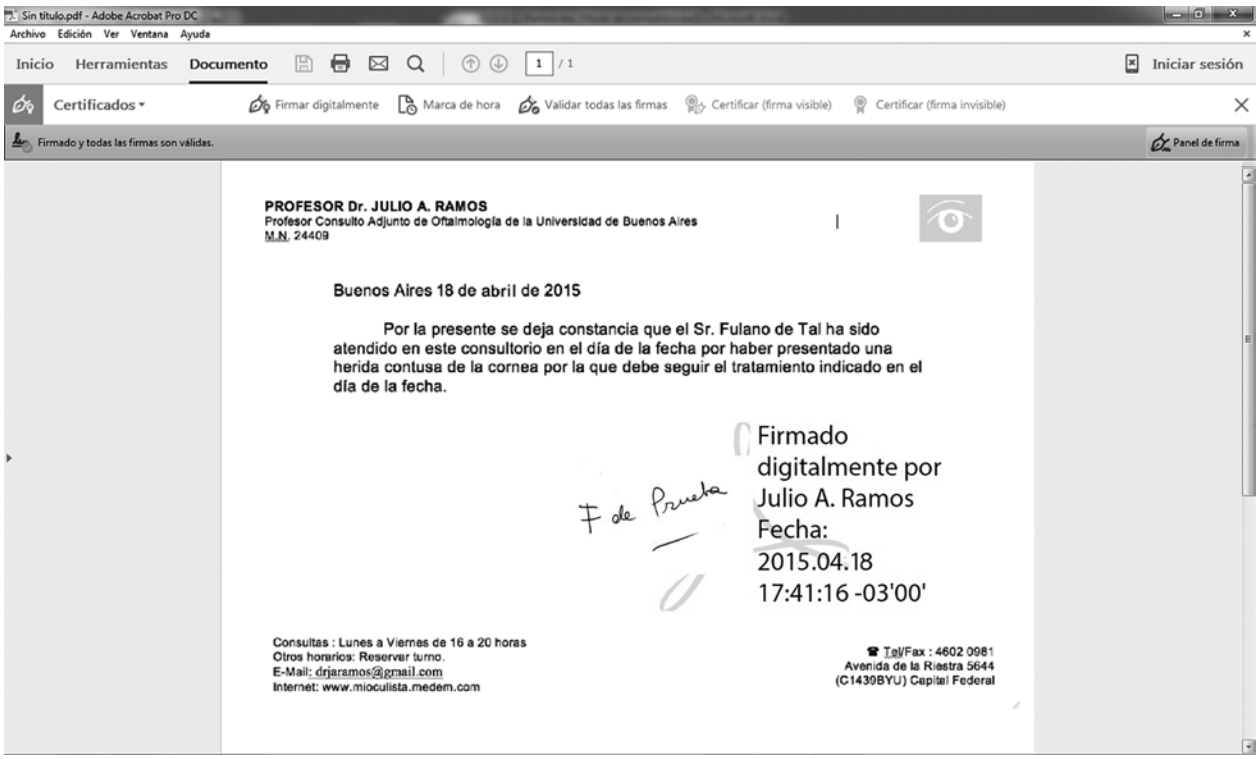


Figura 12.

Procedimiento para usar por el receptor del documento firmado para evaluar su autenticidad

Para que el receptor pueda constatar la validez de la firma el autor del documento firmado debe enviarle por email junto con este documento el certificado de autenticidad (clave pública).

Este archivo creado por Acrobat tiene una extensión .FDF (fig. 13).

Figura 13.

Si es la primera vez que el receptor recibe un documento firmado de esta persona debe proceder a abrirlo con el Acrobat Reader. Al abrirlo se encontrará con el cuadro de la figura 14.

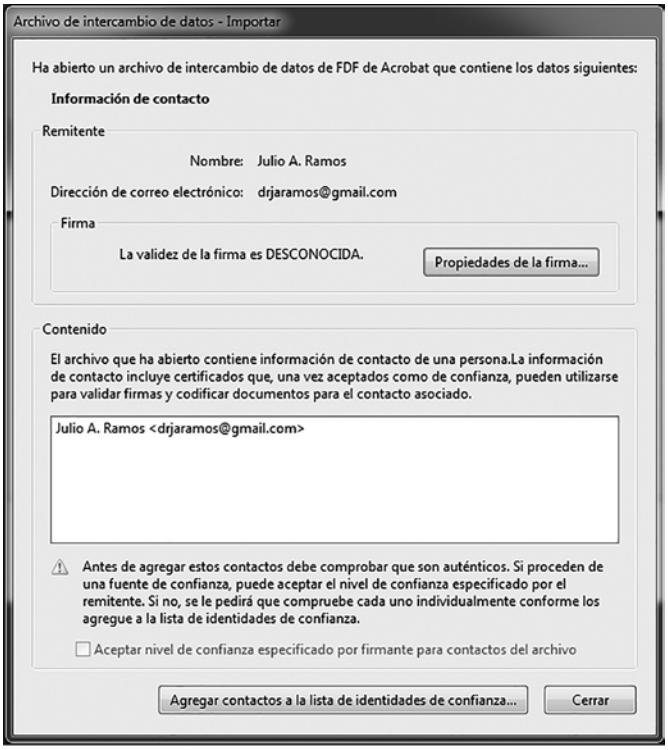


Figura14.

Si uno confía en el contacto debe hacer clic en *Agregar contactos*... para que aparezca la pantalla siguiente, tildar los ítems especificados y luego OK (fig. 15).

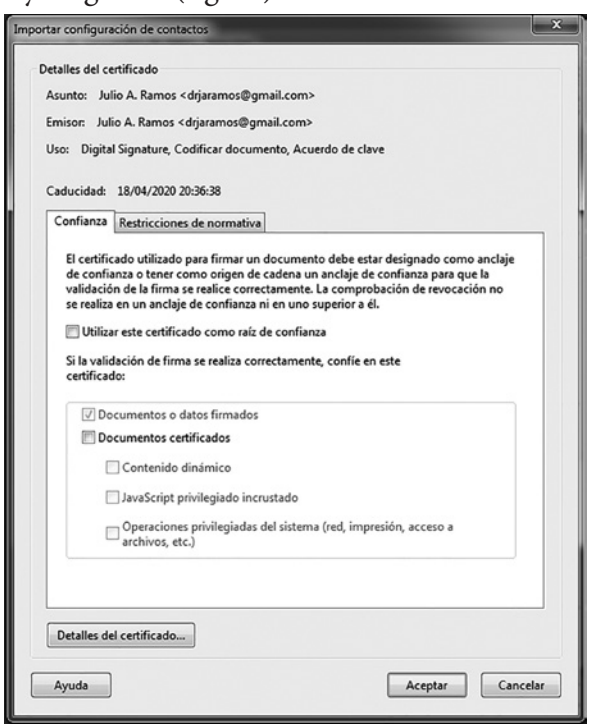


Figura 15.

Si uno quiere ver con más detalle el certificado, puede hacer clic en *Detalles del certificado*... con lo verá la pantalla de la figura 16.

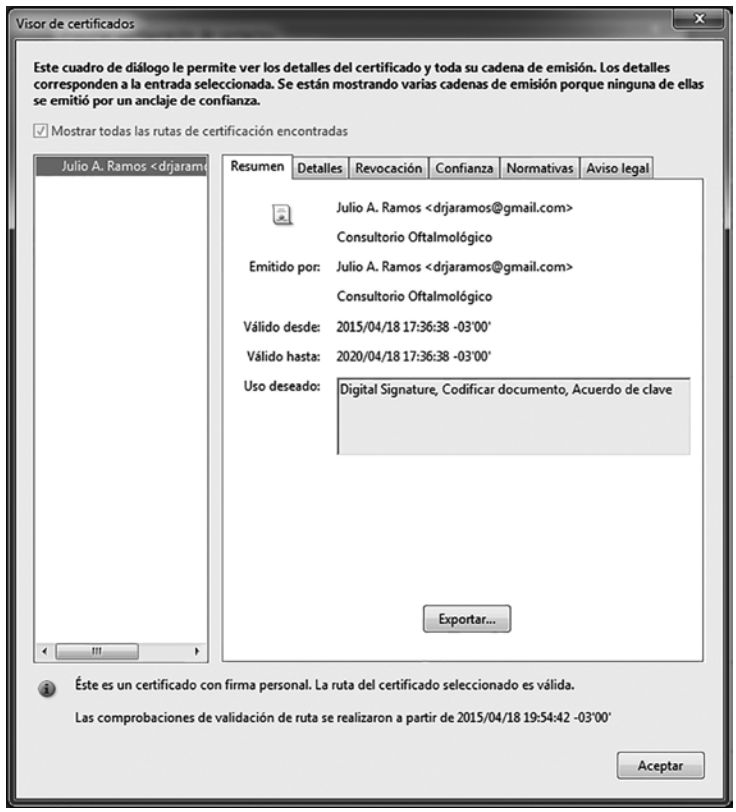


Figura 16.

Al aceptar la última pantalla el programa informará que se ha completado la importación del certificado (fig. 17).

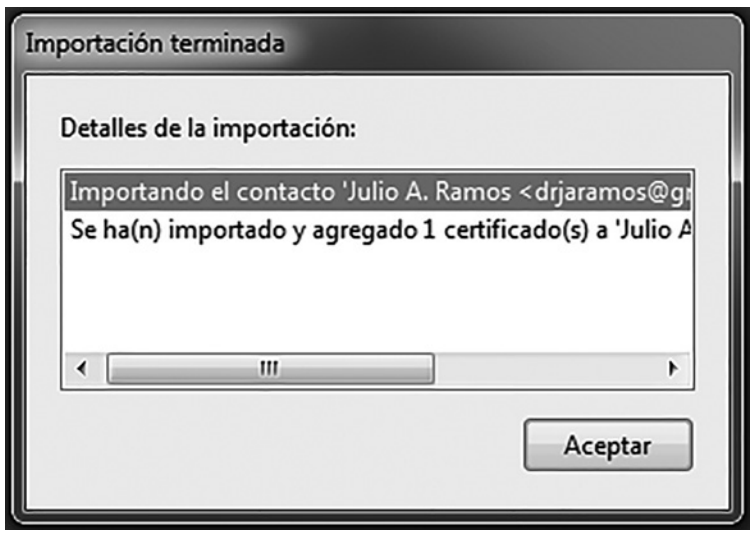


Figura 17.

Teniendo abierto el Acrobat Reader se puede constatar que se ha importado correctamente el certificado haciendo clic en *Más...* en la sección "Identidades y certificados de confianza" en *Edición* > *Preferencias* > *Firmas* (fig. 18).

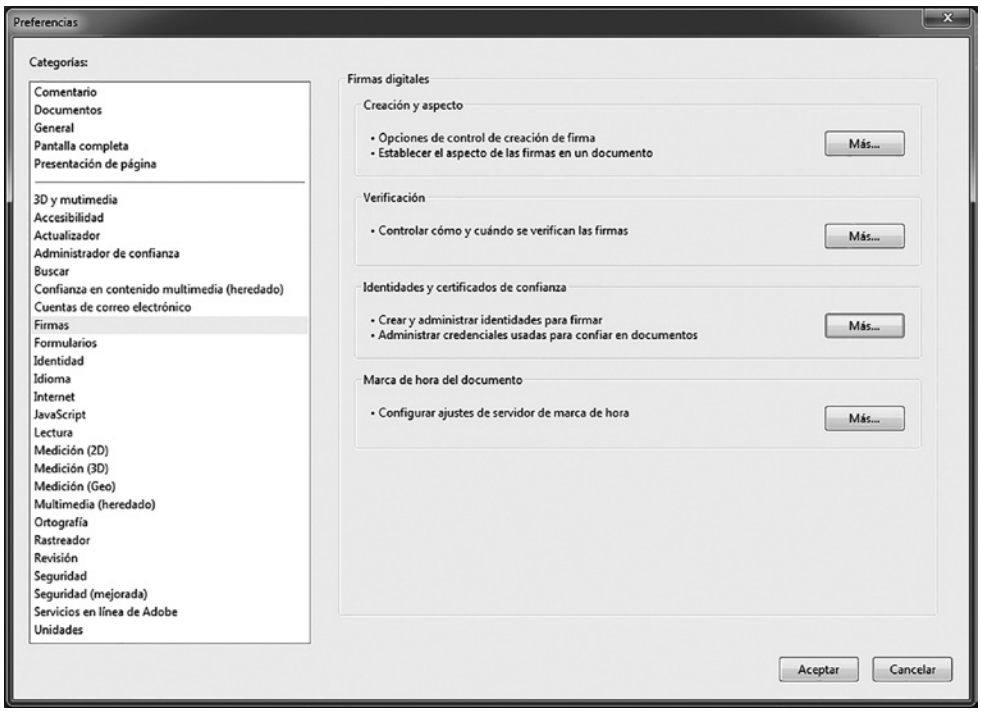


Figura18.

Estos documentos confiables se muestran en dos formas. Una es un listado de nombres y otra es un listado de certificados como puede verse en la figura 19.

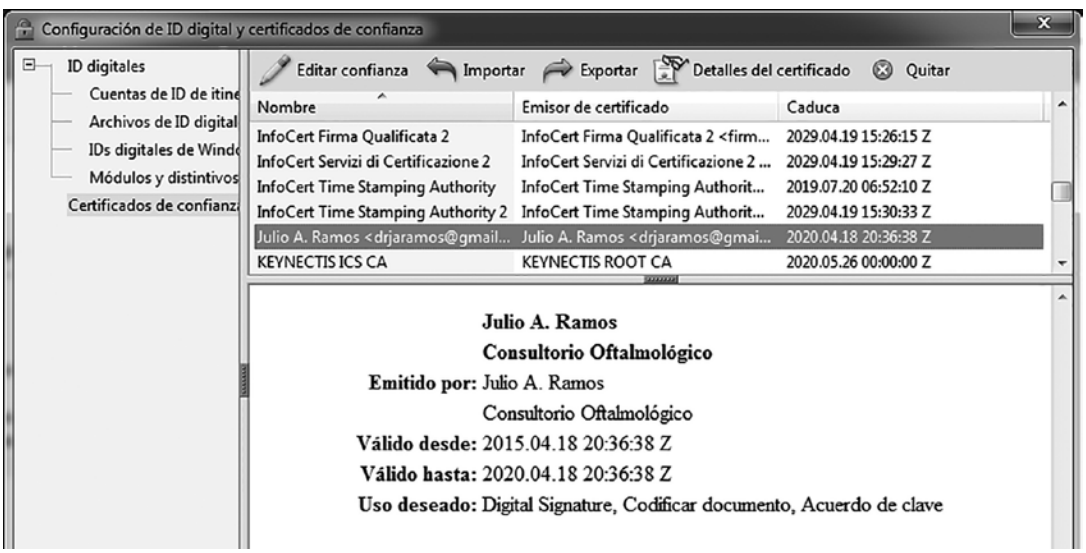


Figura 19.

Este proceso de importación de los certificados debe hacerse solo una vez por cada contacto que así lo requiera.

A partir de este momento, cuando se reciba un documento firmado y uno haga clic sobre la firma aparecerá la pantalla que le otorga validez a la firma digital y al documento que la contiene.

Referencias

1. Lassizuk RA. *Oftalmología medicolegal, laboral y previsional*. Buenos Aires: Quorum, 2003, p. 301.
2. Resumen de curriculum vitae del Dr. Humberto Fernán Mandirola Brieux, 2010. Disponible en: http://biocom.com/staff/mandi.html
3. La historia clínica informatizada apreciaciones sobre su viabilidad. *Revista Asoc Méd Arg* 1997; 110: 40. Disponible en: http://www.ama-med.org.ar/publicaciones_revistas3.asp?id=114.
4. Historia clínica electrónica. En: Proyecto Angel. Disponible en: http://www.proyecto-angel.net/
5. VeriSign: internet infrastructure services for the digital world, Security (SSL certificates), domain name services, DDOS mitigation and identity protection Disponible en: http://www.verisign.com/
6. Thawte SSL Certificates. SSL certificates and SSL certificates with extended validation (EV SSL) from Thawte, the global SSL certificate authority. Disponible en: http://www.thawte.com/ssl/index.html
7. SSL certificates from a leading SSL certificate authority: Geotrust. Disponible en: http://www.geotrust.com/
8. The leader in file encryption software, hard drive encryption, and enterprise security: PGP Corporation. Available from: http://www.pgp.com/index.html
9. Herlocker J. L., Konstan J. A. An algorithmic framework for performing collaborative filtering. *Proceeding SIGIR '99: proceedings of the 22nd annual international ACM SIGIR conference on research and development in information retrieval*. New York: ACM, 1999, p. 230-237.
10. Firma digital. En: *Wikipedia, la enciclopedia libre*. Disponible en: http://es.wikipedia.org/wiki/Firma_digital
11. *Laboratorio de firma digital*. Disponible en: http://www.jefatura.gob.ar/archivos/pki/Laboratorio.pdf
12. *About the national e-prescribing patient safety initiative*. Disponible en: http://www.nationalerx.com/about-us.htm
13. Trajtenberg, Julio O. *La elección de la autoridad certificante.* Disponible en: http://www.powershow.com/view/2806fe-ZGM5Z/LA_FIRMA_DIGITAL_HOY_powerpoint_ppt_presentation
14. *Semana profesional*. Corrientes, 15 enero de 2008. Disponible en: http://www.semanaprofesional.com/?nota=9953
15. Sistema FARO. Disponible en: http://www.sistemafaro.net/index.html

Instrucciones para los autores

La revista Oftalmología Clínica y Experimental acepta trabajos originales de investigación clínica, procedimientos quirúrgicos e investigación básica; informes de series de casos, informes de casos, comunicaciones breves, cartas de lectores, trabajos de revisiones sistemáticas y casos en formato de ateneos. Los trabajos originales pueden ser enviados en español, inglés o portugués.

El Comité Editorial de la revista adhiere a los principios establecidos por el International Committee of Medical Journal Editors, se ajusta a los principios de la Declaración de Helsinki y a los principios de cuidado de animales para experimentación de la Association for Research in Vision and Ophthalmology.

Los manuscritos y las imágenes deben ser enviados por correo electrónico a la siguiente dirección: secretaria@oftalmologos.org.ar

Cada manuscrito debe ser acompañado por una carta indicando la originalidad del trabajo enviado, con la firma de conformidad de todos los autores para que el trabajo sea publicado y puesto en el sitio web. En casos de más de 5 (cinco) autores para trabajos originales y 3 (tres) autores para los demás tipos de trabajo, se debe justificar por escrito la participación de los autores y la tarea que realizó cada uno.

Los trabajos que incluyan sujetos experimentales deben mencionar haber leído y estar de acuerdo con los principios establecidos en las declaraciones para el uso de individuos y animales en proyectos experimentales.

Los trabajos con intervención en pacientes o con información epidemiológica de individuos deben tener una carta de aprobación por el Comité de Etica de la institución donde se realizó el trabajo.

Instrucciones generales

Todos los trabajos deben ser escritos con el programa Word (Microsoft Office) en páginas tipo carta 21,6 x 26,9 cm dejando 2,5 cm de espacio en los cuatro márgenes y utilizando la familia tipográfica *Times New Roman*, tamaño de cuerpo 12, en formato "normal" (sin negrita ni cursiva) y con renglones a doble espacio. Cada página debe ser numerada consecutivamente desde la primera hasta la última con un título abreviado del trabajo y números correlativos automáticos. Aunque la extensión de los trabajos originales tienen un límite variable en general no debe superar las 6.000 palabras.

Formato básico

a) Página inicial: título en español y en inglés, autores y filiación académica, dirección y email del autor responsable; palabras clave en español y en inglés. Se debe incluir toda institución o industria que haya financiado el trabajo en parte o en su totalidad.

b) Resumen en español que no ocupe más de una página o 250 palabras y deberá ser *estructurado*, es decir que tiene que incluir los subtítulos: *Propósito/Objetivo*, *Métodos*, *Resultados* y *Conclusiones*.

c) Abstract (inglés) de la misma extensión al resumen y *estructurado* también según estos ítem: *Purpose*, *Methods*, *Results* y *Conclusions*. No se aceptarán traducciones automáticas con procesadores de texto.

d) Cuerpo del trabajo dividido en: *Introducción*, *Material y métodos*, *Resultados* y *Discusión*.

e) Las referencias bibliográficas de acuerdo con formatos de las publicaciones médicas. Numeradas en forma consecutiva según orden de mención en el texto.

Ejemplos:

- **Artículos en revistas:**

Halpern SD, Ubel PA, Caplan AL. Solidorgan transplantation in HIV-infected patients. *N Engl J Med* 2002; 347:284-7.

- **Libro:**

Murray PR, Rosenthal KS, Kobayashi GS, Pfaller MA. *Medical microbiology*. 4th ed. St. Louis: Mosby, 2002.

- **Texto electrónico en CD:**

Anderson SC, Poulsen KB. *Anderson`s electronic atlas of hematology* [CD-ROM]. Philadelphia: Lippincott Williams & Wilkins; 2002.

- **Sitios web en internet:**

Cancer-Pain.org [sitio en internet]. New York: Association of Cancer Online Resources, Inc.; c2000-01 [actualizado 2002 May 16; citado 2002 Jul 9]. Disponible en: http://www.cancer-pain.org/ (consultado el 20 ene. 2010)

f) Tabla/s escrita/s en Word con espacios entre columnas realizados con el tabulador. Cada tabla debe tener un título breve. No copiar tablas de Excel o Power Point. Cada tabla debe ser numerada en forma consecutiva según mención en el texto. Incluir las tablas al final del manuscrito no entre los párrafos del texto.

g) Leyendas de las ilustraciones (figuras y gráficos). Numerada en forma consecutiva según mención en el texto.

Ilustraciones

Figuras. Deben ser en blanco y negro (escala de grises de alto contraste). La resolución de captura inicial de las imágenes no debe ser menor de 300 dpi y el tamaño mínimo es de 10 cm de ancho. Se enviarán en formato TIFF o JPG *sin comprimir*. En caso de haber sido retocadas con Photoshop debe ser aclarado en que consistió la modificación en la carta que acompaña el envío del manuscrito. Las figuras en color tienen un costo adicional a cargo de los autor/es. Las figuras com-

binadas deben realizarse en Photoshop. Las letras o textos dentro de las figuras tienen que tener un tamaño tal que al reducir la imagen a 10 cm de ancho las letras no sean más chicas que 3 mm de alto. Usar letras de trazos llenos. *No usar figuras extraídas de presentaciones en Power Point*. Ninguna figura debe contener información del paciente ni poder reconocerse el paciente a través de la imagen excepto que éste dé su consentimiento por escrito para hacerlo.

Importante: Todas las imágenes deben ser originales y no pueden ser obtenidas de ningún medio digital que no sea del propio autor. En caso de imágenes cedidas por otro autor esto debe estar claramente mencionado entre paréntesis en la leyenda de la figura.

Gráficos. Los gráficos deben ser realizados en programas destinados a ese fin y guardados en forma TIFF o JPG con resolución inicial de 1200 dpi. No se deben enviar gráficos realizados en Excel o Power Point. Los gráficos serán impresos en blanco y negro aconsejándose el uso de tramas claramente definidas para distintas superficies.

Instrucciones particulares para los distintos formatos

Trabajos originales. Pueden ser de investigación clínica aplicada, técnicas quirúrgicas, procedimientos diagnósticos y de investigación oftalmológica experimental básica. Se seguirán los lineamientos mencionados previamente en términos generales.

Comunicaciones breves. Serán hallazgos diagnósticos, observaciones epidemiológicas, resultados terapéuticos o efectos adversos, maniobras quirúrgicas y otros eventos que por su importancia en el manejo diario de la práctica oftalmológica requieren de una comunicación rápida hacia los médicos oftalmológos.

Series y casos. Se estructurarán en: *Introducción*, *Informe de caso*, *Comentarios*. El resumen consistirá de una breve descripción no estructurada que incluya el porqué de la presentación, la información más destacada de lo observado y una conclusión. El texto tendrá una extensión máxima de 1000 palabras incluyendo no más de 5 a 7 referencias bibliográficas y hasta 4 fotografías representativas.

Cartas de lectores. Serán dirigidas al editor y su texto no podrá exceder las 500 palabras. Pueden tratar sobre dichos y publicaciones en la misma revista o comentarios sobre otras publicaciones o comunicaciones en eventos científicos médicos.

Revisiones sistemáticas. Deben actualizar un tema de interés renovado y debe realizarse basadas en una precisa revisión, lectura y análisis de la bibliografía. Debe incluir un índice de los subtemas desarrollados, las bases de datos bibliográficas utilizadas (tradicionales y no tradicionales) y una descripción de cómo se realizó la búsqueda y criterios de selección de las publicaciones.

Casos en forma de ateneos. Los manuscritos debe incluir: 1) página inicial (igual que en los demás trabajos), 2) presentación del caso con la información necesaria para realizar un diagnóstico presuntivo, 3) discución incluyendo diagnósticos diferenciales y procedimientos que pueden colaborar en la realización del diagnóstico, 4) resultados de los procedimientos diagnósticos, 5) diagnóstico, 6) seguimiento, 7) comentarios y 8) bibliografía. En lugar de resumen final del manuscrito se realizará una síntesis sumaria del caso presentado.

Imágenes en oftalmología. Se recibirán una o dos figuras que ilustren en forma excepcionalmente clara una enfermedad, evolución o resolución quirúrgica. Las imágenes seguirán las normas requeridas para ilustraciones. El texto —excluyendo el título, autores y bibliografía— no deberá exceder las 250 palabras. Se podrán incluir no más de 3 referencias bibliográficas.

Información suplementaria

International Committee of Medical Journal Editors. *Uniform requirements for manuscripts submitted to biomedical journals: writing and editing for biomedical publication.* Se obtiene de http://www.icmje.org. [actualizado a abril 2010, consultado el: 19 de noviembre de 2010].

Nota: El objetivo del Comité editorial es alcanzar un nivel de excelencia en los trabajos aceptados para su publicación con el fin acceder a bases de datos de información médica internacionales. Tanto el Comité editorial como las autoridades del Consejo Argentino de Oftalmología son conscientes de las dificultades que tiene un oftalmólogo de atención primaria para la realización de trabajos, es por eso que a través de la secretaría de la revista se apoyará con los medios técnicos adecuados a aquellos autores que lo soliciten.

Si necesita más información comuníquese con el teléfono (011) 4374-5400 o envíe un mail a: revistacientifica@oftalmologos.org.ar

---

*Los trabajos de poblaciones y estudios comparativos deben seguir los lineamientos de los ensayos clínicos (ver Consort E-Checklist and E-Flowchart. Acceso: http://www.consort-statement.org/ [última consulta: 19 de octubre de 2010]). Aquellos manuscritos con análisis estadísticos deben mencionar los procedimientos utilizados y en la carta de presentación aclarar quién realizó el análisis estadístico. Las abreviaturas deben ser las de uso frecuente y utilizando las siglas generalmente mencionadas en publicaciones de la especialidad. Se desaconseja la creación de nuevas abreviaturas de uso común. La primera vez que aparece la abreviatura debe estar precedida por la/s palabra/s originales. Las unidades de medida deben adecuarse al sistema internacional de unidades métricas (SI). Para las aclaraciones se debe utilizar el siguiente orden de signos: *, †, ‡, §, ‖, ¶, **, ††, ‡‡, §§

CAO 2015

Jornadas Argentinas de Oftalmología

13 AL 16 DE MAYO · HOTEL HILTON · BUENOS AIRES

Mucho más que un congreso

www.oftalmologos.org.ar/jornadas

Ana Juan Congresos.
(+5411) 4958-2504. admin@anajuan.com
Consejo Argentino de Oftalmología.
(+5411) 4374-5400. secretaria@oftalmologos.org.ar

CAO | Consejo Argentino de Oftalmología

Tte. Gral. Juan D. Perón 1479, PB
C1037ACA Buenos Aires, Argentina
Teléfono 54 (11) 4374-5400 líneas rotativas

Oftalmología Clínica y Experimental
www.oftalmologos.org.ar/publicaciones/OCE/