IV Conferencia Científica Internacional
Universidad de las Ciencias Informáticas

Temática: Mecanismos de seguridad

Mecanismo de protección de información basado en la PKI nacional para el sistema XAVIA HIS

Information protection mechanism based on national PKI for XAVIA HIS system

Especialista de Posgrado Yanssel Urquijo Morales [1*], Dr.C. Arturo Orellana García [2]

[1] Universidad de las Ciencias Informáticas, Cuba. Carretera a San Antonio de los Baños, km 2 ½, Torrens, Boyeros, La Habana, CP.: 19370. yurquijo@uci.cu
[2] Universidad de las Ciencias Informáticas, Cuba. Carretera a San Antonio de los Baños, km 2 ½, Torrens, Boyeros, La Habana, CP.: 19370. aorellana@uci.cu

[*] Autor para correspondencia: yurquijo@uci.cu

Resumen
Los sistemas informáticos empleados en el sector de la salud para la gestión de la información sanitaria de un paciente son responsables de la seguridad de los datos. Esto implica garantizar respecto a la información médica: que no se haya alterado o manipulado durante su almacenamiento o transporte (integridad); debe quedar constancia de quién ha llevado a cabo cada acción, de forma que éste no pueda negarlo (no repudio) y tener registro de la fecha y hora de la creación de la información original (temporalidad). Para garantizarlo se emplean instrumentos como la firma digital, de forma que, la identidad del firmante acaba vinculada a este de forma exclusiva (autenticidad). El presente trabajo tiene como objetivo proponer un mecanismo de protección de información clínica electrónica para sistema XAVIA HIS, utilizando firma digital, teniendo como base la infraestructura de llave pública nacional como Autoridad Certificadora Raíz. Para lograrlo se realizó un análisis documental sobre la actualidad del tema, se realizaron entrevistas a administrativos, gestores hospitalarios y especialistas en seguridad informática, lo cual permitió crear las bases de la investigación. Como resultado de la investigación, se obtuvo un mecanismo de protección de información para el intercambio seguro de los registros médicos entre instituciones de salud que cuenten con el sistema XAVIA HIS.

Palabras clave: firma digital; PKI; sector de salud; seguridad de la información

Abstract
The computer systems used in the health sector for the management of a patient's health information are responsible for the security of the data. This implies guaranteeing regarding medical information: that it has not been altered or

manipulated during storage or transport (integrity); It must be recorded who has carried out each action, so that it cannot deny it (non-repudiation) and have a record of the date and time of the creation of the original information (temporality). To guarantee this, instruments such as the digital signature are used, so that the identity of the signer ends up exclusively linked to it (authenticity). The objective of this work is to propose a mechanism for the protection of electronic clinical information for the XAVIA HIS system, using a digital signature, based on the national public key infrastructure as the Root Certification Authority. To achieve this, a documentary analysis was carried out on the current status of the subject, interviews were carried out with administrators, hospital managers and specialists in computer security, which allowed to create the bases of the investigation. As a result of the investigation, an information protection mechanism was obtained for the secure exchange of medical records between health institutions that have the XAVIA HIS system.

Keywords: *digital signature; PKI; health sector; information security.*

Introducción

La informatización del Sistema de Salud constituye un reto para Cuba. En los últimos años se vienen dando pasos para migrar la historia clínica tradicional en papel a un formato electrónico, la llamada historia clínica electrónica (HCE). Un documento digital donde se almacena y organiza la información sanitaria y chequeos rutinarios del paciente, ya sea de la atención primaria, secundaria o una clínica especializada. Esto hecho exige una mayor integración y necesidad de intercambio de información según se establece en los principios de la estrategia de informatización del sector de la salud en Cuba. (Cuba, 2017)

En el entorno sanitario los datos personales de salud son datos sensibles. La protección de la privacidad y la salvaguarda de la intimidad del paciente es uno de los criterios esenciales al tratar la información sanitaria, los aspectos reglamentarios de privacidad y seguridad electrónica son críticos. Los resultados de los actos médicos (consulta, resultados de análisis de laboratorio, procedimientos médicos, informes operatorios, complementarios) requiere que en el intercambio de información entre el emisor y receptor exista absoluta confianza de que los datos no han sido alterados. (Gutiérrez et al., 2017)

Los datos pueden ser transmitidos por medios de comunicación o redes no seguras hasta alcanzar su destino. En cualquiera de ellos se podría leer y hasta modificar el contenido, comprometiéndose así la confidencialidad y la integridad de la información. Es por ello, que, al hacer uso de estas tecnologías de información y comunicaciones los datos del paciente se encuentran expuestos a una serie de peligros tales como: (Holguín García, 2018)

- Ataques a la privacidad de la información: Consiste en que personas no autorizadas puedan conocer la información que no les corresponden.
- Ataques a la integridad de la información: Consiste en que personas no autorizadas intercepten en puntos intermedios entre el origen y destino información y ésta sea modificada y trasmitida nuevamente hacia su destino final.
- Negación de ejecución de transacciones por parte de los usuarios: Consiste en que un usuario que haya realizado una transacción en un sistema, niegue después haberla hecho. Este principio de la seguridad de información se llama No-repudio.

Los sistemas de gestión de la información resultante de los actos médicos requieren del empleo de mecanismos que permitan autenticar, autorizar, administrar y auditar cualquier acceso o modificación de los datos, así como, las transacciones generadas con el fin de resguardar los principios básicos de la Seguridad de Información los cuales son integridad, confidencialidad y disponibilidad. (Crespo Martínez, P. E, 2016)

Uno de los mecanismos empleados en la actualidad para garantizar estos principios es el cifrado asimétrico, basado en el manejo de llaves públicas y privadas a través de certificados digitales. (Joshi and Avinash Karkade, 2015)

El Centro de Informática Médica (CESIM), de la Universidad de las Ciencias Informáticas (UCI), se encarga de desarrollar productos, y brindar servicios y soluciones informáticas para el sector de la salud, contribuyendo con ello a la informatización de esta importante actividad social y a la formación integral de profesionales de la informática y la salud.

Dicho centro cuenta con el Sistema de Información Hospitalaria XAVIA HIS, una solución integral para la gestión médica de hospitales y centros de salud. El mismo permite la recolección, almacenamiento, procesamiento y comunicación de la información relacionada con la atención al paciente. Esta información es manejada de forma integrada y única (Historia Clínica Electrónica única) siguiendo el estándar HL7-CDA. El sistema XAVIA HIS, implementa una infraestructura interna de firma y validación digital que garantiza la integridad, temporalidad, autenticidad y autoría de los documentos clínicos electrónicos que se generan en las entidades hospitalarias.

Después de realizadas las entrevistas a varios técnicos y profesionales de la salud, al equipo de desarrollo del sistema y a varios especialistas en seguridad informática, se identificaron las siguientes limitantes:

Los documentos clínicos firmados solo pueden ser validados por el propio sistema, o por otra instancia del mismo importando un certificado de confianza de la instancia de donde provienen los documentos digitales. Imposibilitando así, la validación por otros sistemas de tecnologías diferentes.

La creación del certificado del usuario se realiza al instante de adición del mismo al sistema y dicha información es almacenada en la base de datos del propio sistema. En el caso de que el medico necesite prestar servicio en otra institución hospitalaria que cuente con el sistema, al agregarlo se le crearía un nuevo certificado digital. Esto conllevaría a que una misma persona contaría con varios identificadores digitales.

El usuario no interactúa directamente con su firma digital y esta solo es aplicada a los documentos clínicos electrónicos (CDA). Esto imposibilita que pueda emplear su firma digital en otras actividades como la de firmar documentos clínicos electrónicos exportados al formato PDF a través del Visor de Historias Clínicas Electrónicas del propio sistema.

En la firma de los documentos clínicos electrónicos el usuario no interviene directamente. Este proceso se hace de manera transparente para él, lo cual, en principio, violaría la presunción de autoría y no repudio en un presunto caso de que sus credenciales de acceso al sistema se vean comprometidas.

Los documentos CDA firmados digitalmente no cuentan con la validez jurídica necesaria pues los certificados digitales empleados en el proceso de firma digital son creados por una Infraestructura de Llave Pública (PKI) nativa, la cual no está reconocida y no tiene validez legal.

A partir de lo anterior, la presente investigación tiene como objetivo proponer un mecanismo de protección de la información clínica electrónica para el intercambio seguro de registros médicos entre las instituciones de salud que utilicen el sistema XAVIA HIS, mediante firma digital con certificados digitales, teniendo como base la PKI nacional como Autoridad de Certificación (CA) raíz.

Métodos

La investigación sigue una estrategia metodológica analítica-descriptiva para la generación de una propuesta de mecanismo de protección de información clínica electrónica para sistema XAVIA HIS, utilizando para su validación un enfoque mixto. Entre los métodos utilizados se encuentra:

Análisis documental: para el estudio de los referentes teóricos de la investigación, con el objetivo de extraer la información necesaria para definir los procesos de firma digital basados en la PKI y su aplicación en entornos sanitarios, de forma tal que el mecanismo propuesto tuviese relevancia científica y aporte práctico.

Entrevista: se aplicó a varios técnicos y profesionales de la salud, al equipo de desarrollo para obtener toda la información necesaria respecto a cómo se realiza el proceso de firma digital de los documentos clínicos del Sistema de Información Hospitalaria XAVIA HIS, se tuvo en cuenta además la experiencia de especialistas en seguridad informática.

Encuesta: mediante su aplicación a partir de cuestionarios elaborados, se obtuvo los criterios evaluativos de los expertos que validan la solución.

Grupo Focal: Se aplicó en dos momentos, un grupo focal exploratorio para analizar la necesidad, el impacto, la pertinencia y actualidad de la propuesta. En el segundo grupo se validó el mecanismo respecto a su capacidad para proteger la información clínica electrónica de los pacientes y los beneficios de su aplicación.

Resultados

Actualmente el sistema XAVIA HIS, cuenta con una Infraestructura de firma y validación digital de los documentos clínicos electrónicos. Dicha solución surgió a partir de la necesidad de garantizar la integridad de los CDA que se generaban en el sistema.

Esta infraestructura brinda la posibilidad de crear una CA Raíz de forma local, que permite generar los certificados digitales de los usuarios en el momento en que estos son añadidos al sistema. Además de crear la Autoridad de

Sellado o Estampado de Tiempo (TSA) para el sellado de tiempo, es posible exportar el certificado raíz y ser cargado posteriormente como certificado de confianza en otra instalación hospitalaria que cuente con el sistema XAVIA HIS (Ledo, 2011). El mecanismo propuesto tiene como objetivo propiciar la validez de la información clínica electrónica en el sistema XAVIA HIS.

Una PKI sanitaria debe necesariamente basarse en la información suministrada por las instituciones de asistencia médica a la que pertenecen sus suscritores, ya que éstas son las entidades que validan y acreditan el ejercicio de la profesión de su personal. Por lo tanto, es prudente considerar que en estas entidades se implementen las Autoridades de Registro Local (LRA) y serán las responsables de solicitar los certificados digitales con los datos de cada profesional, sus roles primarios y atributos.

Por la complejidad y distribución geográfica de las unidades de salud pertenecientes al Sistema Nacional de Salud Cubano (SNS), se requiere la implementación de una PKI compleja. Bajo un esquema jerárquico teniendo como única CA raíz al Servicio Central Cifrado del Ministerio del Interior. Como premisa debe existir una CA intermedia que se encargue de gestionar todos los certificados de las instituciones sanitarias. En un nivel más bajo, las instituciones de salud implementarían una Autoridades de Registro (RA) para la gestión de la información referente a la solicitud de un nuevo certificado. Este esquema permitiría que el intercambio de información entre 2 entidades hospitalarias, pueda ser verificada su integridad a través de la CA raíz o CA intermedia. Ver Figura 1.

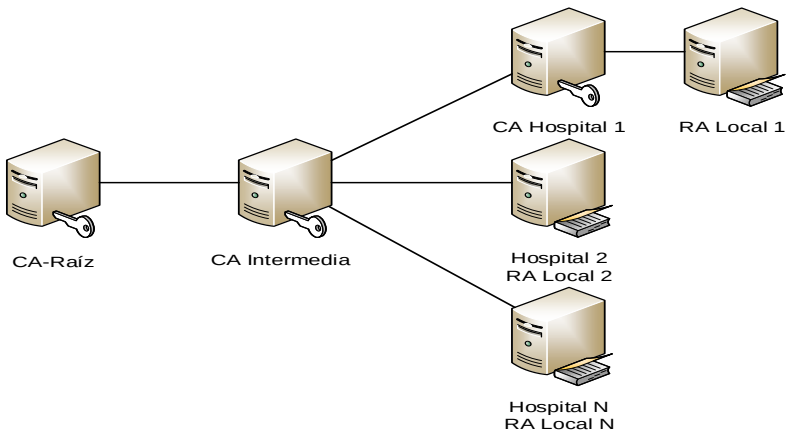

Figura 1. Propuesta de arquitectura PKI para el sistema XAVIA HIS. Fuente: Elaboración propia.

Para el correcto funcionamiento del mecanismo propuesto, previamente las entidades deben registrar los datos del personal que interactuara con el sistema en la Autoridad de Registro (RA) con el fin de obtener su certificado digital que posteriormente utilizara para la firma digital. A continuación, se describen los pasos. Ver figura 2.

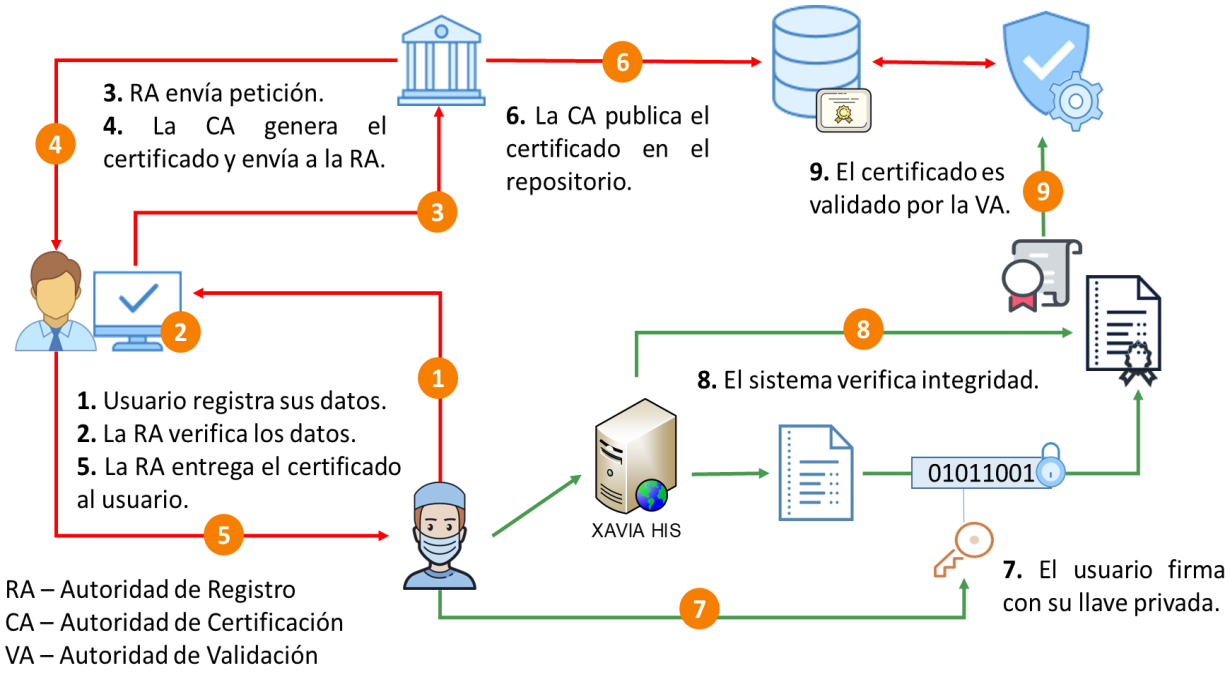

Figura 2. Propuesta de mecanismo de firma digital para el sistema XAVIA HIS. Fuente: Elaboración propia.

1. El personal sanitario registra sus datos en la Autoridad de Registro ya sea mediante el llenado de un formulario online o una planilla impresa.
2. La Autoridad de Registro verifica los datos referidos por los usuarios.
3. Luego de verificar que los datos sean correctos, envía la petición a la Autoridad de Certificación (CA).
4. Una vez aceptada la solicitud, la CA emite el certificado y este es enviado a la RA.
5. La Autoridad de Registro entrega el certificado digital al usuario final.
6. Al mismo tiempo la Autoridad de Certificación publica el certificado en su repositorio.
7. Ya una vez que el usuario posea su certificado digital puede desde el sistema XAVIA HIS realizar la firma digital de los CDA, empleado su llave privada.

8. El sistema durante el proceso de verificación de la firma, comprobar la integridad del documento.
9. El mecanismo verificar a través de la Autoridad de Validación (AV) el estado del certificado digital empleado en la firma.

Con la finalidad de adoptar el uso de los certificados digitales emitidos por una entidad certificadora externa, se hace necesario el cambio en diferentes funcionalidades del sistema XAVIA HIS. A continuación, se detallan la propuesta de cambios a implementar.

El módulo configuración tiene la funcionalidad Gestionar usuario, la cual permite introducir los datos asociados a la creación del usuario. Al adicionar un nuevo usuario al sistema, se genera el *keystore* que contendrá el certificado digital del usuario y su respectiva clave privada y es almacenado en la base de datos del propio sistema XAVIA HIS. Este proceso de generación de la identidad digital se eliminaría una vez se obtengan los certificados de la entidad certificadora externa.

La funcionalidad Configuraciones personales, muestra la interfaz que permite realizar algunas configuraciones de la cuenta de usuario, tal es el caso de la contraseña, la foto que desea, el idioma, el tema visual, así como personalizar el menú. A esta funcionalidad se le debe incluir la opción para especificar la ruta del certificado digital que es entregado por la entidad certificadora externa y poder utilizar este en el sistema.

La funcionalidad Seguridad avanzada, contiene las opciones, Certificado raíz, Certificados de confianza, Identidades digitales y Gestionar servidores.

La opción Certificado raíz, permite visualizar y modificar los detalles del certificado raíz del sistema, el cual es generado en el proceso de instalación. Este certificado es utilizado como raíz para la generación de los certificados de los usuarios y firmar los mismos. Esta opción se eliminaría, esta tarea se delegaría en la Entidad Certificadora externa.

La opción Administrar identidades digitales, permite visualizar el listado de usuarios del sistema y la información referente a la fecha de creación y vencimiento de su certificado digital. Desde esta interfaz es posible regenerar nuevamente todos los certificados de los usuarios mediante la opción “Generar certificados automáticamente”. Esta

interfaz no sería necesaria, todo el procesamiento necesario para la creación de la identidad del usuario recaería en la Autoridad Certificadora externa.

En los módulos que se generan documentos clínicos, estos antes de ser guardados se firman digitalmente. Para realizarlo se recupera el *keystore* del usuario autenticado que se encuentra en la base de datos y de este se extrae la clave privada, la cual es usada para realizar el proceso de firma digital del documento. La propuesta del mecanismo radica en la modificación de cómo es obtenido el *keystore* del usuario y recuperada su llave privada para gestionar la información de la firma. El *keystore* es recuperado mediante la ruta especificada por el usuario en su perfil y no desde la Base de Datos del sistema.

El módulo Visor de Historia Clínica cuenta con una funcionalidad llamada Validar CDA. La misma permite obtener el estado de validez de la firma mediante la comprobación de la identidad del firmante y la integridad del documento. La propuesta del mecanismo incluye además de estas la comprobación de la validez temporal del certificado utilizado, mediante los métodos de Protocolo de estado de certificado en línea (OCSP, *Online Certificate Status Protocol*) o Lista de Revocación de Certificados (CRL, *Certificate Revocation List*).

Como consecuencia de los cambios antes propuestos es necesario actualizar el modelo de datos. La actualización implica la eliminación de varias tablas.

Bajo estas consideraciones, se utilizará para firmar digitalmente la información médica generada en el sistema XAVIA HIS, los certificados digitales proporcionados por los propios profesionales de la salud. Garantizando así, que el intercambio de información sanitaria entre instituciones de salud este respaldado por los esquemas de seguridad que brinda la PKI.

La aplicación de un esquema jerárquico a partir de la Infraestructura Nacional de Llave Pública, donde una CA subordinada emitirá los certificados de los profesionales que interactúen con el sistema XAVIA HIS, le proporciona mayor seguridad y dota de validez jurídica a los documentos clínicos firmados digitalmente.

Discusión

La validación de la estrategia propuesta se realizó mediante los métodos: criterio de experto por el método escalamiento de Likert, se tiene en cuenta que este es un método de validación útil para verificar la fiabilidad de una investigación (Garrote and del Carmen Rojas, 2015), el grupo focal para conocer los criterios e introducir mejoras en la propuesta, a partir del intercambio con personas que pueden aportar ideas y valoraciones importantes sobre la solución, además se aplicó la técnica de Iadov para determinar el grado de satisfacción de los usuarios potenciales del mecanismo definido. Una vez aplicados estos métodos, son triangulados para lograr mayor precisión y objetividad entre las comprobaciones. La Figura 3 representa la estrategia descrita.

Figura 3. Estrategia de validación de la investigación. Fuente: Elaboración propia

Para el escalamiento de Likert se tuvo en cuenta a 13 profesionales. El 40% posee la categoría de máster en ciencias, el 30% de los encuestados trabaja en la producción de software, el otro 30% labora en el campo de la ciberseguridad y el 40% restante labora directamente en la gestión de Infraestructuras de Llave Pública. Todos fueron seleccionados por su experiencia en el área del conocimiento que aborda la presente investigación y tienen más de 5 años de experiencia en los temas relacionados.

Para el procesamiento de los resultados se empleó el método escala Likert, que consiste en identificar la frecuencia en cada categoría de la escala de Likert definida en la encuesta realizada y se calculan los por cientos de concordancia de

cada categoría de acuerdo a las características propuestas. Luego se calcula en un índice porcentual (IP), que integra en un solo valor la aceptación del grupo de evaluadores sobre las características del mecanismo resultando que el IP en todos los casos es mayor que 89. Lo cual evidencia la alta valoración por los expertos sobre la claridad y síntesis de la propuesta. Se identificaron además sugerencias y recomendaciones por parte de los expertos, las cuales fueron tenidas en cuenta para el perfeccionamiento de la propuesta.

Para el desarrollo de la técnica de Iadov se aplicó una encuesta que permitió obtener una valoración de la Satisfacción Individual (SI) de cada experto a partir de sus respuestas. Esta técnica también permite obtener el índice de satisfacción grupal (ISG), el cual arrojó como resultado 0.82, lo que evidencia que los especialistas encuestados están satisfechos con la propuesta.

Conclusiones

Los resultados obtenidos durante el desarrollo de la investigación permiten arribar a las siguientes conclusiones:

- El diagnóstico realizado a la seguridad de la información clínica electrónica en instituciones cubanas que utilicen el sistema XAVIA HIS, evidenció la necesidad de desarrollar un mecanismo que incremente la seguridad de la información sanitaria del paciente y le otorgue validez legal a la misma.
- La propuesta fue valorada positivamente por los expertos, refinándose a partir de mejoras sugeridas por los mismos.
- El mecanismo propuesto permite firmar digitalmente documentos clínicos electrónicos del sistema XAVIA HIS, utilizando los certificados digitales emitidos por la PKI nacional. Lo cual le otorga validez jurídica, autenticidad e integridad a la Historia Clínica Electrónica Única.

Referencias

CUBA (2017). Ministerio De Salud Pública De Cuba. Plan de desarrollo y uso de las Tecnologías de la Información y Comunicaciones del Sistema Nacional de Salud 2017 - 2021. *Revista de Información científica para la Dirección en Salud INFODIR*. Recuperado de http://www.revinfodir.sld.cu/index.php/infodir/article/view/432.

Holguín García, F. (2018). Análisis de la firma digital con base en la infraestructura de clave pública, *Hamut'ay*, ISSN-e 2313-7878, Vol. 5, No. 2, pp. 94 – 104. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=6801245.

Crespo Martínez, P. E. (2016). *Metodología de seguridad de la información para la gestión del riesgo informático aplicable a MPYMES (Tesis de Maestría)*. http://dspace.ucuenca.edu.ec/handle/123456789/26105.

Joshi, M. and R. Avinash Karkade. (2015). Network Security with Cryptography, *International Journal of Scientific Research*, Amravati. Vol. 6, No. 1, pp. 201 – 204. Recuperado de https://www.ijcsmc.com/docs/papers/January2015/V4I1201544.pdf.

Garrote P. R., del Carmen Rojas M. (2015). La validación por juicio de expertos: dos investigaciones cualitativas en Lingüística aplicada. *Rev Nebrija lingüística Apl a la enseñanza lenguas*. (18):124–39. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=6344619.

Gutiérrez t, a.t., Peña g, r., Peña g, n.i., Rosario Cruz, r. y López Silva, S., 2017. Obstáculos y retos para el desarrollo de sistemas de información en el sector salud. *Revista avances en salud*, vol. 2, no. 1, pp. 56-65. doi 10.21897/25394622.1394.

Ledo Báster, D. R. (2011). *Infraestructura de firma y validación digital de los documentos clínicos electrónicos generados por el sistema alas HIS* (Tesis pregrado). Recuperado de https://repositorio.uci.cu/handle/ident/TD_03921_10.