FIRMA DIGITAL BASADA EN CRIPTOGRAFÍA ASIMÉTRICA PARA GENERACIÓN DE HISTORIAL CLÍNICO

DIGITAL SIGNATURE BASED ON ASYMMETRIC CRYPTOGRAPHY FOR GENERATION OF MEDICAL HISTORY

Jose Cordova Ramirez
National University Mayor de San Marcos, (Perú).
E-mail: 12200082@unmsm.edu.pe ORCID: https://orcid.org/0000-0002-0850-7266

Hugo Vega Huerta
National University Mayor de San Marcos, (Perú).
E-mail: hvegah@unmsm.edu.pe ORCID: https://orcid.org/0000-0002-4268-5808

Ciro Rodriguez Rodriguez
National University Mayor de San Marcos, (Perú).
E-mail: crodriguezro@unmsm.edu.pe ORCID: https://orcid.org/0000-0003-2112-1349

Frank Escobedo Bailón
National University Mayor de San Marcos, (Perú).
E-mail: fescobedob@unmsm.edu.pe ORCID: https://orcid.org/0000-0002-2058-0976

Recepción: 07/08/2020 **Aceptación:** 29/09/2020 **Publicación:** 14/12/2020

Citación sugerida:
Cordova, J., Vega, H., Rodriguez, C., y Escobedo, F. (2020). Firma digital basada en criptografía asimétrica para generación de historial clínico. *3C Tecnología. Glosas de innovación aplicadas a la pyme, 9*(4), 65-85. https://doi.org/10.17993/3ctecno/2020.v9n4e36.65-85

RESUMEN

El presente trabajo tiene como objetivo el desarrollo de un sistema de en la cual se propone sistematizar el proceso de la redacción y generación de historiales médicos con los cuales se propone la reducción del tiempo de la generación de historiales y la reducción de recursos físicos, especialmente en lo que respecta al uso del papel, la cual los especialistas de la salud redactan en el transcurso de una consulta médica, esto además implicaría en la optimización en la gestión de los historiales médicos. El sistema planteado a desarrollar consiste en la aplicación del mecanismo de la firma digital en base al método de la criptografía asimétrica o también llamada criptografía de clave pública. Esta tecnología se aplicará principalmente mediante la aplicación de dos herramientas contempladas para el uso de la firma digital: el sistema RSA (Rivest, Shamir y Adleman) y la función hash SHA-256. La aplicación de la firma digital a los historiales médicos se mostrará implementada a través del manejo de interfaces gráficas que está planteada para que el especialista pueda redactar y manejar los historiales a su conveniencia. El sistema abordará el uso del lenguaje de programación Python y el conjunto de herramientas OpenSSL para las funciones criptográficas y PyQt5 para el desarrollo a nivel interfaces gráficas.

Se propone esta solución debido a que la tecnología de firma digital se ha planeado y posteriormente se ha estado desarrollando desde la década de 1980, son en estos últimos años que esta tecnología ha sido tomada más en cuenta para el manejo de documentos, y como este caso, de los historiales médicos.

PALABRAS CLAVE

Firma digital, Historial médico, Criptografía asimétrica, RSA, PyQt5.

https://doi.org/10.17993/3ctecno/2020.v9n4e36.65-85

ABSTRACT

The present work aims to develop a system in which it is proposed to systematize the process of writing and generating medical records which is proposed to reduce the time of generation of records and the reduction of physical resources, especially regarding the use of paper, which health specialists write in the course of a medical consultation, this would also imply the process of optimization in the management of medical records. The proposed system to develop consists of the application of the digital signature mechanism based on the method of asymmetric cryptography or also called public key cryptography.

This technology is applied mainly through the application of two tools contemplated for the use of the digital signature: the RSA system (Rivest, Shamir and Adleman) and the SHA-256 hash function. The application of the digital signature to medical records will be implemented through the handling of graphical interfaces that is proposed so that the specialist can write and manage the records at his convenience. The system will address the use of Python programming language and the software libraries OpenSSL applied for cryptographic functions and PyQt5 for development at the graphical interface level.

This solution is proposed because digital signature technology has been planned and has been subsequently developed since the 1980s, it is in recent years that this technology has been taken more into account for document management, and like this case, medical records.

KEYWORDS

Digital signature, Medical record, Asymmetric key cryptography, RSA, PyQt5.

https://doi.org/10.17993/3ctecno/2020.v9n4e36.65-85

1. INTRODUCCIÓN

De acuerdo al informe del Plan Estratégico Institucional del Hospital Nacional Daniel Alcides Carrión (2017), el hospital, con dirección en la Av. Guardia Chalaca 2176, Bellavista, Callao, es la institución de Salud de mayor complejidad en la red de establecimientos en la Provincia Constitucional del Callo, con Dependencia Administrativa de la Dirección Regional de Salud I, es además un Hospital de referencia nacional y sede de pre y post grado de la Universidad Nacional Mayor de San Marcos y otras universidades públicas y privadas.

El hospital como establecimiento de salud de categoría y nivel de complejidad III – 1 es responsable de satisfacer las necesidades de salud brindando atención ambulatoria y hospitalaria especializada, con énfasis en la recuperación y rehabilitación de problemas de salud a través de unidades productoras de servicios de salud médico-quirúrgicos de alta complejidad, teniendo población de referencia regional y nacional conforma con otros 54 establecimientos la Red de Servicios Hospitalarios de la Dirección Regional de Salud del Callao. Al ser el hospital un establecimiento donde hay tránsito de pacientes, se generan historiales médicos, las cuales recopilan información acerca de un paciente para entender mejor un problema de salud que el paciente sufre, además de tener una validación de carácter legal, lo cual la validación del especialista de la salud con su firma es de vital importancia.

2. FORMULACIÓN DEL PROBLEMA

2.1. DESCRIPCIÓN DEL PROBLEMA

Actualmente, la problemática acerca de los hospitales públicos es documentada de manera extensa en documentos oficiales estatales, reportajes y artículos periodísticos, entre otros.

Es en base a la premisa anterior, las gestiones sobre las operaciones que se realizan en un hospital suelen ser de mucha carga burocrática. Una de estas operaciones es la redacción y el posterior manejo de los

https://doi.org/10.17993/3ctecno/2020.v9n4e36.65-85

historiales médicos que se realizan en el hospital, que se realizan de forma manual y su posterior gestión también es realizada de forma manual.

2.2. BASE DEL PROBLEMA

Para generar un historial médico, se debe emitir una firma manuscrita luego de la redacción manual luego de una consulta médica, la cual es la forma más usada para la validación de las firmas y posteriormente el historial médico.

Es por este motivo que el proceso de validación del historial médico desde la redacción y posterior firma del especialista de la salud hasta su almacenamiento para una futura revisión u otra actividad que implique el uso del historial implica tiempo que se considera en demasía. Otra cuestión importante es el uso cuantioso de papel que se genera por la generación de los reportes de los historiales

2.3. OBJETIVO DE LA INVESTIGACIÓN

Se propone el desarrollo de un sistema que use la herramienta de la firma digital para la redacción y validación de los historiales médicos, con lo cual se propone brindar una reducción de la demora de las validaciones de los historiales médicos y una reducción en el uso del recurso físico del papel. A continuación, nuestros objetivos específicos**:**

- Aplicar la legalidad para el proceso de la generación de los historiales médicos.
- Validar las firmas digitales generadas en archivos PDF.
- Aplicar los estándares válidos para el desarrollo de la generación de la firma.
- Desarrollar el sistema mediante el uso de software no-propietario y libre.

https://doi.org/10.17993/3ctecno/2020.v9n4e36.65-85

3. CONCEPTOS PREVIOS

3.1. CRIPTOGRAFÍA ASIMÉTRICA

La encriptación asimétrica es mejor conocida como criptografía de clave pública. La encriptación asimétrica es diferente a la encriptación simétrica. Mientras ambos son usados para proteger la data de accesos no autorizados, la encriptación asimétrica utiliza dos llaves en vez de una. Este tipo de encriptación fue inventada por Whitfield Diffie y Martin Hellman en 1975 (Conklin *et al.*, 2018).

La encriptación asimétrica ayuda en la creación de firmas digitales y también apunta hacia la mayor debilidad de la encriptación simétrica. Las firmas digitales ayudan en la eficiencia y rapidez de la gestión de los documentos, incluyendo los documentos legales. La encriptación asimétrica envuelve dos claves separadas pero relacionadas matemáticamente. Las claves son usadas en direcciones opuestas, como se verá en la siguiente imagen:

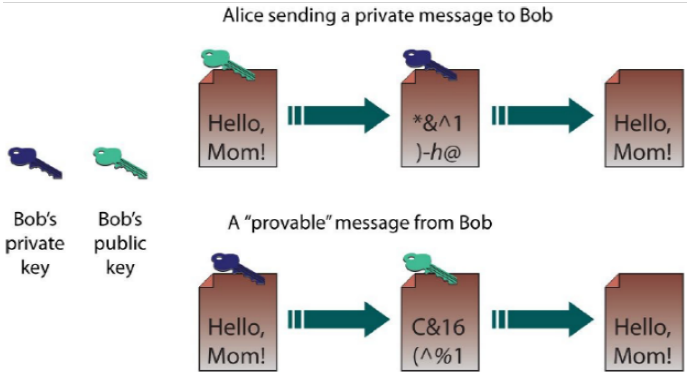


Figura 1. Modelo de encriptación asimétrica. Fuente: (Principles of Computer Security, 2018).

En los procesos de la criptografía asimétrica, se opta por el cifrado, no precisamente de todo el mensaje, sino, de una parte, la cual se realiza mediante una función, conocida como función hash, que extrae de un mensaje de datos una longitud fija. En esta extracción, la cual es un resumen, consiste en un listado de letras y números incompresible, la cual resulta de aplicar los algoritmos de cifrado. Este resultado se caracteriza por su irreversibilidad, la cual no se puede acceder al mensaje cifrado y descifrarlo, y su

https://doi.org/10.17993/3ctecno/2020.v9n4e36.65-85

exclusividad, que sólo existe una para cada mensaje de datos, lo que conlleva que, si se modifica un número o letra del resultado cifrado, el resultado del mensaje cambia.

Los algoritmos y tecnologías más comunes son:

Diffie-Hellman

Según Conklin *et al.* (2018) este protocolo es uno de los más utilizados, toma un rol fundamental en los procesos de SSL (Secure Sockets Layer), además para las tecnologías TLS (Transport Layer Security), SSH (Secure Shell). Este protocolo, usa números primos para trabajar. Utiliza dos números primos, P y G, luego se eligen dos números secretos: a y b. Luego se procesa:

- $X = Ga \bmod P$, siendo X un número público.
- $Y = Gb \bmod P$, siendo Y un número público.

Luego se procede a intercambiar los números públicos.

- Se computa: $Ka = Y^a \bmod P$
- Se computa: $Kb = Y^a \bmod P$

Aunque hay otros métodos que se crearon para reforzarlo, Diffie-Hellman es aún utilizado.

RSA

De acuerdo a Conklin *et al.* (2018), este algoritmo usa el producto de dos números primos y trabaja en el principio de la dificultad en factorizar estos números. Se da por recomendación trabajar con números primos de 100 a 200 dígitos. Estos dos números primos, para este caso, llamados P y Q, aleatoriamente se elige un número E, donde E es mayor que 1. Dado que la seguridad de RSA radica en la dificultad de la factorización de dos números grandes, esto puede llevar a demora a nivel software.

https://doi.org/10.17993/3ctecno/2020.v9n4e36.65-85

ElGamal

Según Conklin *et al.* (2018), es usado para la encriptación y las firmas digitales. Este sistema está basado en el cálculo de logaritmos discretos en un campo finito. Se necesita 3 números para generar el par de llaves. Fue descrito por Taher Elgamal en 1984 y se usa en software GNU Privacy Guard, versiones recientes de PGP, y otros sistemas criptográficos. Este algoritmo no está bajo ninguna patente lo que lo hace de uso libre.

La seguridad del algoritmo se basa en la suposición que la función utilizada es de un solo sentido y la dificultad de calcular un logaritmo discreto. El procedimiento de cifrado y descifrado está basado en cálculos sobre un grupo cíclico cualquiera G lo que lleva a que la seguridad de este dependa de la dificultad de calcular logaritmos discretos en G.

3.2. FIRMA DIGITAL

Según Katz (2014), la firma digital sirve como una poderosa arma que se está aceptando en algunos países, ello se puede utilizar para certificar contratos o notarizar documentos, para autenticación de personas o corporaciones, así como componentes de protocolos más complejos. Su uso y validación está implementado mediante el manejo de las claves criptográficas públicas y privadas. Un esquema de la firma digital por lo general es usado por un firmante y verificadores. El firmante empieza a ejecutar un algoritmo de generador de claves. El firmante luego publica su clave pública, para que un verificador empiece a validarlo, se asume que el verificador tiene las herramientas y opciones necesarias para su validación.

Las características que tiene la firma digital son las siguientes:

- Debe permitir la identificación del usuario. Para lograrse, la firma debe estar asociada solamente al emisario. Se entra en el concepto de la autoría electrónica, de otra forma, la comprobación de las identidades y validaciones y verificaciones de la firma se realizan mediante procesos electrónicos.

https://doi.org/10.17993/3ctecno/2020.v9n4e36.65-85

- La firma digital solo puede ser generada por un único emisor, por lo que debe ser infalsificable e inimitable, lo que quiere decir es que no debe ser suplantada. Significa que solamente el firmante es el único generador de su propia firma.
- Las informaciones que se generen a partir de la firma digital deben ser suficientes para validarla, pero insuficientes para falsificarla.
- Debe permitir detectar la alteración de los mensajes.
- Debe contener los elementos necesarios para probar la participación del signatario en la emisión del mensaje que ha sido firmado digitalmente Se debe facilitar la no-repudiación de los mensajes, quiere decir que el signatario es capaz de autentificar la firma y el mensaje adjunto a la firma.
- La firma digital autentifica documentos y/o mensajes. Una vez identificado, es imposible falsificar o alterar el documento firmado o la firma sin que este acto sea detectado.
- Las firmas digitales por lo general consisten en 3 algoritmos probabilísticos (Gen, Sign, Vrfy):
- El algoritmo generador de clave Gen toma como entrada el parámetro k. Como salida muestra un par de claves: Clave pública, pk y Clave Privada, sk. Se asume que el parámetro de seguridad k está implícitamente en las dos claves: en la clave pública y en la clave privada.
- El algoritmo Sign que es el algoritmo de la firma toma la clave privada sk y un mensaje m, devuelve una firma δ. Si el mensaje no pertenece al emisario, se bloquea y se invalida el proceso. Se describe que la firma pertenece al conjunto de las firmas generadas para el mensaje m. Si se descubre el mensaje no pertenece al emisario, el algoritmo de la firma digital genera un valor vació e invalida el mensaje, o dependiendo del desarrollador, se genera un mensaje de invalidación, un mensaje de error, no se envía el mensaje, entre otras maneras de demostrar una invalidación de una firma.
- El Algoritmo de verificación Vrfy toma la clave pública pk , el mensaje m y la firma δ. Luego de este proceso devuelve un bit b, donde si b=1, significa aceptado y si b=0, significa rechazado. Entendemos que cuando un bit que es 1, significa que el mensaje es válido, por lo que se acepta la verificación y el mensaje se envía sin ningún problema. Caso contrario, cuando el mensaje no está

https://doi.org/10.17993/3ctecno/2020.v9n4e36.65-85

verificado correctamente, el bit de salida es 0, por lo que el algoritmo rechaza la firma, el mensaje y no se provee de un mensaje con la firma digital al emisario que el receptor desea.

A continuación, se muestra un gráfico que describe el esquema de una firma digital:

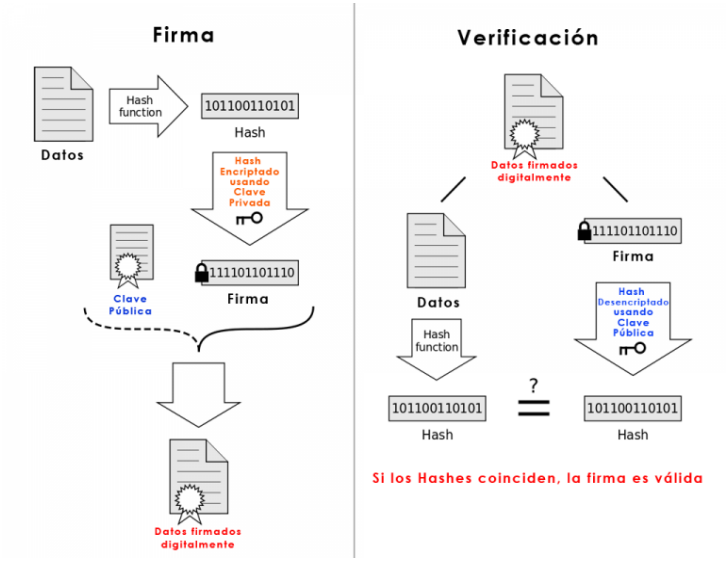


Figura 2. Esquema de firma digital. Fuente: (Iglesias, 2017).

4. REQUERIMIENTOS Y ARQUITECTURA

4.1. REQUERIMIENTOS

Basándonos en Chumbimuni y Vega (2019) y Céspedes, Vega y Bustos (2016), hemos elaborado los siguientes requerimientos:

- El usuario debe ingresar al sistema a través de una cuenta personal.
- El sistema permite redactar un historial médico después de haber realizado una revisión al paciente.
- El sistema permite al especialista de la salud realizar el seguimiento de los historiales médicos.

https://doi.org/10.17993/3ctecno/2020.v9n4e36.65-85

4.2. CASOS DE USO DEL SISTEMA

Según Rodriguez *et al.* (2020) y Sanchez *et al.* (2020) presentamos los siguientes casos de uso:

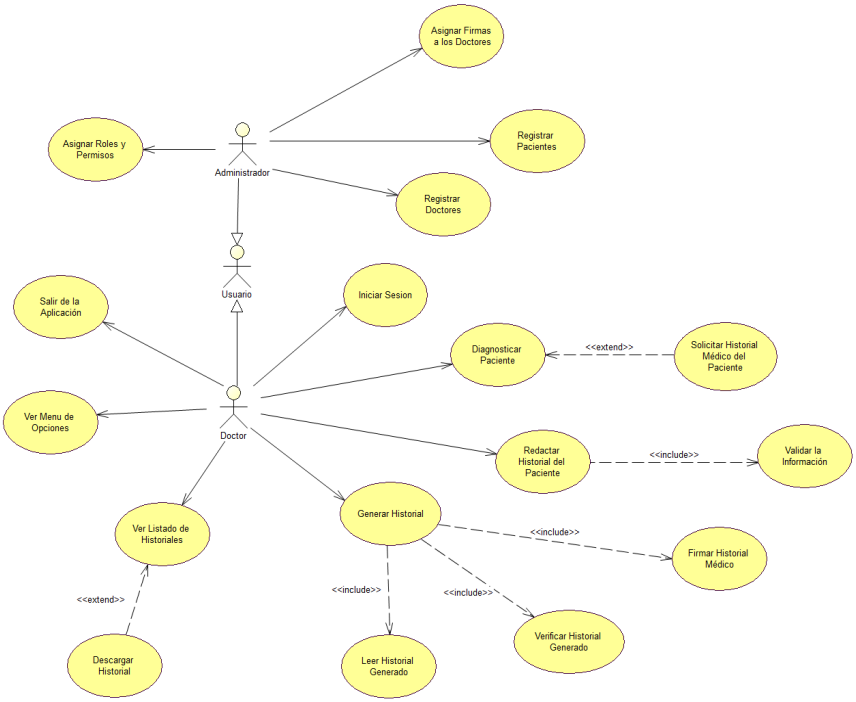


Figura 3. Casos de uso del sistema.
Fuente: elaboración propia.

Los casos de uso más relevantes para el sistema son:

- Asignar Firmas a los Doctores
- Redactar Historial del Paciente
- Generar Historial
- Verificar Historial Generado
- Ver Listado de Historiales

https://doi.org/10.17993/3ctecno/2020.v9n4e36.65-85

4.3. BASE DE DATOS

Apoyados en Soto *et al.* (2020) y Vega, Huayna, y Romero (2009), elaboramos la siguiente base de datos:

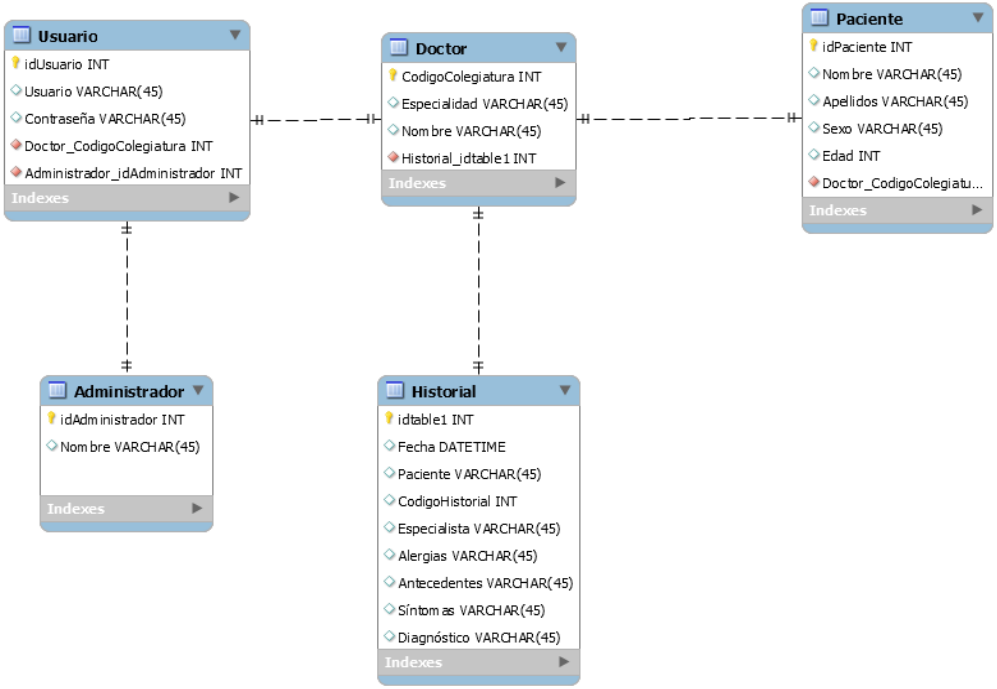


Figura 4. Diagrama de la Base de Datos.
Fuente: elaboración propia.

5. DESARROLLO

Basándonos en Távara *et al.* (2020) y, Vega y Huayna (2010), realizamos nel siguiente planteamiento:

El proyecto implica el desarrollo de un sistema que se plantea el uso para los especialistas de la salud, ya que ellos son las personas responsables de la redacción del historial médico. Las herramientas tecnológicas implementadas son el algoritmo RSA y las funciones criptográficas hash SHA 256.

https://doi.org/10.17993/3ctecno/2020.v9n4e36.65-85

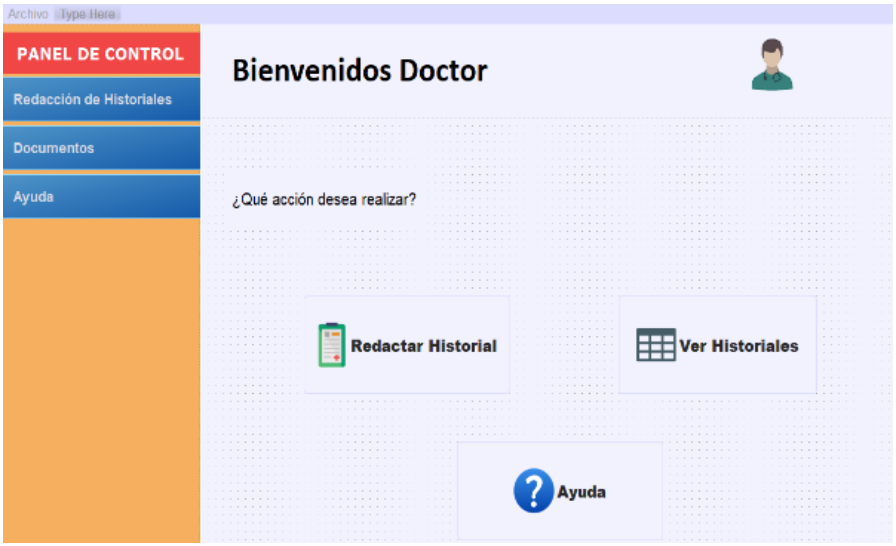


Figura 5. Inicio.
Fuente: elaboración propia.

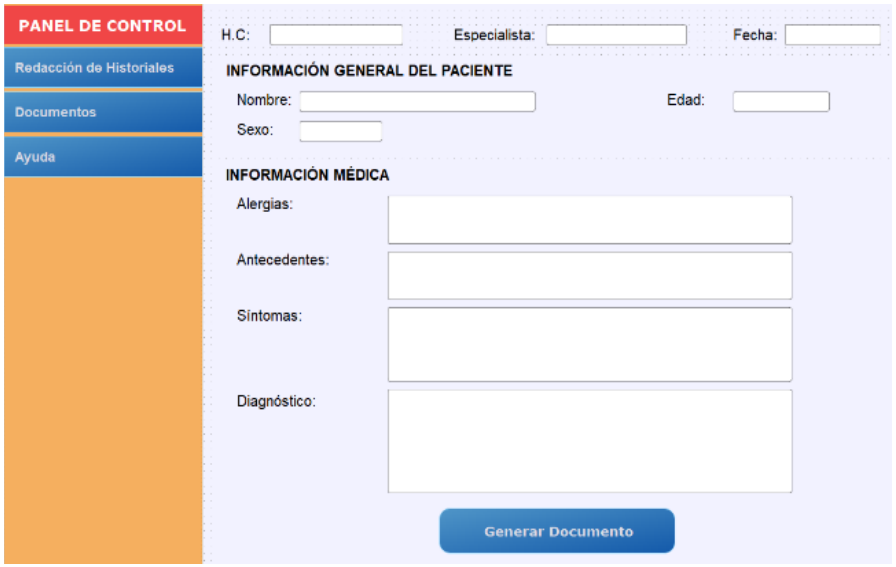


Figura 6. Historial.
Fuente: elaboración propia.

https://doi.org/10.17993/3ctecno/2020.v9n4e36.65-85

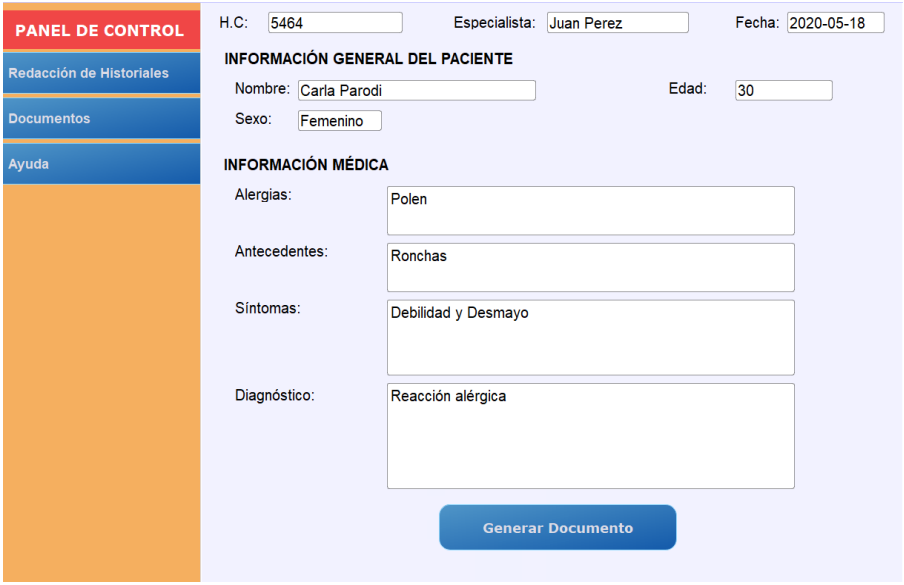
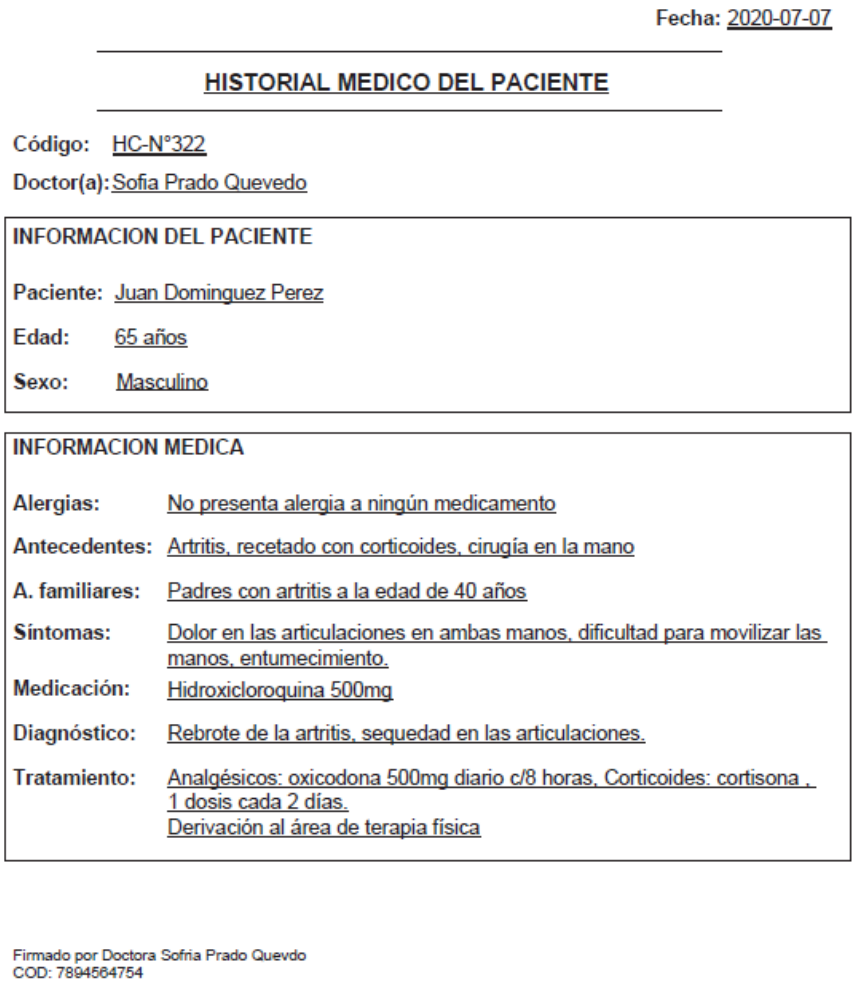


Figura 7. Confirmación de Historial Generado.
Fuente: elaboración propia.

https://doi.org/10.17993/3ctecno/2020.v9n4e36.65-85



Fecha: 2020-07-07

HISTORIAL MEDICO DEL PACIENTE

Código: HC-N°322

Doctor(a): Sofia Prado Quevedo

INFORMACION DEL PACIENTE

Paciente: Juan Dominguez Perez

Edad: 65 años

Sexo: Masculino

INFORMACION MEDICA

Alergias:	No presenta alergia a ningún medicamento
Antecedentes:	Artritis, recetado con corticoides, cirugía en la mano
A. familiares:	Padres con artritis a la edad de 40 años
Síntomas:	Dolor en las articulaciones en ambas manos, dificultad para movilizar las manos, entumecimiento.
Medicación:	Hidroxicloroquina 500mg
Diagnóstico:	Rebrote de la artritis, sequedad en las articulaciones.
Tratamiento:	Analgésicos: oxicodona 500mg diario c/8 horas, Corticoides: cortisona , 1 dosis cada 2 días. Derivación al área de terapia física

Firmado por Doctora Sofria Prado Quevdo
COD: 7894564754

Figura 8. Documento PDF del Historial Generado.
Fuente: elaboración propia.

https://doi.org/10.17993/3ctecno/2020.v9n4e36.65-85

Figura 9. Panel de la firma digital.
Fuente: elaboración propia.

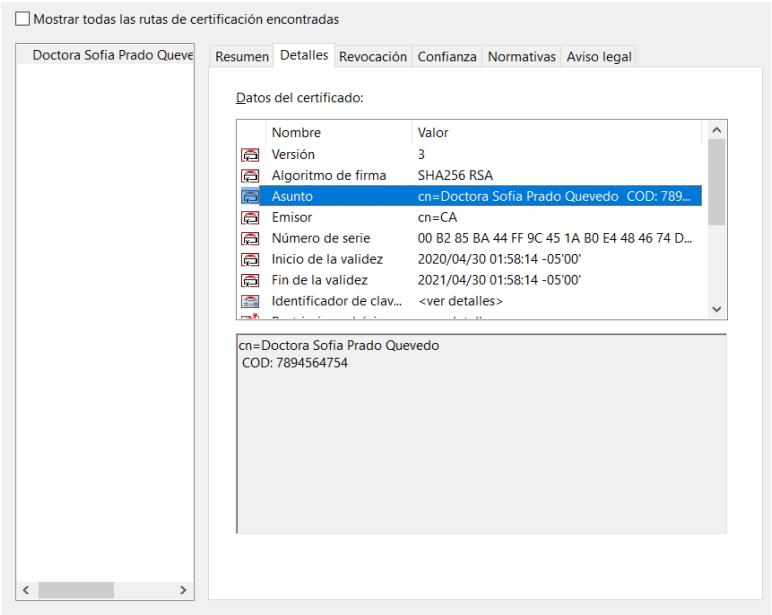


Figura 10. Detalle de la firma digital.
Fuente: elaboración propia.

https://doi.org/10.17993/3ctecno/2020.v9n4e36.65-85

6. RESULTADOS

En base a la investigación anteriormente desarrollada, los resultados son los siguientes:

- El tiempo de la redacción del historial fue entre 2 a 5 minutos.
- La generación del historial es automática, lo cual se da inmediatamente después de proceder a validar lo redactado en el historial.
- La firma adjunta en el documento del historial médico se da de forma conjunta con la generación del historial, dado que los procesos de verificación y validación se da en simultáneo.
- No hubo la necesidad de usar recursos físicos alguno, ya sea papel o algún material para la redacción física.

7. CONCLUSIONES

En base al desarrollo de la solución del sistema para la gestión de historiales médicos mediante el uso de la firma digital, se concluye lo siguiente:

- Después de analizar una serie de sistemas criptográficos, se procedió a implementar el sistema RSA, debido a su versatilidad y robustez.
- El sistema demostró la posibilidad de la implementación de la firma digital aplicado para un historial médico, considerando también su verificación y validación.
- Se demostró que el proceso de la generación de un historial médico trae consigo la posibilidad de reducir el uso de recursos, especialmente los recursos de tiempo y consumo de papel físico.
- El desarrollo del software además tuvo la intención de generar un software amigable al usuario, con la idea de no generar dificultad o inconveniente en el manejo de esta.

https://doi.org/10.17993/3ctecno/2020.v9n4e36.65-85

8. RECOMENDACIONES

Se recomienda la futura interconexión con otros establecimientos de salud para una futura mejora en la gestión de los historiales médicos de los pacientes, cumpliendo con la privacidad y seguridad del manejo de estos documentos. Además, se recomienda contemplar a otros actores del hospital para una mayor integración del sistema.

REFERENCIAS BIBLIOGRÁFICAS

Céspedes, C., Vega, H., y Bustos, S. (2016). *CRM para optimizar la gestión del proceso de venta de una inmobiliaria: Solución basada en tecnologías Web para el sector construcción, centrada en el proceso de venta.* Editorial Académica Española.

Chumbimuni, J., y Vega, H. (2019). Mejora de la calidad de atención del servicio de Depósito Legal de la Biblioteca Nacional del Perú mediante la implementación del módulo de consulta en línea de certificados digitales basado en la tecnología de firma digital. En *10th International Symposium on Innovation and Technology.*

Conklin, A., White, G., Dwayne W., Davis, R., y Cothren, C. (2018). *Principles of Computer Security. CompTIA Security+ and Beyond* (5.ª ed.). McGraw-Hill Education.

Hospital Nacional Daniel Alcides Carrion. (2017). *Plan Estratégico Institucional.*

Iglesias, V. (2017). *Cómo funciona la firma digital*. https://www.victoriglesias.net/como-funciona-la-firma-digital/

Katz, J. (2014). *Digital Signatures.* Springer, Boston, MA. https://doi.org/10.1007/978-0-387-27712-7

Ley N.° 27269. Ley de Firmas y Certificados Digitales. https://www.minjus.gob.pe/wp-content/uploads/2014/03/Ley27269.pdf

https://doi.org/10.17993/3ctecno/2020.v9n4e36.65-85

Metzgar, C. N. (2017). *RSA cryptosystem: an analysis and python simulator*. https://libres.uncg.edu/ir/asu/f/Metzgar,%20Ciscily%20Spring%202017.pdf

Rodriguez, C., Lezama, P., Kaseng, F., y Chávez, D. (2020). Bayesian model to determine genealogical links of family descendants. *Test Engineering and Management, 83,* 17937- 17946.

Sanchez, J., Vega, H., Guzmán, Y., Rodriguez C., y Quinto, D. (2020). Data Mart Design to Improve the Decision-Making Process of the After-Sales Service. *Test Engineering and Management, 83*, 15481–15494.

Soto, B., Vega, H., Guzmán, Y., Rodriguez C., y Quinto, D. (2020). Classification Algorithm Based on machine learning to optimize athletes talent detection. *Test Engineering and Management, 83,* 13464–13461.

Távara, A., Vega, H., Guzmán, Y., Rodriguez, C., y Quinto D. (2020). Wearable technology to improve health care infants in the yomibato peruvian community. *Test Engineering and Management, 83,*17960- 17968.

Torres, H. (2005). *El sistema de seguridad jurídica en el comercio electrónico*. Fondo Editorial De La Pontificia Universidad Católica Del Perú.

Vega, H., Huayna, M., y Romero, P. (2009). Reconocimiento de patrones mediante redes neuronales artificiales. *Revista de Ingeniería de Sistemas e Informática, 6*(2). https://sisbib.unmsm.edu.pe/BibVirtual/Publicaciones/risi/2009_n2/v6n2/a03v6n2.pdf

Vega, H., y Huayna, M. (2010). Sistema experto para la prevención de enfermedades basado en consumo de alimentos cotidianos. *Revista del Encuentro Científico Internacional, 7*(2). https://sisbib.unmsm.edu.pe/BibVirtual/publicaciones/risi/2009_n1/v6n1/a02v6n1.pdf

https://doi.org/10.17993/3ctecno/2020.v9n4e36.65-85

Verma, A., Guha, P., y Mishra, S. (2016). Comparative Study of Different Cryptographic Algorithms. *Journal of Emerging Trends & Technology in Computer Science, 11*(3). https://doi.org/10.4236/jis.2020.113009

https://doi.org/10.17993/3ctecno/2020.v9n4e36.65-85