# Protocolo de seguridad basado en firmas digitales para un expediente clínico electrónico

Carlos E. Alvarado-Rivera, Andrés J. González-Ayala, Ángel F. López-García[a] and Lourdes López-García[b]

[a]Universidad Don Bosco, La Libertad, El Salvador.
[b]Centro Universitario UAEM Valle de Chalco, Estado de México, México.

## ABSTRACT

El constante crecimiento de las tecnologías ha hecho que todas las instituciones se acomoden a una nueva forma de ejecutar sus procesos. Esto aplica y es muy relevante en el área de la salud, donde, con el fin de mejorar la atención brindada a los pacientes y la calidad de los servicios prestados, se están adaptando e impulsando tecnologías de la información y comunicaciones, siendo una de las más importantes el Expediente Clínico Electrónico (ECE).

En El Salvador, por parte del Ministerio de Salud, quien es la entidad gubernamental encargada de velar por la salud del pueblo salvadoreño, se desarrollan esfuerzos para la adopción del ECE a través de la implementación del Sistema Integral de Atención de Pacientes (SIAP), que centraliza los esfuerzos de digitalización del expediente clínico físico y sirve de respaldo y automatización para las estadísticas nacionales de salud.

Ante lo anterior, el trabajo de investigación se direcciona al diseño de un módulo de seguridad y la metodología adecuada que permita la implementación de la firma digital en el SIAP, para garantizar que todos los datos que la institución genera en el esquema de atención médica a pacientes se mantengan íntegros a través del tiempo y sin rechazo o repudio de sus autores.

**Keywords:** ECE, firmas agregadas, PKI.

## 1. INTRODUCCIÓN

El avance tecnológico ha permitido considerar el área de la salud para brindar a los pacientes servicios automatizados como el Expediente Clínico Electrónico (ECE). Esta nueva forma de hacer las cosas no solo trae consigo mejoras, sino, que también, nuevos retos de cómo resguardar la información de una forma segura y precisa, brindar validez y legalidad al ECE y mejorar la efectividad de los servicios de atención médica. Para alcanzar la integración de la información de un paciente desde el momento que nace hasta el que fallece, el brindar acceso oportuno al personal autorizado y lograr un nivel de confidencialidad, integridad y trazabilidad de los procesos de archivo, registro y consulta de la información se debe apostar por la sustitución completa del expediente físico por el expediente clínico electrónico único.

Partiendo que en El Salvador ya se encuentra vigente aunque no ejecutada tanto la Ley de Firma Electrónica como su reglamento, las cuales habilitan a partir de un procedimiento a entes gubernamentales como el MINSAL a tomar el rol de Autoridades Certificadoras y equipara a la firma digital simple y certificada con la firma autógrafa,[1] se ve la oportunidad de diseñar una metodología para implementar una estructura de llave pública para el SIAP del ministerio de salud, en un módulo de seguridad, que logre mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados y brinde el no repudio entre el autor y la información generada por este, permitiendo dirimir responsabilidades y definir cronología de eventos.

Dado lo anterior, en este artículo se propone un protocolo de seguridad basado en firmas digitales que cumpla con la confidencialidad, integridad y no repudio de la información del Expediente Clínico Electrónico del Ministerio de Salud. Al contar con un Expediente Clínico Electrónico Seguro (ECES) se ayudará en gran

Lourdes López-García, e-mail:mllopezg@uaemex.mx.

medida a los centros de atención pública de El Salvador, para brindar un mejor servicio de calidad, seguridad y rapidez a cada uno de los usuarios y permitirá ser el precursor de un sistema de información médica que pueda ser implementado por otras instituciones de salud nacionales o regionales de forma segura que tome en cuenta el contexto y recursos tecnológicos que actualmente el MINSAL posee, buscando ofrecer un proceso seguro, económico y técnicamente factible que posibilite la adopción plena del ECE como un documento con validez para auditoría clínica, administrativa y legal.

## 2. EXPEDIENTES CLÍNICOS ELECTRÓNICOS

El expediente clínico, es el conjunto de información ordenada y detallada que recopila cronológicamente todos los aspectos relativos a la salud de un paciente en un periodo determinado de su vida, representa una base histórica que nos ayuda a conocer las condiciones de salud y los diferentes procedimientos ejecutados por el equipo médico a lo largo de un proceso asistencial.

El expediente clínico electrónico (ECE) es una fuente de información que amplía el dictamen médico de un experto, conformándose por una descripción de la propedéutica médica aunado a documentos, imágenes, procedimientos, pruebas diversas, análisis e información de estudios practicados al paciente. Mediante el ECE se puede brindar información más completa a los médicos y personal de salud, así como habilitar la comunicación al instante entre las diferentes unidades médicas.

En México, el proceso de implementación y actualización del ECE se contempló alrededor de los años 2009,[2] para dar seguimiento y mejorar la calidad de los servicios de salud, se establecieron los objetivos funcionales y las funciones que deben observar los productos del sistema (software) del ECE para garantizar la interoperabilidad, el procesamiento, la interpretación, la confidencialidad, la seguridad, el uso de estándares y los catálogos de información a través de la Norma Oficial Mexicana NOM-024-SSA3-2010.[3]

En Uruguay se emprendió una reforma integral del sector salud, teniendo como objetivo proporcionar accesos universales a servicios de salud de calidad y en el 2012, se creó el programa "Salud.uy", como parte de la agenda Digital Uruguay 2011-2015, en una colaboración del BID con el ministerio de economía y finanzas, el ministerio de salud pública y la Agencia de gobierno Electrónico y Sociedad de la información y el conocimiento, logrando la creación del sistema de Historia Clínica Electrónica Nacional, que consiste en digitalizar todas las historias clínicas para facilitar su distribución a la red de centros de salud del país.[4]

Muchos de los diseños de sistemas del ECE han desarrollado de la mano con la creación y adopción de estándares y regulaciones en el ámbito de la seguridad, los cuales marcan y delimitan los requisitos mínimos que estos sistemas deben cumplir para garantizar la privacidad, confidencialidad, integridad y disponibilidad de la información médica. A continuación, se mencionan algunos estándares y normas ya establecidos :

1. HL7: Estándar de mensajería para el intercambio electrónico de información clínica basada en el RIM (Reference Information Model).[5]
2. CIE-10: Es la Clasificación Internacional de Enfermedades, correspondiente a la versión en español de la ICD, por sus siglas en inglés: International Statistical Classification of Diseases and Related Health Problems.[6]
3. DICOM: Estándar reconocido mundialmente para el intercambio de imágenes médicas, pensado para el manejo, almacenamiento, impresión y transmisión de imágenes médicas.[7]
4. LOINC: Logical Observation Identifiers Names and Codes (códigos universales para identificar observaciones clínicas y laboratorio)[8]
5. CEN/ISO EN 13606 - en su apartado IV, define directivas de seguridad y privacidad de los datos médicos que permite un marco de referencia común para alcanzar sistemas de expediente electrónico clínico interoperables.[9]
6. ISO 27799:2016 ha sido especialmente diseñado para la aplicación en la atención en salud, definiendo guías prácticas para brindar apoyo a la interpretación e implementación de la ISO/IEC 27002 en la informática médica.[?]

La implementación de estas guías prácticas permite a las organizaciones o instituciones en el área de la atención en salud reducir el número y severidad de los incidentes de seguridad y asegurar un mínimo nivel de confidencialidad, integridad y disponibilidad de toda la información clínica personal.

## 3. FUNCIONALIDAD DEL SISTEMA INTEGRAL DE ATENCIÓN AL PACIENTE (SIAP)

El SIAP es un sistema informático que permite registrar la historia clínica y obtener la información de los usuarios que consultan en los diferentes niveles de atención del MINSAL con el objetivo de mejorar la atención en los servicios brindados. Es uno de los componentes fundamentales del Sistema Único de Información en Salud.[10]

Este sistema es utilizado por el momento en 27 hospitales públicos, así como en la mayoría de las unidades de salud del territorio salvadoreño para la recopilación de información de cada uno de los pacientes que visitan estos centros de salud, se debe de mencionar y tener claro que este sistema no está centralizado; esto quiere decir que la información que es recopilada en un centro de atención médica no se replica de forma instantánea o automática hacia las otras unidades de salud u hospitales.

En la Figura 1,se muestra el flujo de información del SIAP, en cada establecimiento de salud, pasos que se detallan a continuación:

1. Los pacientes acuden a consulta médica, ya sea a un hospital o unidad de salud.
2. En la recepción se identifica a los pacientes, por medio de su DUI (Módulo de identificación).
3. Si ya cuentan con un expediente clínico, son enviados al área de emergencia para su evaluación y posterior consulta.
4. Si no cuentan con un expediente clínico en el establecimiento visitado, son enviados al área de Estadísticas y Documentos Médicos (ESDOMED), para que se le cree el registro correspondiente.
5. Aquellos pacientes con cita programada son enviados directamente a la consulta externa para seguimiento clínico.
6. Algunos pacientes, que solo asisten por toma de exámenes, ya sean de laboratorio clínico o de imagenología, son remitidos hacia el área correspondiente.
7. En el módulo de seguimiento clínico, se verifican las consultas anteriores del paciente y se proporciona un nuevo diagnóstico, según la mejoría del mismo.
8. Los módulos de imagenología y laboratorio clínico anexan los resultados de exámenes al seguimiento del paciente, el módulo de farmacia permite verificar si los medicamentos prescritos, fueron retirados a tiempo por el consultante.

### 3.1 Análisis de Vulnerabilidad

Un proceso de los más importantes es la protección o el resguardo de la información, se ha identificado que el MINSAL realiza una serie de respaldos de cada una de las máquinas que se encuentran en los hospitales y unidades de salud, y según su periodicidad de respaldos incrementales se establece su RPO (Recovery Point Objective) en una hora, esto de forma digital, pues siempre queda una copia en papel, ya que según normativa, se debe tener el expediente en digital y en físico, por ello obligatoriamente se imprimen todos los datos de consultas, exámenes, etcétera.

Otro problema grave que se encuentra es la parte del no repudio, integridad y la confidencialidad de la información, debido al resguardo de los certificados, llaves y contraseñas que no cuentan con un sistema de PKI real, sino más bien se guardan en la misma máquina en la que se encuentra instalada el SIAP, exponiendo esta información a ser visualizadas por personas ajenas a la administración, que cuenten únicamente con el acceso físico a los equipos.

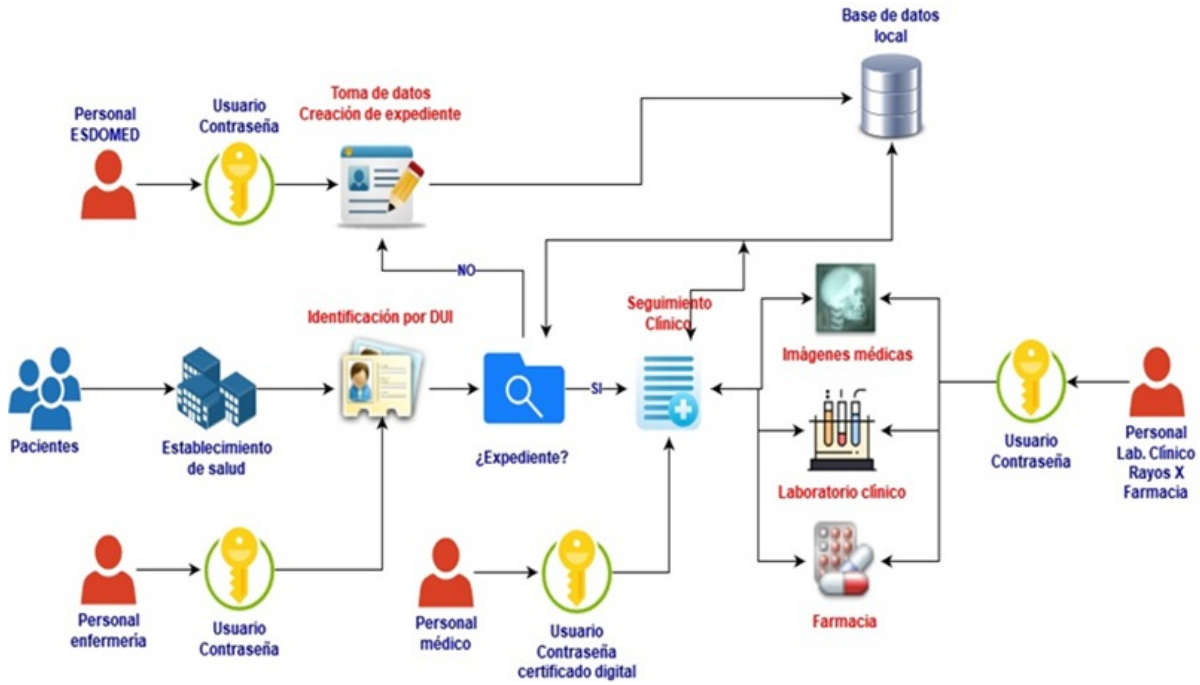


Figura 1. Flujo actual de datos del SIAP [Elaboración propia]

Esto puede permitir sustraer y entregar esta información sensible a otras personas no autorizadas, abriendo paso en el peor de los casos a la suplantación de un médico que diagnostica, proporciona un tratamiento o solicita exámenes a un paciente con el cual no haya tenido consulta médica; robo o modificación de información clínica o la no disponibilidad de los servicios de atención médica debido a perdida de acceso a los módulos de seguimiento clínico, agenda médica o citas.

## 4. PROTOCOLO DE SEGURIDAD PROPUESTO

Se propone el siguiente protocolo como solución a la problemática de seguridad que presenta el esquema actual del SIAP, y permita brindar los servicios confidencialidad, integridad y no repudio de la información médica contenida en los ECE. Por lo que se realizan las siguientes acciones:

1. Generación de llaves: para garantizar la confidencialidad de dicha información se definirán las entidades autorizadas para su manipulación, para adición o consulta de la misma. Únicamente los usuarios autenticados tendrán acceso a la información y para ello se debe realizar un proceso de generación de llaves privadas y públicas para cada entidad.

2. Certificado digital: la autoridad certificadora (AC), en este caso la institución de salud y el Ministerio de Salud, certifican la relación entre cada una de las entidades y su llave pública. Esta vinculación permite más adelante comprobar la validez de la firma y garantiza el no repudio, ya que la persona no puede negar que la firma ha sido generada por él, cuando esta ha sido verificada con la llave pública certificada.

3. Descifrado del expediente: el expediente es protegido con cifrado simétrico y para obtener la información que en él se encuentra deberá descifrarse, haciendo lo siguiente:

   *a*) La entidad clínica se autentica por medio de un usuario/contraseña.

   *b*) Una vez autenticado se genera una clave de sesión que será la clave compartida con el servidor.

*c*) El servidor de llaves entrega al usuario autenticado la llave simétrica que permitirá descifrar y cifrar la información del expediente almacenada en un segundo servidor, que contiene todos los expedientes clínicos.

*d*) La persona autenticada puede descifrar el expediente, ya sea para consultar o agregar información.

4. Verificar y agregar información con estampa de tiempo: la información que se adicione al expediente es registrada y firmada por el último doctor o personal clínico responsable de dicha acción, haciendo uso de firma agregada, acompañada de la fecha y hora en que el documento fue modificado o consultado, para lo que se usa estampa de tiempo. Se siguen los siguientes pasos:

   *a*) Se realiza la verificación de la firma para lo que se necesita la llave pública de la entidad clínica que ha agregado información y firmado el expediente anteriormente.

   *b*) Si la verificación es correcta, procede a agregar información y firma con su llave privada y esta es agregada a la firma verificada en paso anterior.

   *c*) Se adiciona la estampa de tiempo a la firma generada.

   La firma permite verificar la autoría e integridad del documento desde la firma de la última entidad clínica y a la vez ofrece no repudio ya que la entidad clínica que agrega información al expediente no puede negar que realizó dicha acción, además la estampa de tiempo permite determinar el momento exacto en que se generó dicha información.

5. Cifrado de expediente: una vez agregada la información al ECE, esta debe ser cifrada nuevamente con la llave simétrica obtenida del servidor de llaves. El expediente cifrado es almacenado en el servidor que contiene los datos de los expedientes clínicos.

En la Figura 2, se puede apreciar el flujo que sigue el protocolo de seguridad propuesto.

### 4.1 Flujo de datos

El protocolo consiste en tres fases y al menos cuatro entidades, para mayor entendimiento, la notación con su respectiva descripción se muestra en el Cuadro 1.

Cuadro 1. Noración utilizada en el protcolo propuesto.

| | |
|---|---|
| $(e_X, n_X)$ | LLave pública y privada de la entidad $X$ |
| $Cert_X$ | Certificado correspondiente a la entidad $X$ |
| $H(msj)$ | Función hash aplicado al mensaje $msj$ |
| $a\|\|b$ | Denota la concatenación entre el mensaje $a$ con el mensaje $b$ |
| $S_m$ | Denota la firma para el mensaje $m$ |
| $t_y$ | Indica la estampa de tiempo correspondiente al evento $y$ |
| $AC$ | Autoridad Cetificadora de primer nivel |
| $AC_2$ | Autoridad Cetificadora de segundo nivel |
| $AA$ | Autoridad Autenticadora de tercer nivel |

**Fase 1. Generación de certificados**

1. Las Autoridades $AC$, $AC_2$, $AA$ y cada entidad clínica que labora en la institución debe poseer sus llaves RSA.

2. La $AC$ (Ministerio de Salud) genera el certificado raíz. La $AC_2$ (Institución) solicita su certificado digital de la $AC$; y la $AA$ en conjunto con cada entidad clínica solicita certificado digital a la $AC_2$.

**Fase 2. Autenticación**

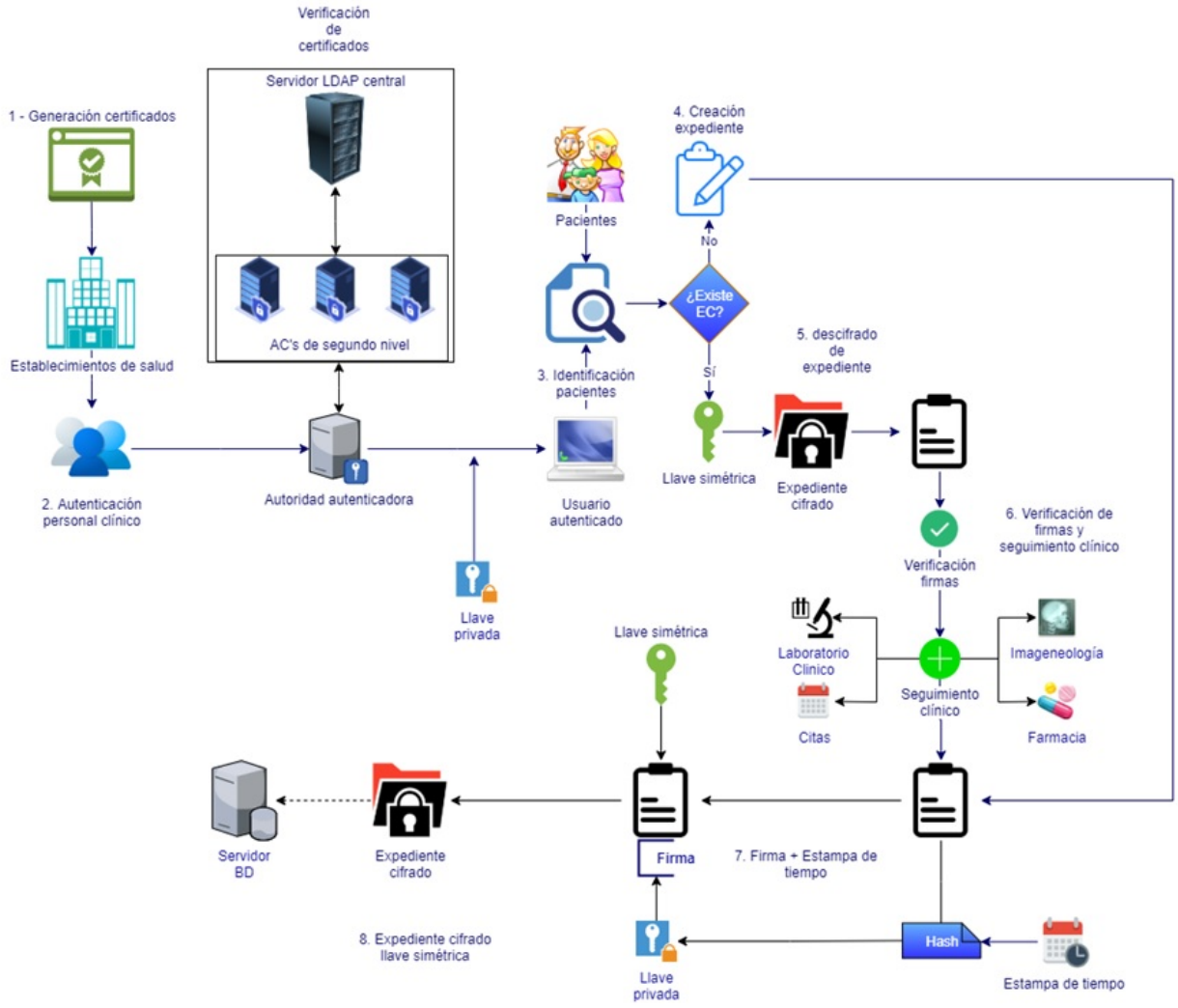


Figura 2. Flujo del protocolo de seguridad propuesto [Elaboración propia].

1. Cuando un usuario clínico como, por ejemplo, $Padmin_1$, solicite acceso a la información contenida en el ECE, primero deberá autenticarse presentando su usuario y contraseña, en donde su contraseña servirá para descifrar simétricamente la llave privada contenida en un dispositivo externo como USB o smartcard.

2. Habiéndose autenticado $Padmin_1$ por lo que sabe, deberá autenticarse por lo que tiene, debido a que debe superar un reto para el cual necesita introducir su llave privada; cumpliéndose un doble factor de autenticación para ingresar al sistema. Este reto define que cuando $Padmin_1$ solicite acceso al ECE.

3. La $AA$ deberá solicitar al repositorio de certificados, el $Cert_{AC_2}$ y el $Cert_{Padmin_1}$, corroborando con la lista de revocación de certificados (CRL) que este último no se encuentre listado como invalido y no olvidando validar primero la lista a partir de su firma digital ($S_{CRL}$).

4. Si los certificados son válidos, se puede garantizar la vinculación de la llave pública con el usuario $Padmin_1$, Si no son válidos, se finaliza el proceso y no se autentica al usuario.

5. En el caso de la validez, de los certificados, la $AA$ genera un número aleatorio de 128 bits, denotado como $K_{AA}$.

6. La $AA$ utiliza los exponentes públicos extraídos del certificado del usuario para cifrar $K_{AA}$ y con su exponente privado firma el mensaje cifrado, el resultado de esta firma es enviado al usuario.

7. Ahora $Padmin_1$ deberá solicitar al repositorio de certificados: $Cert_{AC_2}$, $Cert_{AA}$, la CRL y su firma, para primero validar la CRL con el $Cert_{AC_2}$ y después corroborar la validez del $Cert_{AA}$, si no aparece listado como invalido en la CRL.

8. Si los certificados son válidos, se puede garantizar la vinculación de la llave pública con la $AC_2$. Si no son válidos, se finaliza el proceso y no se autentica al usuario.

9. El usuario utiliza los exponentes públicos extraídos del certificado de $AA$ para verificar la firma $S_{CK}$ y utiliza su llave privada para descifrar el mensaje $C_k$. Si la firma es válida, cifra el reto con la llave pública de $AA$ y se lo reenvía. Como se ilustra en el Cuadro 2.

Cuadro 2. Paso de Mensajes entre las entidades AA y $Padmin_1$

| AA | | $Padmin_1$ |
|---|---|---|
| $C_k = K_{AA}^{e_{Padmin_1}} \, mod \, n_{Padmin_1}$ | | |
| $S_{C_K} = C_k^{d_{AA}} \, mod \, n_{AA}$ | $\xrightarrow{S_{C_k}, C_{C_k}}$ | $K_{AA'} = C_k^{d_{Padmin_1}} \, mod \, n_{Padmin_1}$ |
| | | $h_1 = S_{C_k}^{e_{AA}} \, mod \, n_{AA}$ |
| | | $h_2 = H(K_{AA'})$ |
| | | Si $h_1 = h_2$ |
| | | $C_{K_1} = K_{AA'}^{e_{AA}} \, mod \, n_{AA}$ |

10. La $AA$ descifra $C_{k_1}$ con su llave privada y compara el valor obtenido con el valor $K_{AA}$, previamente generado, si los valores coinciden, el reto es superado y $Padmin_1$ es autenticado. Si no coinciden los valores se finaliza el proceso y no se autentica al usuario.

**Fase 3. Creación, modificación o eliminación de la información contenida en el ECE**

1. La entidad clínica autenticada, como por ejemplo, $Padmin_1$, solicita el DUI y el número de expediente al paciente y verifica si este ya cuenta con un número de ECE registrado en la base de datos. Si el ECE no existe se salta hasta el paso No. 5 de esta fase, pero si este ya existe, primero se valida que el paciente sea el dueño del DUI (inspección visual) y solicita a partir de una sesión segura con la base de datos del ECE la llave simétrica $K_{simetrica}$ para descifrar el expediente correspondiente.

2. La entidad clínica descifra el ECE, obteniendo el mensaje que es toda la información contenida en el expediente, la firma del último o de los dos últimos signatarios y la estampa de tiempo del último signatario.

3. Dependiendo si el expediente cuenta con una o dos firmas se realiza la verificación de estas de la siguiente manera:

   *i* Si el mensaje solo cuenta con una firma, se realiza la verificación como cualquier verificación de firma RSA, utilizando los exponentes del último signatario extraídos del mensaje descifrado. Si los digestos no coinciden se finaliza el proceso y no se valida la última firma del expediente.

$$h_1 = S_{ultimo}^{e_n} \, mod n_n$$

$$h_2 = H(m)$$

$$Sih_1 = h_2 la firma es valida$$

*ii* Si el mensaje cuenta con dos firmas, utilizando los exponentes del último signatario extraídos del mensaje, se realiza la verificación de la siguiente manera:

$$y = S_{ultimo}^{e_n} mod n_n$$
$$h_2 = H(m)$$
$$S = y - S_{penultimo} = 0$$

*iii* Si las firmas no coinciden y el valor no es cero, se finaliza el proceso y no se válida la última firma del expediente.

4. Si las firmas coinciden, se hace la verificación de la firma de la estampa de tiempo, utilizando los exponentes públicos ya extraídos del certificado de la $AA$ y validados en el paso No. 9. Se elimina del último mensaje generado $m_n$ de la concatenación con $s_{t_ultimo}$ y se comparan los valores obtenidos de $r$ para validar la estampa de tiempo. Si estos no coinciden se finaliza el proceso y no se válida la última estampa de tiempo.

$$r' = s_{t_{ultimo}}^{e_{AA}} \, mod \, n_{AA}$$
$$m_{estampa} = m_n - s_{t_{ultimo}}$$
$$H(m_{estampa}||t_{ultimo} = r' = 0$$

5. Para agregar información al ECE se puede realizar de dos formas, ya sea que no se tenga el expediente creado o si se requiere adicionar más información a este a partir de un segundo acceso.

   *i* Si el expediente no está creado, primero se genera un número correlativo de no más de 32 bits con el identificativo que muestre la institución en donde se crea el expediente, a partir de esto se adiciona la información personal y Clínica correspondiente.

   *ii* Si el expediente ya está creado solo se adiciona la información correspondiente a esta nueva consulta, resultados de exámenes, recetas, tratamientos, imágenes médicas, etc.

6. Una vez creado el nuevo mensaje (nuevo expediente o información adicional), el usuario solicita la estampa de tiempo a la $AA$, la cual obtiene el tiempo de un servidor NTP y responde con la firma de la estampa de tiempo, que reemplazará al valor de la última firma denotada por $s_{t_{ultimo}}$.

7. Se firmará el mensaje creado en conjunto con la firma de la estampa de tiempo, lo cual se convierte en $m_{(n+1)}$, (donde $n$ puede ser 0, que significa que es la primera firma) adicionando al mensaje completo en conjunto con las llaves públicas de la entidad que generó el nuevo mensaje que este caso particular correspondería a $(e_{Padmin_1}, n_{Padmin_1}$. Este proceso es la agregación de la firma a la firma previa que respalda la integridad del expediente y que selló la penúltima entidad que revisó el expediente.

8. Una vez actualizado el expediente, la entidad clínica cifra los campos necesarios del ECE, parte del mensaje de la información contenida en el expediente, la firma del último o de los dos últimos signatarios y la estampa de tiempo del último signatario, con la llave simétrica del sistema. Todo esto se actualiza en la base de datos del servidor de ECE. Si en una misma consulta se requiere una nueva adición de datos al ECE por parte de otra entidad clínica se retoma este algoritmo desde la fase 2, omitiendo la verificación nuevamente del DUI del paso 1, de esta fase.

9. Si ya no es necesario adicionar o consultar el ECE se finaliza el protocolo.

## 4.2 Análisis de seguridad

A continuación, en la Tabla 4.2.se presenta una lista de los problemas que se identificaron en el ECE actual, los tipos de ataques que se pueden derivar y la solución que ofrece el protocolo propuesto.

Respecto al análisis de eficiencia, el protocolo propuesto garantiza rapidez en el proceso ya que sólo se calculan 2 operaciones pública y a lo más 3 operaciones privadas por fase para cada entidad.

Cuadro 3. Resumen de análisis de seguridad en el escenario incluyendo el protocolo propuesto.

| Problema | Ataque | Solución |
|---|---|---|
| Manipulación no autorizada del expediente clínico | Visualización y modificación del expediente clínico | Autenticación de doble factor (algo que sabe y algo que tiene) |
| Pérdida total o parcial de la información del ECE | Extracción o eliminación | Creación de un documento digital único para el paciente, que podrá ser consultado bajo la doble autenticación |
| Repudio | Negación de la modificación o extracción del ECE | Uso de la infraestructura PKI |
| Duplicidad | Creación de varios expedientes | El protocolo cumple con la unicidad al generar solo un expediente para consultar a nivel nacional. |
| Información abierta | Divulgación de la información privada | Uso de los esquemas criptográficos firma digital RSA, funcion picadillo, función de cifrado RSA y esquema de cifrado AES. |
| Poca disponibilidad | Denegación de servicios (DDoS), pérdida de información. | Desarrollar una infraestructura de alta disponibilidad que contemple, la creación de clúster de servidores, bases de datos, servidores de autenticación (PKI), así como también el contrato de diferentes proveedores que brinden los enlaces de internet, para poder contar con un balance de los servicios. |

## 5. METODOLOGÍA PROPUESTA PARA LA IMPLEMENTACIÓN DEL MÓDULO DE SEGURIDAD

La aplicación de esta metodología es válida para la implementación del protocolo criptográfico propuesto para el sistema SIAP desarrollado por el MINSAL, donde a partir de un análisis profundo de las características principales, funcionamiento e infraestructura del sistema y sus respectivos módulos: identificación de pacientes, seguimiento clínico, citas médicas, farmacia, laboratorio clínico e imagenología; se propone esta guía de ayuda en la integración del módulo de seguridad que facilite la adopción plena y confiable del expediente clínico electrónico.

- *Requerimientos generales*

  *i.* Es necesario contar con infraestructura que permita la implementación del PKI, a nivel local, regional y nacional, tanto equipo para usuarios finales, medios de comunicación, servidores de infraestructura de llave pública a nivel hospitalario, regional de salud y nivel central.

  - La validez de los certificados deberá tener un periodo no mayor a un año.

  *ii.* Es importante contar con un medio seguro para el almacenamiento portátil de las llaves y certificados de todos los usuarios del esquema de atención clínica del MINSAL, siendo estos: USB's cifrados o tarjetas inteligentes.

  - Toda información correspondiente a credenciales, llave privada y certificados que sea almacenada en un dispositivo externo tendrá que ser cifrada simétricamente, cuya llave será la contraseña establecida al momento de la creación del usuario correspondiente y renovada cada 3 meses.

- *Integración de PKI*

- *i*. Para ser posible la integración de PKI con el SIAP es necesario contar con herramientas que permitan la creación de todos los componentes con el menor costo posible, para esto se han evaluado dos opciones de software libre, las cuales no tienen ningún costo de licencia, además proporcionan todas las facilidades de implementación del PKI, como lo son OpenCA y EJBCA. Para esto es necesario que el MINSAL cuente con la infraestructura de hardware y red necesaria para la implementación del PKI, los cuales son un servidor para la instalación de EJBCA, otro más para registros (logs) y un servicio de enlaces de red para cada establecimiento de salud.

- *Integración de protocolo en el SIAP*: en la Figura 3 se puede apreciar la integración de PKI en el apartado de autenticación de usuarios del SIAP.

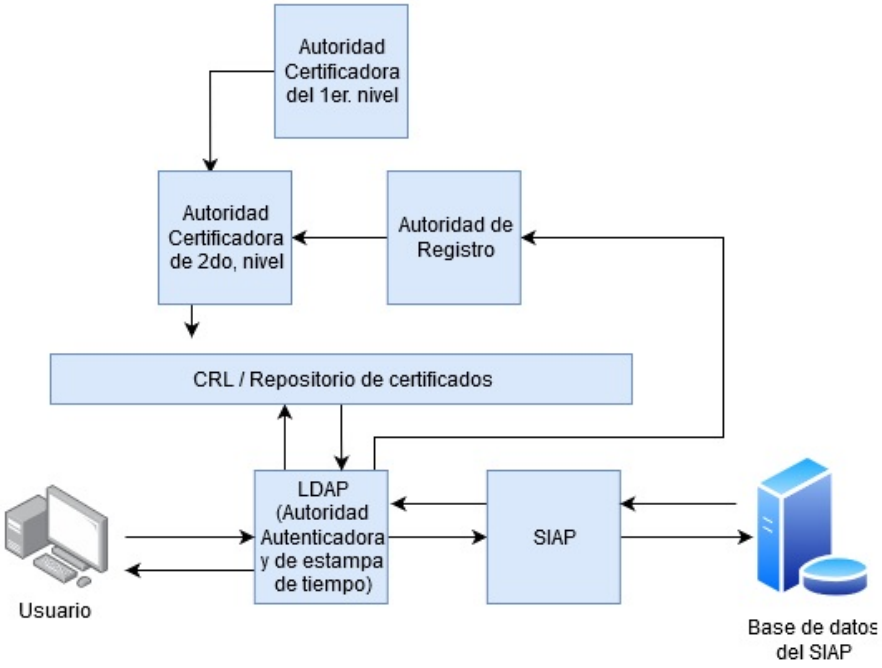


Figura 3. Integración de PKI en el SIAP [Elaboración propia [Elaboración propia].

*i*. Para ingresar al SIAP, el usuario debe colocar sus credenciales (usuario y contraseña) y llave privada (la cual debe estar almacenada en un dispositivo seguro, ya sea tarjetas inteligentes o USB cifrada).

*ii*. Una vez se colocan los datos, el sistema deba hacer una comprobación de las credenciales a través del servidor LDAP siguiendo los pasos establecidos en el protocolo, y apoyándose en el CRL y el repositorio de certificados en donde se resguardan los datos del usuario, así como también su certificado.

*iii*. Cuando estos datos son comprobados y aceptados, se guardarán en una variable temporal, que permanecerá activa durante la sesión del usuario, para el posterior proceso de verificación de firmas agregadas y firma de información agregada al sistema, acorde a los pasos del protocolo en la fase 3.

- *Recomendaciones generales en el sistema*

*i*. La sesión de usuario autenticado no debe superar 60 minutos de inactividad en el sistema.

*ii*. Habilitación de registros de auditorías.

*iii*. El control de acceso debe definirse a partir de la política del menor privilegio y establecerse basándose en roles o atributos que cada usuario de los diferentes sistemas del SIAP necesite para cumplir con sus labores.

*iv*. Capacitación a los usuarios finales.

*v*. Desarrollo de manuales de usuario.

*vi*. Se recomienda aplicar un ataque de vulnerabilidades controlado (Pen-testing) al código fuente del sistema SIAP.

*vii*. Utilizar para llave simétrica el estándar AES-128, para llave pública RSA-1024, para función picadillo SHA-256, generación de certificados con estándar X.509

- *Recomendaciones generales en la base de datos*

*i*. Para poder tener un mejor resguardo de la información ingresada para los pacientes, se recomienda la normalización de la estructura entidad relación de la base de datos, crear tablas de relación que realicen un match de los datos generales del paciente con los datos de diagnósticos, exámenes clínicos, citas, etc. y así poder cifrar estas tablas y tener un mejor control de la información ingresada.

*ii*. Si la primera opción, de realizar cambios a la estructura de la base de datos para crear nuevas tablas de relación resulta demasiado complicada, en tema de tiempos y costos, se recomienda cifrar sólo una parte de las tablas. Cifrar únicamente las columnas que permitan realizar un match de una tabla con información general del paciente, con otra tabla que presente la información de diagnóstico, citas, exámenes médicos etc. Con esta opción el cambio no se realizaría directamente en la base de datos, sino que se ejecutaría en la parte del código al momento de ingresar la información (cifrar) y al momento de consultar la información (descifrar), para que esto sea más sencillo se recomienda la creación de procedimientos almacenados de cifrado y descifrado, para que la aplicación únicamente vaya a consumir dichos procesos.

*iii*. Bases de datos en alta disponibilidad.

*iv*. Creación de servidores clusterizados

*v*. Resguardo de información hacia sitio de contingencia en tiempo real.

*vi*. Creación de políticas de respaldo, resguardo y recuperación de la información.

## 6. CONCLUSIONES

En El Salvador surge la oportunidad a partir de la iniciativa pública en búsqueda de un gobierno electrónico, de impulsar la implementación del expediente clínico electrónico, es así como tomando de referencia y ejemplo a otros países de Latinoamérica, esquemas criptográficos utilizados en la implementación de ECE a nivel internacional, la normativa y regulación nacional e internacional aplicable, y un análisis profundo de la implementación actual del SIAP, se diseña y propone un módulo de seguridad basado en un protocolo criptográfico que busca facilitar la implementación plena y equivalente de expediente digital con respecto al físico y sirva como puente en la adopción confiable de procesos y servicios del estado de manera digital.

La implementación del módulo de seguridad, en cuanto a sus insumos, es alcanzable a corto o mediano plazo por parte del MINSAL, esto como resultado del proceso de diseño y planificación de las características y requerimientos que tendría que cumplir el protocolo, en donde se tomó en cuenta el contexto y los recursos que posee la institución, para que el diseño facilite la adopción del módulo de seguridad e impulse la apuesta por el ECE que ha hecho el gobierno.

Con la implementación del módulo de seguridad se cumple la meta de mitigar las vulnerabilidades más importantes que presenta el SIAP actualmente, y existe una brecha significativa en las vulnerabilidades encontradas ahora y aquellas que se presentan posteriores a la implementación del protocolo, observándose una mejora significativa en conceptos de confidencialidad, integridad y no repudio.

La metodología fue diseñada para servir como un guía general, flexible para ser utilizada por cualquier proceso dentro de los módulos que componen el SIAP, brindando respuestas a las necesidades de seguridad que cada flujo de información en la identificación de pacientes, citas, seguimiento clínico, agenda de médicos, laboratorio clínico, farmacia o imagenología presente.

El módulo de seguridad si bien cumple con los requerimientos de los servicios de confidencialidad, integridad y no repudio, si no se complementa con controles enfocados al control de acceso y disponibilidad, la futura implementación quedará desprotegida de atacantes que exploten las vulnerabilidades de estos dos servicios. En el futuro se deberá plantear utilizar otros esquemas de arquitectura que incorporen arquitecturas como la nube, o la utilización de protocolo criptográficos innovadores como blockchain para responder ante la creciente demanda de servicios de seguridad en ambientes clínicos hospitalarios de manera eficiente y eficaz.

## REFERENCES


[1] Legislativa, A., "Asamblea Legislativa de la República de El Salvador: Ley de firma electrónica, Decreto 133." Diario oficial de la Nación, Octubre 2015.

[2] Hernandez-Ávila JE, Palacio-Mejía LS, L.-E. A., "Expediente Clínico Electrónico en Colima." Measure Evaluation: Informe Especial, Mayo 2012.

[3] NOM-024-SSA3-2012, N. O. M., "Sistemas de Información de Registro Electrónico para la Salud. Intercambio de Información en Salud." Diario Oficial de la Federación, Noviembre 2012.

[4] Vidas, I. M., "Salud a golpe de tecla." Banco Interamericano de Desarrollo, Consultado Noviembre 2019.

[5] Licensed, H. S., "Health Level Seven International ." ©2007 − 2020 Health Level Seven International.

[6] de la Salud, O. P., "CIE-10, Clasificación Estadística Internacional de Enfermedades y Problemas Relacionados con la Salud." Publicación Cientfica, © Ginebra, OMS, 1992.

[7] DICOM®, "Digital Imaging and Communications in Medicine PS3.1 2020a." International Standard, 2020.

[8] LOINC®, "The International Standard for identifying health measurements, observations, and documents.." url=https://loinc.org/, 2020.

[9] Informatics, T. C. I. . H., "ISO 136061:2008 health informatics (electronic health record communication) part 1: Reference model." url: https://www.iso.org/standard/40784.html, 2020.

[10] Técnico, C., "Manual de usuario, sistema integral de atención al paciente."