UNIVERSIDAD DON BOSCO
VICERRECTORÍA ACADÉMICA
FACULTAD DE INGENIERÍA

TRABAJO DE GRADUACIÓN PARA OPTAR AL GRADO DE

Maestro en Seguridad y Gestión de Riesgos Informáticos

PROYECTO

Metodología para implementación de módulo de seguridad basado en firmas digitales del expediente clínico electrónico del MINSAL

PRESENTADO POR

Ing. Carlos Ernesto Alvarado Rivera

Ing. Andrés de Jesús González Ayala

Ing. Ángel Fernando López García

ASESORA

Dra. María de Lourdes López García

Antiguo Cuscatlán, La Libertad, El Salvador, Centro América

Enero 2020

Metodología para implementación de módulo de seguridad basado en firmas digitales del expediente clínico electrónico del MINSAL

Carlos Ernesto Alvarado Rivera & Andrés de Jesús González & Ángel Fernando López

Enero 2020

Universidad Don Bosco

Vicerrectoría Académica

Facultad de Ingeniería

Maestría en Seguridad y Gestión de Riesgos Informáticos

Dedicatoria

Le dedico a Dios primero que todo, puesto que su guía ilumina y bendice los esfuerzos realizados en este trabajo, y se lo dedico a mi familia, en especial a mi madre, ya que ella me ha servido siempre de apoyo y ejemplo de superación, me ha impulsado a cumplir con lo que me propongo y a superarme a mí mismo.

Carlos E. Alvarado

Quiero dedicar este trabajo primeramente a Dios, quien me ha dado sabiduría y fortaleza, dedicárselo también a mi esposa que incondicionalmente me ha apoyado y motivado a seguir adelante, a mis padres quienes siempre me inculcaron los buenos valores.

Andrés González

Se lo dedico a mis padres por ser los principales promotores de mis sueños, gracias a ellos por cada día confiar y creer en mí y en mis expectativas, a mi madre por enseñarme que puedo lograr todo lo que me proponga y darme siempre su apoyo incondicional, a mi padre por siempre desear y anhelar lo mejor para mi vida, por sus consejos y cada una de sus palabras. A Dios por la vida de mis padres, porque cada día bendice la mía con la hermosa oportunidad de estar y disfrutar al lado de las personas que sé que me aman y a las que yo amo. Y finalmente a mis compañeros y amigos de tesis que estuvieron conmigo a cada momento con los cuales dedicamos largas jornadas para poder cumplir este sueño.

Ángel López

Agradecimientos

Agradecemos a la Dra. Lourdes López, asesora de esta tesis, puesto nos demostró que es ser un verdadero líder en su guía para el desarrollo de este proyecto, y agradecemos la colaboración del personal de la DTIC del Ministerio de Salud por su tiempo y accesibilidad para el diseño de la propuesta.

Abstract

El presente proyecto de investigación busca dar respuesta a la demanda de servicios digitales que el gobierno de El Salvador propone como ejes estratégicos de gestión, principalmente en el área de salud en la utilización del expediente clínico electrónico para la atención de pacientes que hacen uso del sistema nacional de salud pública, dicha apuesta propone retos a nivel tecnológico para cumplir con los requerimientos de seguridad, funcionalidad y regulatorios que permitan la adopción plena y equivalente del documento digital en lugar del físico.

Ante lo anterior se propone el diseño de un módulo de seguridad basado en firmas digitales e infraestructura de llave pública que permita mitigar los riesgos y vulnerabilidades de la implementación actual de ECE, con un diseño robusto y alcanzable de protocolo de seguridad que satisface los requerimientos en confidencialidad, integridad y no repudio a partir de un doble factor de autenticación, utilización de firmas agregadas, estampa de tiempo, infraestructura de llave publica y cifrado simétrico de la información clínica relevante.

Tabla de Contenidos

Lista de tablas

Lista de figuras

Capítulo I

Introducción

El constante crecimiento de las tecnologías ha hecho que todas las instituciones se acomoden a una nueva forma de ejecutar sus procesos, lo que antes se hacía de forma manual, ahora puede realizarse de forma automatizada. Esto aplica y es muy relevante en el área de la salud, dónde, 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).

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.

En El Salvador, por parte del Ministerio de Salud (MINSAL), 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.

Planteamiento del problema

En muchas de las instituciones de atención médica no se cuenta con un control real de la información, primero la información médica de un paciente particular no se encuentra en un mismo sitio, más bien en cada centro de atención en donde este paciente ha pasado consulta o se le ha brindado tratamiento en un momento dado, se guardan segmentos de su historial clínico de manera física, información únicamente accesible en el centro de atención particular, lo que limita de gran manera la efectividad del historial clínico como una herramienta de diagnóstico y tratamiento de una enfermedad ya que no se cuenta con la información clínica completa y de manera oportuna.

Sumado a lo anterior, es una realidad que no existen controles que aseguren la confidencialidad de los expedientes, a parte de los "accesos restringidos" a las áreas donde se resguardan los archivos, que fácilmente pueden ser vulnerados por los mismos empleados, no se cuenta con una bitácora de proceso, lo que abre la puerta a consultas o manipulación de la información sin la autorización correspondiente.

Ahora bien, en el caso donde ya se cuenta con la información en formato digital, la disponibilidad y confidencialidad de la información mejora, pero surge otro desafío ya que no se puede garantizar la integridad y autoría de la información de manera inequívoca, lo que genera un vacío en la validez del expediente clínico electrónico, cuya implementación actual en el MINSAL no es más que un sistema de registro de estadísticas o respaldo digital de los expedientes físicos.

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.

Está sustitución radica en equiparar en cuanto a validez el uso del ECE en el Sistema Nacional Salvadoreño y particularmente en el MINSAL, con el expediente clínico físico del esquema de atención médica tradicional, por lo que se necesita de una estructura de seguridad que brinde no solo confidencialidad, disponibilidad e integridad de la información, sino que también ofrezca el servicio de no repudio de la información, muy importante en el esquema de atención médica puesto que permite cumplir con procedimientos de auditoría y los requerimientos legales de la información clínica.

Objetivos

Partiendo que en el país 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.

El SIAP, el cual es un sistema de desarrollo propio de la DTIC, tiene como objetivo la implementación del expediente electrónico único, haciendo uso de herramientas de software libre, cuya implementación ha sido paulatina y que actualmente es utilizado en las áreas de farmacia, seguimiento médico (consulta externa), citas, identificación de pacientes (archivo), laboratorio clínico de 27 de los 30 hospitales nacionales y la mayoría de las unidades comunitarias de salud familiar a lo largo de los 14 departamentos del país.

Finalmente es primordial que en la propuesta de metodología de implementación de infraestructura de llave pública se considere el contexto económico, tecnológico y técnico que el ministerio ya posee, puesto que se busca complementar los esfuerzos para la adopción del ECE, ofrecer procedimientos alcanzables que vayan de la mano a los objetivos y requerimientos funcionales del SIAP, y permitir al MINSAL ser referencia a nivel nacional en la ejecución de proyectos enfocados a cumplir la estrategia de gobierno electrónico. Dado lo anterior, los objetivos, general y específicos, se listan a continuación.

Objetivo General

Diseñar un módulo 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.

Objetivos específicos

1. Recopilar la información sobre la implementación y uso del expediente clínico electrónico del Ministerio de Salud.
2. Identificar las vulnerabilidades del expediente en su versión manual y digital.

3. Proponer el protocolo para la implementación de firma digital, en el expediente clínico electrónico del Ministerio de Salud.
4. Validar el protocolo a partir de un análisis de escenarios de seguridad.
5. Definir una metodología para la adición del módulo de seguridad propuesto y de la adecuada infraestructura de llave pública a partir de las necesidades y características del expediente clínico electrónico del MINSAL.

Justificación

Un paciente al presentarse a la red de salud pública, ya sea un Hospital o las distintas unidades de salud de todo el país, no cuenta con un expediente único, es decir que muy probablemente el expediente clínico de esta persona está únicamente disponible en la entidad en la cual fue creado al realizar su primera consulta, y si por alguna razón o emergencia el paciente no puede acudir a la misma institución a realizar sus consultas, la información de este vuelve a ser ingresada a un nuevo expediente, teniendo así una disgregación de información en varios centros de atención médica, y perdiendo la retroalimentación o información histórica de consultas anteriores como también exámenes, recetas, etcétera, antes realizadas.

Aunque en el MINSAL se maneja un sistema que centraliza toda la información de los diferentes centros médicos en el SIAP, este no resuelve el problema, ya que solo funciona como una herramienta de respaldo y los “verdaderos” expedientes clínicos se crean de forma manual, “ordenados” en grandes estantes, dentro de enormes cuartos que apenas cumplen con las condiciones mínimas de almacenamiento idóneo, donde sólo “unas

cuantas" personas tienen acceso. Este sistema de control es vulnerable a ciertos problemas como la usurpación de identidad, duplicidad, repudio o pérdida de la información.

Por este motivo, se requiere un módulo de seguridad, que permita la protección de toda la información de los pacientes; esfuerzo necesario para desarrollar un ECE que se equipare técnica, y legalmente con el expediente clínico físico, lo que ayudará a garantizar el no repudio, resguardar la integridad y la confidencialidad de la información.

Al contar con un Expediente Clínico Electrónico Seguro (ECES) se ayudará en gran 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.

Además, en la metodología propuesta se tomará 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.

Alcance

La metodología para implementar el módulo de seguridad abarca todos los procesos involucrados en el ECE del MINSAL englobados en el SIAP: Creación del ECE, consultas, recetas, exámenes de laboratorio clínico, citas.

Por lo tanto, se dejará un procedimiento de firma de forma general, el cual permitirá escalar el módulo de forma automática a todos los centros de salud que dependen del MINSAL y que cuenten con SIAP, como son los hospitales, regionales y unidades de salud.

Metodología

La investigación realizada fue de tipo documental tanto en las implementaciones del ECE como las propuestas de los protocolos criptográficos utilizados para un expediente digital. Además, se realizó una investigación por capas que cubre cada una de las fases requeridas para el diseño de la metodología propuesta y que se listan a continuación:

1) Análisis de seguridad del escenario actual del SIAP

2) Identificación de las vulnerabilidades presentadas en cuanto a los servicios de seguridad: integridad, confidencialidad y no repudio.

3) Desarrollo del protocolo de seguridad

4) Comprobación de la propuesta a partir de un análisis de seguridad y eficiencia.

Organización del documento

El resto del documento se compone del capítulo II que menciona el estado del arte respecto a los expedientes electrónicos dentro y fuera del país. En el capítulo III se explica el funcionamiento actual del SIAP, así como, las vulnerabilidades de seguridad identificadas. El capítulo IV, se propone el protocolo de seguridad y se realiza el análisis de seguridad y eficiencia, mientras que en el capítulo V, se presenta la metodología de implementación del

módulo de seguridad. En el capítulo VI se realiza una discusión de los resultados y finalmente en el capítulo VII se presentan las conclusiones de este trabajo.

Adicionalmente, en el apéndice A, se presentan los fundamentos de las herramientas criptográficas utilizadas en el protocolo de seguridad, para su mayor entendimiento y en apéndice B, se listan las normativas y regulaciones respecto a la salud de los ciudadanos.

Capítulo II

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 ayuda a conocer las condiciones de salud y los diferentes procedimientos ejecutados por el personal médico a lo largo de un proceso asistencial.

Con el avance de las ciencias y la tecnología este concepto se puede considerar como un sistema informático que almacenará los datos de un paciente en formato digital, que puede ser compartida y resguardada de una manera segura para luego ser accedido por otros usuarios autorizados.

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 expediente clínico electrónico 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 u hospitales.

En nuestra región, el expediente clínico ya es toda una realidad, en ciertos países esto se ha venido trabajando desde hace ya mucho tiempo y ya se cuentan con las estructuras informáticas, así como los procedimientos y normativas requeridas por cada uno de los países para que este expediente pueda ser utilizado por los usuarios de la salud pública.

Entre los países en los cuales el ECE ya se tiene un avance significativo, se pueden mencionar a México, Uruguay, Chile y Colombia.

En México el proceso de implementación y actualización del ECE se contempló alrededor de los años 2009 hasta el 2015 teniendo como meta para el año 2011 llegar a un 99% de unidades de salud que lo habían implementado [2]. Para poder dar seguimiento y mejorar la calidad de los servicios de salud, México estableció 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]. Esta Norma Oficial Mexicana es de observancia obligatoria en todo el territorio nacional para todos los productos de Expediente Clínico Electrónico que se utilicen en el Sector Público, así como para todos los establecimientos que presten servicios de atención médica, personas físicas y morales de los sectores social y privado que adopten un sistema de registros electrónicos en salud en términos de la presente norma y de la legislación aplicable.

Como se definió antes esta norma tiene por objeto establecer los objetivos funcionales y funcionalidades que deberán observar los productos de Sistemas de Expediente Clínico Electrónico, en esta se detallan los procesos de transferencia de información, así como el protocolo de firma a utilizar. Se detallan los tipos de sistemas en los que el ECE será aplicable, como por ejemplo, consulta externa, hospitalización, urgencias, farmacia, laboratorio, imagenología y quirófano.

Con esta norma el proceso de aplicación del expediente clínico para todos los estados mexicanos se hace un poco más fácil ya que siguiendo esta guía se tiene un estándar de las funcionalidades y el desarrollo del software de cada uno de ellos, logrando así una integración general de todos los ECE.

En otro caso, Uruguay que al igual que México es uno de los más avanzados en la región con respecto al ECE, y es el primer país de América Latina en implementarlo a nivel nacional.

"El historial clínico electrónico es una modificación efectiva a la gestión de los servicios de salud de emergencia", explica Roberto Fernández, especialista líder en modernización del estado en el Banco Interamericano de Desarrollo (BID). A través de fondos donados por el Fondo Especial Japonés (FEJ), el BID apoyó a la Administración de los Servicios de Salud del Estado (ASSE) a implementar la historia clínica electrónica en 58 centros de salud distribuidos por todo el país [4].

En 2007, Uruguay emprendió una reforma integral del sector salud, teniendo como objetivo proporcionar accesos universales a servicios de salud de calidad. Se detectó que la falta de sistemas adecuados de tecnología de información y de comunicación limitaba al estado para lograr sus objetivos.

Para gestionar bien los recursos humanos y materiales disponibles y enfocar los servicios hacia la salud preventiva era prioritario tener información actualizada sobre:

1. El estado de salud de la población
2. La cantidad de servicios y cuidados ofrecidos
3. El nivel de calidad de proveedores de servicios de salud

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. En este sentido, el mayor logro fue la creación del sistema de Historia Clínica Electrónica Nacional, en las que, todas las historias clínicas fueron digitalizadas con un formato único que facilita su distribución a la red de centros de salud del país. Los médicos tienen acceso actualizado al historial clínico de los usuarios y estos reciben el mejor tratamiento posible en cualquier parte del país que se encuentren. La plataforma espera incluir la mayoría de los datos clínicos del 80% de la población en formato electrónico para 2020.

En estos casos, ante la posibilidad de tener información sensible y ante la falta de uniformidad en los registros médicos y la necesidad de compartirlos, es imprescindible consensuar un conjunto básico de elementos definidos que puedan transformarse en información relevante. La interoperabilidad es obligada si se desea obtener información homogénea y desarrollar un trabajo eficaz.

La información normalizada, además de ser clínicamente ventajosa, es imprescindible en la formación, investigación, evaluación, gestión y planificación. Un objetivo clave es lograr definir por consenso un conjunto mínimo de datos, así como determinar su significado.

Es por lo anterior y, para garantizar la interoperabilidad entre sistemas, que se hace necesario el uso de estándares que permitan el intercambio de datos, así como la utilización de catálogos estandarizados, los cuales son aquellos que unifican los datos empleados en

distintas instituciones derivando en el intercambio correcto de información. A continuación, se mencionan algunos estándares ya establecidos:

- HL7: Estándar de mensajería para el intercambio electrónico de información clínica basada en el RIM (*Reference Information Model*).
- 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.*
- DICOM: Estándar reconocido mundialmente para el intercambio de imágenes médicas, pensado para el manejo, almacenamiento, impresión y transmisión de imágenes médicas.
- *LOINC: Logical Observation Identifiers Names and Codes* (códigos universales para identificar observaciones clínicas y laboratorio).

Estos estándares permiten que la historia clínica sea transformada en un expediente virtual que circulará por la red, que será accesible a otros profesionales y cuya llave de acceso estará en poder del paciente por medio de su clave médica. Lo cierto es que la historia clínica se transforma en un sistema electrónico que resguarda la identidad y la información clínica de un paciente y a su vez, la pone a disposición de las autoridades que le brindan los servicios médicos requeridos. Garantizar estas cuestiones es responsabilidad del cuerpo médico quien deberá respetar las normas de utilización de la historia clínica del paciente, dirigidas a salvaguardar la confidencialidad y la seguridad de la información.

Por otro lado, estudiar las soluciones que instituciones internacionales han desarrollado para la implementación de un ECE seguro bajo distintos esquemas criptográficos y extraer

ideas, experiencias y/o herramientas que faciliten el diseño del protocolo criptográfico es el primer paso del diseño del módulo de seguridad para el SIAP.

Se debe reiterar que la protección y seguridad de la información personal es crítica en el sector salud, buscando fundamentalmente brindar confidencialidad, integridad y disponibilidad para los datos clínicos producto de la interacción entre pacientes y un sistema o institución de salud.

Esta información clínica es también considerada por muchos, como uno de los tipos de información personal más confidencial y sensible, por lo que la protección de esta confidencialidad es esencial si se quiere cumplir con el derecho constitucional a la privacidad de cada paciente.

No se omite manifestar que la seguridad de los datos médicos, en estos últimos años, se ha visto comprometida por ataques que buscan la pérdida, robo o secuestro de la información [5-7], siendo estos algunos de los casos en donde ha ocurrido una filtración y sirven como ejemplos concretos que ilustran de mejor manera los riesgos actuales que debe enfrentar una implementación de ECE.

Otro riesgo surge a partir del paradigma de brindar acceso a los pacientes de sus respectivos ECE, lo cual tiene efectos positivos en el involucramiento del paciente y la mejora en la atención del sistema de salud [8], pero también cuenta con efectos negativos como el aumento de la superficie de ataque.

Otra preocupación real, son los niveles de acceso, que tanto las personas como las entidades tienen a los ECE de pacientes, puesto que un ECE de un paciente podría estar fragmentado y accesible desde varios sitios, en donde una falla de seguridad en cualquiera de estos

sistemas podría revelar la información a personas o entidades no autorizadas, o en otro caso una falla en la privacidad puede existir a tal punto que personal administrativo de una institución pueda acceder a información clínica de un paciente sin el expreso consentimiento de éste; en definitiva los datos médicos necesitan protección contra la manipulación, accesos no autorizados y abusos, que incluye tomar en consideración problemas en la privacidad, confianza, autenticación, responsabilidad y disponibilidad de la información.

Estándares y regulaciones internacionales para un ECE seguro

Muchos de los diseños de sistemas de Expediente Clínico Electrónico se 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.

Una de estas regulaciones que puede servir de referencia es la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA por sus siglas en inglés) de 1996, la cual define las reglas de privacidad que rigen la informática médica en EEUU y asegura que los pacientes tengan acceso a su propia información clínica, definiendo por ejemplo 18 tipos de identificadores principales que deben ser ocultados, cifrados o eliminados de la información médica protegida, los cuales son nombres, direcciones, fechas, números telefónicos, FAX, números de seguridad social, beneficiarios del plan médico, números de cuenta, licencia, certificados, identificadores de vehículos o dispositivos, URLs, direcciones IP, datos

biométricos, retratos fotográficos, o cualquier identificador único ya sea numérico, características, rasgos o código [9].

Una regulación a tomar en consideración es el recientemente aprobado Reglamento General de Protección de Datos de la Unión Europea (RGPD), donde establece los datos médicos como una categoría especial de datos que requiere una especial protección, otorgando la propiedad de los datos personales médicos en exclusiva al paciente, lo que permite exigir un consentimiento explícito para la manipulación de estos datos por parte de este o en casos especiales donde impere la necesidad por razones médicas, salud pública, investigación clínica o científica.

Hablando de estándares que abordan los ECE, es necesario mencionar el CEN/ISO EN 13606 – en su apartado IV, que 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.

El estándar ISO 27799 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 [10]. 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.

Protocolos de seguridad y privacidad

Existen muchos esquemas que permiten proteger la privacidad de los pacientes, pero por lo general se utilizan dos diferentes técnicas para proteger la información clínica, el cifrado que permite la confidencialidad y anonimizar la información logrando así la privacidad de los pacientes desvinculando la información entre esta y su origen.

Según la Real Academia Española, anonimizar es expresar un dato relativo a entidades o personas, eliminando la referencia de su identidad. En el expediente clínico, es el proceso de eliminar o modificar cualquier identificador de la información clínica personal, de tal forma que la identificación sobre a quién le pertenece los datos médicos no sea razonablemente posible. Ventajas de este método en comparación con el cifrado completo de la información médica es que permite la divulgación de los datos médicos para ser utilizados en la enseñanza, estadísticas, estudios médicos etc., sin necesidad de personalizar dicha información.

El proceso de pseudo-anonimizar es una aplicación del concepto anterior utilizando herramientas criptográficas, que consiste principalmente en transformar y después reemplazar información personal con un pseudónimo que no puede ser asociado con la información de identificación sin conocer un secreto. Permitiendo el uso directo de los datos clínicos por los proveedores de servicios sanitarios e indirecto por parte de instituciones para la investigación clínica.

Para pseudo-anonimizar se usan las funciones picadillo (*Hash*) selectivamente a los datos de identificación del paciente, siendo esta operación no reversible [11]. Es posible pseudo-anonimizar en modo reversible, con la aplicación selectiva de un algoritmo de cifrado

simétrico, en donde se incorpora nuevamente la función *hash* de los identificadores para brindar el servicio de integridad además de la confidencialidad para los datos de identificación de los expedientes [12].

Los esquemas criptográficos deben ser introducidos para proveer confidencialidad en un sistema ECE. Y estos esquemas se apoyan en llave pública, llave simétrica o un híbrido entre ambas. Para mayor entendimiento de los esquemas criptográficos utilizados en este documento, se puede consultar el Apéndice B.

Existen propuestas en donde la información clínica se encuentra cifrada en servidores y el proveedor de la misma manera almacena las claves simétricas en servidores distintos [13], otro enfoque es que el paciente genere sus propias llaves de cifrado asimétricas [14], lo que empodera al paciente a controlar el acceso a su información clínica, pero aumenta el gasto computacional necesario para cifrado de la información.

Esto último, dificulta la implementación de esquemas de llave asimétricos cuando los recursos son escasos y se tienen alto volumen de información (ej. imágenes médicas), por lo que se puede proponer el uso de esquemas híbridos de infraestructura de llave pública (HPKI), utilizando la opción de usar un esquema PKI para información sensible pero no demandante en recursos computacionales como el texto de un diagnóstico médico, complementándose con tecnología de criptografía simétrica para el almacenamiento y transmisión de información médica como imágenes [15].

Capítulo III

Funcionalidad del Sistema Integral de Atención al Paciente

Este capítulo tiene como objetivo explicar el diseño de la infraestructura y flujo del SIAP, el cual es utilizado por el MINSAL para la recopilación de la información clínica de cada uno de sus pacientes, así como, llevar el control de los accesos y credenciales del personal clínico que presta sus servicios en cada establecimiento.

Igualmente, se presentará el análisis de vulnerabilidad realizado al ECE conformado por el SIAP del MINSAL, describiendo a detalle las principales debilidades, ataques y riesgos en seguridad que presenta el escenario actual.

Funcionalidad

El SIAP (Sistema Integral de Atención al Paciente) 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 (SUIS) [16].

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 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. La Figura 1 describe de manera general los

procesos e involucrados, identificando los pasos que cada usuario realiza, en el esquema de atención médica.

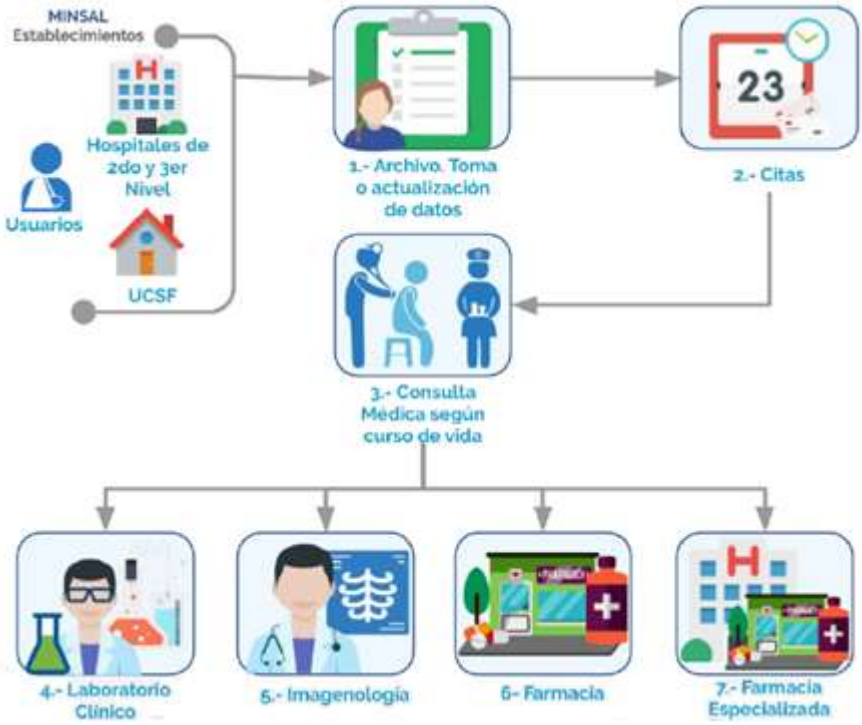

Figura 1. Flujo general del SIAP [16].

La información de cada uno de los pacientes es ingresada a una base de datos (Máquina o equipo informático que se encuentra en el centro de atención, el cual cuenta con su propia base de datos instalada en el equipo), es en este punto en donde se crea un "expediente clínico", por medio del módulo de identificación, mostrado en la Figura 2, de los pacientes del SIAP. En este módulo es también donde se lleva la administración de los empleados y se generan los reportes.

Figura 2. Esquema del módulo de identificación [17].

Este módulo presenta todos los requisitos que se deben ingresar para crear un expediente clínico. Es importante tener en cuenta que estos datos se ingresan cada vez que un paciente visita una unidad de salud o un hospital diferente, debido a que no se cuenta con replicación e integración de datos.

Algunos datos que son necesarios para crear el expediente para pacientes adultos son: NEC (Número de Expediente Clínico), primer nombre, segundo nombre, primer apellido, segundo apellido, tercer apellido (si lo hubiere), conocido por, fecha de nacimiento y DUI. Si es ingresada al sistema por nacimiento: nombre de madre, apellido de madre y establecimiento donde se verificó el parto.

Al ingresar la información obligatoria permitirá la creación del "expediente clínico" en el SIAP, una vez creado, se procede a realizar el seguimiento clínico, exámenes, diagnósticos, etc., de cada uno de los pacientes. Al entregar el diagnóstico a un paciente, el médico crea una cita (en caso de que sea necesario que el paciente regrese por un seguimiento médico, exámenes de laboratorio, imágenes o se le programe un procedimiento quirúrgico), la cual se puede ingresar en el módulo de citas que se ilustra en la Figura 3.

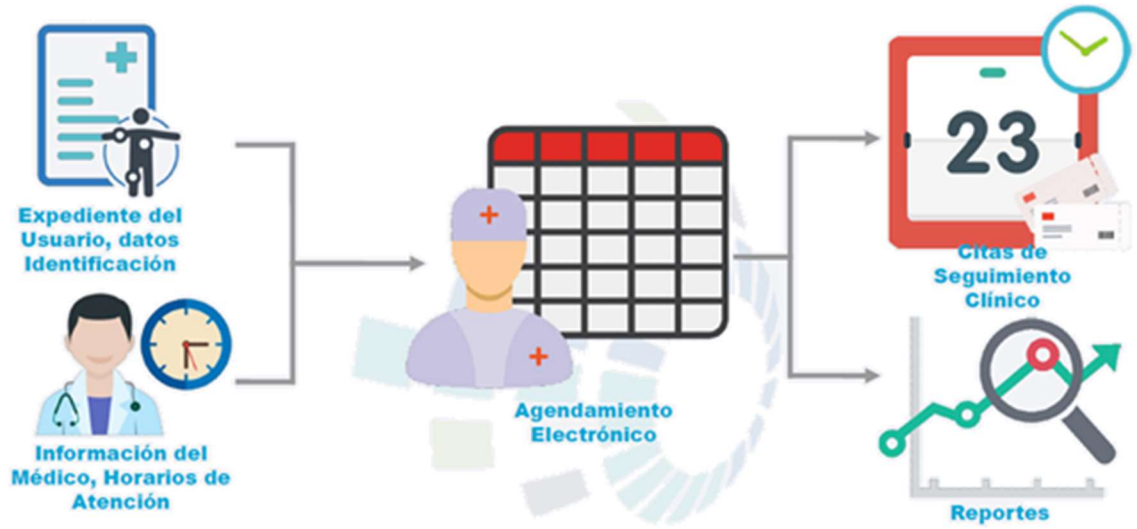

Figura 3. Módulo de citas [18].

En este módulo se tiene la calendarización de la atención de los pacientes por cada uno de los médicos, así como los procedimientos que se realizarán por parte de ellos [18].

Es importante puntualizar, que esto sería para cada uno de los centros de atención y solo se pueden visualizar las consultas de ese centro de atención ya que la información no está distribuida hacia los otros hospitales y unidades de salud.

Una vez creado el expediente, se cuenta con un Módulo de seguimiento clínico (ilustrado en la Figura 4), en este se puede observar, agregar y editar la historia clínica de un paciente desde la creación de su expediente; esta información es fundamental para el médico, puesto que contribuye a un proceso de atención más efectivo, dónde se puede revisar todo antecedente e historial clínico, que incluye la prescripción de medicamento, diagnósticos recientes, padecimientos crónicos, indicación y resultados de exámenes, próximas citas, tratamientos indicados, operaciones quirúrgicas, entre otros[19].

Figura 4. Módulo de seguimiento clínico [19].

En el módulo de laboratorio se lleva el detalle de los análisis y resultados de los exámenes solicitados por el médico para cada uno de los pacientes, como se observa en el flujo presentado en la Figura 5. Este módulo ya cuenta con los estándares HL7 para el intercambio electrónico de la información clínica de los pacientes.

Figura 5. Módulo de laboratorio [20].

Por último, se tiene el módulo de farmacia, con el flujo de operación presentado en la Figura 6. En él se puede realizar el registro, verificación de existencia y asignación de medicamento.

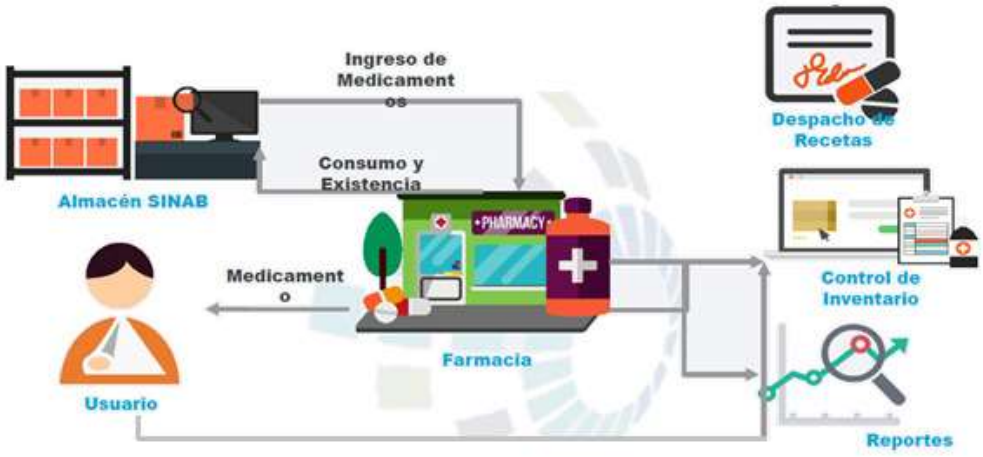

Figura 6. Módulo de farmacia [21].

En la Figura 7, 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).
    a. Si ya cuentan con un expediente clínico, son enviados al área de emergencia para su evaluación y posterior consulta.
    b. 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.

c. Aquellos pacientes con cita programada son enviados directamente a la consulta externa para seguimiento clínico.

d. Algunos pacientes, que solo asisten por toma de exámenes, ya sean de laboratorio clínico o de imagenología, son remitidos hacia el área correspondiente.

3. En el módulo de seguimiento clínico, se verifican las consultas anteriores del paciente y se proporciona un nuevo diagnóstico, según la mejoría del mismo.
4. 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.

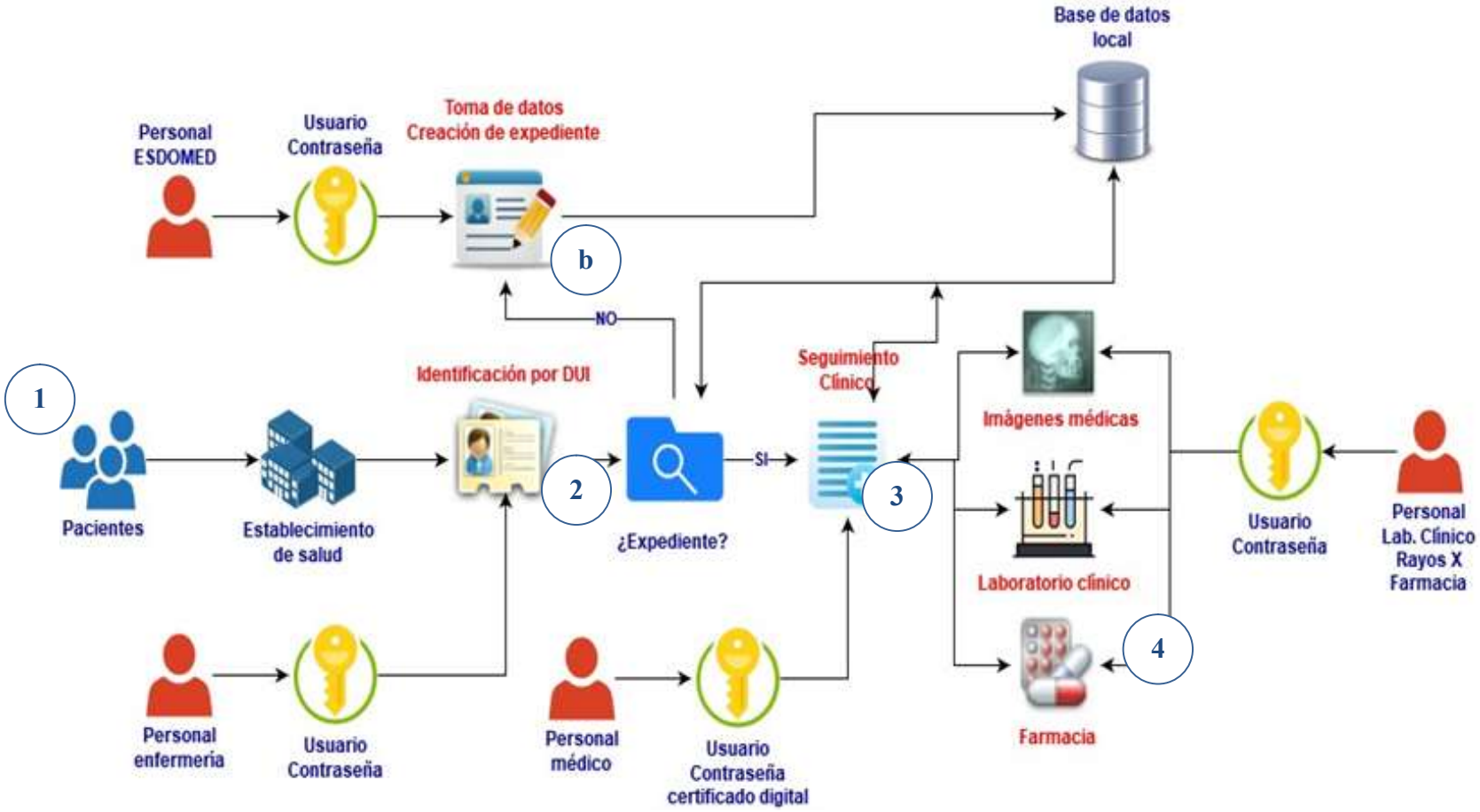

Figura 7. Flujo actual de datos del SIAP [Elaboración propia].

Respaldo de datos

Actualmente, el SIAP se utiliza de forma local, en cada establecimiento de salud en donde se ha implementado, por lo que existe una base de datos por cada establecimiento, esto con el fin de evitar problemas de conexión a una base de datos centralizada, por lo que periódicamente se realiza un respaldo de cada una de esas bases, las cuales son enviadas a servidores ubicados en las 5 regiones de salud (occidental, oriental, central, metropolitana y paracentral), que a su vez son replicados por éstos a un servidor en el MINSAL.

Para este respaldo se crea un archivo comprimido, el cual contiene la base junto con los datos de esta. Estos respaldos son enviados a través de la red del MINSAL, en horarios de menor uso del sistema, para evitar la saturación de los enlaces y de las conexiones hacia los servidores regionales. En la Figura 8, se observa la distribución de los diferentes servidores de respaldo, así como cada centro de atención que envía la información al servidor de base de datos central.

Cabe mencionar que, de ocurrir una falla en el SIAP, ya sea por hardware o por software, puede instalarse todo el sistema operativo y expandir los datos contenidos en los archivos de respaldo, previamente almacenados.

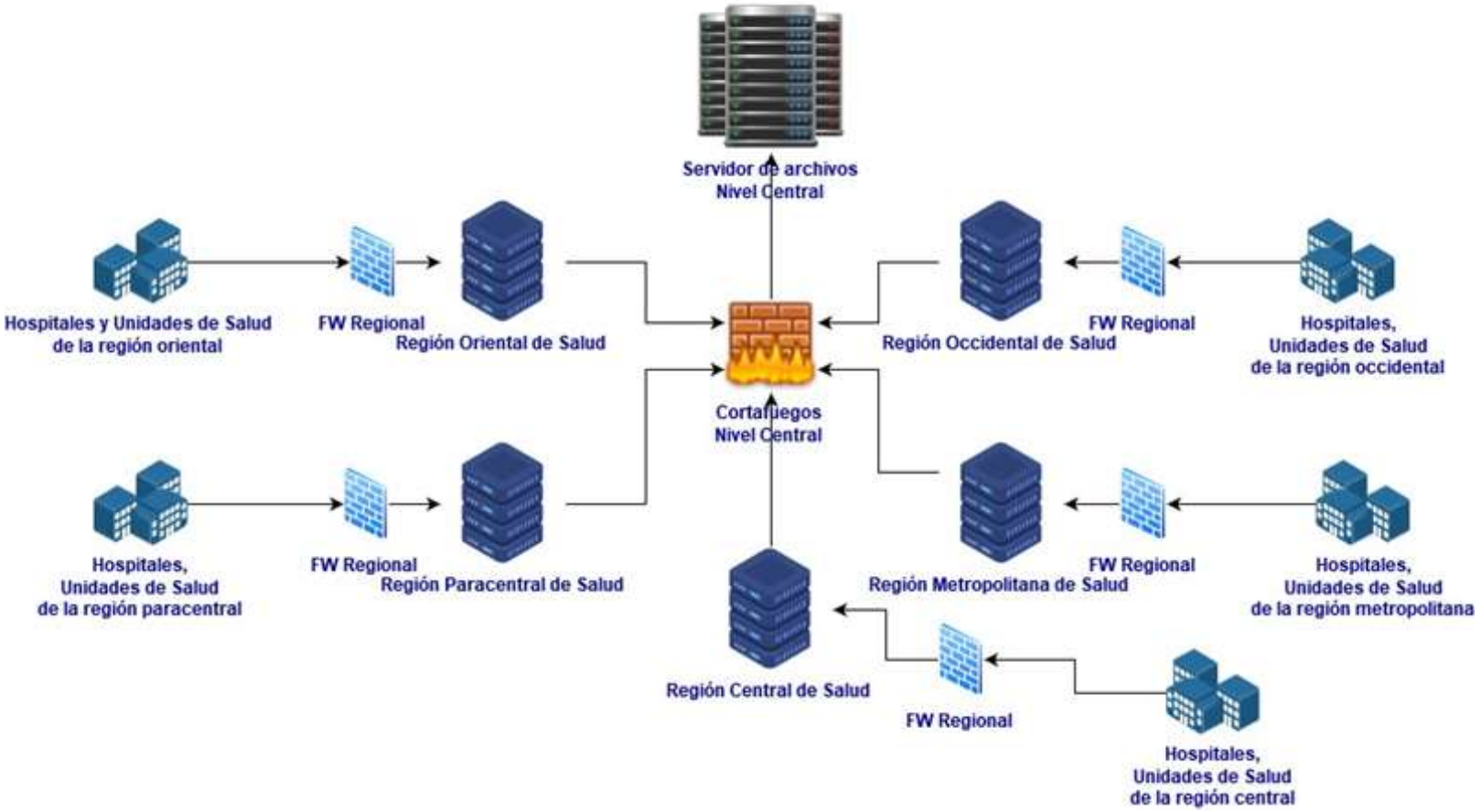

Figura 8. Respaldo de la base de datos del SIAP [Elaboración propia]

Análisis de Vulnerabilidad

Teniendo en cuenta que toda esta información es ingresada en una base de datos que se encuentra instalada en un equipo de cómputo en cada uno de los centros de atención se pueden identificar fácilmente algunas vulnerabilidades en el sistema.

Una 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.

Estos respaldos son enviados hacia un servidor central del MINSAL, pero no se realiza una carga hacia una base de datos centralizada, este servidor solamente sirve como repositorio de estos respaldos, para poderlos recuperar en algún momento que la base de datos de cada uno de los centros de atención sufra alguna falla.

Realizar estos respaldos tal vez pueda ayudar en alguna medida a la parte de la disponibilidad del sistema, pero se presenta otra vulnerabilidad, ya que no se utilizan enlaces cifrados en ninguno de los centros de atención hacia el servidor central del MINSAL, por lo que la información al viajar en un enlace sin protección es susceptible a ser modificada, borrada o robada.

Al no tener la información integrada y centralizada en una sola base de datos para todos los centros hospitalarios, se crea un problema de duplicidad en cada una de las unidades de salud y hospitales ya que al momento que el paciente llegue a otra unidad de salud u hospital deberán de tomar nuevamente sus datos para poder atenderlo.

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.

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.

Además, la base de datos no lleva una auditoría interna de las modificaciones que realizan los administradores dentro del mismo sistema, se utilizan esquemas criptográficos vulnerables como MD5 y toda la información se encuentra en texto plano, sin utilizar ninguna herramienta criptográfica para cifrar la información de cada paciente atendido.

Una vez se ha presentado el funcionamiento general y especifico del SIAP, detallando cada uno de los módulos que lo conforman, así como también indicando las fortalezas y las debilidades que presenta este sistema.

Se resume en la Tabla 1, lo expuesto anteriormente, con el objetivo de tener una perspectiva más clara de las vulnerabilidades encontradas en el escenario actual del SIAP.

Tabla 1. Vulnerabilidades del escenario actual del SIAP

Problema (Vulnerabilidad)	**Ataques**	**Riesgos de Seguridad**
Información descentralizada	Dificultad al acceso de la información almacenada en el resto de los ordenadores	Robo de información Pérdida de información
No cuenta con alta disponibilidad	Ataques de denegación de servicios (DDoS)	Servicios inaccesibles Pérdida de conectividad
Pérdida de certificados, llaves y/o contraseñas	Ataques de no repudio	Suplantación de usuarios Robo de información Pérdida de información
Certificados inseguros	Ataques de no repudio	Robo de información Pérdida de información
Protocolos obsoletos (MD5)	Virus, Troyanos, *Ransomware*	Servicios inaccesibles Robo de información
Enlaces no cifrados	Hombre en el medio	Robo de información suplantación de identidad
No se cuenta con cortafuegos en cada centro de Atención	Ataques de denegación de servicios (DDoS), Virus, Troyanos, Ransomware	Servicios inaccesibles Pérdida de conectividad Robo de información
No hay cifrado de la información de las bases de datos, solo usuarios y contraseñas	Abuso de privilegios Ataques de denegación de servicios (DDoS), *malware*, *spearphishing,* Inyecciones SQL Desbordamientos del búfer	Datos sensibles mal gestionados Robo de información

Capítulo IV

Protocolo de seguridad propuesto

Se propone el siguiente diseño de protocolo como solución a la problemática de seguridad, con el cual se eliminen o reduzcan los ataques y vulnerabilidades identificados en el escenario 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 realizarán las siguientes acciones:

a) **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.

b) **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.

c) **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:

    1. La entidad clínica se autentica por medio de un usuario/contraseña.
    2. Una vez autenticado se genera una clave de sesión que será la clave compartida con el servidor.

3. 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.
4. La persona autenticada puede descifrar el expediente, ya sea para consultar o agregar información.

d) 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:

1. 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.
2. 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.
3. 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.

e) 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 9, se puede apreciar el flujo que sigue el protocolo de seguridad propuesto.

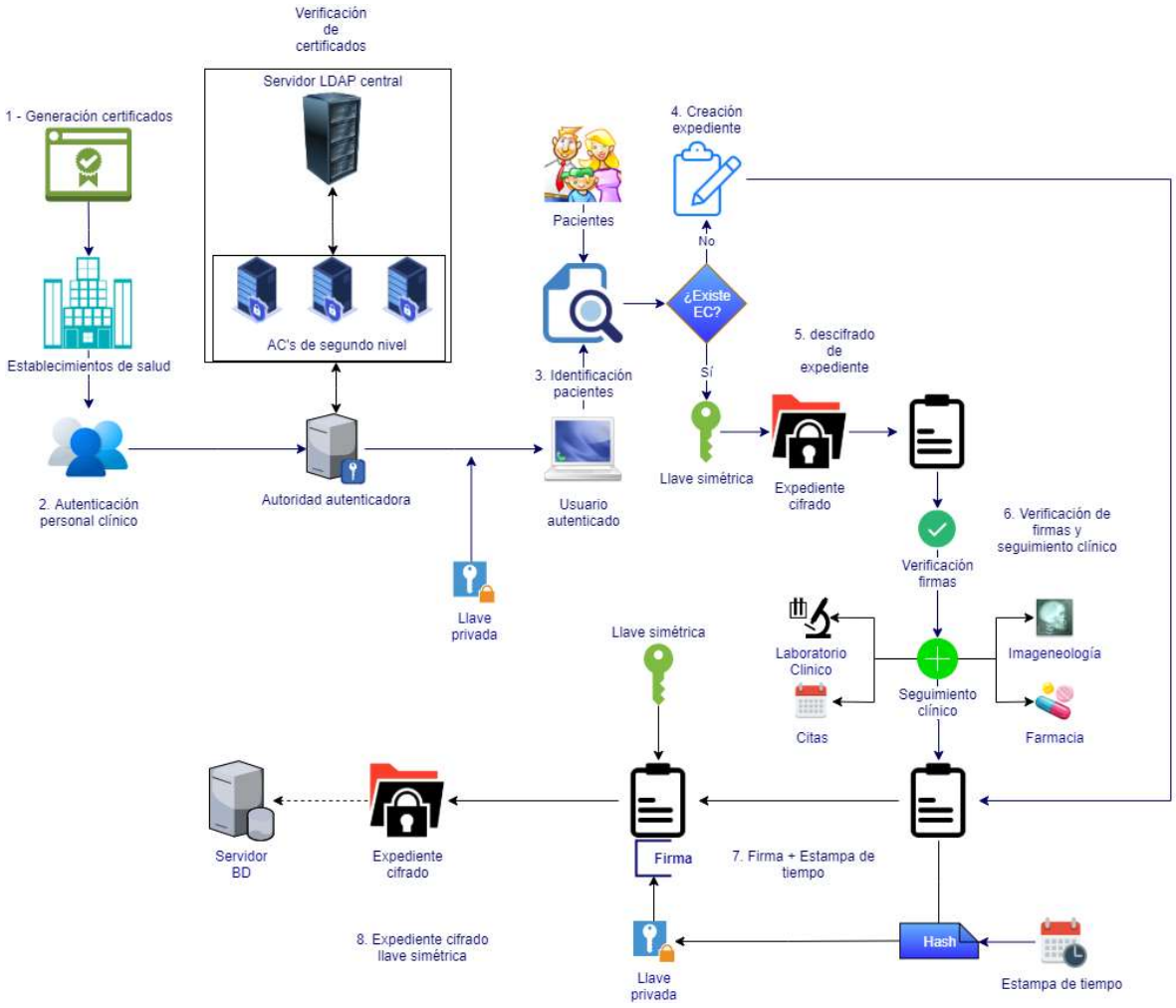

Figura 9. Flujo del protocolo de seguridad propuesto [Elaboración propia].

Como puede observar, es necesario establecer las entidades, los requerimientos de seguridad, las políticas de seguridad y los lineamientos del proceso para que el protocolo de seguridad cumpla con los servicios de seguridad, y que se listan a continuación:

→Entidades

- Ministerio de Salud (AC)
- Institución (AC de 2do Nivel)
- Autoridad de autenticación y estampa de tiempo (AA)
- Personal clínico

→Requerimientos de seguridad

- Confidencialidad
- Integridad
- No repudio
- Autenticación

→Herramientas criptográficas

- Firma agregada
- Funciones *Hash* o picadillo
- PKI
- Llave simétrica
- Estampa de tiempo

→Política

“Toda entidad perteneciente a la institución de salud debe hacer cumplir los requerimientos de confidencialidad, integridad, no repudio y autenticación necesarios para la administración, manipulación y uso de los expedientes clínicos electrónicos que permita garantizar la privacidad y seguridad de la información clínica de cada paciente”.

→Lineamientos:

- Toda persona debe contar con un ECE para recibir la atención médica en la institución de salud, en el caso de no tener, este tiene que ser creado.
- Todo el personal involucrado, contará con un usuario y contraseña para acceder al Sistema de Expedientes Clínicos Electrónicos (ECE), siendo su responsabilidad hacer buen uso de todas estas credenciales.
- Todo el personal usuario involucrado deberá poseer su certificado digital válido por el PKI del MINSAL y su correspondiente llave privada, para acceder e interactuar con el Sistema de Expedientes Clínicos Electrónicos (ECE), siendo su responsabilidad el resguardo adecuado de estas credenciales.
- La información del expediente clínico podrá ser consultada por todas las áreas de la institución de salud (a excepción del área administrativa), con el fin de consultar y/o añadir información al ECE, como: farmacia, laboratorio clínico, personal médico, personal de enfermería, entre otros, por lo tanto, se debe garantizar que a esta información solamente puedan acceder las personas de las áreas antes mencionadas según sus roles.

- Toda entidad de personal clínico al momento de abrir el expediente clínico electrónico debe realizar la verificación de las firmas agregadas anteriores para garantizar la integridad de los antecedentes médicos.
- Toda información como diagnóstico, exámenes de laboratorio clínico, estudios, recetas, y otros deben de ser registradas en el ECE, con la firma digital que corresponde al personal clínico responsable de dicha acción. Para ello cada empleado debe contar con sus llaves privada y pública, certificado digital extendido por la Autoridad Certificadora y cerrar el expediente con su firma digital al finalizar la adición de información.
- Cada consulta y/o cada adición de información al expediente clínico será registrado y sellado con una estampa de tiempo junto con una firma digital agregada, de las personas que realizan estas actividades, con el fin de garantizar la veracidad de los datos adicionados.
- Se debe proporcionar, al personal clínico, los medios tecnológicos necesarios para el acceso a los expedientes clínicos electrónicos.

Protocolo de seguridad

El proceso que realiza el protocolo de seguridad se presenta a continuación:

1. Generación de certificados por parte del MINSAL para cada establecimiento de salud de segundo nivel (hospitales y regionales de Salud)
2. Los usuarios del sistema deben autenticarse con las credenciales del servidor LDAP del MINSAL además de utilizar su llave privada.

3. Una vez el personal clínico ha sido autenticado, pueden ingresar a los módulos del SIAP según su rol, el cual inicia con el módulo de identificación del paciente.
4. Si el paciente no cuenta con un expediente, se solicita un documento de identidad para crearle uno:
    i. Se capturan los datos a través del documento presentado
    ii. Se agrega estampa de tiempo y se hace realiza un *hash* del expediente + estampa de tiempo.
    iii. El personal de ESDOMED firma el expediente con su llave privada.
    iv. Se cifra el expediente con la llave simétrica.
    v. Se guarda la data en la base de datos correspondiente, para ser utilizada dentro del establecimiento.
5. Si el paciente ya cuenta con un expediente, es enviado al área correspondiente para el seguimiento clínico:
    i. Se descifra el expediente con la llave simétrica con la que fue cifrado.
6. El sistema hace una verificación de las firmas anteriores.
    i. Se realiza el seguimiento clínico (Consultas, procedimientos, laboratorio, imágenes médicas, farmacia).
7. Se agrega estampa de tiempo y se hace realiza un *hash* del expediente + estampa de tiempo.
    i. El personal clínico firma el expediente con su llave privada.
8. Se cifra el expediente con la llave simétrica.

i. Se guarda la data en la base de datos correspondiente, para ser utilizada dentro del establecimiento

El diagrama de flujo del protocolo se observa en la Figura 10 parte superior izquierda, que corresponde a la generación de los certificados digitales según el nivel de la Autoridad Certificadora, mientras que en la parte derecha se presenta el diagrama de flujo de la consulta y posible modificación del ECE.

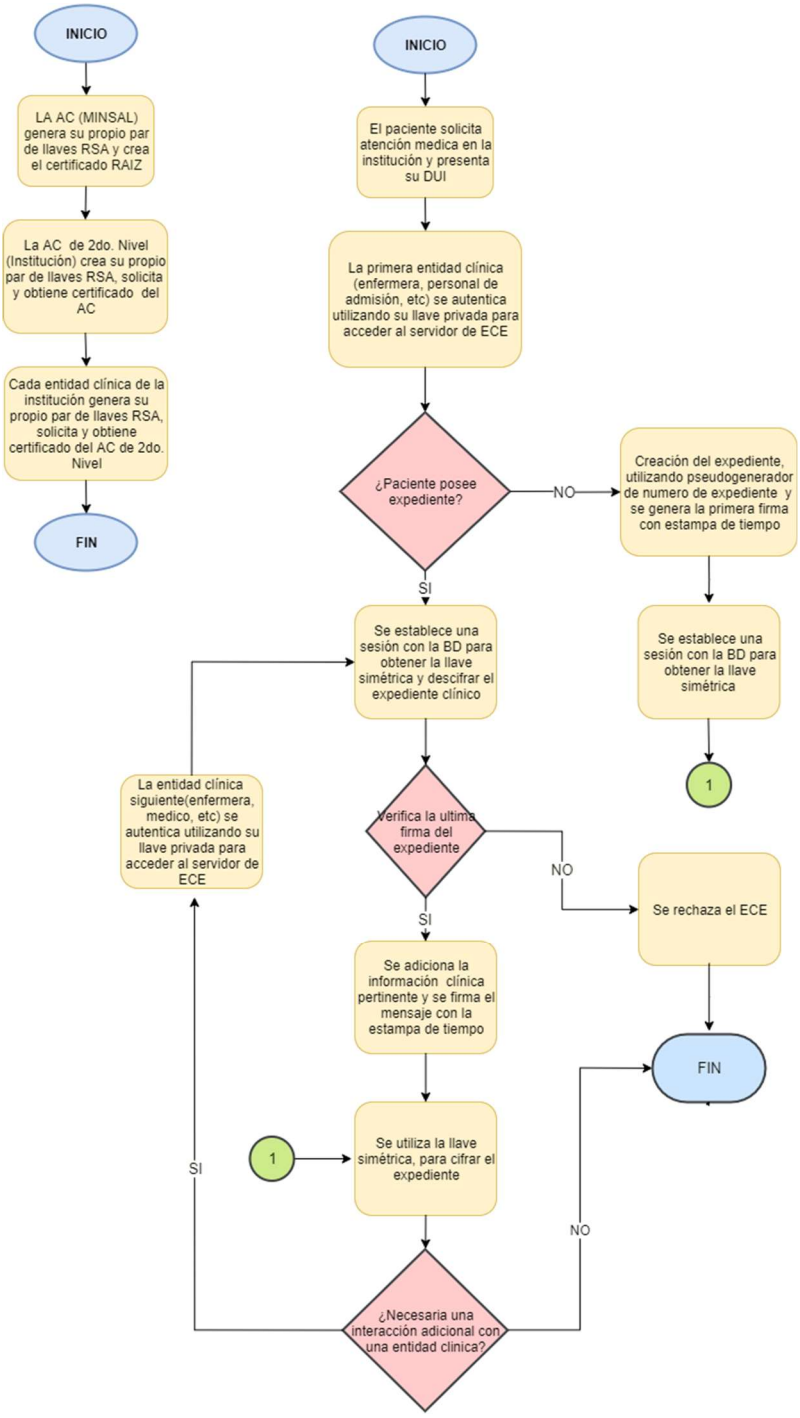

Figura 10. Diagrama de flujo para protocolo del expediente clínico electrónico del MINSAL [Elaboración propia].

Flujo de datos del protocolo

Los datos que se transmiten entre las entidades del protocolo son representados con variables que corresponden a las entidades y las operaciones criptográficas básicas, por lo que, para mayor entendimiento, la notación con su respectiva descripción se muestra en la Tabla 2.

Tabla 2. Notación general del flujo de datos del protocolo

(e_{AC}, d_{AC}, n_{AC})	Llaves RSA de la Autoridad de Certificación de primer nivel (MINSAL nivel central)
$(e_{AC2}, d_{AC2}, n_{AC2})$	Llaves RSA de la Autoridad de Certificación de 2do. Nivel (Hospitales y regionales de Salud)
(e_{AA}, d_{AA}, n_{AA})	Llaves RSA de la Autoridad de Autenticación y Estampa de Tiempo (Servidor de autenticación local)
$(e_{PadminX}, d_{PadminX}, n_{PadminX})$	Llaves RSA de cualquier individuo, representado por X, del personal de admisión (Usuario clínico de admisión)
$(e_{EnfX}, d_{EnfX}, n_{EnfX})$	Llaves RSA de cualquier individuo, representado por X, del personal de enfermería (Usuario clínico de enfermería)
$(e_{MedX}, d_{MedX}, n_{MedX})$	Llaves RSA de cualquier individuo del personal médico (Usuario personal médico)
$H(\cdot)$	Función picadillo
$\|$	Función de concatenación
$Cert_{AC}$	Certificado auto firmado de la Autoridad de Certificación de primer nivel (MINSAL nivel central)
$Cert_{AC2}$	Certificado de la Autoridad de Certificación de 2do. Nivel (Hospitales y regionales de Salud)
$Cert_{AA}$	Certificado de la Autoridad de Autenticación y Estampa de Tiempo (Servidor de autenticación local)

$Cert_{PadminX}$	Certificado de cualquier individuo del personal de admisión, representado por X, (Usuario clínico de admisión)
$Cert_{EnfX}$	Certificado de cualquier individuo del personal de enfermería, representado por X, (Usuario clínico de enfermería)
$Cert_{MedX}$	Certificado de cualquier individuo del personal médico, representado por X, (Usuario personal médico)
$m = (m_1, \dots, m_n, (e_1, n_1), \dots, (e_n, n_n))$	Mensaje o información clínica contenida en el ECE, al igual que los exponentes públicos desde el primero hasta el último signatario.
S_{ultimo}	Firma digital del último signatario
$S_{penultimo}$	Firma digital del penúltimo signatario
t_{ultimo}	La última estampa de tiempo
S_{t_ultimo}	Firma digital de la última estampa de tiempo

Fase 1. Generación de certificados

1. Las Autoridades AC, AC 2do Nivel, AA y cada entidad clínica que labora en la institución debe poseer sus llaves RSA.
2. La autoridad certificadora de primer nivel (Ministerio de Salud) genera el certificado raíz, la autoridad certificadora de 2do. Nivel (Institución) solicita certificado digital a la AC y la AA en conjunto con cada entidad clínica solicita certificado digital a la AC de 2do. Nivel.

Fase 2. Autenticación

1. Cuando un usuario clínico como, por ejemplo, $Padmin_1$, solicite acceso a la información contenida en el ECE, primero deberá autenticarse presentando usuario y contraseña, en donde su contraseña servirá para descifrar simétricamente la llave privada contenida en un dispositivo externo como USB o tarjetas inteligentes.
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.
3. Este reto define que cuando $Padmin_1$ solicite acceso al ECE, la AA deberá solicitar al repositorio de certificados, el $Cert_{AC2}$ y el $Cert_{Padmin1}$, 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}).

   AC2 $\xrightarrow{Cert_{AC2}, Cert_{Padmin1}, CRL, S_{CRL}}$ AA

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: $Cert_{AC2}$, $Cert_{AA}$, la CRL y su firma, para primero validar la CRL con el $Cert_{AC2}$ 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 de nivel 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 la Tabla 3.

Tabla 3. Paso de mensajes entre las entidades AA y Padmin1

AA		$Padmin_1$
$C_K = {K_{AA}}^{e_{Padmin1}} \ mod \ n_{Padmin1}$	$\xrightarrow{\{S_{Ck}, C_k\}}$	
$S_{CK} = {C_k}^{d_{AA}} mod \ n_{AA}$		$K'_{AA} = {C_k}^{d_{Padmin1}} \ mod \ n_{Padmin1}$ $h_1 = {S_{Ck}}^{e_{AA}} mod \ n_{AA}$ $h_2 = H(K'_{AA})$ Si $h_1 = h_2$ $C_{K1} = {K'_{AA}}^{e_{AA}} \ mod \ n_{AA}$
	$\xleftarrow{\{C_{k1}\}}$	

10. La AA descifra C_{k1} 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 $K_{simétrica}$ 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.

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

$$h_2 = H(m)$$

Si $h_1 = h_2$ la firma es válida.

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:

$$y = S_{ultimo}{}^{e_n} mod\ n_n$$

$$h_2 = H(m)$$

$$S = y - S_{penultimo} = 0$$

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.

$$r' = (s_{t\_ultimo})^{e_{AA}}\ mod n_{AA}$$

$$m_{estampa} = m_n - s_{t\_ultimo}$$

$$H\left(m_{estampa} || t_{ultimo}\right) = r' = 0$$

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_{Padmi} , n_{Padmi} . 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.

Análisis de seguridad

A continuación, en la Tabla 5.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.

Tabla 4. Resumen de análisis de seguridad en el escenario incluyendo el protocolo

Problema	**Ataque**	**Solución**
Manipulación no autorizada del expediente clínico	Posible modificación de la información del expediente clínico, por parte del personal de la institución de salud no autorizado para la manipulación del mismo	El personal médico realiza una autenticación por doble factor, por lo que sabe y por lo que tiene; se ingresa el usuario, contraseña acompañada de la llave privada almacenada en un dispositivo externo, que se le ha proporcionado para poder ingresar al sistema y demostrar que es la persona autorizada para la manipulación de los datos del ECE.
Pérdida total o parcial de la información del ECE	Durante el traslado del expediente físico, el o los encargados del traslado pueden perder parte o todo el historial clínico.	Se reducirá paulatinamente la manipulación y el traslado físico de los expedientes clínicos, creando un documento digital único para el paciente, que podrá ser consultado únicamente por

		las personas autorizadas y el cual pueda ser accesible en todos los centros de atención de salud pública, aplicando protocolos criptográficos de integridad como *hash* para la validación de los documentos e insertando estampas de tiempo.
Repudio	Realizar acciones que puedan dañar la integridad de la información.	Este problema se solucionara con la creación de certificados digitales y firmas electrónicas de llave pública o PKI para garantizar que el personal médico que acceden a los ECE no puedan negar el haber realizado algún tipo de adición de información del historial clínico del paciente, ya que al finalizar cada actualización, eliminación o inserción se colocará una estampa de tiempo y se firmará con su llave privada realizando un proceso de firmas agregadas, lo que permite tener un mejor control de los diagnósticos y pruebas realizadas por entidad clínica.
Duplicidad de la información	Creación de diferentes expedientes, con la misma información de un paciente, creados en distintos tiempos y por diferentes entidades	El protocolo que presentamos dará la pauta para comenzar un proceso de unificación del ECE en un solo servidor, basados en las metodologías de la creación de certificados y firmas digitales y así evitar la creación del ECE en cada

		uno de los establecimientos de unidades de salud y hospitales del país, y en estos únicamente se estarían realizando las consultas (búsquedas) de los pacientes.
No existe una forma de autenticar a las entidades de forma segura	Posible usurpación de identidad	Se realizará una autenticación por doble factor, nombre de usuarios y contraseña unido con el uso de certificados digitales para la autenticación de los usuarios además de la estructura de PKI, para poder identificar adecuadamente a cada uno de los involucrados en la manipulación de los ECE.
La información de cada expediente es vista y entendible por cualquier persona	Divulgación de la información sensible del estado de salud de los pacientes	El uso de cifrado por clave simétrica garantiza que la información de los ECE no puede ser visualizada por cualquier persona lo que permite la confidencialidad del estado de salud de los pacientes.
Pérdida de certificados, llaves y/o contraseñas	Ataques de no repudio	Al tener un repositorio central de certificados, estas llaves no serán guardadas en los equipos electrónicos de cada unidad de salud u hospital, evitando así la pérdida o el robo de estas.
No se cuenta con alta disponibilidad en las agencias de salud	Ataques de 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. También se requiere la aplicación de las políticas de respaldo y recuperación de información, y colocar una infraestructura de recuperación de desastres, al contar con este esquema de alta disponibilidad y unificación de información, se eliminaría la creación de certificados por cada una de las unidades de salud y hospitales de manera independiente.

Análisis de eficiencia

A continuación, se define el número de operaciones privadas y públicas, que se realizan a lo largo del protocolo por cada entidad. Es importante considerar que el protocolo será aplicado en tres casos que son los siguientes:

- Creación de Expediente Clínico Electrónico
- Adicionar información al expediente, ya sea diagnóstico, exámenes clínicos o recetas.
- Consultar información.

A partir de ello se plantea el siguiente análisis de eficiencia del protocolo por casos.

<u>Creación de Expediente Clínico Electrónico</u>

<u>Entidad de Autoridad de Autenticación (AA)</u>

1. Realiza un descifrado del medio donde se almacena la llave privada (AES en modo de descifrado)
2. Genera *hash* de la lista de revocación de certificados (*Hash*)
3. Verifica firma de la lista de revocación de certificados con la llave pública de AC2. (Operación Pública)
4. Cifra el reto (valor aleatorio K_{AA}) con llave pública de Entidad clínica. (Operación Pública)
5. Firma C_k con su llave privada (Operación Privada)
6. Descifra C_{k1}, recibida de Entidad Clínica, con su llave privada. (Operación Privada)
7. Posteriormente firma la estampa de tiempo. (Operación Privada)

Entidad Clínica (Enfermera / Personal de Admisión)

1. Se autentica con llave privada para acceder al sistema ECE.
   - Genera *hash* de la lista de revocación de certificados (*Hash*)
   - Verifica firma de la lista de revocación de certificados con la llave pública de AC2 (Operación Pública)
   - Verifica firma S_{CK} con la llave publica de AA y obtiene C_k (Operación Pública)
   - Descifra reto (K_{AA}) con llave privada (Operación Privada)
   - Cifra K_{AA} obtenida con llave pública de AA para enviar C_{k1} a la AA (Operación Pública)
2. Genera *hash* de expediente con los datos generales del paciente sin estampa de tiempo. (*Hash*)

3. Genera *hash* de expediente con los datos generales del paciente, incluyendo firma de estampa de tiempo y las llaves públicas de la entidad clínica (*Hash*)
4. Realiza primera firma con llave privada (Operación Privada)
5. Cifra expediente con llave simétrica de BD (AES en modo cifrado)

Haciendo una suma de todas las operaciones públicas y privadas por entidad, el total se muestra en la Tabla. 5.

Tabla 5. Cantidad de operaciones públicas, privadas, cifrado simétrico y funciones hash realizadas en caso "Creación de expediente clínico electrónico"

Entidad	**Operaciones Públicas**	**Operaciones Privadas**	**Simétrico**	***Hash***
Autoridad de Autenticación	2	3	1	1
Entidad Clínica	3	2	1	3

Adición de información a Expediente Clínico Electrónico

Entidad de Autoridad de Autenticación (AA)

1. Realiza un descifrado del medio donde se almacena la llave privada (AES en modo de descifrado)
2. Genera *hash* de la lista de revocación de certificados (*Hash*)
3. Verifica firma de la lista de revocación de certificados con la llave pública de AC2. (Operación Pública)

4. Cifra el reto (valor aleatorio K_{AA}) con llave pública de Entidad clínica. (Operación Pública)
5. Firma C_k con su llave privada. (Operación Privada)
6. Descifra C_{k1}, recibida de Entidad Clínica, con su llave privada. (Operación Privada)
7. Posteriormente firma la estampa de tiempo. (Operación Privada)

Entidad Clínica (Doctor, enfermera, etc.)

1. Se autentica con llave privada para acceder al sistema ECE.
   - Genera *hash* de la lista de revocación de certificados (*Hash*)
   - Verifica firma de la lista de revocación de certificados con la llave pública de AC2 (Operación Pública)
   - Verifica firma S_{CK} con la llave publica de AA y obtiene C_k (Operación Pública)
   - Descifra reto (K_{AA}) con llave privada (Operación Privada)
   - Cifra K_{AA} obtenida con llave pública de AA para enviar C_{k1} a la AA (Operación Pública).
2. Obtiene la llave simétrica de BD.
1. Descifra expediente. (AES en modo descifrado)
2. Genera *hash* del mensaje. (*Hash*)
3. Verifica última firma con la llave pública de entidad anterior (Operación Pública)
4. Genera *hash* del mensaje sin estampa. (*Hash*)
5. Verifica firma de AA/AET con pública de AA/AET obtenida en autenticación. (Operación Pública)

6. Genera *hash* de expediente con los datos generales del paciente sin estampa de tiempo. (*Hash*)
7. Genera *hash* de expediente con los datos generales del paciente, incluyendo firma de estampa de tiempo y las llaves públicas de la entidad clínica. (*Hash*)
8. Firma mensaje nuevo. (Operación Privada)
9. Cifrado de expediente. (AES modo de cifrado)

Haciendo una suma de todas las operaciones públicas y privadas por entidad, el total se muestra en la Tabla. 6.

Tabla 6. Cantidad de operaciones públicas, privadas, cifrado simétrico y funciones hash realizadas en caso "Adición de información de expediente clínico electrónico"

Entidad	**Operaciones Públicas**	**Operación Privadas**	**Simétrico**	***Hash***
Autoridad de Autenticación	2	3	1	1
Entidad Clínica	5	2	2	5

Consulta del Expediente Clínico Electrónico

Entidad de Autoridad de Autenticación (AA)

1. Realiza un descifrado del medio donde se almacena la llave privada (AES en modo de descifrado)
2. Genera *hash* de la lista de revocación de certificados (*Hash*)

3. Verifica firma de la lista de revocación de certificados con la llave pública de AC2. (Operación Pública)
4. Cifra el reto (valor aleatorio K_{AA}) con llave pública de Entidad clínica. (Operación Pública)
5. Firma C_k con su llave privada. (Operación Privada)
6. Descifra C_{k1}, recibida de Entidad Clínica, con su llave privada. (Operación Privada)

Entidad Clínica

1. Se autentica con llave privada para acceder al sistema ECE.
   - Genera *hash* de la lista de revocación de certificados (*Hash*)
   - Verifica firma de la lista de revocación de certificados con la llave pública de AC2 (Operación Pública)
   - Verifica firma S_{CK} con la llave publica de AA y obtiene C_k (Operación Pública)
   - Descifra reto (K_{AA}) con llave privada (Operación Privada)
   - Cifra K_{AA} obtenida con llave pública de AA para enviar C_{k1} a la AA (Operación Pública).
2. Obtiene llave simétrica de BD
3. Descifra expediente (AES en modo descifrado)
4. Genera *hash* del mensaje (*Hash*)
5. Verifica última firma con la llave pública de entidad anterior. (Operación Pública)
6. Genera *hash* del mensaje sin estampa. (*Hash*)

7. Verifica firma de AA/ET con pública de AA/ET obtenida en autenticación. (Operación Pública)
8. Cifrado de expediente (AES en modo cifrado)

Haciendo una suma de todas las operaciones públicas y privadas por entidad, el total se muestra en la Tabla. 7.

Tabla 7. Cantidad de operaciones públicas, privadas, cifrado simétrico y funciones hash realizadas en caso "Consulta de Expediente Clínico Electrónico"

Entidad	**Operación Pública**	**Operación Privada**	**Simétrico**	***Hash***
Autoridad de Autenticación	2	2	1	1
Entidad Clínica	5	1	2	3

La entidad de autenticación realiza como máximo 2 operaciones públicas, 3 operaciones privadas, 1 función picadillo y 1 cifrado simétrico. Mientras que la entidad clínica realiza como máximo 5 operaciones públicas, 2 privadas, 5 funciones picadillo y 2 cifrados simétricos.

La eficiencia del protocolo depende del número de operaciones privadas y públicas que se realizan ya que esto implica más trabajo de cómputo.

Pruebas de funcionalidad al protocolo implementado

En la Tabla 8, se presentan las pruebas que se realizaron para verificar la funcionalidad y la efectividad del protocolo propuesto.

Tabla 8. Efectividad de ejecuciones y ataques en la implementación del protocolo

NO.	Evento o escenario	Descripción	Efectividad del protocolo
1	Autenticación de un personal de admisión	Flujo normal para autenticación de personal que labora en el área de admisión	**COMPLETA**
2	Creación de Expediente Clínico Electrónico	Flujo normal de información cuando un paciente asiste por primera vez a la institución de salud	**COMPLETA**
3	Autenticación de un personal de enfermería	Flujo normal para autenticación de personal que labora en el área de enfermería.	**COMPLETA**
4	Autenticación de un personal médico	Flujo normal para autenticación de personal que labora en el área de atención médica.	**COMPLETA**
5	Adición de información al expediente clínico	Flujo normal de información cuando un paciente ya cuenta con un ECE en la institución	**COMPLETA**
6	Adición de solicitud de exámenes con estampa de tiempo	Flujo normal de información para añadir solicitudes de exámenes de laboratorio con la fecha y hora de la solicitud.	**COMPLETA**
7	Adición de	Flujo normal de información para	**COMPLETA**

	diagnóstico con estampa de tiempo	añadir diagnósticos con la fecha y hora de la consulta.	
8	Adición de receta médica con estampa de tiempo	Flujo normal de información para añadir recetas médicas con la fecha y hora de la dispensación.	**COMPLETA**
9	Adición de información consecutiva en una misma consulta por varias entidades clínicas.	Flujo normal de la información donde en una misma visita al centro de salud al expediente se le realizan o realiza varias acciones que incorporar información de distintas entidades clínicas al expediente.	**COMPLETA**
10	Paciente con homónimos	Problema que se puede encontrar cuando se crea o se busca un paciente con un nombre muy común	**COMPLETA**
11	Paciente menor de edad	Paciente no cuenta con Documento Único de Identidad por ser menor de edad	**NINGUNA**
12	Paciente sin número de expediente	Paciente olvida o pierde su número de expediente	**NINGUNA**
13	Paciente con número de expediente equivocado	Paciente posee un número de expediente erróneo que no le corresponde.	**NINGUNA**
14	Modificación no autorizada de horario en la computadora para alterar la estampa de tiempo	Entidad ya sea ajena o perteneciente a la institución de salud realiza la modificación del horario del ordenador con la intención de alterar la hora	**COMPLETA**

		registrada en la estampa de tiempo.	
15	Perdida de llave privada por entidad clínica	Perdida de la llave privada correspondiente al certificado digital de la entidad clínica	**COMPLETA**
16	Robo de llave privada por atacante	Robo de la llave privada correspondiente al certificado digital de una entidad clínica por parte de una persona perteneciente o no a la institución de salud	**NINGUNA**
17	Modificación no autorizada del ECE	Modificación por parte de una persona ajena a la institución de la información contenida en el ECE	**COMPLETA**
18	Pérdida total o parcial del ECE por acceso no autorizado	Eliminación total o parcial de la información contenida en el ECE por parte de una entidad ajena a la institución de salud	**COMPLETA**
19	Lectura y/o divulgación del ECE por parte de un atacante	Lectura, obtención y/o divulgación del ECE por parte de una persona ajena a la institución de salud	**COMPLETA**
20	Lectura del ECE por parte de personal de la institución no autorizado	Lectura, obtención y/o divulgación del ECE por parte de una persona perteneciente a la institución de salud, pero sin la autorización necesaria.	**COMPLETA**
21	Entidad clínica no	Personal médico rechaza la	**COMPLETA**

	asume responsabilidades de acciones o eventos descritos en el expediente clínico	información o las acciones llevadas a cabo durante la atención a un paciente y que han quedado registradas dentro del ECE.	
22	Mala praxis en la atención clínica	Se puede investigar los procedimientos clínicos realizados cuando se sospecha de una atención médica negligente.	**COMPLETA**
23	Duplicidad de la información	Registros idénticos de información dentro del expediente	**COMPLETA**
24	Duplicidad del ECE para un mismo paciente	Un paciente cuenta con más de un expediente dentro de la institución de salud	**COMPLETA**
25	Usurpación de identidad de pacientes	Falsificación de DUI para obtener atención medica con la identidad de otro individuo	**COMPLETA**
26	Usurpación de identidad de usuarios o entidades clínicas	Falsificación de credenciales para obtener acceso a la información clínica de pacientes	**COMPLETA**
27	Acceso no autorizado al servidor de expedientes clínicos electrónicos	Acceso físico al servidor de expedientes clínicos electrónicos para obtener y leer la información personal clínica de pacientes	**COMPLETA**
28	Acceso no autorizado a los certificados digitales	Acceso al repositorio de certificados digitales por parte de una persona ajena a la institución de salud	**COMPLETA**

29	Modificación de los certificados digitales de una entidad clínica	Modificación ya sea completa o parcial de un certificado digital almacenado en el repositorio.	**COMPLETA**
30	Ataque de hombre en el medio durante la autenticación de la entidad.	Ataque de hombre en el medio durante la autenticación entre la entidad clínica y la Autoridad de autenticación con la intención de monitorear, modificar la información y/o usurpar la identidad de una entidad clínica confiable	**COMPLETA**

Capítulo V

Metodología propuesta para la implementación del módulo de seguridad

La aplicación de esta metodología es válida para la implementación del protocolo criptográfico, diseñado en el capítulo anterior, en 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

- 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.
- 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

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.

Las opciones a considerar son OpenCA y EJBCA, las cuales ofrecen los mismo servicios y ventajas que las herramientas de paga, para esta implementación se recomienda el uso de EJBCA ya que tiene una mejor integración, además de ser escalable, una vez instalado se puede ir agregando módulos que permitan una infraestructura mucho más sólida [22]. Para esto es necesario que el MINSAL cuente con la infraestructura de hardware y red necesaria para la implementación del PKI, los cuales son:

- Servidor para la instalación de EJBCA.
- Servidor para logs.
- Servicio de enlaces de red para cada establecimiento de salud.

Integración de protocolo en el SIAP

En la Figura 11 se puede apreciar la integración de PKI en el apartado de autenticación de usuarios del SIAP.

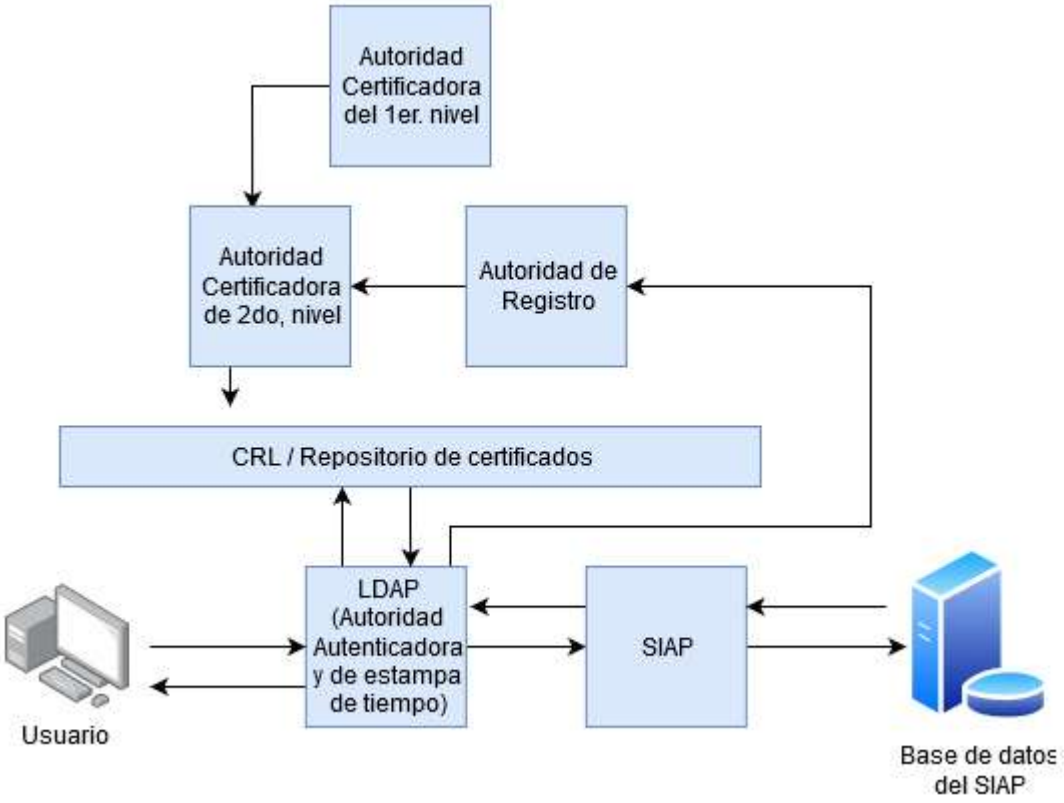

Figura 11. Integración de PKI en el SIAP [Elaboración propia].

- 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).
- 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.
- 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:

- La sesión de usuario autenticado no debe superar 60 minutos de inactividad en el sistema.
- Habilitación de registros de auditorías.
- 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.
- Capacitación a los usuarios finales.
- Desarrollo de manuales de usuario.
- Se recomienda aplicar un ataque de vulnerabilidades controlado (*Pen-testing*) al código fuente del sistema SIAP.
- 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

En la base de datos:

- 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.

- 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.
- Bases de datos en alta disponibilidad.
- Creación de servidores clusterizados
- Resguardo de información hacia sitio de contingencia en tiempo real.
- Creación de políticas de respaldo, resguardo y recuperación de la información.

Capítulo VI

Discusión y resultados

En este capítulo se presenta y expone el cumplimiento de los objetivos planteados al inicio, ofreciendo un repaso a los resultados de los diseños propuestos a nivel de concepto y cotejando su cumplimiento para medir la validez y aplicación de este trabajo de investigación.

Por ello, este capítulo se divide a partir del cumplimiento individual y general de los objetivos, detallando en qué medida los resultados ofrecen evidencia de la culminación de las metas planteadas, matizándolos en el contexto nacional y ofreciendo oportunidades de mejora, tanto para el módulo de seguridad como para futuros trabajos en la digitalización de servicios públicos en El Salvador.

¿Información sobre el ECE del MINSAL?

De la información que se obtuvo de los módulos de ingreso de pacientes, seguimiento clínico, citas, agenda médica y laboratorio del sistema SIAP, algunos documentos se encontraron incompletos o ausentes y lo que se logró recopilar no estaba enfocado completamente para el personal de IT, sino más bien, estaba desarrollada como un manual de usuario de cómo utilizar los sistemas.

Otro detalle es que por razones de seguridad no se tuvo acceso al código fuente, pero sí a los módulos de manera funcional, por lo que la propuesta nace de un punto general de funcionamiento y no específico a nivel de programación.

No omitiendo manifestar que a pesar de los inconvenientes y limitaciones presentados por la ausencia de documentación, o la imposibilidad de observar código fuente del SIAP, se tiene que hacer énfasis que a través de la manipulación directa del sistema; la información documental que si está completa de los módulos de identificación de pacientes, seguimiento clínico, citas, agenda médica, laboratorio clínico y farmacia; y las reuniones desarrolladas con el personal técnico, se logró consolidar un marco de referencia adecuado en el funcionamiento y características que ofrecen los módulos como insumo para desarrollar el análisis de seguridad del escenario actual.

Vulnerabilidades encontradas en el sistema actual

La evaluación de vulnerabilidad que se realizó se hizo en base a una evaluación y análisis teórico, no contemplándose realizar pruebas prácticas como podía ser una prueba de penetración (*pen-testing*) o de estrés al SIAP, cuyo alcance iba enfocado a la propuesta de mejora a partir de un protocolo de seguridad y no una propuesta tecnológica.

El proceso de valoración inició con la recopilación de la información necesaria de cómo se encuentra estructurado el SIAP, y tomando de referencia fuentes confiables para la identificación de vulnerabilidades como lo son: el top ten de OWASP, ISACA, la Base de Datos Nacional de Vulnerabilidades del NIST, u otras páginas y noticias relevantes sobre ciberseguridad.

Desarrollándose la revisión de cada uno de los manuales obtenidos y reuniones con las partes comprometidas de IT que brindan mantenimiento al sistema, se logró identificar como vulnerabilidades más significativas la información descentralizada, la pérdida de

certificados, certificados inseguros debido a la ausencia de infraestructura de llave pública y el uso de esquemas criptográficos obsoletos.

Una propuesta de protocolo a la medida de las necesidades del MINSAL

El principal reto del diseño del protocolo fue la definición de su alcance, identificando qué acciones se espera que proteja en el esquema en el flujo de información: la autenticación de los usuarios, creación de expediente y la adición o modificación de información en el expediente; y que otras se complementarán con controles a nivel de aplicación o infraestructura.

Este diseño tomó en cuenta como insumo las principales vulnerabilidades encontradas en el sistema, se estudiaron las implementaciones desarrolladas por otros países en el despliegue del ECE, regulaciones nacionales a cumplir, así como regulaciones y normativas internacionales a considerar y finalmente los últimos avances en esquemas criptográficos para la protección de datos médicos.

Hablando de esto último, existen muchas propuestas de esquemas basados en *blockchain*, pseudo-anonimizar, ADN, firmas a ciegas, esquema de Shamir, llaves biométricas o HPKI; pero una limitante se estableció a partir del contexto y capacidades que tiene el MINSAL y sus regulaciones aplicables, que restringe el uso de cualquier esquema por muy funcional e innovador que sea, por tal motivo el diseño de la propuesta arranca teniendo como meta la utilización de herramientas alcanzables para nuestro entorno.

Algo no negociable en cambio, es que el protocolo se basa en el supuesto que se implemente una infraestructura de llave pública, donde es necesario un rediseño de la

infraestructura que actualmente posee la institución para adoptar a nivel de aplicación el protocolo.

Detallando el protocolo, se identifican 3 momentos, el de autenticación, el de creación de expediente y el de adición o modificación del expediente dentro del diseño o, y como puede observarse este es general y no específico, de tal forma que puede ser aplicable a todo el flujo de datos del SIAP, sin importar con qué módulo el usuario interactúe.

Se brinda confidencialidad en el uso de esquemas de cifrado simétrico en base de datos, se brinda integridad en el uso de firmas agregadas y su comprobación en los momentos de creación, adición, modificación o eliminación de información en el expediente clínico, se brinda autenticación y no repudio en el uso de estructura de llave pública al momento de iniciar sesión y verificar firmas con el uso de certificados válidos.

Si bien el cifrado simétrico de la base de datos otorga cierto nivel de confidencialidad, esto se puede mejorar a partir de la implementación de un control de acceso por roles o atributos, que permita brindar acceso a información sensible de una manera más granular, protegiendo la información no solo de atacantes externos sino también de atacantes internos.

En cuanto a anonimizar la información clínica, deseable para escenarios en donde un seguro médico solicite información, se soliciten los datos médicos para la realización de estadísticas, investigación clínica, investigación científica o docencia; se decidió no incorporar ninguna acción dentro del protocolo al entender que esto puede lograrse a nivel de aplicación siendo cuidadosos de cifrar sólo la información que vincula los datos personales con los datos clínico en una base de datos.

Validación del diseño

Para el desarrollo de la propuesta se tomaron en cuenta ciertas características que debe tener un protocolo para que pueda ser seguro, pero a la vez ser eficaz, tomando en consideración el flujo de información que presenta el SIAP.

En la propuesta, se da a conocer un flujo del protocolo donde se cuenta con lo mínimo de operaciones de cifrado, esto para no afectar la disponibilidad y el procesamiento de la información, ya que los procesos de cifrado sobrecargan el sistema y la transaccionalidad de este, especialmente los esquemas de cifrado público.

Dentro del diseño se implementan soluciones pertinentes para mejorar los aspectos donde el flujo del SIAP cuenta con mayores vulnerabilidades, colocando puntos de verificación o autenticación en los flujos más importantes y en los de mayor riesgo, haciendo del SIAP un sistema mucho más confiable debido al nivel de confidencialidad, integridad y no repudio que ofrece.

Ahora hablando específicamente de las soluciones, la implementación de este protocolo permitirá la plena adopción del ECE en el MINSAL de manera integrada, lo que indirectamente mitigará la vulnerabilidad de la duplicidad de la información.

Con la aplicación del protocolo de PKI, se evita el no repudio de la información ingresada por los usuarios del sistema, ya que este es el que permite la autenticación, utilizando los certificados que se encuentran en el repositorio, llave privadas que deberá poseer el usuario, y comprobando a través de estas que el usuario es quien dice ser.

Al contar con una infraestructura de PKI, el proceso de actualización y validaciones de los certificados es más segura, evitando certificados inseguros, la suplantación y/o pérdidas de

estos, la función de este protocolo es proporcionar estos certificados digitales los cuales permiten llevar a cabo las operaciones criptográficas, como el cifrado y la firma electrónica. Estas operaciones sirven para garantizar la confidencialidad, autenticación, integridad y no repudio en las transacciones electrónicas.

Es así como, al aplicar los controles que surgen de lo dispuesto en el diseño del protocolo, en cada uno de los módulos del sistema, se tendrá información más confiable, un resguardo más certero y confidencial y una verificación integral de toda la información de que se esté ingresando, así como quien, cuando y donde la ingresa.

Luego de haber realizado el estudio del escenario de seguridad del SIAP, así como también la creación del protocolo para mejorar la seguridad del sistema, se crea la metodología para la implementación de las herramientas necesarias que se recomienda utilizar dentro de MINSAL.

Una metodología para el módulo de seguridad en el protocolo

Para facilitar la implementación del protocolo de seguridad para los módulos del SIAP, se propone la metodología que permite ejecutar las acciones necesarias que le posibilitará al MINSAL, ofrecer a los usuarios una notable mejora en el resguardo de la información clínica de cada uno de ellos. Cabe mencionar que para implementar de forma correcta el protocolo se deben cumplir requisitos previos, los cuales están definidos en el capítulo V de este documento. El principal es que el MINSAL debe contar con todo el hardware e infraestructura de red necesaria para implementar el PKI y su buen funcionamiento.

Una vez se cumpla con estos requisitos previos, se pone en marcha la adición de componentes de seguridad, para cada uno de los servicios del SIAP, es de destacar que el protocolo en sí, aunque se describa de forma general, se integra perfectamente a cada uno de éstos. Por ejemplo, en el módulo de laboratorio clínico, el personal deberá utilizar sus credenciales más su certificado para acceder al SIAP, luego que termine de adicionar datos, firmará y se cifrara el expediente.

Capítulo VII

Conclusiones y Recomendaciones

Como se ha mencionado en capítulos anteriores y en la introducción de este documento, en nuestro país, 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.

Se sabe que hay muchas barreras por derribar antes de colocar este módulo de seguridad y protocolo en los hospitales y unidades de salud, de una forma integral, pero este es el primer paso para poder implementar en nuestro país un sistema que beneficie a la población, brindando un servicio en el cual el paciente tenga la confianza que la información de su historial clínico, así como la información personal brindada por este, sea la correcta, que sea resguardada y no sea manipulada por personas externas a los centros médicos y que al asistir a cualquier centro de atención su información podrá ser presentada de forma oportuna, cumpliendo con los principios de la seguridad de la información en la integridad, no repudio y confidencialidad, beneficiando a la población que hace uso de los servicios públicos de salud, y en un futuro se pueda completar con los entes privados y

conformar una red integral de salud a nivel país, equiparándonos en implementaciones del ECE al nivel de países Latinoamericanos como México, Uruguay, Brasil, etc.

Es necesario considerar que si bien ya existe proyectos de ley sobre la Protección de Datos y Habeas Data, actualmente no existe en el país ninguna legislatura o regulación que defina claramente los deberes y derechos de las personas, organizaciones e instituciones en cuanto a la protección y manipulación de datos personales, este es un reto que determinara futuras modificaciones al protocolo, puesto que el diseño propuesto se basa desde la idea que el dueño, responsable o al menos quien debe custodiar la información clínica únicamente es el MINSAL o la institución de atención médica autónoma o privada, creando incertidumbre entonces la posibilidad que se le otorgue irrevocablemente el derecho a los pacientes para decidir, empoderarse y autorizar cómo, dónde y a quién le permiten acceso a su información en la nueva ley.

Habiendo cumplido cada etapa en el desarrollo del proyecto, alcanzando las metas planteadas y desplegado una propuesta de metodología para un módulo de seguridad basado en firmas digitales y arquitectura de llave pública, se puede validar el cumplimiento de los servicios de seguridad perseguidos al inicio del proyecto a partir del uso esquemas de cifrado simétrico, la recomendación de un control de acceso por atributos o roles y el cifrado granular en base de datos para lograr la confidencialidad; el uso de funciones picadillo, firmas agregadas y su verificación en los momentos de creación, adición, modificación o eliminación de la información para lograr la integridad; y el uso de infraestructura de llave pública para lograr el no repudio.

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, ya que existe una brecha significativa en las vulnerabilidades encontradas previo a la implementación del protocolo, en comparación con el diseño propuesto del protocolo, en donde se observa una mejora sustancial en los servicios de confidencialidad, integridad y no repudio que el SIAP ofrece.

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 protocolo 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.

Recomendaciones

Ya que a la fecha no existe una certificación desde el gobierno central, se recomienda al MINSAL, crear los certificados internos con la plataforma EJBCA, para ser utilizados por el personal y establecimientos de salud, involucrados en la atención médica. Una vez se cuente con un certificado raíz nacional, se deberán revocar paulatinamente los certificados internos por los creados y proporcionados a partir del certificado país emitido por el Ministerio de Economía.

Se recomienda difundir las normativas y leyes sobre temas de salud y seguridad de la información, para que el personal esté consciente de cuáles son sus derechos y obligaciones, así como las sanciones a las faltas cometidas, esto ayudará en gran medida a mejorar no solo la custodia de la información clínica, sino que también ayudará a elevar los estándares de atención en los servicios de salud.

Referencias

[1] Asamblea legislativa de la República de El Salvador (2015). Ley de firma electrónica, Decreto No. 133, Diario Oficial de la Republica de El Salvador, Tomo 409. 26 de octubre de 2015.

[2] Documento: Expediente Clínico electrónico en Colima. Estudio de caso sobre su implementación. Mayo 2012, recuperado de: https://www.measureevaluation.org/resources/publications/sr-12-70-es

[3] NORMA Oficial Mexicana NOM-024-SSA3-2012, Sistemas de información de registro electrónico para la salud. Intercambio de información en salud. Viernes 30 de noviembre de 2012, recuperado de https://www.gob.mx/salud/documentos/norma-oficial-mexicana-nom-024-ssa3-2012.

[4] Salud a golpe de tecla, Banco Interamericano de Desarrollo, 20 de enero de 2020, recuperado de https://www.iadb.org/es/mejorandovidas/salud-golpe-de-tecla

[5] LifeLabs – Customer Notice. (2020). 21 de enero de 2020, Recuperado de https://customernotice.lifelabs.com/

[6] AMCA Files Chapter 11 After Data Breach Impacting Quest, LabCorp. (2020). 21 de enero de 2020, Recuperado de https://healthitsecurity.com/news/amca-files-chapter-11-after-data-breach-impacting-quest-labcorp

[7] Alford, J. (2020). NHS cyber-attacks could delay life-saving care and cost millions | Imperial News | Imperial College London. 21 de enero de 2020, recuperado de https://www.imperial.ac.uk/news/193151/nhs-cyber-attacks-could-delay-life-saving-care/

[8] Wiljer D, Urowitz S, Apatu E, DeLenardo C, Eysenbach G, Harth T, et al. Patient accessible electronic health records: exploring recommendations for successful implementation strategies. J Med Internet Res 2008;10(4): e34.

[9] Pianykh Oleg S., (2012) Digital Imaging and Communication in Medicine (DICOM), A Practical Introduction and Survival Guide, London, Springer, DOI: 10.1007/978-3-642-10850-1

[10] ISO 27799:2008. Health informatics – information security management in health using ISO/IEC 27002. Recuperado en 21 de enero de 2020.

[11] Quantin C, Jaquet-Chiffelle DO, Coatrieux G, Benzenine E, Allaert FA. Medical record search engines, using pseudonymised patient identity: an alternative to centralised medical records. Int J Med Inform 2011;80(2): e6–11

[12] Elger BS, Iavindrasana J, Lo Iacono L, Müller H, Roduit N, Summers P, et al. Strategies for health data exchange for secondary, cross-institutional clinical research. Comput Methods Programs Biomed 2010;99(3):230–51.

[13] Sun J, Fang Y. Cross-domain data sharing in distributed electronic health record systems. IEEE Trans Parallel Distrib Syst 2010;21(6):754–64

[14] Benaloh J, Chase M, Horvitz E, Lauter K. Patient controlled encryption: ensuring privacy of electronic medical records. In: Proc ACM workshop on cloud computing security; 2009. p. 103–14

[15] Hu J, Chen HH, Hou TW. A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations. Computer Standards & Interfaces 2010;32(5–6):274–80

[16] Manual de usuario - Flujo del SIAP

[17] Manual de usuario - Modulo de Identificación Paciente SIAP-SUIS, Sep. 2019

[18] Manual de usuario - Modulo Citas Médicas SIAP-SUIS, feb. 2017

[19] Manual de usuario - Modulo Seguimiento Clínico SIAP-SUIS, dic. 2018

[20] Manual de usuario - Modulo laboratorio clínico SIAP-SUIS, Feb. 2018

[21] Manual de usuario - Modulo de farmacia SIAP-SUIS, Feb. 2018

[22] EJBCA Introduction. (2020). 20 de enero de 2020, recuperado de https://doc.primekey.com/ejbca6152/ejbca-introduction

[23] Asamblea Legislativa de la República de El Salvador (1983). Constitución de la Republica de El Salvador, Decreto No. 234, Diario Oficial de la Republica de El Salvador, Tomo 281, 16 de diciembre de 1983.

[24] Asamblea legislativa de la República de El Salvador (2016). Ley de deberes y derecho de los pacientes y prestadores de servicios de salud. Decreto No. 307. Diario Oficial de la República de El Salvador, Tomo 411. 8 de abril de 2016.

[25] Asamblea legislativa de la República de El Salvador (2019). Ley del Sistema Nacional Integrado de Salud. Decreto No. 302. Diario Oficial de la República de El Salvador, Tomo. 423. 2 de mayo de 2019.

[26] Gobierno de la Republica de El Salvador, (2019). Recuperado de: http://www.plancuscatlan.com/home.php

[27] Ministerio de Salud (2019). Norma Técnica para la Conformación, Custodia y Consulta de Expediente Clínico, Acuerdo No. 941, Diario Oficial de la Republica de El Salvador, Tomo 424. 25 de septiembre de 2019.

Apéndice A

Herramientas utilizadas en el diseño del protocolo

Funciones picadillo

Una función picadillo es una función *HASH*, de solo ida (esto significa que una función *Hash* no se puede regresar a texto en claro) que recibe como parámetro de entrada una cadena de determinada longitud y devuelve una cadena de longitud fija.

Formalmente definida como: H:{0,1}*{0,1}l, donde l representa la longitud en bits de cadena.

Propiedades las cuales debe cumplir:

- Transformación mezclada: un cambio a la entrada incluso en un bit, produce una salida diferente.
- Pre-imagen: dado y {0,1}^l, encontrar x {0,1}^* tal que H(x)=y.
- Colisión: dado x {0,1}^*, encontrar x' {0,1}^* tal que x≠x' y H(x)=H(x^').
- Eficiencia: dado x {0,1}^* es fácil calcular H(x).

Las funciones picadillo son ampliamente utilizadas en diversos procesos criptográficos para garantizar integridad, ya que garantiza que cualquier modificación utilizando los datos originales, modificará el picadillo de los mismos.

Requisitos que deben cumplir las funciones *hash*:

- Imposibilidad de obtener el texto original a partir del digesto.
- Imposibilidad de encontrar un conjunto de datos diferentes que tengan el mismo digesto (aunque puede ser posible que este requisito no se cumpla).
- Facilidad de empleo e implementación.

Firmas Agregadas basadas en RSA

El esquema de firmas agregadas es un método para combinar *x* firmas, para *x* usuarios y *x* mensajes, todos ellos con valores diferentes. Propuesto por Boneh, Lynn y Shacham en 2003.

El esquema de firma agregada secuencial requiere de tres algoritmos que se presentan a continuación:

Generación de llaves: cada usuario genera su par de llaves (d,e), (e,n) de acuerdo al algoritmo de generación de llaves RSA.

- Seleccionar 2 números grandes primos: p y q
- Calcular n= p*q
- Calcular phi(n) = (p-1)*(q-1)
- Seleccionar e < n, mcd(e, phi(n)) =1
- Calcular d =1/e mod phi(n)

Firma agregada:

- El primer signatario genera la firma de forma s_1
- El signatario i verifica la firma del signatario i−1
- Si la firma es verdadera entonces el signatario i agrega el mensaje y produce la firma s_i

$$h_i = H((m_1,...,m_i),(N_1,e_1,...,N_i,e_i))$$

$$y = h_i + s_{i-1}$$

$$s_i = y^{di} \bmod n_i$$

Verificación de la firma: dada una firma, los mensajes $M_1,...,M_{(i-1)}$ y sus correspondientes llaves públicas $((N_1,e_1),\ldots,(N_{i-1},e_{i-1}))$, el verificador realiza lo siguiente:

- Verifica que no haya duplicidad en las llaves públicas
- Calcula y = s(i-1)^(e(i-1)) mod n(i-1)
- Calcula $h(i-1)=H((M_1,,M_{i-1}),((N_1,e_1),...,(N_{i-1},)\ e_{i-1}))$
- Calcula s'=y-hx
- Verificar s' de forma recursiva hasta llegar a la primera firma, donde s'=0.

Certificados digitales y PKI

Un Certificado Digital consta de dos partes de información, una para la parte de los datos y la otra parte la firma, la primera incluye la información de identificación del usuario y su llave pública y la segunda contiene la firma digital que certifica la validez de la información de la primera zona, expedida por alguna autoridad de confianza.

Esta autoridad de confianza se le conoce como Autoridad Certificadora (AC) y es la entidad de confianza que certifica la relación del usuario con su llave pública.

El titular del certificado debe mantener bajo su poder la llave privada, ya que, si ésta es sustraída, el sustractor podría suplantar la identidad del titular. En este caso el titular debe revocar el certificado lo antes posible, igual que se anula una tarjeta de crédito sustraída.

Los certificados mantienen una estructura ordenada que permite la rápida localización de la información. El estándar establecido es el X.509 de la Unión Internacional de Telecomunicaciones.

Los certificados digitales tienen gran relación con las firmas digitales, ya que obligan a la entidad signataria a vincular su identidad con la llave pública que será utilizada para verificar la firma. De esta manera, el signatario no puede negar que la firma fue generada por él, si ha sido verificada correctamente con la llave pública contenida en el certificado, cumpliendo con esto el servicio de seguridad de no repudio.

La idea detrás de un criptosistema de llave pública es el de tener un par de llaves e_k, d_k en donde es computacionalmente difícil determinar d_k dado e_e. Esto quiere decir que la llave e_k puede ser pública en una página web u otro medio.

Diffie and Hellman fueron los que propusieron la idea de un criptosistema de llave pública en 1976 y en 1977 Rivest, Shamir y Adleman inventaron el criptosistema RSA el cual está basado en el problema de factorización. Otro criptosistema propuesto fue El Gamal, cuya seguridad descansa en el problema de logaritmo discreto.

Una infraestructura de llave pública (PKI) es un sistema de certificados digitales, entidades de certificación (CA) y autoridades de registro que comprueban y autentican la validez de cada entidad implicada en una transacción electrónica mediante el uso de la criptografía de llave pública. Los estándares para PKI siguen evolucionando al mismo tiempo que se están implementando ampliamente como un elemento necesario del comercio electrónico.

Una PKI engloba todo el software y componentes de hardware junto con los usuarios, políticas y procedimientos que permiten la creación y gestión de los certificados digitales basados en la criptografía asimétrica o de llave pública.

Componentes básicos:

- La autoridad de certificación (CA, Certification Authority): es la encargada de emitir y revocar certificados. Es la entidad de confianza que da legitimidad a la relación de una llave pública con la identidad de un usuario o servicio.
- La autoridad de registro (RA, Registration Authority): es la responsable de verificar el enlace entre los certificados, concretamente, entre la llave pública del certificado y la identidad de sus titulares
- Los repositorios: son las estructuras encargadas de almacenar la información relativa a la PKI. Los dos repositorios más importantes son el repositorio de certificados y el repositorio de listas de revocación de certificados.
- Los usuarios y entidades finales: son aquellos que poseen un par de claves (pública y privada) y un certificado asociado a su llave pública.

Protocolo Diffie and Hellman

Entidad A

1. Seleccionar: $a \in [1, n-1]$

2. Calcular: $y_a = g^a \bmod n$

3. Enviar: y_a a B

4. Calcular: $y_{ab} = (y_b)^a \bmod n$

Entidad B

1. Seleccionar: $b \in [1, n-1]$

2. Calcular: $y_b = g^b \bmod n$

3. Enviar: y a B

4. Calcular: $y_{ab} = (y_a)^b \text{mod } n$

Estampa de tiempo

Una estampa de tiempo provee una prueba de la existencia de un dato en un instante en el tiempo.

Consiste en adicionar la fecha y la hora (en un formato específico) a la información contenida en un mensaje, principalmente en transacciones electrónicas, con lo cual, se previene la corrupción en la generación de la fecha y la hora.

La estampa de tiempo que incluye la firma digital permite determinar que la firma digital existe antes de la fecha y hora dada por la estampa. Lo que permite determinar que el certificado estaba vigente y no ha sido revocado antes del momento indicado por la estampa.

Esta estampa es generada por una autoridad de estampado de tiempo confiables, que puede ser un servidor local o una página web, es decir podemos estar seguros de que esa autoridad siempre suministrará la fecha y la hora correctas.

Generación de estampa de tiempo por la autoridad certificadora:

- Recibe el picadillo del documento a estampar.
- Obtiene el tiempo del servidor de tiempo.
- Genera la firma para la estampa de tiempo
- Produce la respuesta que contenga el picadillo, el tiempo y el certificado de la autoridad.

Verificación de la estampa: usuario final

- Se verifica que el picadillo sea el mismo que en el documento.
- Se verifica que el certificado de la Autoridad de estampa de
- tiempo sea correcto (que no se encuentra revocado).
- Se verifica el tiempo incluido en la respuesta contra una referencia de tiempo local

Estampado de tiempo basado en RSA

El Usuario:

1. selecciona el mensaje m

2. calcula el picadillo del mensaje h = H(m)

3. envía el picadillo a la AET

La AET

1. obtiene el tiempo t de un servidor de tiempo
2. adjunta la estampa al picadillo del mensaje r=(h||t)
3. firma la estampa $s_r = r_{AET}^{(d)} \mod n_{AET}$
4. responde al usuario con t, r, s_r

Llave de sesión

Llave generada de forma única para el establecimiento de una comunicación entre dos o más entidades. Los algoritmos asimétricos (que tienen un papel en los criptosistemas de llave pública) permite eliminar problemas relacionados con las claves compartidas

mediante un canal seguro. Sin embargo, son mucho menos eficaces (en términos de cálculos de tiempo) que los algoritmos simétricos.

El concepto de clave de sesión es un término medio entre el cifrado simétrico y asimétrico que permite combinar las dos técnicas.

El principio de las claves de sesión es simple: consiste en generar de forma aleatoria una clave de sesión de un tamaño razonable y cifrar esta clave utilizando un algoritmo de cifrado de llave pública (más precisamente, utilizando la llave pública del receptor)

El receptor puede descifrar la clave de sesión con su llave privada. El emisor y el receptor comparten una clave que sólo ellos conocen. Por lo tanto, pueden enviar otros documentos cifrados utilizando un algoritmo de cifrado simétrico.

Apéndice B

Normativas y regulaciones

En el país, le corresponde al gobierno velar por la salud de los ciudadanos, ya que es un derecho, tal y como lo expresa el art. 65 de La Constitución de la República.

"La salud de los habitantes de la República constituye un bien público. El Estado y las personas están obligados a velar por su conservación y restablecimiento.

El Estado determinará la política nacional de salud y controlará y supervisará su aplicación" [23].

Es por eso que se han creado leyes y normativas, para mejorar los servicios de la red nacional de salud, y uno de ellos es la modernización de los procesos involucrados en la atención de los pacientes, es así como, en el año 2016, la Asamblea Legislativa, aprueba la ley de deberes y derechos de los pacientes y prestadores de servicios de salud, con el fin de regular y garantizar los derechos y deberes de los pacientes que soliciten o reciban servicios de salud, así como de los prestadores de servicios en el ámbito público, privado y autónomo, incluyendo el Instituto Salvadoreño del Seguro Social.

En el art. 20, del derecho a la confidencialidad, expresa que: "Los pacientes tendrán derecho a que se respete el carácter confidencial de su expediente clínico y toda la información relativa al diagnóstico, tratamiento, estancia, pronósticos y datos de su enfermedad o padecimiento, a menos que por autorización escrita del mismo o porque existan razones legales o médicas imperiosas, se deba divulgar tal información" [24].

Además, en el artículo 33, deberes de los prestadores de los servicios de salud, literal d) manda: "Custodiar los expedientes clínicos de los pacientes, adoptando las medidas

técnicas y procedimientos adecuados para el resguardo y protección de los datos contenidos en los mismos y evitar su destrucción o pérdida" [24].

Con esta ley se da paso a la nueva reforma de salud, de la cual se puede apreciar la importancia de contar con expediente médico y la confidencialidad del mismo, así como también da la pauta para poder adoptar las medidas técnicas necesarias para el resguardo y la protección del expediente.

En mayo de 2019, se aprueba la Ley del sistema integrado de salud, la cual tiene por objeto establecer los principios y normas generales para la organización y funcionamiento del Sistema Nacional Integrado de Salud, mediante un proceso progresivo hacia el acceso universal a la salud y cobertura universal en forma equitativa, oportuna y de calidad para la población en los diferentes niveles de atención [25].

Esta ley busca garantizar a la población el acceso a la salud de una forma integral, esto como parte de los esfuerzos por unificar la información clínica de los ciudadanos, y que en su artículo 26, Expediente Médico Único, expresa lo siguiente: "Los integrantes del Sistema, que son prestadores públicos de servicios de salud, crearán un Expediente Médico Único por cada usuario; este Expediente estará disponible en forma digital para todos los prestadores públicos, y además, de manera física en la institución tratante. El Sistema definirá la forma de identificar a la persona en este Expediente, al igual que establecerá la información y contenido del mismo" [25].

En el caso de los prestadores privados de salud, están obligados a proporcionar un resumen de cualquier información médica solicitada oficialmente" [25].

Con la entrada de un nuevo gobierno, en marzo de 2019, se presenta el "Plan Cuscatlán", con el que se busca mejorar las condiciones de los ciudadanos, el cual consta de varios componentes, uno de ellos es el componente 7 que corresponde a innovación tecnológica, subcomponente 4 de "firma electrónica", en donde se especifican las condiciones necesarias para la aplicación de la firma, y en el subcomponente 7 de "identidad digital", en los que se puede apreciar la importancia de contar con herramientas seguras que permitan brindar a los pacientes una mejor atención en salud, creando las condiciones idóneas para el resguardo de su historial clínico [26].

Algo muy importante de destacar es que recientemente, en septiembre de 2019, el gobierno central a través del Ministerio de Salud, logran que la Asamblea Legislativa, aprobó la Norma Técnica para la Conformación, Custodia y Consulta de Expediente Clínico, la cual en su Capítulo IV, del art. 40 al 79, dan validez legal al ECE, ya que no existía, ley, normativa o regulación que le permitiera al ECE ser un instrumento válido para llevar un seguimiento de clínico de los ciudadanos. Esto quiere decir que se ha dado un paso importante hacia la digitalización de la información o historial de salud, tanto en el sector público como privado [27].

También permite al usuario final (paciente), tener acceso a su información clínica, la cual durante años ha sido de carácter confidencial. Por esta razón en particular y gracias a la norma, se puede trabajar de lleno en un protocolo de seguridad que no solo garantice que la información contenida en cada expediente sea fidedigna, sino que también, garantice a los usuarios que su información estará resguardada, para evitar que personas mal intencionadas hagan un mal uso de ella, además se hace hincapié en la forma de trabajar sobre los

respaldos dela información, así como una unificación del historial clínico en todo el país, evitando así, la duplicidad de diagnósticos en distintos centros de salud alrededor del país. También explica el mecanismo de cómo trabajar y manejar la información contenida dentro del ECE, proporciona directrices claras de como resguardar la información, de quienes son los responsables de dichos ECE's y cómo se deben garantizar los servicios de seguridad de la información, como la confidencialidad, la disponibilidad y el no repudio.