Institución Universitaria

Metodología integral de protección de datos electrónicos médicos, aplicado al almacenamiento, acceso y análisis forense de las historias clínicas en Colombia

Manuel Alejandro Ramírez Timana

Instituto Tecnológico Metropolitano

Facultad de Ingenierías, Departamento de Sistemas de Información

Medellín, Colombia

2019

Metodología integral de protección de datos electrónicos médicos, aplicado al almacenamiento, acceso y análisis forense de las historias clínicas en Colombia

Manuel Alejandro Ramírez Timana

Tesis presentada como requisito para optar al título de:

Magíster en Seguridad Informática

Director (a):

Msc, Andrés Felipe Ramírez Barrera

Codirector (a):

Msc, Gabriel Enrique Taborda Blandón

Línea de Investigación:

Ciencias Ingenieriles Biomédicas

Grupo de Investigación:

Investigación e innovación biomédica

Línea de Investigación:

Ciencias Computacionales

Grupo de Investigación:

Automática, Electrónica y Ciencias Computaciones

Instituto Tecnológico Metropolitano

Facultad de Ingenierías, Departamento de Sistemas de Información

Medellín, Colombia

2019

Esta tesis está dedicada:

A Mis padres, seres a quienes adoro desde lo más profundo de mi corazón por ser artífices en la culminación de mis estudios superiores quienes con sus consejos y ayuda me dieron impulso para salir adelante.

A Juan Botero que me sirvió de inspiración para ser lo que hoy en día soy y que aun en el cielo siento tu apoyo en cada una de las decisiones que tomo.

Finalmente quiero agradecer a todas las personas especiales que me acompañaron en esta etapa, aportando a mi formación tanto profesional y como ser humano.

Agradecimientos

A mis padres por ser mi pilar fundamental y haberme apoyado incondicionalmente, pese a las adversidades e inconvenientes que se presentaron.

Agradezco a mis directores de tesis Msc, Andrés Felipe Ramírez Barrera y a Msc, Gabriel Enrique Taborda Blandón quienes con su experiencia, conocimiento y motivación me orientaron en la investigación.

Agradezco a los docentes que, con su sabiduría, conocimiento y apoyo, motivaron a desarrollarme como persona y profesional en el ITM.

Resumen

La Historia Clínica tiene unas características especiales que requieren un manejo diferente desde el punto de vista de la seguridad informática. Dadas las condiciones que anteceden para mantener su integridad, además de cumplir con la normatividad propia de cada país, se hace conveniente la transformación de la forma tradicional mediante manuscritos, a la utilización de las tecnologías de información. Con esta evolución, los incidentes de seguridad cibernética en un sector tan crítico como este, tienen un gran impacto en la sociedad, considerando que la información de la historia clínica podría ser usada de manera inadecuada, permitiendo el robo de identidad, ingreso no autorizado, daño de la información u alteración de los datos del paciente. Aplicando la Resolución Colombiana 1995 de 1999 [1], se desprende que la información del paciente debe registrarse cronológicamente, de la misma manera que los actos médicos, procedimientos ejecutados por el equipo de médico o cualquiera intervenga en su atención, a lo largo de los planteamientos hechos, los sistemas de salud se van volviendo cada vez más vulnerables a incidentes de seguridad informática, en consecuencia a la automatización, las tecnologías de información, los volúmenes de información y la conexión con los pacientes; Al mismo tiempo la inclusión de la seguridad en los sistemas de información de salud no es una prioridad. El resultado de esta investigación es una metodología integral que permita asegurar la accesibilidad al sistema, garantizar la integridad de los datos, además de la posibilidad de realizar un análisis forense en caso de ser vulnerado, al mismo tiempo logrando mitigar las causas, generando alertas, y factores por los cuales los datos electrónicos médicos en historias clínicas no logran ser protegidos.

Palabras clave: Seguridad de información, Historia clínica, Privacidad, Registro Médico Electrónico, Accesibilidad, Seguridad Cibernética, Seguridad de los datos, Análisis forense.

Abstract

The Clinical History has some special characteristics that require different management from the point of view of computer security. Given the above conditions to maintain its integrity, in addition for complying with the regulations of each country, it is convenient to modify the traditional form by means of manuscripts, to the use of information technologies. With this evolution, the incidents of cybersecurity in a sector as critical as this one, have a great impact on society, such as information on history. Damage to information or alteration of patient data. Applying Colombian Resolution 1995 of 1999 [1], it follows that patient information must correspond chronologically, in the same way as medical acts, procedures performed by the doctor's team or any intervention in their care, throughout the given the facts, health systems are becoming increasingly vulnerable to computer security, automation, information technology, information and connection with patients; At the same time, the inclusion of security in health information systems is not a priority. The result of this research is a comprehensive methodology that allows accessibility in the system, the integrity of the data, the possibility of carrying out an analysis in the case of vulnerability, the same time in which mitigation of the causes is being achieved, generating alerts, electronic data in clinics cannot be protected.

Keywords: Information Security, Clinic history, Privacity, Electronic Health Record, Accesibility, Cyber Security, Data Security, Forensic analysis.

Contenido

Pág.

Lista de figuras

Pág.

Lista de tablas

Pág.

Abreviaturas

Abreviatura	Término
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
EHR	Electronic Health Record
ACL	Access Control List
RBAC	Rol-Based Access Control
AAC	Autenticación, autorización y cuentas de usuario
HIPAA	Health Insurance Portability and Accountability Act
VIH	Virus de Inmunodeficiencia Humana
PIPE	Pseudonymization of Information for Privacy in e-Health
DUKPT	Derive Unique Key Per Transaction
PKI	Public Key Infrastructure
AES	Advanced Encryption Standard
ABE	Attribute-based encryption
EMR	Electronic health record
ACM	Association for Computing Machinery
IEEE	Institute of Electrical and Electronics Engineers
HL7	Health Level Seven
PHR	Personal health record
RBTBAC	Role-based and time-bound access control
HCE	Host card emulation
IMEI	International Mobile Station Equipment Identity
SMS	Short Message Service
SHA	Secure Hash Algorithm
AAA	Authentication, Authorization and Accounting
ZKP	Zero Knowledge Proofs
MSP	Membership Service Provider
GPG	GNU Privacy Guard

Introducción

El valor comercial de la información ha aumentado dramáticamente en las últimas décadas. Los sistemas de información han penetrado el mundo de los negocios en un ritmo rápido y se han convertido en activos críticos en la mayoría de los sectores organizacionales. Desafortunadamente, en el sector salud, existen muchas amenazas que afectan la confiabilidad de la información, el control de acceso y la disponibilidad del sistema informático. En general, las organizaciones de salud están cada vez más expuestos en comparación con los servicios financieros y otras organizaciones, debido a que los tipos de información que poseen son más valiosos para un cibercriminal, inclusive aún más valioso que los números de tarjetas de crédito, pues pueden crear identidades falsas, realizar fraudes y un sin número de ataques [1]. Patricia Sorokin y Elizabeth Estupiñan [2] hablan de un caso muy sonado en el centro médico de la Universidad de California (UCLA), en el que por lo menos 13 empleados del centro médico fueron despedidos por fisgonear la historia clínica de Britney Spears, la cual fue ingresada al área psiquiátrica de este centro médico. Debido a lo anteriormente expuesto no solo tiene efectos monetarios y de reputación para la entidad afectada, sino que en efecto esto se extiende hacia los pacientes y usuarios. Ante las situaciones anteriormente vistas la seguridad es una composición de factores tecnológicos y humanos, que si no se tienen en cuenta ambos factores no se puede mitigar, transferir o evitar los riesgos asociados a los activos informáticos, por sobre todo se debe concientizar a los empleados internos de las amenazas y las vulnerabilidades que pueden presentarse. Para ilustrar algunos ejemplos, el filtrado de información a través de unidades extraíbles, publicación de información, información no cifrada que pueden filtrarse a través de intercambio de archivos, robo de datos a través de cuentas comprometidas, violación de sistemas de red por ataques o malware, robo de bases de datos por falta de controles de monitoreo, actualmente para las entidades prestadoras de servicios de salud, existen mecanismos de seguridad disponibles tales como la gestión del sistema, control de acceso, IDS, IPS y las técnicas de cifrado, que pueden ser suficientes

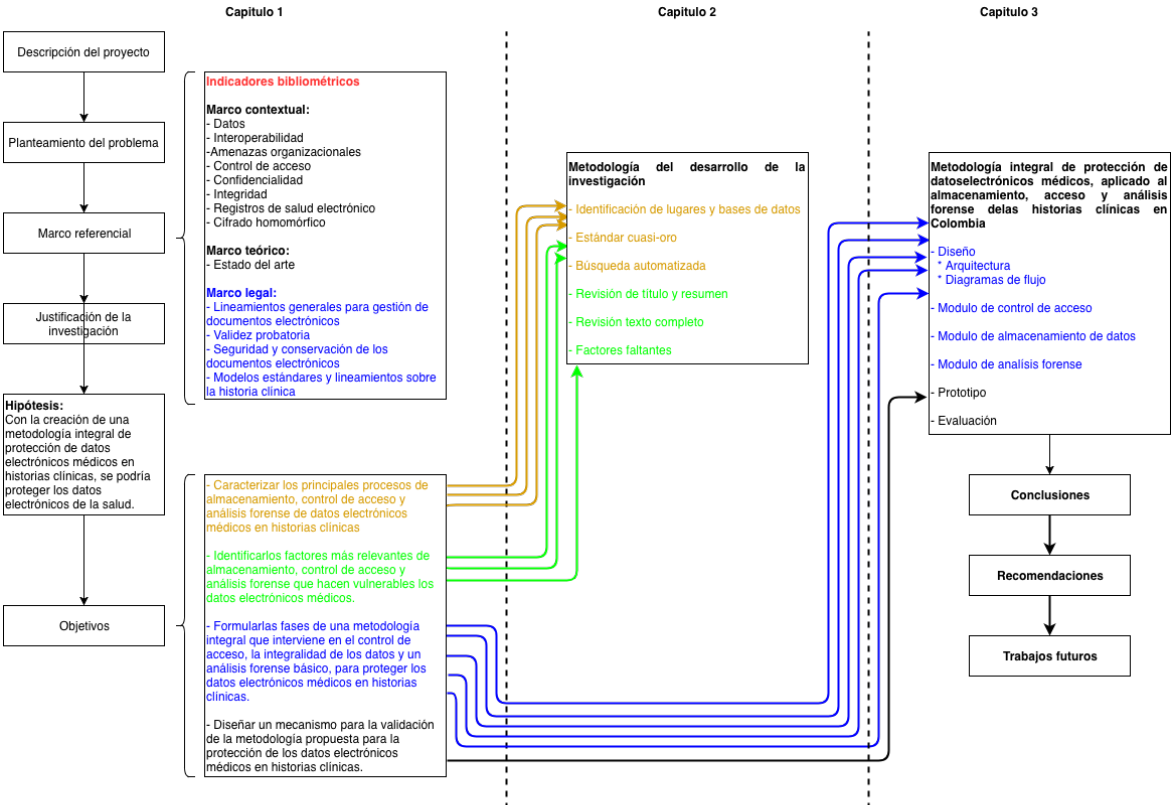
para impedir o detectar las actividades encubiertas de los empleados del hospital, periodistas, familiares y otros atacantes poco sofisticados, pero serán insuficientes para un atacante profesional. Por otra parte, a medida que la tecnología sigue evolucionando de un día para el otro, se vuelve difícil asegurar que la tecnología de los datos electrónicos médicos está al día con las últimas prácticas de seguridad. Como se puede imaginar, mantenerse al día con esta tecnología en constante cambio puede ser costoso y difícil, no sólo la aplicación de la nueva tecnología como el tener que actualizar los servidores y sistemas, sino que también conduce a temas de procesamiento de datos y problemas de flujo de trabajo. Se observa claramente que la seguridad informática debe asegurar la protección de información, la restricción de acceso, fuga de información, alteración, además de tener especial cuidado otras situaciones en las que personas no autorizadas tengan acceso o posibilidad de acceso a dicha información para fines no autorizados. Ahora bien, Colombia es un país que en este momento no cuenta con una norma específica o regulación creada especialmente para la industria de la salud que establezca estándares de seguridad como lo hacen otras normas en el mundo, como lo hace HIPAA en Estados Unidos. No obstante, en Colombia existe la ley 1581 de 2012, la cual expone el tratamiento de los datos personales, así mismo, la ley 1438 de 2011, habla sobre la unificación de la estructura de la Historia Clínica Electrónica, en la misma forma habla de un sistema de comunicaciones electrónicas que permite la intercomunicación virtual de las diferentes entidades sobre un usuario en particular. Cabe agregar que en el artículo 5 de la Ley 1581 de 2012 categoriza a los datos electrónicos médicos como sensibles, los datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación. En efecto las entidades prestadoras de salud, incluyendo todo su ecosistema de servicios asociados, como lo son farmacias, laboratorios y demás incluidos en la cadena de la salud, intercambian información de un número elevado de personas, esto puede ser riesgoso al dejar la información desprotegida o por un mal manejo de la misma. A manera de ejemplo, el olvido de un documento en un escritorio o impresora o dejar un computador descuidado durante varios minutos puede ser realmente peligroso. Ante la situación planteada y ver los efectos de este el factor humano es determinante y muchos de los incidentes que se han presentado han sido debido a la falta de cuidado. Los datos electrónicos médicos sobre el cuidado de la salud es quizás la más íntima, personal y sensible de cualquier información mantenida sobre un individuo. A medida que el sistema de salud crece en tamaño, el alcance y la integración, la vulnerabilidad de esa información también aumentara si no se toman medidas de protección [3]. Los objetivos

de la integridad, disponibilidad y confidencialidad de los datos de asistencia sanitaria solo pueden lograrse mediante el establecimiento de un marco de privacidad y seguridad adecuada. Comparativamente, no se tienen controles para los procedimientos de actualización de los sistemas. Ahora bien los registros almacenados de los pacientes en estos sistemas vulnerables son aún más valiosos para los ciberdelincuentes que la información de las tarjetas de crédito [1]. Hecha la observación anterior, esto se debe a que la información de los pacientes contiene datos detallados del comportamiento en la persona en la entidad de salud, entre diagnósticos y formulas médicas que pueden ser usados por cibercriminales para cometer fraudes. Precisando de una vez, un ciberdelincuente fácilmente puede usar esta información para comprar medicinas reguladas y después vender en el mercado negro. De la misma forma, los ciberdelincuentes según se ha visto están encontrando información clínica acompañada de información financiera de los pacientes, en los cuales se ingresa la información de tarjetas de crédito además de pagarés firmados en blanco que incrementan su interés en vulnerar los sistemas de las instituciones de salud. De acuerdo con los razonamientos que se han venido realizando, es demasiado difícil identificar que ha sido robada por lo que aumenta el valor. A manera de resumen las tarjetas de crédito se pueden cambiar fácilmente y las tarjetas clonadas pueden ser fácilmente canceladas luego de que un cliente observe irregularidades en su estado de cuenta. Comparado, con un paciente que puede tardarse más de un año en darse cuenta de que su identidad ha sido robada. Debido a esto se ve la necesidad de crear una metodología para implementar el control de acceso, cifrado de datos y análisis forense básico para evitar la vulneración o perdida de los datos electrónicos médicos. Cabe aclarar, que esta tesis no se centra en un formato de historia clínica especifico, como por ejemplo, HL7, se centra en la protección de los datos, que es el nivel más básico de la pirámide de datos [4], por lo que es una implementación de la seguridad de la información de manera integral, holística e independiente de la tecnología usada por cada hospital, o de la cantidad y calidad de las historias clínicas, ni de los formatos empleados en cada sistema de información de las entidades de salud. Con la creación de esta metodología se pretende garantizar los pilares básicos de la seguridad informática, confidencialidad, integridad y disponibilidad en los registros electrónicos médicos.

Estructura general de la tesis

La presente figura resume el proceso de este trabajo de maestría descrito en 3 capítulos.

Figura 4-1 Estructura general de la tesis.



Autor: Construcción propia

En el capítulo 1, se presenta el Estado del Arte para los datos electrónicos médicos, el marco normativo y los estándares nacionales e internacionales. Además, se hace referencia a los antecedentes y trabajos relacionados.

En el capítulo 2, se construye una metodología para la protección de los datos electrónicos médicos en Colombia. La metodología es aplicada al almacenamiento, control de acceso y análisis forense de las historias clínicas de Colombia.

En el capítulo 3, se presenta la realización de un prototipo usando la metodología con la aplicación práctica y el uso para la protección de los datos electrónicos médicos, además se concluye y hace una breve reseña que se propone para trabajo futuro.

1. Contextualización

1.1 Descripción del proyecto

Los registros médicos electrónicos son vulnerables a posibles abusos, pérdidas, fugas y amenazas. En los últimos años, la información de salud de los pacientes se ha hecho susceptible de peligro debido a fallas de seguridad informática en hospitales y entidades prestadoras de servicios de salud.

1.2 Planteamiento del problema

Con frecuencia se desarrollan e incorporan nuevos procesos, más eficaces y eficientes en el sector de la salud. Sin embargo, en la era del siglo XXI donde los modelos de tecnología, la sociedad y operación evolucionan rápidamente, la experiencia de atención médica es a menudo deficiente. Una mejor asistencia para el paciente a un costo altamente controlable debe ser el objetivo principal. La complejidad de los sistemas de salud en línea es muy alta, lo que hace que la calidad de la información (exhaustividad, integridad), la accesibilidad y la disponibilidad sea una tarea muy difícil [5].

Hoy en día son más comunes los incidentes que afectan la disponibilidad de los sistemas de salud en línea. Las organizaciones de salud están siendo blanco de los cibercriminales sofisticados y altamente organizados que están mostrando todos los días lo vulnerable que son los sistemas de salud electrónica. Y la situación se pone cada vez más difícil. Las naciones deben darse cuenta de lo vital que son sus sistemas nacionales de salud y tomar todas las medidas necesarias para protegerlos [5].

Dadas las condiciones que anteceden una brecha de seguridad no solo tiene efectos financieros y de imagen para la entidad afectada, sino que en consecuencia esto se extienden hacia los pacientes y usuarios. Debido a las consecuencias las empresas del sector salud deben enfrentar estos retos ahora mismo.

La falta de concientización sobre los problemas de seguridad informática a todo el personal involucrado en la atención de los pacientes conduce a un aumento en los problemas de seguridad, porque el personal no entiende ni conoce las mejores prácticas para mantener a salvo los datos del paciente. El principal problema de seguridad de la información en el cuidado de la salud no es la tecnología, sino la falta de una política de seguridad coherente. Los tipos de ataques más habituales son cometidos por personas que son usuarios del sistema con privilegios legítimos, pero que abusan de sus privilegios por motivos financieros (al ser sobornados) o personales (porque le pide el favor un tercero o por curiosidad). El valor monetario que se puede obtener de los datos de salud de la mayoría de los individuos es relativamente bajo (comparado con algunos datos financieros o secretos militares) a no ser que sean solicitados como un encargo por la competencia, farmacéuticas, empresas de seguros, entre otras, por lo tanto, es lógico (o si se prefiere en la redacción claro) asumir que un atacante no gastará recursos excesivos (dinero y tiempo) en intentar adquirir estos datos a través de robo o ataque informático. Exceptuando los datos sobre la salud de las celebridades, personas prominentes o públicas pueden ser de mayor valor monetario en el mercado ilegal. Actualmente hay disponibles mecanismos de seguridad (aunque no necesariamente implementado), tales como la gestión del sistema, control de acceso, IDS, IPS y las técnicas de cifrado, que pueden ser suficientes para impedir o detectar las actividades encubiertas de los empleados del hospital, periodistas, familiares y otros atacantes poco sofisticados, pero serán suficientes para un atacante profesional.

Significa entonces que las entidades prestadoras de servicios de salud que recolecten, transmitan y almacenen información de los pacientes electrónicamente, de cualquier procedimiento realizado al paciente, deberán asegurar que la información cumpla con lo dictado por la Ley o se pueden enfrentar a multas y otras medidas sancionatorias [6].

Para proteger los datos electrónicos médicos de las actividades maliciosas y la exposición descuidada, los sistemas necesitan emplear las soluciones tecnológicas adecuadas. Y a medida que la tecnología sigue evolucionando de un día para el otro, se vuelve difícil asegurarse de que la propia tecnología de los datos electrónicos médicos está al día con las últimas prácticas de seguridad. Como se puede imaginar, mantenerse al día con esta tecnología en constante cambio puede ser costoso y difícil. No sólo la aplicación de la nueva tecnología como el tener que actualizar los servidores y sistemas, sino que también conduce a temas de procesamiento de datos y problemas de flujo de trabajo [5].

Las amenazas a los datos electrónicos médicos se pueden clasificar así: (1) las amenazas humanas, como la de los empleados o los piratas informáticos. Desastres hechos por el hombre pueden ser intencionales (por ejemplo, un acto terrorista) o no intencional. (2) Los desastres naturales y ambientales, tales como inundaciones, terremotos, huracanes e incendios; y (3) los fallos tecnológicos, tales como fallos del sistema informático [5].

Otro ejemplo de las posibles amenazas proviene de los empleadores ávidos de información, compañías de seguros y organizaciones de atención médica administrada. Estas organizaciones tienen mayores recursos económicos, junto con la motivación de la ganancia significativa de lo que pueden conocer acerca de los individuos. Operaciones no éticas en estas industrias podrían asignar un equipo de gama alta a la tarea de romper una clave criptográfica utilizada en la transmisión de los datos de salud a través de canales públicos de bajo costo. En 1995, el costo de una máquina capaz de romper el cifrado de datos del gobierno de EE. UU. era de $ 64,000 dólares. Algunas organizaciones relacionadas con la salud o personas poco éticas podrían estar dispuestos a realizar esta inversión y, por ejemplo; recopilar datos sobre el VIH, los cuales podrían ser utilizados de forma encubierta para negar la cobertura de seguro médico o para extorsionar a estos pacientes, dado lo penosa de esta enfermedad [6].

Las amenazas anteriores se refieren a los ataques a la privacidad que pueden sufrir los datos del paciente, pero los modelos de seguridad también deben considerar amenaza como los ataques a la integridad y disponibilidad de los datos de salud. Estas amenazas pueden provenir de delincuentes informáticos, desastres naturales o fallos físico del sistema informático, que potencialmente podrían causar la pérdida parcial o total de datos, que sea modificado a conveniencia o la denegación del servicio [6].

En concreto, se desea que la información de salud siempre esté disponible, pero segura, sin problemas o sin riesgo a la “ingeniería social” en la que se observa: el soborno, la extorsión, la falsificación de la identidad personal o ataque directo al sistema de información o denegación de servicios.

Una planificación de recuperación de desastres, es una serie de pasos que debe seguir la organización cuando se presentan eventualidades que afectan su funcionamiento, en el caso específico de los sistemas de información de las empresas prestadoras de servicios de salud, dicho plan puede proteger los datos electrónicos médicos, y en caso de incidente permiten restaurar lo más pronto posible el servicio y mitigar los daños sufrido por la infraestructura de tecnología [5]. Todas las organizaciones deberían poseer un plan de

recuperación de desastres informáticos, porque ninguna está exenta de sufrir un ataque cibernético.

A lo largo de los planteamientos hechos se debe garantizar la protección de información a los datos personales, el acceso sin autorización, vulneración, difusión, destrucción, inclusive otras alteraciones en las que personas no autorizadas tengan acceso. Si estos riesgos percibidos no son controlados, los pacientes pueden recurrir a la falsificación de la veracidad e integridad de los datos almacenados como una alternativa, con el fin de preservar su privacidad [7].

Cuanta mayor seguridad tenga el sistema, menos reparos podrán realizarse sobre su valor probatorio en un litigio. Mecanismos de seguridad, tales como la gestión del sistema, control de acceso, y las técnicas de cifrado, son suficientes para impedir o detectar las actividades encubiertas de los empleados del hospital, periodistas, familiares y otros atacantes poco sofisticados [8].

1.3 Indicadores bibliométricos

Los registros electrónicos en salud están definidos comúnmente como un mecanismo digital centralizado de datos del paciente almacenados en un formato digital [9]. Los EHR contienen información confidencial sobre el cuidado de salud o tratamientos médicos del paciente, almacenados electrónicamente. Cabe decir que estos registros se pueden compartir entre los diferentes centros de salud [2]. En relación con lo anterior expuesto los EHR pueden incluir datos demográficos, procedimientos médicos, recetas médicas, alergias, resultados de exámenes de laboratorio, radiografías, entre otros [10]. En Colombia la Ley 1438 de 2011 en el Artículo 112, establece que “la historia clínica única electrónica será de obligatoria aplicación antes del 31 de diciembre de 2013” [11]. Como consecuencia de lo anteriormente expuesto es muy remoto que tal logro no ha sido alcanzado dado que según reportes del Ministerio de Salud Nacional todavía algunas entidades prestadoras de salud en Colombia no cuentan con una sistematización de las historias clínicas [9]. En tal sentido, toda esta estrategia se centra sin duda en la información, para lo que se requiere una propuesta de manejo integral, que combine toda una serie de características que permitan garantizar la seguridad y el almacenamiento de las historias clínicas de los datos del sistema de salud. Tal como se ha visto la historia

clínica digital [12] debe existir sobre la base de que es mecanismos para proteger la privacidad y la seguridad porque esta información es clasificada, además de su alto riesgo al ser publicada ilegalmente no solo a nivel de Colombia [2], sino también a nivel internacional, se debe garantizar todas las protecciones legales y tecnológicas que estén en todo el marco legal. No obstante, en la revisión de la literatura cabe destacar que no se encontró un estudio que refleje la situación en de los países latinoamericanos y en particular de Colombia en esta materia, adicionalmente, es importante generar conocimiento en esta área dado que su impacto es importante en el sector salud, por ello, se hace necesario incrementar la producción científica y académica en el campo de la seguridad de los datos electrónicos en salud, esto basado en un análisis bibliométrico, que permite realizar un diagnóstico de la evolución y estado actual del tema. En este último estudio, se realizó un extensivo análisis de publicaciones y revistas en la seguridad de los registros electrónicos en salud durante el periodo 1999-2017 por medio de una bibliometría que busca analizar de forma genérica el conjunto de la actividad de investigación académico-científica.

1.3.1 Metodología

En primer lugar, el estudio se inicia con la definición de los campos de búsqueda que se denomina ecuación de búsqueda en la cienciométria [13] como consecuencia de la definición de campos, podemos construir los mapas con base a los datos obtenidos de dichos documentos, de la misma manera poder identificar a los actores referentes en la generación del conocimiento en la seguridad de los registros electrónicos en salud. Así mismo para la realización de las búsquedas y clasificación de la información, se utilizó el motor de búsqueda SCOPUS. Es importante destacar que este motor de búsqueda ofrece la posibilidad de hacer exploraciones en todo el contenido de las bases de datos bibliográficas multidisciplinarias. Una característica importante es que es una Base de Datos referencial y su período de actualización es semanal. Algo que resaltar de este motor de búsqueda es que su contenido es bastante amplio y reconocido, pero cabe decir que no cubre la totalidad de las revistas en el área de la seguridad de los datos electrónicos médicos. Para realizar la búsqueda se usaron varias palabras claves, en las que están incluidas “EHR” y “Security”, como resultado se pudo cubrir muchas posibles coincidencias. Además de las anteriores palabras claves, también se incluyeron los siguientes términos

para obtener un mejor resultado: “healthcare”, “Electronic health record”, “Access control”, “protection”, “security”, “privacy” y “forensic”. Finalmente, la ecuación de búsqueda utilizada fue:

healthcare AND “Electronic health record” AND “Access control” AND protection AND security AND privacy

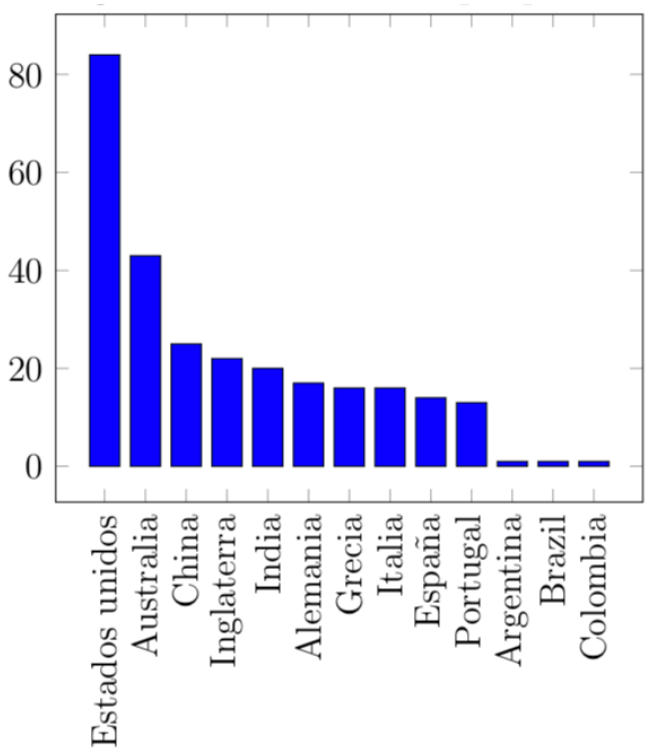
En la (Tabla 1-1) y la (Figura 1-1) se ilustran los documentos encontrados por país como resultado de la ecuación en el motor de búsqueda.

Tabla 1-1 Documentos por país

País	Documentos
Estados unidos	84
Australia	43
China	25
Inglaterra	22
India	20
Alemania	17
Grecia	16
Italia	16
España	14
Portugal	13
Argentina	1
Brasil	1
Colombia	1

Autor: Construcción propia

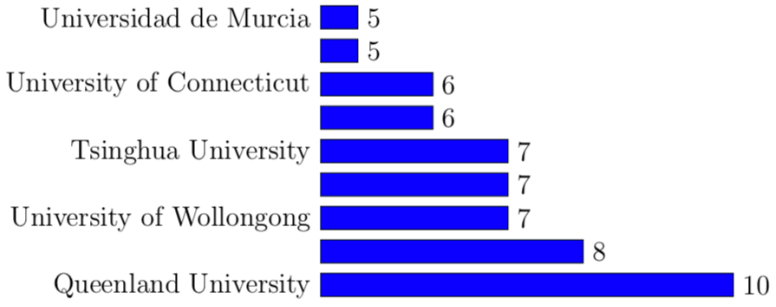
Figura 1-1 Documentos por país.



Autor: Construcción propia

En la (Figura 1-2) se aprecian las Universidades que en el periodo del 1999 al 2017 han promovido la producción correspondiente a la protección de los datos electrónicos médicos.

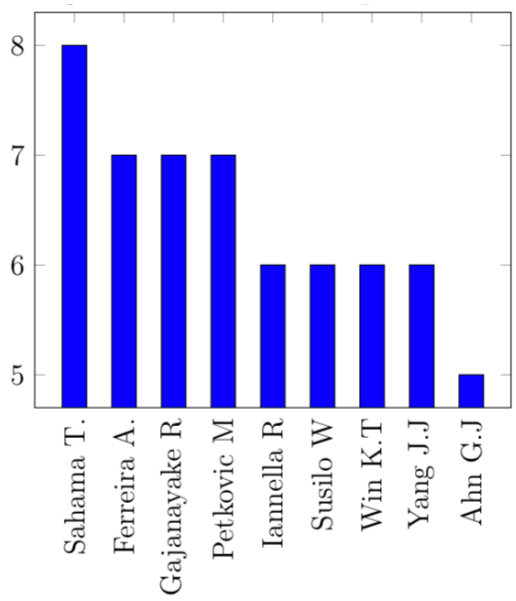
Figura 1-2 Documentos por Universidad.



Autor: Construcción propia

De igual manera, la búsqueda arrojo las personas más importantes que generan conocimiento en esta área, las cuales se relacionan en la (Figura 1-3).

Figura 1-3 Documentos por autor



Autor: Construcción propia

1.3.2 Resultados

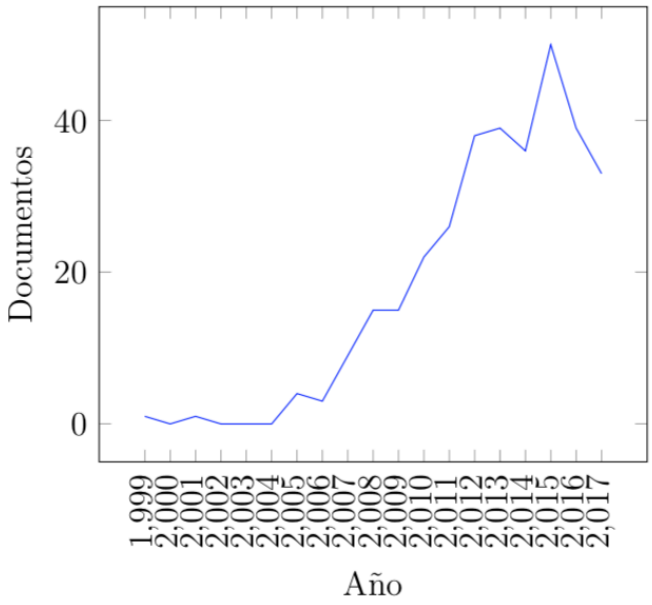
Se observa claramente que haciendo uso del total de publicaciones por países indicados en la (Figura 1-1), cabe decir que los resultados indican que existen grandes diferencias entre los países analizados. Con referencia a lo anterior, los países como Estados Unidos y Australia son las que cuentan con un mayor número de documentos publicados. Tal como se ha visto, Estados Unidos tiene un número mayor de contribuciones, entendiendo esto como uno de los países a referenciar, por esta causa tienen un alto grado de madurez en el campo de la seguridad de los registros electrónicos en salud. En igual forma destaca Australia, donde esta tiene un total de 43 publicaciones totales. Dadas las condiciones que antecede, los países latinoamericanos tienen poca representación, siendo Argentina, Brasil y Colombia los únicos con publicaciones. A lo largo de los planteamientos hechos,

los países participantes son, en una gran mayoría, americanos, europeos, asiáticos y en una proporción menor latinoamericanos.

De acuerdo con los razonamientos que se han venido realizando, este se centró en la identificación de producción de documentos por año, además de los países y líneas temáticas emergentes. Con referencia a lo anterior se han identificado la producción de documentos por año y además de la relación de interés de las temáticas tratadas en estos documentos se procedió a la visualización de los resultados se utilizan histogramas.

A continuación, en la (Figura 1-4) se muestran los resultados obtenidos por medio de una bibliometría [14] de las publicaciones indexadas realizadas por investigadores de todo el mundo sobre la seguridad de los registros electrónicos en salud, durante el periodo 1999-2017, utilizando la Base de Datos “SCOPUS”. La siguiente grafica muestra que los últimos años no indican un crecimiento de la producción científica en revistas indexadas a través del tiempo

Figura 1-4 Documentos por año



Autor: Construcción propia

Los contenidos científicos correspondiente a los temas centrales de las publicaciones, se extraen a partir de las palabras claves de la base de datos. En este campo se encuentra una lista estandarizada de términos que forman parte del Tesauro de la base de datos.

Tabla 1-2 Documentos por área temática

Temática	Documentos	Porcentaje
Ciencias de la computación	209	63.1
Medicina	129	39.0
Ingeniería	74	22.4
Profesiones de la salud	61	18.4
Matemáticas	29	8.8
Ciencias sociales	27	8.2
Bioquímica, Genética y Biología Molecular	16	4.8
Negocios, Gestión y Contabilidad	15	4.5
Ciencias de la Decisión	13	3.9
Física y Astronomía	5	1.5
Ingeniería química	4	1.2
Economía, Econometría y Finanzas	4	1.2
Inmunología y Microbiología	4	1.2
Enfermería	4	1.2
Ciencias agrícolas y Biológicas	2	0.6
Artes y Humanidades	2	0.6
Ciencia de los materiales	2	0.6
Multidisciplinario	2	0.6
Química	1	0.3
Farmacología, Toxicología y Farmacéutica	1	0.3
Psicología	1	0.3
Total	**331**	

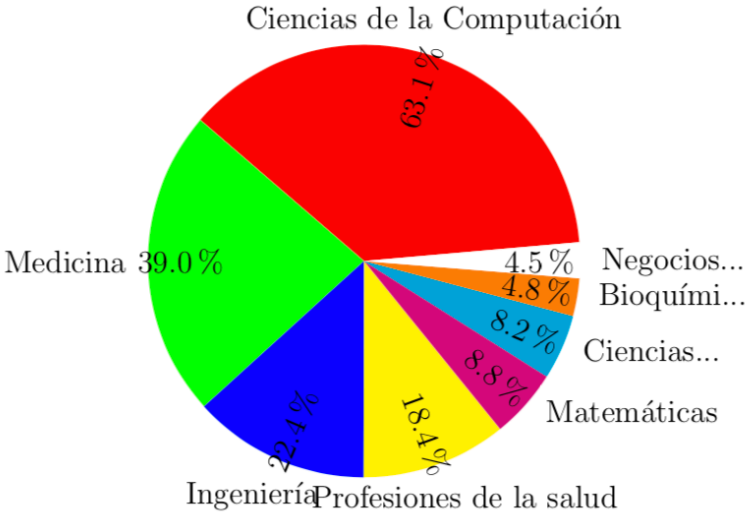
Autor: Construcción propia

Los resultados de la (Tabla 1-2) indican, como es de esperar, que la mayor parte de los artículos se clasifican dentro del área de Ciencias de la Computación, seguidos de artículos de Medicina y de los Ingeniería.

Es de anotar que el área temática que más genera nuevo conocimiento en el área de la seguridad de los datos electrónicos médicos es Ciencias de la Computación y Medicina son los que se ajustan mejor al criterio del área de la seguridad de los datos electrónicos,

dado que un 63.1 % de los artículos publicados pertenecen a la línea de Ciencias de la Computación, mientras el 39.0 % se clasifica dentro de la categoría Medicina como se muestra en la (Figura 1-5).

Figura 1-5 Porcentaje documentos por área temática



Autor: Construcción propia

En la (Tabla 1-3) se muestra que los campos con mayor producción científica son conferencias y artículos, de los cuales 146 son conferencias y 114 artículos los cuales incluyen el conocimiento actual, así como contribuciones teóricas y metodológicas en la protección de los datos electrónicos médicos.

Tabla 1-3 Documentos por tipo

Tipo de documento	Documentos
Conferencias	146
Artículos	114
Capítulos de libro	39
Revisiones	14
Libros	12
Editoriales	1

Total	**326**

Autor: Construcción propia

Para finalizar, es conveniente indicar que la pertinencia de este tipo de estudios reside en la posibilidad de identificar las fortalezas y las debilidades de las distintas publicaciones, siempre con un carácter constructivo que permita analizar otros puntos de vista, y en función de los diferentes intereses, buscar el mejoramiento de los medios de divulgación de los trabajos de investigación que permitan un mayor nivel de competencia de las publicaciones dentro del marco de las exigencias de la comunidad científica.

1.4 Marco contextual

En esta sección se suministra el marco contextual de las áreas de investigación abarcadas, significa entonces, que en adelante se presentarán los conceptos básicos que serán utilizados frecuentemente en la tesis, con el propósito de ilustrar la terminología incluida en el documento.

1.4.1 Interoperabilidad

La interoperabilidad es una característica que permite a dos o más sistemas el intercambio de información, mejorando de este modo la disponibilidad de esta. Interoperabilidad exige seguridad de la información, incluyendo la restricción del acceso no autorizado, uso, divulgación y modificación de los datos, con el fin de garantizar la confidencialidad, integridad y la disponibilidad [15].

1.4.2 Amenazas organizacionales

Este tipo de amenazas pueden asumir diferentes formas, tales como un empleado que tiene acceso a datos sin necesidad legítima o un atacante externo (hacker) que se infiltra en la infraestructura de información de la organización para robar datos o dejar inoperante. Al principio, estas amenazas organizacionales se podrían caracterizar por cuatro componentes motivos, recursos, accesibilidad y capacidad técnica [16]. En función de

estos componentes, diferentes amenazas pueden plantear diferentes niveles de riesgo para la organización que requieren diferentes estrategias de mitigación y prevención.

1.4.3 Control de acceso

El control de acceso consiste en un conjunto de normas que determinan que usuarios pueden leer, ejecutar, compartir y modificar elementos específicos en el sistema, con el objetivo final de garantizar que solo quien tenga el acceso autorizado puede realizar una acción[17]. Hechas las observaciones anteriores, el control de acceso debe estar dirigido a proporcionar confidencialidad mediante la limitación de los derechos de acceso de los usuarios del sistema a los datos del paciente y a una adecuada asignación de los derechos de acceso al establecer el sistema de lista de control de acceso (ACL) [15].

1.4.4 Confidencialidad

El objetivo de la confidencialidad en datos informáticos es mantener en secreto los datos sensibles de personas malintencionadas o, dicho de otra manera, garantizar que las personas malintencionadas no se apropien de información que no les pertenece [18].

1.4.5 Integridad

La integridad tiene como objetivo que cualquier modificación no autorizada en los datos debe ser detectable. Es decir, un adversario malicioso no debe ser capaz de modificar estos datos sin dejar rastro. Esto es muy importante para ayudar a garantizar la veracidad de los datos recogidos en las aplicaciones grandes [24].

1.4.6 Registro de salud electrónico

Un EHR, o Electronic Health Record, también definido comúnmente como un repositorio de datos del paciente almacenados en un formato digital [19], está diseñado para ser usado como parte de un sistema. En referencia a la clasificación anterior, estos pueden incluir datos demográficos, historial médico, medicamentos, pruebas de laboratorio, radiologías, estadísticas personales como la edad y el peso, entre otros. Adicionalmente, eliminan la necesidad de buscar en los medios físicos los registros anteriores de asistencias médicas

de un paciente y se aseguran datos precisos y legibles. Reducen el riesgo de replicación de datos ya que solo hay un archivo modificable [20].

1.4.7 Cifrado homomórfico

El cifrado homomórfico es una técnica que realiza cálculos sobre un texto cifrado, el cual produce el mismo resultado que con los cálculos sobre los datos originales [21]. Los sistemas de cifrado homomórfico se utilizan para realizar operaciones sobre datos cifrados sin conocer la clave secreta, el único propietario de la clave secreta es el cliente. Significa entonces, que el cifrado homomórfico es la conversión de datos en texto cifrado que puede ser analizado y trabajado como si todavía estuviera en su forma original. [22].

1.4.8 Blockchain

Blockchain es una base de datos distribuida, descentralizado, solo para aplicaciones digitales. Cuenta con una red de computadoras que mantienen y validan transacciones a través de consenso con pistas de auditoría criptográfica. Fue descrito por primera vez por Satoshi Nakamoto en 2008 [23]. Satoshi diseñó principalmente Blockchain como una base para la tecnología de criptomoneda como Bitcoin. La idea central de blockchain es un movimiento rápido, barato, seguro, transparente y confiable de activos entre dos partes, sin ningún tercero de confianza, como un banco, una compañía de tarjetas de crédito. Los activos digitales pueden ser dinero, documentos notariales, propiedades, contratos. Por ejemplo, el movimiento de activos se necesita para pagar impuestos, pagar salarios, facturas y mostrar la posesión de documentos particulares. Blockchain se basa en un libro de contabilidad distribuido. Cada transacción creada es verificada y validada por la mayoría de los participantes en la red. La transacción se encadena con base a gastos y se agrega al libro de contabilidad que nunca se puede borrar.

El libro de contabilidad no es propiedad de una autoridad central o servidores centrales. Más bien, se distribuye a los nodos (computadoras en la red) a través de la red descentralizada. Por lo tanto, todos los nodos en la red tienen exactamente la misma copia del libro de contabilidad. Cualquier persona de la red puede verla, verificarla y validarla en cualquier momento. Además, la transacción puede incluso rastrearse hasta la génesis del bloque de transacción. Básicamente, esto elimina la dependencia de un servidor centralizado y disminuye las posibilidades de fraude.

1.5 Marco teórico y estado del arte

En la literatura sobre metodologías de protección de datos médicos, se puede observar que existen trabajos realizados con el objetivo de proteger los datos electrónicos médicos sensibles. A continuación, se relacionan algunos trabajos.

(Neubauer y Heurix, 2011) [24], proponen una metodología de seudónimos llamada PIPE (Pseudonymization of Information for Privacy in e-Health). Esta desacopla los datos médicos a partir de los datos de identificación del paciente, así como la restauración de la relación de las partes autorizadas, mientras que los registros médicos actuales se mantienen y se accede por medio de una aplicación externa. Esta metodología se basa en un dispositivo especialmente protegido el cual realiza las operaciones de cifrar y descifrar. Los datos de identificación del paciente están en un lugar separado de los datos de salud del paciente, lo que resulta en la disociación de la identificación y los registros de salud. La relación del registro de identificación y los datos de salud se establece como el seudónimo, cuya unión solo se puede bajo unas condiciones específicas. La relación entre la identificación y los datos de los pacientes se cifran con claves secretas que solo pueden ser utilizados por personas autenticados y autorizados. Los seudónimos también se utilizan para los permisos de acceso a datos compartidos. Para denegar el acceso a los datos lo hace mediante la supresión de estos seudónimos.

En (Alabdulatif, Khalil, y Mai, 2013) [25], se hace un nuevo modelo de control de acceso para cifrar los EHR en la nube, este mecanismo de comunicación sirve como un sistema integrado entre el paciente y el proveedor de servicios de salud. Los solicitantes deben proporcionar toda la información relacionada con sus derechos de acceso, así como los documentos necesarios. La base de datos está diseñada de una manera jerárquica. Esta estructura proporciona un mecanismo de gestión eficiente y permite la distribución segura de claves de cifrado y descifrado para los participantes. Debido a que cada participante en el sistema accede solamente a documentos específicos, en lugar de todos los registros del paciente, se especifica el permiso de cada parte mediante el establecimiento de diferentes claves de cifrado y descifrado para cada grupo de documentos, dependiendo de quien deba tener el acceso a dichos documentos. Cada documento que se produce por cualquier participante deberá incluir los datos del paciente, detalles del proveedor, tipo de documento, categoría y editor de documentos. Esta información, junto con los parámetros

de autenticación que demuestran la elegibilidad del solicitante para cargar y descargar los EHR, será utilizada para permitir el acceso a diferentes EHR en la base de datos.

(CACDS y CPhA, 2009) [26], proponen el uso de la infraestructura de clave pública (PKI) como una solución ideal para hacer frente a las transacciones e integridad de datos; hay dos opciones para la autenticación, y una serie de normas para el enrutamiento seguro. El cifrado asegura la integridad y confidencialidad de una transacción por medio de una operación matemáticamente aleatoria del texto original, de modo que los datos no pueden ser modificados por cualquier persona, excepto por un usuario autorizado. El cifrado utiliza llaves digitales (una combinación única de unos y ceros) que se utilizan para encriptar, descifrar y verificar los datos digitales. El cifrado de datos se puede realizar mediante diversas tecnologías. PKI satisface los requisitos de firma digital, cifrado y la autenticación electrónica de las personas. A través del uso de un par de claves diferentes pero relacionadas entre sí, PKI garantiza que una transacción ha tenido lugar y que las partes de la transacción puedan ser identificadas por sus firmas digitales únicas. Cada usuario tiene una clave privada y una clave pública. La clave privada se mantiene segura, conocida solo por el usuario; la otra llave puede hacerse pública, se envía a través de una red para cada persona de contacto, o se coloca en un directorio publico seguro, casi como el equivalente electrónico de una guía telefónica. La tecnología PKI también utiliza una combinación de algoritmos, protocolos y herramientas derivadas, diseñados para la comunicación segura. Para utilizar este tipo de sistema, el remitente cifra un mensaje con la clave pública del destinatario. Solo la clave privada del destinatario puede descifrar el mensaje. Por lo tanto, la criptografía de clave pública permite la transmisión segura de datos a través de redes abiertas como Internet sin la necesidad de intercambiar previamente una clave secreta. Esto permite a las partes intercambiar y autenticar la información de una manera segura.

Dado que esta tecnología garantiza la confidencialidad, la autenticidad y la validación de las formulas médicas, se recomienda que los PKI deben ser implementados para la transmisión segura de las EHR. La investigación inicial indica que un nivel de seguridad a nivel de PKI ofrece las garantías necesarias a un costo que no es muy alto para su implementación.

En (Calvillo-Arbizu, Roman-Martinez, y Roa-Romero, 2014) [27], hacen hincapié en como los principios de autorización de la norma estándar ISO 13606 influyen en el proceso de autorización, principalmente lo que se refiere a las políticas y la inclusión de niveles de sensibilidad. Para utilizar cualquier otro tipo de sistema de EHR, se deben considerar algunos puntos. Para los sistemas de EHR no normalizados, el proceso relacionado con los atributos de sensibilidad debe ser ignorado, y las políticas tienen que ser recogidas de los proveedores de políticas adecuadas. Para los sistemas de EHR estandarizados, el estándar seguido en cada caso es una característica determinante. Propone la integración de los principios de control de acceso de la norma ISO 13606 estándar y el enfoque XACML.

En (Cankaya y Kywe, 2015) [28], implementan un sistema de EHR que integra la seguridad mediante la incorporación de la criptografía. Cuando un usuario inicia sesión en el sistema, se comprueba en primer lugar el nombre de usuario en la base de datos, si lo encuentra, correspondiente a una contraseña cifrada, se recupera de la base de datos y se descifra. La contraseña introducida por el usuario se compara con la contraseña de descifrado. Si coinciden, la contraseña es válida y el sistema continúa controlando el nivel de permiso del usuario para permitir el acceso apropiado, de lo contrario, el acceso es denegado.
Utiliza un algoritmo de cifrado simétrico AES que se utiliza para cifrar el archivo de registro con el fin de proporcionar la confidencialidad del archivo de registro de terceras partes no deseadas. La razón de uso de AES es doble: una porque es rápido (en comparación con un algoritmo de cifrado asimétrico), y también computacionalmente difícil de romper debido al gran tamaño de la clave (128 bits).

(Chen et al., 2014) [29], propone un esquema de control de acceso novedoso para darse cuenta de la privacidad del paciente centrado en los registros personales de salud en la computación en nube. Teniendo en cuenta los servidores de confianza parcial en la nube, que argumentan que los pacientes deberán tener un control total de su propia intimidad a través de la encriptación de sus archivos EHR multiatributo de autoridad basada en sets para cifrar los datos de EHR, por lo que los pacientes pueden permitir el acceso no solo a los usuarios personales, sino también a varios usuarios de diferentes dominios públicos con diferentes funciones, las calificaciones profesionales y afiliaciones.

(Akinyele et al., 2011) [30], proporciona un diseño y prueba de concepto de autoprotección de la implementación de los EMR mediante el cifrado basado en atributos en los dispositivos móviles. Uno de los retos de diseño de attribute-based encryption (ABE) está en que debe permitir acceder a un usuario a un registro médico. Una de las principales debilidades es la falta de anonimato, ya que el usuario tiene que revelar su identidad al sistema. En un escenario de salud que requiere una respuesta más rápida, la ABE no puede ser un buen procedimiento, debido al tiempo que tarda.

Una síntesis de la información relacionada con la revisión de la literatura de algunos de los autores que realizan investigaciones en proteger los datos electrónicos médicos se muestra en la (Tabla 1-4).

Los criterios que se analizan para los trabajos presentados en este capítulo son los siguientes: (I) utiliza algún tipo de cifrado de datos, (II) presenta alguna forma de protección de identificación de pacientes, (III) plantea algún tipo de método de señuelos para la identificación, (IV) presenta cifrado homomórfico, (V) plantea algún tipo de análisis forense para identificar pistas sobre ataques informáticos y robo de información, (VI) define algún tipo de mecanismo para identificar intrusos, (VII) presenta algún método de acceso compartido, (VIII) plantea algún mecanismo de recuperación de claves.

La (Tabla 1-4) presenta un resumen de los trabajos que utilizan diferentes metodologías orientados a proteger los datos electrónicos médicos sensibles.

Tabla 1-4 Resumen de trabajos

	(I)	**(II)**	**(III)**	**(IV)**	**(V)**	**(VI)**	**(VII)**	**(VIII)**	**Observación**
Neubauer, et al. (2011)	Si	Si	No	No	No	No	Si	No	Presenta una metodología que no plantea seguimiento a incidentes, ni mecanismo de recuperación de claves.
Alabdulatif, et al. (2013)	Si	Si	No	No	No	No	No	No	Presenta una metodología que no plantea seguimiento

	(I)	(II)	(III)	(IV)	(V)	(VI)	(VII)	(VIII)	Observación
									a incidentes, ni mecanismo de recuperación de claves.
CACDS, et al. (2011)	Si	Si	No	No	No	No	No	No	Presenta una metodología que no plantea seguimiento a incidentes, ni mecanismo de recuperación de claves.
Calvillo Arbizu, et al. (2014)	Si	No	No	No	No	No	No	No	Solo plantea un mecanismo de control de acceso.
Cankaya, et al. (2015)	No	Si	No	No	No	No	No	No	Este solo presenta un mecanismo para la protección de los datos.
Chen, et al. (2014)	Si	Si	No	No	No	No	Si	No	Plantea un mecanismo de creación de acceso compartido, pero se evidencia la falta de seguimiento a incidentes y mecanismo de recuperación de claves.
Akinyele, et al. (2011)	Si	Si	No	No	No	No	No	No	Plantea un mecanismo de cifrado de datos, pero este es demasiado lento.

Autor: Construcción propia

1.6 Marco legal en Colombia

La relación más importante de un paciente y su médico es la historia clínica, esto se puede observar claramente en la ley 23 de 1981 en el artículo IV [31], que fundamentalmente dice el compromiso responsable entre las partes es la base fundamental de la relación. En 1981 con la ley 23 y el decreto 3380 unificaron el termino historia clínica [32], en el mismo orden y dirección en el año 1999 con la resolución 1995 se trae a colación las

características de integridad, secuencialidad, disponibilidad, oportunidad, y en el mismo sentido también se habla del acceso a la historia clínica, características, legibilidad. No obstante, el desarrollo e implementación de las tecnologías de información para el sector de salud, se realizó en la resolución 1448 del 2006 [33], la ley 1122 del 2007 [34] y la ley 1438 del 2011 [11], esta última también posteriormente a tener leyes y legislación que formalizan la implementación de TIC en la salud, así mismo, se dicta el uso de las historias clínicas electrónicas a nivel nacional por medio de la ley 1438 del 2011, de modo que en Colombia, de acuerdo con los artículos 112 y 114 de la Ley 1438 de 2011 todas las instituciones del país que presten servicios de salud, deben informar de manera confiable, oportuna y clara toda la información solicitada. Aunque la historia electrónica médica es obligatoria y tuvo como plazo máximo el 31 de diciembre de 2013 de acuerdo a la Ley 1438 de 2011 en su parágrafo transitorio del Articulo 112, no se tiene un dato exacto con respecto a cuantas instituciones de salud lo tienen implementado, esto causa que aunque la historia electrónica médica puede ser usado como elemento probatorio de primer orden si la ley lo requiere, existe una falta de sincronización en cuanto a en manejo de la información sobre pacientes. El eje de estas estrategias es sin duda la información, para lo que se requiere una propuesta de manejo integral, sistemático y sistémico de los datos del sistema de salud, agregando que debe promover una mejor "conectividad" entre las partes interesadas de la atención médica mediante el intercambio oportuno y la presentación de información precisa y pertinente [35]. La historia clínica digital [12] debe existir teniendo en cuenta mecanismos para proteger la privacidad y la seguridad dado que esta información es clasificada, y de alto riesgo no solo a nivel de Colombia [2], sino a nivel internacional y debe tener todas las protecciones legales y tecnológicas que estén enmarcadas en el cumplimiento de las condiciones legales. En este estudio se utilizó la normativa Colombiana y un análisis bibliométrico el cual es una descripción cuantitativa de la literatura y ayuda a medir los patrones de todas las formas de información registrada y sus productores [14], además permite realizar estudios de las tendencias en un tema, formular políticas de desarrollo basadas en las necesidades y proporciona datos objetivos [36].

1.6.1 Lineamientos generales para la gestión de documentos electrónicos en Colombia

En Colombia el Acuerdo No 003 de 2015 del Archivo General de la Nación [37] constituye la forma general en cuanto a la gestión de documentos electrónicos generados, en consecuencia a esto se habla de varios términos, primero de medio electrónico que es un mecanismo tecnológico permite producir, almacenar o transmitir documentos datos o información, seguidamente se habla de que expediente electrónico que su mejor descripción es un conjunto de documentos electrónicos correspondientes a un proceso administrativo, al mismo tiempo se tiene que un archivo electrónico de documentos corresponde a el almacenamiento electrónico de uno o varios documentos, posteriormente se establece que la autenticación electrónica permite la acreditación por medios electrónicos de la identidad de una persona o autoridad, también es necesario decir que un foliado electrónico asocia documento electrónico a un índice electrónico en un mismo expediente electrónico lo cual garantizar su integridad, orden y autenticidad. Finalmente aparecen 3 términos muy importantes autenticidad, integridad y disponibilidad.

1.6.2 Validez probatoria de los documentos electrónicos en Colombia

La validez del documento electrónico [38] se encuentra un alcance definido en la Ley 527 de 1999 [39] en la cual en el artículo 10 otorga la posibilidad y legitima a los sujetos procesales para que dentro de una instancia judicial sea válido la presentación de documentos electrónicos. Los criterios por los cuales se entrará a valorar probatoriamente un mensaje de datos se especifican en el Artículo 11 de la Ley 527 de 1999.

1.6.3 Seguridad y conservación de los documentos electrónicos en Colombia

La administración de los datos electrónicos constituye un elemento clave para que los documentos electrónicos se puedan conservar [40], después de lo anteriormente expuesto debe asegurar su originalidad, además de que se debe garantizar la autenticidad, la integridad, la disponibilidad y confiabilidad necesaria para reproducirlo [41]. En este mismo orden, se debe garantizar que la migración de los documentos electrónicos a otros

formatos debe ser transparente, el acceso y la disponibilidad en el tiempo establecido indicado en el artículo 13 del acuerdo 03 de 2015. Así mismo, la Resolución 1995 de 1999 en el artículo 18, establece que se debe adicionar mecanismos de seguridad que impidan la incorporación de modificaciones, al mismo tiempo, habla que se debe incluir en las aplicaciones, el sistema de registros de usuarios y monitoreo del paciente. Por, sobre todo, se de prohibir el acceso a personal no autorizado para garantizar la historia clínica, inhabilitando el acceso a personal no autorizado para conocerla y adoptando las medidas que se necesiten para evitar la adulteración o destrucción de los registros en forma accidental o provocada.

1.6.4 Estándares, modelos y lineamientos sobre la historia clínica en Colombia

En la actualidad los estándares y de igual manera los lineamientos sobre los datos electrónicos médicos en Colombia fueron dados por el Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC) introduce la Ley 1753 de 2015 [42], la cual ilustra el Plan Nacional de Desarrollo 2014-2018 Todos por un nuevo país, cuyo propósito es definir y estandarizar, modelos, lineamientos y normas técnicas. Como efectos de lo anteriormente expuesto, la historia clínica electrónica debe cumplir con los requisitos pertinentes señalados en la Ley 527 de 1999, la Resolución 1995 de 1999, el Decreto 2364 de 2012 [43], además de la Ley 1753 de 2015 y el artículo 1 de la Ley 1755 de 2015 [44].

1.7 Hipótesis

Con la creación de una metodología integral de protección de datos electrónicos médicos en historias clínicas, se podría proteger los datos electrónicos de la salud.

1.8 Preguntas de investigación

- ¿Cómo se pueden manejar y asegurar las claves?
- ¿Cómo están protegidos los datos electrónicos médicos?

- ¿Cuáles son las tecnologías actuales de seguridad de la información en los datos electrónicos médicos?
- ¿Cómo se puede realizar un análisis forense a los datos electrónicos médicos?
- ¿Cómo se puede cifrar los datos electrónicos médicos?

1.9 Objetivos

1.9.1 General

Proponer una metodología integral de protección de datos electrónicos médicos aplicado al almacenamiento, control de acceso y análisis forense en historias clínicas de Colombia.

1.9.2 Específicos

- Caracterizar los principales procesos de almacenamiento, control de acceso y análisis forense de datos electrónicos médicos en historias clínicas.
- Identificar los factores más relevantes de almacenamiento, control de acceso y análisis forense que hacen vulnerables los datos electrónicos médicos.
- Formular las fases de una metodología integral que interviene en el control de acceso, la integralidad de los datos y un análisis forense básico, para proteger los datos electrónicos médicos en historias clínicas.
- Diseñar un mecanismo para la validación de la metodología propuesta para la protección de los datos electrónicos médicos en historias clínicas.

2. Metodología del desarrollo de la investigación

En este capítulo se busca caracterizar y encontrar los factores más relevantes en los procesos de almacenamiento, control de acceso y análisis forense de datos electrónicos médicos en historias clínicas, cabe aclarar que el Capítulo 1 sirve como apoyo a esta revisión sistemática, la cual ayuda a categorizar las investigaciones existentes sobre la protección de datos electrónicos médicos, específicamente en el almacenamiento, acceso y análisis forense de las historias clínicas; además de identificar los mecanismos de cifrado típicos utilizados en las historias clínicas electrónicas y revelar factores de contexto y medidas para evaluar los softwares de acceso; consecuentemente de identificar la actividad de los usuarios para su uso en algún caso forense. La información obtenida a través de estudios de mapeo sistemático puede ayudar a formular nuevos estudios de investigación o replicar los estudios existentes.

Se realizó un estudio de mapeo sistemático [45] sobre investigaciones realizadas acerca de la protección de datos electrónicos médicos específicamente en el almacenamiento, acceso y análisis forense de las historias clínicas electrónicas. El objetivo del mapeo sistemático es caracterizar los estudios existentes que exploran los mecanismos para la protección de datos electrónicos médicos específicamente en el almacenamiento, acceso y análisis forense de las historias clínicas electrónicas.

Se definieron las siguientes preguntas de investigación para guiar nuestro estudio de mapeo:

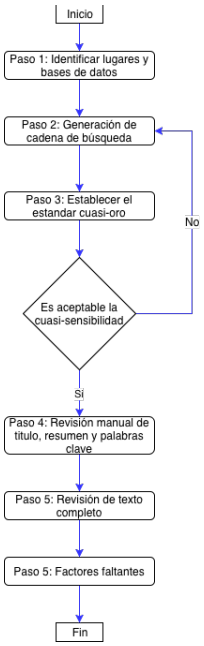
- ¿Cuáles son las técnicas de cifrado de datos que utilizan con más frecuencia los sistemas de historias clínicas?
- ¿Qué tipos de técnicas de control de acceso tienen los sistemas de historias clínicas?
- ¿Qué eventos deberían ser capturados por los mecanismos de registro para un análisis forense de cuentas de los usuarios?

- ¿Qué técnicas existen para evaluar los mecanismos de registro de software para para un análisis forense de cuentas de los usuarios?

2.1 Caracterización

En la caracterización de los procesos de almacenamiento, control de acceso y análisis forense de datos electrónicos médicos en historias clínicas, se basa en la realización de un mapeo sistemático planteado por Petersen [46], por lo tanto, se siguieron algunos de los pasos representados en el proceso dado en el trabajo de Zhang [47] para la identificación de documentos relevantes. En la (Figura 2-1) se muestra la versión del proceso modificada para el objeto de este trabajo. En primer lugar, se identifican las bases de datos para buscar estudios relevantes. A continuación, se establece un estándar cuasi-oro a través de una búsqueda manual. Además, se generan las cadenas de búsqueda basadas en el análisis de palabras clave de los artículos estándar cuasi-oro [46]. Luego, se realizó una búsqueda automatizada utilizando las cadenas de búsqueda obtenidas. Dicho lo anterior se evaluó el desempeño de búsqueda, finalmente se aplicaron criterios de inclusión / exclusión a nuestros resultados de búsqueda para identificar los documentos relevantes.

Figura 2-1 Flujo del proceso de mapeo sistemático



Autor: Figura tomada y adaptada de Petersen [54]

2.2 Identificación de lugares y bases de datos

Para seleccionar posibles lugares (por ejemplo, conferencias o revistas) con documentos relevantes, primero recopilamos un conjunto de lugares relevantes de tres organizaciones primarias de ciencias de la computación: La Asociación para la Maquinaria Informática (ACM), El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) y ELSEVIER. Se recopilaron el conjunto completo de lugares para cada organización utilizando el índice de lugares y calendario de eventos publicado por la organización. Para incluir un lugar relevante para el estudio se usaron los siguientes criterios:

- El nombre del lugar está relacionado con la protección de los datos electrónicos médicos; o
- El nombre del lugar se refiere a seguridad, privacidad, acceso, cifrado y / o forense de los datos electrónicos médicos; o
- El lugar es importante en ingeniería de software y además está relacionado con la salud.

La (Tabla 2-1) resume el número de lugares incluidos recogidos de cada organización.

Tabla 2-1 Resumen del número de lugares incluidos

Organización	Lugares incluidos
ACM	1
China Institute of Communication	1
Commonwealth Fund	1
Pontificia Universidad Javeriana	1
Elsevier	6
ScienceDirect	7
IEEE	16

Autor: Construcción propia

Se usaron las bases de datos más comunes para revisar sistemáticamente la literatura (SLR) de acuerdo con las directrices para identificar los estudios pertinentes [47]:

- Elsevier
- ScienceDirect
- ACM Digital Library

- IEEE Xplore

2.3 Búsqueda automatizada

Se implementó la búsqueda automatizada utilizando un enfoque de definición subjetiva, en el cual las cadenas de búsqueda fueron construidas sobre la base de los conocimientos de los autores, y su observación de los artículos incluidos en el estándar cuasi-oro. Intuitivamente se inició la búsqueda automatizada con la cadena.

(EHR OR Electronic Health Record) AND (Encryption) AND (access control) AND audit

Una vez que tenemos una cadena de consulta de búsqueda, abrimos cada base de datos (IEEE Xplore, ACM, ScienceDirect) e ingresamos la cadena de consulta de búsqueda para realizar la búsqueda automatizada.

Se identificaron 83 publicaciones más relevantes para incluirlas en el estándar cuasi-oro. En la (Tabla 2-2) se muestra el lugar y cuantos artículos fueron incluidos.

Tabla 2-2 Resumen de los lugares relevantes y número de artículos escogidos

Lugar	Organización	Artículos
ACM Computing Surveys	ACM	1
China Communications	China Institute of Communication	1
Issue brief (Commonwealth Fund)	Commonwealth Fund	1
Decision Support Systems	Elsevier	2
Computer Methods and Programs in Biomedicine	Elsevier	3
Computers in Biology and Medicine	Elsevier	2
Health Policy	Elsevier	1
International Journal of Medical Informatics	Elsevier	33
Health Policy and Technology	Elsevier	4

Lugar	Organización	Artículos
Journal of Biomedical and Health Informatics	IEEE	1
IEEE Symposium on Security and Privacy	IEEE	3
Proceedings of the Annual Hawaii International Conference on System Sciences	IEEE	3
Proceedings - IEEE Symposium on Computer- Based Medical Systems	IEEE	1
2011 IEEE 13th International Conference on e- Health Networking, Applications and Services	IEEE	1
2009 3rd IEEE International Conference on Digital Ecosystems and Technologies	IEEE	1
2010 6th International Conference on Information Assurance and Security, IAS 2010	IEEE	1
2010 International Conference on Biomedical Engineering and Computer Science	IEEE	1
Proceedings - 2012 4th International Conference on Multimedia and Security, MINES 2012	IEEE	1
Proceedings - 2012 IEEE 2nd Conference on Healthcare Informatics, Imaging and Systems Bio- logy, HISB 2012	IEEE	1
Proceedings - International Carnahan Conference on Security Technology	IEEE	1
2010 IEEE International Symposium on. A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)	IEEE	1
2012 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2012	IEEE	1
2015 10th Colombian Computing Conference, 10CCC 2015	IEEE	1
2014 IEEE-EMBS International Conference on Biomedical and Health Informatics, BHI 2014	IEEE	1

Lugar	Organización	Artículos
Proceedings - 2014 IEEE 13th International Symposium on Network Computing and Applications, NCA 2014	IEEE	1
Revista Gerencia y Políticas de Salud	Pontificia Universidad Javeriana	1
Knowledge-Based Systems	ScienceDirect	1
Procedia Computer Science	ScienceDirect	4
Journal of Network and Computer Applications	ScienceDirect	1
Journal of Biomedical Informatics	ScienceDirect	3
Journal of Visual Communication and Image Re-presentation	ScienceDirect	1
Electronic Commerce Research and Applications	ScienceDirect	1
Procedia Technology	ScienceDirect	3
	Total	**83**

Autor: Construcción propia

2.4 Estándar cuasi-oro

El concepto de "patrón cuasi-oro" utilizado en el trabajo de Petersen [46], es un conjunto de estudios conocidos de lugares relacionados, por ejemplo, conferencias y revistas específicas de dominio reconocidas por la comunidad en el tema, durante un período de tiempo determinado.

2.5 Revisión manual de título, resumen y palabras clave

Se revisaron manualmente el título, el resumen y las palabras clave de todos los trabajos hechos en estos lugares de publicaciones y voto para incluir publicaciones basadas en los siguientes criterios de inclusión:

- La publicación esta entre los años 1999 y 2015.

- El título de la publicación, el resumen o las palabras clave se refieren a la protección de los datos electrónicos médicos; o
- El título de la publicación, el resumen o las palabras claves están relacionados con la salud; o
- El título de la publicación, el resumen o las palabras clave se refieren seguridad, privacidad, acceso, cifrado y / o forense de los datos electrónicos médicos.

En total, 73 publicaciones fueron consideradas como relevantes sobre la base de nuestros criterios de inclusión. La (Tabla 2-3) presenta las publicaciones relevantes para el estándar cuasi-oro.

Tabla 2-3 Resumen de las publicaciones cuasi-oro

Nombre	Acrónimo	Lugar	Año
6 Privacy in the Genomic Era [48]	CSUR	ACM	2015
Securing patient-centric personal health records sharing system in cloud computing [29]	CC	China Institute of Communication	2014
A Secure and Flexible e-Health Access Control System with Provisions for Emergency Access Overrides and Delegation of Access Privileges [49]	CC	China Institute of Communication	2016
Electronic health records: an international perspective on ”meaningful use” [50]	IB	Commonwealth Fund	2011
Information systems in health sector in Colombia [51]	RGPS	Pontificia Universidad Javeriana	2008
Security in healthcare information systems–current trends. [52]	IJMI	Elsevier	1999
An open, component-based information infrastructure for integrated health information networks [53]	IJMI	Elsevier	2002

Nombre	Acrónimo	Lugar	Año
Risk analysis of information security in a mobile instant messaging and presence system for healthcare [54]	IJMI	Elsevier	2007
Definition, structure, content, use and impacts of electronic health records: A review of the research literature [19]	IJMI	Elsevier	2008
XML technologies for the Omaha System: A data model, a Java tool and several case studies supporting home healthcare [55]	CMPB	Elsevier	2009
Strategies for health data exchange for secondary, cross institutional clinical research [56]	CMPB	Elsevier	2010
Transforming healthcare with information technology in Japan: A review of policy, people, and progress [45]	IJMI	Elsevier	2011
A methodology for the pseudonymization of medical data [24]	IJMI	Elsevier	2011
Online detection of potential duplicate medications and changes of physician behavior for outpatients visiting multiple hospitals using national health insurance smart cards in Taiwan [57]	IJMI	Elsevier	2011
Aspects of privacy for electronic health records [58]	IJMI	Elsevier	2011
Physicians' potential use and preferences related to health information Exchange [59]	IJMI	Elsevier	2011
Medical record search engines, using pseudonymized patient identity: An	IJMI	Elsevier	2011

Nombre	Acrónimo	Lugar	Año
alternative to centralized medical records [60]			
EHRs connect research and practice: Where predictive modeling, artificial intelligence, and clinical decision support intersect [61]	HPT	Elsevier	2012
A decision methodology for managing operational efficiency and information disclosure risk in healthcare processes [62]	DSS	Elsevier	2014
Optimal information security investment in a Healthcare Information Exchange: An economic analysis [63]	DSS	Elsevier	2014
A general framework for interoperability with applications to healthcare [64]	HPT	Elsevier	2014
An empirical study of healthcare providers and patients' perceptions of electronic health records [65]	CBM	Elsevier	2015
A novel fuzzy logic-based image steganography method to ensure medical data security [66]	CBM	Elsevier	2015
Anytime, anywhere access to secure, privacy-aware healthcare services: Issues, approaches and challenges [67]	HPT	Elsevier	2015
Analysis of health professional security behaviors in a real clinical setting: An empirical study [68]	IJMI	Elsevier	2015
Electronic health records, adoption, quality of care, legal and privacy issues	HP	Elsevier	2015

Nombre	Acrónimo	Lugar	Año
and their implementation in emergency departments [69]			
The disconnect between healthcare provider tasks and privacy requirements [70]	HPT	Elsevier	2016
A methodology based on open EHR archetypes and software agents for developing e-health applications reusing legacy systems [71]	CMPB	Elsevier	2016
Pseudonymization for improving the privacy in e-health applications [72]	HICSS	IEEE	2008
Securing an EHR in a health sector digital ecosystem [73]	DEST	IEEE	2009
Credential based hybrid access control methodology for shared Electronic Health Records [74]	ICIME	IEEE	2009
A semantic based methodology to classify and protect sensitive data in medical records [75]	IAS	IEEE	2010
Security and privacy for mobile electronic health monitoring and recording systems [76]	WOWMOM	IEEE	2010
Security Design for Electronic Medical Record Sharing System [53]	ICBECS	IEEE	2010
Pseudonymization with metadata encryption for privacy-preserving searchable documents [77]	HICSS	IEEE	2011
Secure and reliable distributed health records: Achieving query assurance across repositories of encrypted health data [78]	HICSS	IEEE	2011

Nombre	Acrónimo	Lugar	Año
Secure Solution for Mobile Access to Patients Health Care Record [79]	HEALTHCOM	IEEE	2011
RBTBAC: Secure Access and Management of EHR Data [80]	IE	IEEE	2011
Information security of EHRs [81]	MINES	IEEE	2012
Privacy-preserving biometric system for secure fingerprint authentication [82]	HISB	IEEE	2012
Impacts of legislation on electronic health records systems and security implementation [83]	LISAT	IEEE	2012
Multiparty Privacy Protection for Electronic Health Records [84]	GLOBECOM	IEEE	2013
Privacy Handling for Critical Information Infrastructures [85]	GEN	IEEE	2013
Security issues for data sharing and service interoperability in eHealth systems: The Nu.Sa. test bed [86]	ICCST	IEEE	2014
Standardized access control mechanisms for protecting ISO 13606-based electronic health record systems [27]	BHI	IEEE	2014
Health records protection in cloud environment [87]	NCA	IEEE	2014
Integrated Modeling and Analysis of Attribute Based Access Control Policies and Workflows in Healthcare [88]	ICTSTA	IEEE	2014
Securing Patient Privacy in E-Health Cloud Using Homomorphic Encryption and Access Control [22]	IJCN	IEEE	2014

Nombre	Acrónimo	Lugar	Año
Privacy and access control for outsourced personal records [89]	S&P	IEEE	2015
GenoGuard: Protecting genomic data against brute force attacks [90]	S&P	IEEE	2015
Cracking-resistant password vaults using natural language encoders [91]	S&P	IEEE	2015
Privacy threats and practical solutions for genetic risk tests [92]	S&P	IEEE	2015
Secure and private management of healthcare databases for data mining [93]	CBMS	IEEE	2015
Historia Clinical Electronica como Servicio de Software en la Nube [94]	CCC	IEEE	2015
A Biometric Based Authentication and Encryption Framework for Sensor Health Data in Cloud [95]	ICIMU	IEEE	2015
A secure revocable personal health record system with policy-based fine-grained access control [96]	PST	IEEE	2015
Authentication and Access Control in e-Health Systems in the Cloud [97]	BigData	IEEE	2016
Security of MBAN based health records in mobile broadband environment [98]	PCS	ScienceDirect	2011
e-Health Cloud: Opportunities and Challenges [41]	FI	ScienceDirect	2012
Security and privacy in electronic health records: A systematic literature review [99]	JBI	ScienceDirect	2013
Security Challenges and Success Factors of Electronic Healthcare System [100]	PT	ScienceDirect	2013

Nombre	Acrónimo	Lugar	Año
Improving Information Security Behaviour in the Healthcare Context [101]	PT	ScienceDirect	2013
Private predictive analysis on encrypted medical data [102]	JBI	ScienceDirect	2014
Internet of Things and Smart Objects for health Monitoring and Control [103]	PT	ScienceDirect	2014
Trust assessment of security for e-health systems [104]	ECRA	ScienceDirect	2014
A semantic authorization model for pervasive healthcare [105]	JNCA	ScienceDirect	2014
Private Predictive Analysis on Encrypted Medical Data[102]	JC	ScienceDirect	2014
Antecedents of health information privacy concerns [106]	PCS	ScienceDirect	2015
A Secure Healthcare System: From Design to Implementation [28]	PCS	ScienceDirect	2015
An integrated framework for securing semi-tructured health records [17]	KBS	ScienceDirect	2015
Increasing EHR system usability through standards: Conformance criteria in the HL7 EHR-system functional model [107]	JBI	ScienceDirect	2016
Issues in Achieving Complete Interoperability while Sharing Electronic Health Records [108]	PCS	ScienceDirect	2016
Reversible Data Hiding in Paillier Cryptosystem [109]	JVCIR	ScienceDirect	2016

Autor: Construcción propia

2.6 Revisión de texto completo

Posterior a lo definido anteriormente, se realizó interpretación de los textos completos de las 73 publicaciones antes filtradas y así determinar si la publicación debería estar en el estándar cuasi-oro. Para poder ser incluidas en el estándar cuasi-oro, se usaron los siguientes criterios de inclusión por cada uno de los temas tratados en esta tesis:

Tabla 2-4 Criterios de inclusión

Control de acceso
1. La publicación se centra en presentar alguna forma de protección de identificación de pacientes.
2. La publicación se centra en plantear algún tipo de método de ser señuelos para la identificación.
3. La publicación se centra en presenta algún método de acceso compartido.
4. La publicación se centra en plantear algún mecanismo de recuperación de claves.
Cifrado de datos
1. La publicación se centra en utilizar algún tipo de cifrado de datos.
2. La publicación presenta cifrado homomórfico.
3. La publicación se centra en utilizar cifrado biométrico.
4. La publicación se centra en utilizar Seudónimos.
5. La publicación se centra en utilizar cifrado multiparte.
6. La publicación presenta cifrado basado en atributo.
Análisis forense
1. La publicación se centra en plantear algún tipo de análisis forense para identificar pistas sobre ataques informáticos y robo de información.
2. La publicación se centra en definir algún tipo de mecanismo para identificar intrusos.
3. La publicación tiene algún mecanismo de auditoria de logs.

Autor: Construcción propia

Del mismo modo, se excluyeron las publicaciones de nuestro estándar cuasi-oro sobre la base de los siguientes criterios:

- La publicación se centra en registros de consultas.
- La publicación se centra en los registros de la red.
- La publicación se centra en el proceso financiero o de auditoría.
- La publicación no está escrita en inglés o español.

2.7 Resultados

- **Control de acceso**

En los artículos proponen el uso de un esquema de firma digital basado en PKI. Otros mecanismos de acceso presentados en los estudios son: nombre de usuario y contraseña, y con diferentes variaciones como con certificado digital PIN, tarjeta inteligente y huella digital.

La asociación a la clasificación de los criterios de inclusión tratados está en la tabla (Tabla 2-4)

Tabla 2-5 Control de acceso

Control de acceso					
Articulo	**Año**	**1**	**2**	**3**	**4**
Credential based hybrid access control methodology for shared Electronic Health Records	2009				
RBTBAC: Secure Access and Management of EHR Data	2011				
Integrated Modeling and Analysis of Attribute Based Access Control Policies and Workflows in Healthcare	2014				
Securing Patient Privacy in E-Health Cloud Using Homomorphic Encryption and Access Control	2014				
Authentication and Access Control in e-Health Systems in the Cloud	2016				
A Secure and Flexible e-Health Access Control System with Provisions for Emergency Access Overrides and Delegation of Access Privileges	2016				

Autor: Construcción propia

Un total de 6 artículos utilizan modelos de control de acceso, de los cuales la mayoría hablan de RBAC que es, por lo tanto, el modelo de control de acceso por excelencia. Cada uno de los usuarios que acceden al sistema tiene un rol que define sus permisos y restricciones. M. Fahim et al. [49] Establece un sistema de control de acceso seguro y flexible para la salud electrónica, en el cual se modelan las funciones y permisos mediante el control de acceso basado en roles (RBAC), e implementan una "emergencia" como un contexto o atributo sobre la base RBAC para tomar la decisión de acceso final; además utiliza los estándares HL7 para definir las funciones y privilegios de RBAC. Para la delegación de privilegios de acceso, se basa en un marco para la creación, transferencia y verificación de una delegación-token, aprovechando la arquitectura de seguridad eTRON y eTNet. La arquitectura eTRON implementa la criptografía de clave pública donde los certificados son proporcionados por la autoridad de certificación eTRON. Para entregar la delegación de derechos de acceso, utiliza un enfoque basado en DAC (control de acceso discrecional) para implementar una delegación-token que se transferirá al delegado a través de la arquitectura eTNet, que es una red superpuesta de dispositivos eTRON que incluye tarjetas inteligentes que permiten que las transacciones electrónicas se ejecuten de forma segura a través de Internet, sin tener que depender de ningún servidor autorizado centralmente. La autenticación mutua eTRON se realiza mediante un protocolo de respuesta de desafío que utiliza criptografía de clave pública. Después de una autenticación exitosa, se crea una sesión para compartir una clave segura mediante el algoritmo Diffie-Hellman. En la arquitectura eTRON, esta sesión se establece en dos fases: generación de claves y confirmación de claves. El proceso de control de acceso se realiza de la siguiente forma: Lo primero es que se crea el token de delegación que contiene el ID de token, fecha de inicio, fecha de finalización y, opcionalmente, nombre del delegador. Las fechas de inicio y fin indican el período de validez del token. Después de haber creado el token se hace la transferencia de la tarjeta eTRON del delegador a la tarjeta eTRON del delegado. Una vez realizada la transferencia, se cierra la sesión y se crea una transacción que se define como una sesión con función de retroceso, la cual garantiza que el sistema volverá al estado consistente anterior en caso de cualquier problema con conectividad o dispositivo periférico durante la transferencia de una delegación-token. Por último, se establece una sesión entre el delegado y el verificador en la cual se revisa que el token sea emitido por un usuario autorizado (registrado con eTRON) y además que el token no haya caducado (como indica el intervalo de validez escrito en el token). Sandeep Lakkaraju et al. [88] Integra las políticas de ABAC con los flujos de trabajo (cadena de actividades

que se ejecutan para realizar ciertas tareas en cierto orden) de las organizaciones. La metodología propuesta contempla las actividades del flujo de trabajo en términos de sujeto, recurso, acción y entorno. Aderonke Justina et al. [22] Propone sistema de privacidad basado en la nube en el cual se utiliza el cifrado homomórfico y el control de acceso (SECHA). SECHA comprende cinco componentes básicos: Paciente, PHR, Módulo de Control de Acceso, Usuario y Nube. La PHR se almacena en la nube, y se puede acceder a través de un portal web por múltiples propietarios y usuarios. El paciente que es el propietario del PHR lo cifra y almacena el texto cifrado en el servidor de la nube. Cuando se realiza una solicitud de acceso, primero se verifica la política asociada con el objeto solicitado para ver si el solicitante (usuario) tiene la clave requerida o no. Si el solicitante tiene la clave correcta, se comprueban las reglas dentro de las políticas para obtener restricciones adicionales para aprobar o denegar la solicitud de acceso. Un Cifrado Homomórfico es la conversión de datos en texto cifrado que puede ser analizado y trabajado como si todavía estuviera en su forma original. El cifrado homomórfico juega un papel importante en el cloud computing, permitiendo a los pacientes almacenar archivos PHR cifrados en una nube pública y aprovechar los servicios analíticos del proveedor de la nube. El plan impide que los intrusos violentos violen la privacidad y previene la fuga accidental de información privada. Los sistemas de cifrado homomórfico se utilizan para realizar operaciones en datos cifrados sin conocer la clave privada (es decir, sin descifrado), el cliente es el único titular de la clave secreta. Cuando el resultado de la operación es descifrado, es igual que si hubiera realizado el cálculo en los datos brutos.

Nirmal Dagdee et al. [74] habla de un sistema híbrido que utiliza tres categorías de credenciales: credenciales estándar, credenciales de identidad y credenciales de autorización para definir reglas de control de acceso. Cada categoría de credenciales contiene un ID de credencial único que lo distingue de otras dos categorías de credenciales. La credencial estándar propuesta contiene el nombre y valor de uno o más atributos asociados con esta credencial, información de autenticación del propietario como su clave pública y la firma digital de la compañía que registró la credencial; puede ser utilizada con múltiples fuentes de datos. La credencial de identidad contiene Id de categoría, número de serie, nombre de compañía, fecha de emisión y período de caducidad o validez, Información de identidad del propietario conocida por el sistema y firma digital de la compañía, tal como se conoce en el origen de datos. Por lo tanto, se supone que la credencial de identidad suele ser emitida por el propietario de la fuente de datos. La credencial de autorización es un documento digital que describe un permiso del

emisor para usar un servicio o un recurso que el emisor controla. Contiene la Identificación de la categoría, número de serie, nombre de la compañía, fecha de emisión y período de validez o de expiración, entidad en la que se debe definir la autorización, tipo de acceso en la entidad y firma digital de la compañía.

Nafiseh Kahani et al. [97] habla de asignar y limitar los derechos de los usuarios basandose en los roles. Proporciona privacidad de datos a través de técnicas de cifrado mientras se habilita la búsqueda sobre datos cifrados. Para establecer una comunicación segura entre las entidades que interactúan, utiliza una combinación de una clave pública del sistema y una clave de sesión secreta generada por un esquema Derive Unique Key Per Transaction (DUKPT). En este método, la clave de sesión cambia en cada sesión, lo que refuerza la seguridad de la conexión. Por lo tanto, si una clave derivada se ve comprometida, los datos transmitidos futuros y pasados permanecen protegidos, ya que las claves siguiente y anterior no pueden determinarse.

Rui Zhang et al. [80] Propone el modelo RBTBAC (Control de acceso basado en roles y tiempo limitado), el cual integra la dimensión temporal en el control de acceso basado en roles de datos EHR sensibles, permitiendo a los pacientes y profesionales de la salud personalizar el control de acceso de los datos EHR en diferentes granularidades espaciales y temporales de preferencia.

- **Cifrado de datos**

Solo 9 artículos que presentan técnicas como la de pseudo anonimato, que permite a terceros acceder a los datos de salud de los pacientes sin revelar los datos personales de los pacientes. De estos, nueve estudios proponen recopilar todos los datos de HCE de un paciente con un identificador de paciente hash.

La asociación a la clasificación de los criterios de inclusión tratados está en la tabla (Tabla 2-4)

Tabla 2-6 Cifrado de datos

Cifrado de datos							
Articulo	**Año**	**1**	**2**	**3**	**4**	**5**	**6**
A methodology for the pseudonymization of medical data	2010						

Cifrado de datos							
Articulo	**Año**	**1**	**2**	**3**	**4**	**5**	**6**
Strategies for health data exchange for secondary, cross institutional clinical research	2010	■				■	
Secure Solution for Mobile Access to Patient's Health Care Record	2011	■				■	
Multiparty Privacy Protection for Electronic Health Records	2013	■		■			
A Biometric Based Authentication and Encryption Framework for Sensor Health Data in Cloud	2014		■				
Private Predictive Analysis on Encrypted Medical Data	2014	■					
A secure revocable personal health record system with policy-based fine-grained access control	2015	■					
GenoGuard: Protecting Genomic Data against Brute-Force Attacks	2015	■				■	
Anytime, anywhere access to secure, privacy-aware healthcare services: Issues, approaches and challenges	2015	■					■

Autor: Construcción propia

Thomas Neubauer et al. [24] Propone una metodología PIPE para la seudinimización de datos médicos en la que se almacena los datos de salud desvinculados de la información de identificación del paciente, permitiendo el uso secundario de los registros de salud en estudios clínicos sin necesidad de anonimizar los pacientes. La pseudonimización es donde los datos de identificación se transforman y luego son reemplazados por un especificador que no puede ser asociado con los datos de identificación sin conocer un cierto secreto. Además, permite que los datos se asocien con un paciente sólo bajo circunstancias específicas y controladas. Jelena Mirkovic et al. [79] Propone una autenticación a una aplicación móvil por medio de un número PIN que el usuario sabe y establece un segundo canal de comunicación en el cual se cifra un código de seguridad construido en el dispositivo móvil basado en el código PIN del usuario, el IMEI del dispositivo y la referencia de la sesión del usuario; además se añade un factor de autenticación adicional mediante el envío de un mensaje de texto SMS de activación. Así

el usuario está protegido contra perder su dispositivo móvil, su tarjeta SIM o comprometer el número PIN secreto. Xun Yi ed al. [84] Propone un sistema de control de acceso en el que múltiples servidores gestionan conjuntamente una base de datos de EHR. Los servidores generan y publican conjuntamente una clave pública común. Cada EHR se cifra mediante la clave pública común y se almacena en la base de datos. Los EHR cifrados sólo pueden descifrarse mediante la cooperación de todos los servidores. Al igual que DABE, el modelo asume que varios servidores cooperan para proporcionar servicios. A diferencia de DABE, este modelo se basa en el umbral ElGamal cifrado homomórfico en lugar de la idea de ABE. Además, utiliza la PKI para el manejo de claves públicas y por lo tanto facilita el registro y la revocación del clínico.

Surender Sharma ed al. [95] Propone la autenticación biométrica y servidor de cifrado para la nube (BaesC), el cual, a diferencia de las técnicas criptográficas existentes, no requiere proteger o administrar una clave de descifrado, ya que las características biométricas del individuo pueden funcionar como una clave de descifrado. Los datos sensibles deben ser protegidos y ser accesibles sólo por el usuario autorizado, incluso en el almacenamiento compartido o en la nube. Debido a que los datos biométricos no son digitales y ruidosos por naturaleza, se capturan múltiples variantes de identidad biométrica para tolerancia al ruido, de modo que cualquier derivado escaneado sea similar a la identidad biométrica en vivo del usuario y no pueda ser falsificado. El ruido en los datos biométricos de huellas dactilares es una variación aleatoria de las imágenes capturadas que se utilizan para generar una plantilla biométrica Bt. Una plantilla biométrica es una representación digital de las características distintas de un individuo que se han extraído de una identidad, es decir, datos obtenidos por un dispositivo de captura de un sistema de lectura electrónica, tal como un escáner de huella dactilar. Estás plantillas se utilizan durante el proceso de autenticación biométrica. Utiliza el esquema extractor primitivo fuzzy, introducido por primera vez por Jules et al. Los extractores difusos se utilizan para convertir datos de huellas dactilares escaneadas en cadenas aleatorias y cadena auxiliar que hace posible aplicar técnicas criptográficas. Sin extractores difusos, la biometría se puede utilizar para la autenticación, pero no para el cifrado. La Bt procesado con la cadena aleatoria y el algoritmo de seguridad SHA-2 genera una clave de cifrado biométrico asimétrico. El algoritmo SHA-2 proporciona una mejor protección contra ataques criptográficos, como ataques de colisión.

Joppe W. Bos ed al. [102] Presenta una implementación funcional de un servicio en la nube que demuestra una aplicación de algoritmos de predicción externalizados en datos

médicos cifrados y confidenciales. El algoritmo predice la posibilidad de tener un ataque al corazón basado en unas pocas mediciones del cuerpo. La aplicación cliente recopila datos de salud del usuario, lo cifra y envía el registro cifrado homomorficamente a la aplicación de nube, que ejecuta el algoritmo de predicción en el registro cifrado. La nube produce un resultado de predicción cifrado, que devuelve a la aplicación cliente. El usuario puede entonces descifrar y aprender la probabilidad de tener un ataque al corazón.

Mitu Kumar Debnath ed al. [96] Propone un control de acceso de grano fino y administración eficiente de claves al mismo tiempo. Utiliza el esquema mCP-ABE en el cual la clave secreta del usuario se divide en dos partes. Una parte de la clave secreta va al usuario y otra parte va al servidor de revocación. Para descifrar los datos de EHR el usuario tiene que obtener el token de descifrado del servidor de revocación.

El esquema de cifrado basado en atributos de políticas de cifrado (mCP-ABE) extiende el esquema CP-ABE con mecanismo de revocación instantánea. En este esquema las claves secretas de usuario están asociadas con conjuntos de atributos, mientras que los textos cifrados están asociados con las políticas. Generalmente, CP-ABE consta de cuatro procedimientos: Setup, Encrypt, KeyGen y Decrypt, mientras que mCP-ABE incluye un procedimiento más, que es m-Decrypt. Sin embargo, los procedimientos de configuración y cifrado son iguales que el esquema CP-ABE original.

- **Análisis forense**

En esta búsqueda solo se encontraron 3 artículos que referencia lo importante incluir registros de auditoría, además de que creen que es importante incluir registros de auditoría.

La asociación a la clasificación de los criterios de inclusión tratados está en la tabla (Tabla 2-4)

Tabla 2-7 Análisis forense

Análisis forense				
Articulo	**Año**	**1**	**2**	**3**
e-Health Cloud: Opportunities and Challenges	2012			
Privacy Handling for Critical Information Infrastructures	2013			

Anytime, anywhere access to secure, privacy-aware healthcare services: Issues, approaches and challenges	2015			

Autor: Construcción propia

Estos registros incluían información sobre quiénes [67] acceden a HME, con qué objetivo y limitando tiempo de las acciones, además afirman que los registros de auditoría deben ser accesibles y comprensibles para el paciente. El registro de auditoría también se utiliza para cumplir con la HIPAA y las leyes existentes para prevenir o descubrir posibles abusos más tarde y el uso indebido de mecanismos de excepción y para definir mejores políticas de acceso. Algunos autores [41] abogan por que los registros de auditoría deben ser accesibles y comprensibles para los pacientes.

Los pacientes deben tener información relacionada con la creación del registro, las instancias específicas de cómo se utiliza el registro, el proceso o procesos por los cuales el registro se actualiza y, finalmente, se elimina. En el caso de un flujo de información no deseado, los pacientes pueden identificar la fuente de datos o la fuga. Cuando un médico inicia un procedimiento de romper el cristal en situaciones de emergencia, los datos de ese médico (nombre, identificador nacional del proveedor, nombre de la organización de atención médica) se copian de la tarjeta del médico en el registro de auditoría de la tarjeta médica del paciente. Zhang y Liu [110] proponen mantener un registro de cada acceso y modificación de los datos en su modelo de referencia de seguridad EHR para gestionar los problemas de seguridad en las nubes de atención médica.

2.8 Limitaciones

Este estudio puede tener varias limitaciones entre las cuales están:

- Para el proceso de selección de las fuentes de información y artículos se organizó una búsqueda manual de varias bases de datos. Cabe aclarar que la cadena de búsqueda no haya incluido palabras que hubieran seleccionado otros estudios relevantes.
- Para esta tesis se limitó el rango de idiomas de los artículos solo a inglés y español, lo que significa que estos resultados deben considerarse dentro del alcance de la literatura de estos 2 idiomas.

- Solo se ha trabajado con estudios publicados en el tiempo de desarrollo de la tesis.
- Los criterios de evaluación utilizados podrían no haber sido apropiados.

2.9 Conclusiones

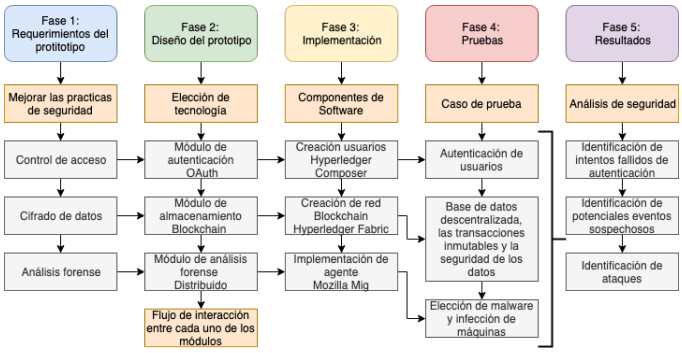
Los datos electrónicos médicos por su naturaleza digital permiten la transferencia entre las partes interesadas y autorizadas, todo esto con el fin de mejorar la calidad de la atención médica. Pero según los antecedentes vistos, las preocupaciones de privacidad y seguridad son altamente importantes, dado que el paciente puede encontrar serios problemas si se filtra su información confidencial. Ante la situación planteada, se han identificado y analizado aspectos críticos de privacidad y seguridad de los datos electrónicos médicos, con una muestra de 73 artículos de investigación. Con base a los artículos en la revisión, y a los 3 tópicos analizados, podemos concluir lo siguiente:

- Cifrado de datos: Se han propuesto varios algoritmos de encriptación. Es conveniente la implementación de un esquema de cifrado de datos eficiente que permita ser usado tanto para los pacientes como para el personal de las entidades prestadoras de salud, que permita escalabilidad para incluir nuevos registros y que el acceso a las llaves de cifrado sea restringido.
- Control de acceso: Con respecto a la forma preferida para controlar el acceso en sistemas de salud está el RBAC. Por preferencia los mecanismos de autenticación más usados son los de firma digital basados en PKI y los inicios de sesión / contraseñas.
- Análisis forense: Se observó que la auditoría es particularmente útil para identificar accesos sospechosos y prácticas de acceso comunes. Sin embargo, se reconoce que deben implementarse mejores controles y herramientas que permitan hacer esta tarea de una forma distribuida y más automática.

3. Metodología integral de protección de datos electrónicos médicos, aplicado al almacenamiento, acceso y análisis forense de las historias clínicas en Colombia

Dadas las condiciones que se anteceden a este capítulo se desarrolla toda la metodología propuesta para poder mitigar todos los hallazgos encontrados en la investigación, para ilustrar los principales inconvenientes que posee la propiedad de los datos del usuario y el alto costo de implementar y operar los sistemas de información. Las principales razones detrás de estos inconvenientes son la arquitectura cliente-servidor adoptada por las entidades prestadoras de salud. Por lo tanto, con la arquitectura cliente-servidor, los datos del usuario se guardan en los servidores centrales, las entidades prestadoras de salud tienen acceso total a estos datos que pueden monitorear, rastrear, filtrar y controlar a su voluntad. Esto se traduce en las posibles vulnerabilidades de datos de los usuarios y el fraude. Por lo tanto, aunque los datos pertenecen al usuario, finalmente es controlado por las entidades prestadoras de salud, lo cual es uno de los temas cruciales de la privacidad y la seguridad de los datos. La (Figura 3-1) muestra las fases de este capitulo.

Figura 3-1 Fases de la metodología



Autor: Construcción propia

3.1 Necesidades del prototipo

Como se describe en el capítulo 1, el objetivo de esta tesis es desarrollar una metodología integral de protección de datos electrónicos médicos, aplicado al almacenamiento, acceso y análisis forense de las historias clínicas en Colombia.

La necesidad real de un prototipo proviene de los sistemas de información a hoy implementados en los proveedores de salud, los cuales no siguen las mejores prácticas de seguridad informática. La identidad en estos sistemas es un único punto de falla. También son vulnerables a diferentes tipos de ataques y puerta trasera de fugas de datos del usuario. Por lo tanto, los proveedores de salud en Colombia necesitan un sistema descentralizado distribuido común. Este sistema puede autenticar y autorizar a los usuarios sin un punto único de falla y disminuir la posibilidad de ataques y fugas de datos de usuarios a través de puertas traseras. Otro propósito esencial del prototipo es la propiedad de los datos de los usuarios, además de hacer un análisis forense de las maquinas en tiempo real.

3.2 Diseño

El diseño del prototipo se describe en esta sección. Se explica el razonamiento detrás del diseño y desarrollo del prototipo, así como la arquitectura del software. Cabe destacar que este prototipo es una simulación definida y el resultado puede variar según la red de blockchain seleccionada.

3.2.1 Elección de tecnología

En el orden de las ideas anteriormente planteadas en el capítulo 2 se observa claramente que las implementaciones actuales de los sistemas de salud tienen varias vulnerabilidades y limitaciones. Estas vulnerabilidades han provocado el secuestro y la violación de los datos del usuario, el robo de identidad y la pérdida financiera. Estas cuestiones son cada vez más comunes y frecuentes. Los usuarios finales están cada vez más preocupados por su identidad digital y privacidad. Además de estos problemas, el registro repetido de usuarios en diferentes servicios es inconveniente. Los registros múltiples aumentan las vulnerabilidades de los datos del usuario, por lo tanto, se requiere una solución alternativa

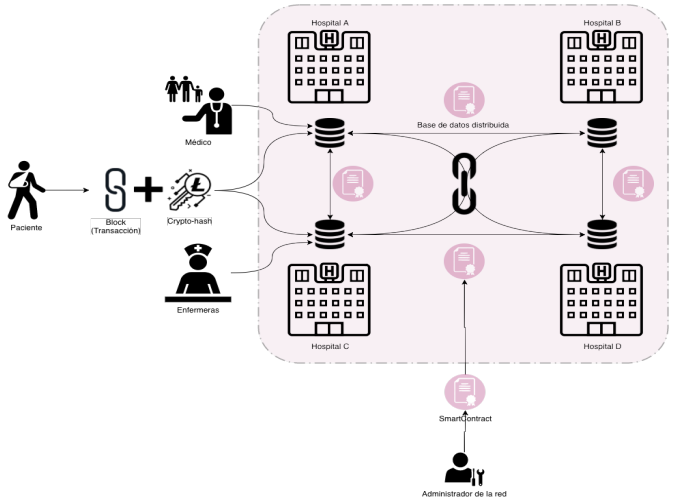
para enfrentar estos desafíos. Como se discutió en la Sección 1.4.8, Blockchain es una tecnología basada en el P2P, el protocolo de consenso y las firmas digitales. La red P2P es la red blockchain que, por diseño, está descentralizada, distribuida sin un único punto de falla. El protocolo de consenso garantiza que una transacción se realice solo una vez. Esta transacción se agrega a libros de contabilidad públicos distribuidos que no se pueden revertir. Además, cualquier persona en la red puede validar y verificar esta transacción. Esto hace que el sistema sea transparente y confiable. El usuario emite su identidad con criptografía de clave pública-privada. Esta identidad utiliza un algoritmo de hash digital que es casi imposible de descifrar con las tecnologías actuales. Además, la identidad y los datos del usuario firmados pueden ser verificados y validados por cualquier persona en la red, pero las transacciones firmadas por la clave privada solo pueden ser vistas por el propietario, dado lo anterior, blockchain garantiza que la identidad no se puede rastrear y que el usuario posee la propiedad completa de los datos y el anonimato en la red, además de reducir las posibilidades de piratería, ya que los datos no se comparten con el servidor central. Los datos son guardados por el usuario y esos datos están protegidos por el último algoritmo hash. Este algoritmo hash es de los más avanzados y aún no se ha descifrado. Es fácil de usar la tecnología blockchain en múltiples servicios, dado que los datos del propietario solo están con el y no se envían al servidor central. Estas características otorgan la propiedad de los datos al cliente y no a los proveedores de servicios. Blockchain también disminuye las posibilidades de violación de datos, la infracción solo es posible con el consentimiento del cliente o descuido, los proveedores no pueden compartir datos con organizaciones de terceros, ya que no tienen datos de usuario y no tienen control sobre sus datos. Consecuentemente, no es escalable en comparación con el sistema actual debido al tiempo de las transacciones, pero, a pesar de estos inconvenientes, es más seguro, fácil de usar, confiable y tolerante a fallas que los sistemas actuales. Hyperledger fabric es la plataforma de blockchain la cual ha sido diseñado para desarrollar aplicaciones de blockchain en la parte superior de la blockchain mediante chaincode. Los Chaincode se escriben usando un lenguaje Golang, el cual es un lenguaje fácil de aprender y escribir. Los chaincode se pueden implementar fácilmente en redes privadas, de prueba o principales el cual es interpretado por hyperledger fabric. Por lo tanto, por un lado, la plataforma hyperledger fabric oculta la mayor parte de la profundidad técnica de la cadena de bloques y permite al desarrollador concentrarse en escribir la lógica de su aplicación, mientras que, por otro lado, hace que la implementación de la aplicación sea indolora. La gran comunidad de hyperledger fabric brinda apoyo activo para los posibles problemas.

Por estas razones, se seleccionó hyperledger fabric Blockchain para el desarrollo y prueba del prototipo.

3.2.2 Arquitectura red blockchain

La arquitectura de software presentada en la (Figura 3-2) muestra la solución completa sobre cómo las entidades prestadoras de salud pueden aprovechar la tecnología de blockchain para tener una identidad común. La solución también presenta cómo los usuarios podrían usar la tecnología blockchain para la propiedad de los datos y pagar sus facturas sin compartir sus datos financieros. Se implementaron los contratos inteligentes en la red de blockchain y se describió en detalle la relación entre proveedores, blockchain, contrato inteligente y usuarios. La arquitectura del software tiene tres tipos de participantes: proveedores de infraestructura, red Blockchain y un usuario, como se muestra en la (Figura 3-2) Los proveedores de infraestructura son proveedores que brindan servicios de infraestructura tales como computación, almacenamiento y red. Cada hospital tiene su propio chaincode o contrato inteligente, como se muestra en la (Figura 3-2), con conjuntos de instrucciones sobre cómo autenticar y autorizar a los usuarios finales. La red Blockchain proporciona un backend de identidad descentralizado y distribuido. Finalmente, hay un usuario final que consume los servicios de infraestructura a través de la Interfaz de Programa de Aplicación (API).

Figura 3-2 Arquitectura red blockchain



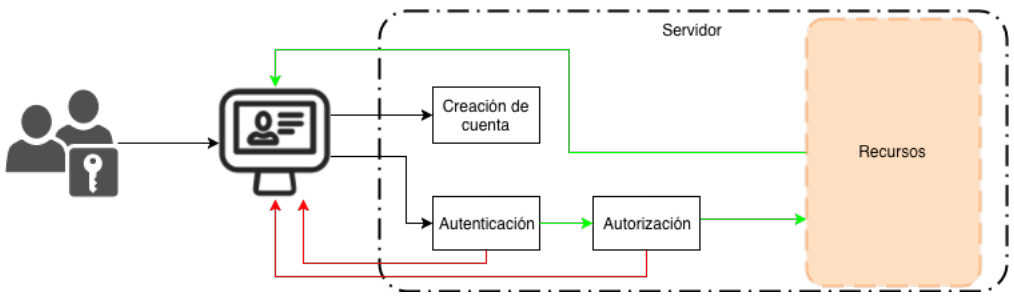
Autor: Construcción propia

3.2.3 Módulo de control de acceso

La autenticación, autorización y las cuentas de usuario (AAC) es un marco utilizado por las entidades prestadoras de salud para controlar el acceso de los recursos a los sistemas de información, hacer cumplir las políticas, auditar y medir el uso de los recursos. La AAC se basa en el modelo cliente-servidor donde el usuario interactúa con el cliente, y el servidor tiene la lógica de negocios necesaria para los recursos, el usuario, la red y la administración de seguridad. La autenticación es un proceso de verificación de la identidad del usuario y la autorización es el proceso de decidir si un usuario tiene los derechos suficientes para utilizar el servicio solicitado. La contabilidad es el proceso de seguimiento del uso de recursos por parte del usuario para facturación, auditoría, análisis de datos.

La (Figura 3-3) muestra la arquitectura general AAA con el modelo cliente-servidor donde el cliente es una aplicación web o móvil y la autenticación, autorización, recursos de contabilidad y servicios del servidor.

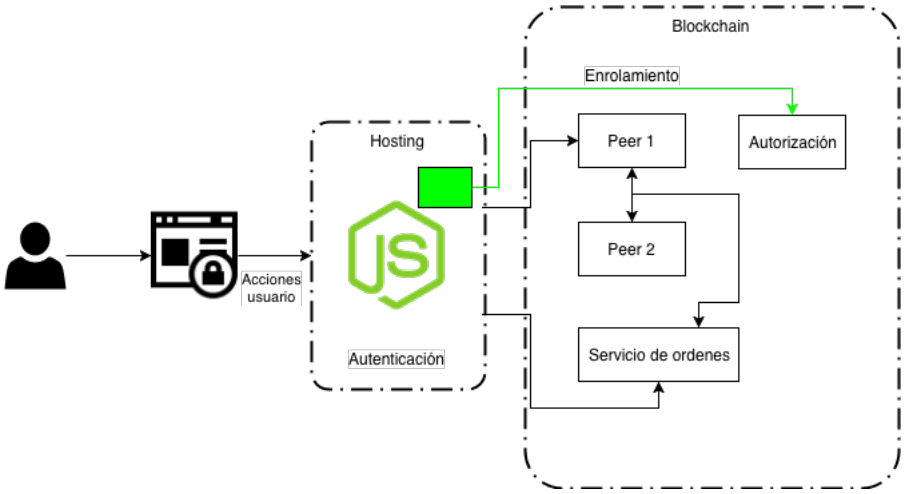
Figura 3-3 Arquitectura AAA



Autor: Construcción propia

Ahora la arquitectura propuesta para esta tesis es la representada en la (Figura 3-4) la cual está dada por una autenticación externa para dar acceso a la red blockchain.

Figura 3-4 Arquitectura propuesta para la autenticación



Autor: Construcción propia

3.2.4 Módulo de almacenamiento de datos

Poner los datos privados en el libro de contabilidad conlleva un dilema inherente: si todos ven el mismo libro de contabilidad, ¿cómo podemos tener datos privados que algunos pueden ver, pero otros no? Una solución común en muchos sistemas es colocar en el libro mayor solo un cifrado (o un hash) de los datos privados, mientras se mantienen los datos bajo el control de la parte que los posee. Por supuesto, esta solución por sí sola no es suficiente si los contratos inteligentes dependen de alguna manera de los datos privados (como en los casos de uso anteriores). Hyperledger Fabric implementa canales, que son esencialmente Libros de contabilidad separados. Los datos en un canal solo son visibles para los miembros de esos canales, pero no para otros pares en el sistema. Esta solución proporciona cierta medida de privacidad, además implementa pruebas de conocimiento cero (ZKP) permiten que un investigador convenza a otros de que cierta afirmación es cierta, sin revelar información adicional. Blockstream CA [9] usa ZKP simples junto con compromisos homomórficos [111] aditivos para manipular datos secretos en el libro mayor. Por ejemplo, dos usuarios cuyos saldos de cuentas secretas están cifrados con compromisos homomórficos aditivos, pueden acordar de forma privada (fuera de cadena) el precio de un artículo. El primer usuario puede luego restar esta cantidad de su saldo y sumarla al saldo del otro usuario (utilizando homomorfismo), y demostrarles a todos (usando ZKP) que la cantidad agregada al segundo saldo es igual a la cantidad restada

del primero. Pero tenga en cuenta que el monto de la transacción en sí debe ser totalmente conocido por la primera parte, esta combinación de ZKP y los compromisos adicionales homomorfos todavía no es lo suficientemente fuerte como para comparar dos valores secretos, o para cualquiera de los casos de uso anteriores.

3.2.5 Módulo de análisis forense

Las técnicas modernas de almacenamiento, como el almacenamiento distribuido, el proceso estandarizado para hacer análisis forense no funcionará en todos los detalles. Considerando que grandes empresas como Google, Facebook y Mozilla tienen un incidente dentro de su infraestructura de decenas de miles de clientes, apagar cada (probablemente) computadora afectada no funcionará sin causar enormes costos al proveedor de infraestructura. Por lo tanto, las compañías como esas tres estructuras desarrolladas, llamadas herramientas forenses en tiempo real, no requieren el cierre del cliente, pero pueden copiar datos importantes a través de la red a una estación centralizada para una investigación adicional. Teniendo en cuenta un cliente infectado, estas herramientas forenses en tiempo real son capaces de escanear todos los clientes en el rango de los detalles de la infección para encontrar otros clientes infectados, y algunos de esos marcos pueden acceder directamente al cliente y evitar la propagación del malware, por ejemplo, desactivando ciertas interfaces de red. Por un lado, este enfoque definitivamente se considera alterar los datos en el cliente, sin embargo, por otro lado, este enfoque es rápido y no afecta el tiempo de actividad de los clientes (o las redes). Ciertos marcos (por ejemplo, Mozilla MIG) son capaces de producir imágenes de los clientes, Forensics en tiempo real a través de la visibilidad de endpoint, que podría considerarse como un punto de partida para un entorno forense dirigido a entornos en vivo usando herramientas forenses en tiempo real.

3.2.6 Flujo

El diagrama de flujo describe cómo un usuario del sistema de salud interactúa con un contrato inteligente implementado en la red de blockchain.

Los componentes clave en la figura son los contratos inteligentes implementados por las entidades prestadoras de salud y un usuario capaz de realizar transacciones utilizando el contrato inteligente en la red de blockchain.

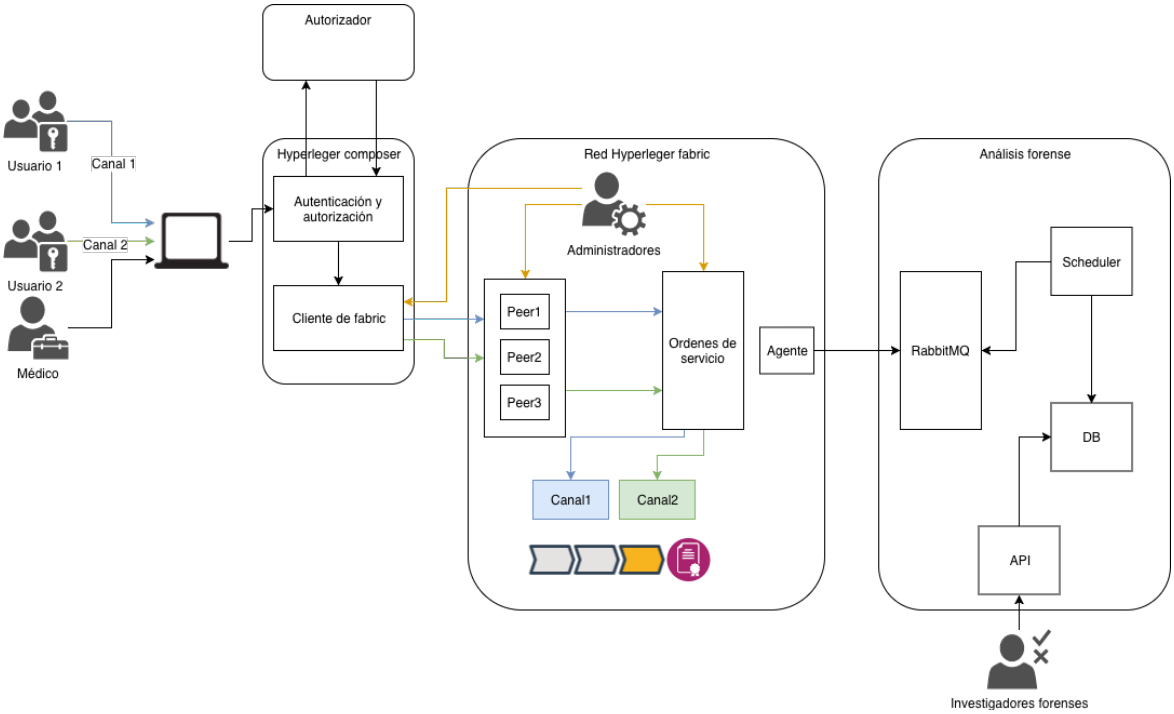
El usuario del sistema de salud debe estar autenticado y autorizado para acceder a los recursos del sistema de salud, así como consultar los registros electrónicos médicos. Hay dos tipos de autenticación. El usuario de la entidad prestadora de salud y el usuario se autentican en la blockchain para utilizar los recursos de la red blockchain y ejecutar las transacciones respectivamente. La autenticidad del usuario es aprobada recuperando la clave pública del usuario en la aplicación de blockchain de la firma del mensaje que está firmada con la clave privada del usuario. La autenticidad de la entidad prestadora de salud se prueba, ya que todas las transacciones ejecutadas por la entidad prestadora de salud se firman con la clave privada.

Estas firmas son verificadas por defecto por la blockchain antes de ejecutar las transacciones. Por lo tanto, esto garantiza, por un lado, que el usuario del sistema de salud es un usuario legítimo y que solo él es capaz de ejecutar la transacción. La entidad prestadora de salud autoriza al usuario al verificar si la dirección del usuario es válida y existe en la blockchain. Si la respuesta es positiva, la entidad prestadora de salud agrega al usuario a su base de datos de la blockchain y lo marca como autorizado para acceder a sus recursos. Además, solo la clave pública de la entidad prestadora de salud, así como la clave pública del usuario del sistema de salud, se distribuyen a la cadena de bloques. Por lo tanto, el prototipo mantiene el anonimato del usuario y la entidad prestadora de salud.

En primera instancia, la entidad prestadora de salud implementa los contratos en la red de blockchain privada con Hyperledger fabric como se muestra en la (Figura 3-5). Mientras tanto, un usuario administrador crea su identidad digital como se muestra en la (Figura 3-5) Ahora, el usuario puede acceder a los recursos para tales fines como visualizar su historia clínica, entre otros. Si el usuario está autenticado y autorizado, puede acceder a los recursos, de lo contrario, este debe realizar el respectivo registro. En una autorización exitosa, el usuario puede acceder al recurso. La identidad del usuario aún necesita ser verificada. En caso de éxito, el prototipo prueba la autenticidad del usuario y el usuario está autorizado y autenticado para acceder a los recursos como se muestra en la (Figura 3-5). Adicionalmente como la información está distribuida por toda la red blockchain, esta se encuentra almacenada de manera segura por lo que Hyperledger fabric implementa algoritmos de homomorfic encryption para el cifrado de la información en reposo. Toda la infraestructura montada en esta implementación está monitoreada por Mozilla MIG, esta

es una herramienta de análisis forense distribuido con la cual se obtiene información en tiempo real de comportamientos anómalos en la red.

Figura 3-5 Flujo en la red blockchain



Autor: Construcción propia

3.3 Implementación

Esta sección describe los componentes de hardware y software necesarios para implementar el prototipo. También describe los chaincode o contratos inteligentes, la configuración del entorno del prototipo y cómo se ejecutó el prototipo. La idea principal es que, después de leer esta sección, sería posible configurar el entorno de desarrollo y ejecutar el prototipo.

3.3.1 Componentes de hardware

El prototipo fue desarrollado y probado en MacBook Pro, computadora de mediados de 2018 [112]. La computadora tiene procesador de 2.6 GHz 6-core Intel Core i7, memoria de 16 GB y sistema operativo macOS Mojave versión 10.14. Todos los componentes de

software descritos a continuación se descargaron y ejecutaron manualmente en este hardware.

3.3.2 Componentes de software

Esta sección describe los componentes de software utilizados para el desarrollo y prueba de prototipos. Los componentes son Hyperledger fabric, Hyperledger composer y Mozilla MIG.

- **Hyperledger fabric**

La Linux Fundation fundó Hyperledger en 2015 para avanzar en las tecnologías de blockchain de la industria. En lugar de declarar un único estándar de blockchain, fomenta un enfoque de colaboración para desarrollar tecnologías de blockchain a través de un proceso comunitario, con derechos de propiedad intelectual que fomentan el desarrollo abierto y la adopción de estándares clave a lo largo del tiempo.

Hyperledger Fabric es uno de los proyectos de blockchain dentro de Hyperledger. Al igual que otras tecnologías de blockchain, tiene un libro de contabilidad, utiliza contratos inteligentes y es un sistema mediante el cual los participantes administran sus transacciones.

Donde Hyperledger Fabric es diferente con otros sistemas de blockchain es que es privado y está autorizado. Los miembros de una red Hyperledger Fabric, en lugar de un sistema sin permisos abierto que permite que participen identidades desconocidas en la red (que requieren protocolos como Proof of Work para validar las transacciones y asegurar la red), en hyperledger fabric se inscriben a través de un proveedor de servicios confiable de Membership Service Provider (MSP).

Hyperledger Fabric también ofrece varias opciones conectables. Los datos del libro de contabilidad se pueden almacenar en múltiples formatos, los mecanismos de consenso se pueden intercambiar dentro y fuera, y se admiten diferentes MSP.

Hyperledger Fabric también ofrece la posibilidad de crear canales, lo que permite a un grupo de participantes crear un libro de contabilidad separado de transacciones. Esta es una opción especialmente importante para las redes donde algunos participantes pueden ser competidores y no quieren todas las transacciones que realizan, un precio especial que están ofreciendo a algunos participantes y no a otros, por ejemplo, conocidos por todos los participantes. Si dos participantes forman un canal, entonces esos participantes, y no otros, tienen copias del libro de contabilidad para ese canal.

Hyperledger fabric tiene varios conceptos claves entre ellos están:

1. **Shared Ledger (Libro de contabilidad compartido):** Hyperledger Fabric tiene un subsistema de libro de contabilidad que consta de dos componentes: el world state y el transaction log. Cada participante tiene una copia del libro de contabilidad para cada red de Hyperledger Fabric a la que pertenece. El componente de world state describe el estado del libro de contabilidad en un momento dado en el tiempo. Es la base de datos del libro de contabilidad. El componente de transaction log registra todas las transacciones que han resultado en el valor actual del world state; Es el historial de actualización para el world state. El libro de contabilidad, entonces, es una combinación de la base de datos de world state y el transaction log. El libro de contabilidad tiene un almacén de datos reemplazable para el world state. De forma predeterminada, esta es una base de datos de almacén de valor-clave de LevelDB. El registro de transacciones no necesita ser conectable. Simplemente registra los valores de antes y después de la base de datos de contabilidad que está utilizando la red blockchain.
2. **Chaincode (Contratos inteligentes):** Los contratos inteligentes de Hyperledger Fabric están escritos en blockchain y son invocados por una aplicación externa a la blockchain cuando esa aplicación necesita interactuar con el libro de contabilidad. En la mayoría de los casos, el chaincode interactúa solo con el componente de base de datos del libro de contabilidad, el world state (por ejemplo, consultándolo) y no el registro de transacciones. Los Chaincode se puede implementar en varios lenguajes de programación. El lenguaje de código de cadena actualmente soportado es Go con soporte para Java y otros lenguajes que vendrán en futuras versiones.

3. **Privacy:** Dependiendo de las necesidades de una red, los participantes en una red Business-to-Business (B2B) pueden ser extremadamente sensibles a la cantidad de información que comparten. Para otras redes, la privacidad no será una de las principales preocupaciones. Hyperledger Fabric es compatible con redes donde la privacidad (el uso de canales) es un requisito operacional clave, así como redes que son comparativamente abiertas.
4. **Consensus (Consenso):** Las transacciones deben escribirse en el libro de contabilidad en el orden en que ocurren, incluso aunque se encuentren entre diferentes conjuntos de participantes dentro de la red. Para que esto suceda, se debe establecer el orden de las transacciones y se debe implementar un método para rechazar las transacciones incorrectas que se insertaron en el libro de contabilidad por error (o de manera malintencionada).

- **Hyperledger composer**

Hyperledger Composer es un marco de desarrollo que une varias herramientas para posibilitar el desarrollo de aplicaciones de blockchain. De la misma manera ayuda desarrollar aceleradamente e implementar una solución de blockchain.

Hyperledger Composer tiene varios conceptos claves entre ellos están:

1. **Blockchain State Storage:** Las transacciones enviadas a través de la red se almacenan en el libro mayor de blockchain, y el estado actual de los activos y participantes se almacena en la base de datos del estado de blockchain. El blockchain distribuye el libro de contabilidad y la base de datos de estado a través de un conjunto de pares y asegura que las actualizaciones del libro de contabilidad y la base de datos de estado sean consistentes en todos los pares utilizando un algoritmo de consenso.
2. **Connection Profiles (Perfiles de conexión):** Hyperledger Composer utiliza los perfiles de conexión para definir el sistema al que se conectará. Un perfil de conexión es un documento JSON que forma parte de una tarjeta de red comercial. Estos perfiles normalmente los proporciona el creador del sistema al que hacen

referencia y deben usarse para crear tarjetas de red de negocios para poder conectarse a ese sistema.

3. **Assets (Bienes):** Los activos son bienes, servicios o bienes tangibles o intangibles, y se almacenan en registros. Los activos pueden representar casi cualquier cosa en una red de negocios, por ejemplo, una historia clínica, una casa en venta, el listado de ventas, el certificado de registro de propiedad de esa casa y los documentos de seguro de esa casa pueden ser activos en una o más redes comerciales.
4. **Participants (Participantes):** Los participantes son miembros de una red. Pueden poseer activos y enviar transacciones. Los tipos de participantes se modelan y, al igual que los activos, deben tener un identificador y pueden tener cualquier otra propiedad según sea necesario. Un participante puede asignarse a una o varias identidades.
5. **Identities (Identidades):** Una identidad es un certificado digital y una clave privada. Las identidades se utilizan para realizar transacciones en una red de negocios y deben asignarse a un participante en la red de negocios. Una sola identidad se almacena en una tarjeta de red comercial y, si esa identidad se ha asignado a un participante, le permite al usuario de esa tarjeta de red comercial realizar transacciones en una red comercial como ese participante.
6. **Business Network cards (Tarjetas de red de negocios):** Las tarjetas de red de negocios son una combinación de una identidad, un perfil de conexión y metadatos, los metadatos que contienen opcionalmente el nombre de la red de negocios para conectarse. Las tarjetas de red de negocios simplifican el proceso de conexión a una red de negocios y extienden el concepto de una identidad fuera de la red de negocios a una "cartera" de identidades, cada una asociada con una red de negocios específica y un perfil de conexión.
7. **Transactions (Transacciones):** Las transacciones son el mecanismo por el cual los participantes interactúan con los activos. Esto podría ser tan simple como un participante que hace una oferta por un activo en una subasta, o un subastador que marca una subasta cerrada, transfiriendo automáticamente la propiedad del activo al mejor postor.
8. **Queries (Consultas):** Las consultas se utilizan para devolver datos sobre el estado mundial de la cadena de bloques. Las consultas se definen dentro de una red empresarial y pueden incluir parámetros variables para una personalización simple.

Mediante consultas, los datos se pueden extraer fácilmente de su red de blockchain. Las consultas se envían utilizando la API de Hyperledger Composer.

9. **Events (Eventos):** Los eventos se declaran en la definición de la red empresarial de la misma manera que los activos o los participantes. Una vez que se han definido los eventos, pueden ser emitidos por las funciones del procesador de transacciones para indicar a los sistemas externos que algo importante le ha sucedido al libro mayor. Las aplicaciones pueden suscribirse a eventos emitidos a través de la API cliente-compositor.
10. **Access Control (Control de acceso):** Las redes de negocios pueden contener un conjunto de reglas de control de acceso. Las reglas de control de acceso permiten un control preciso sobre qué participantes tienen acceso a qué activos en la red y en qué condiciones.
11. **Historian registry (Registro de historiadores):** El historiador es un registro especializado que registra las transacciones exitosas, incluidos los participantes y las identidades que los enviaron. El historiador almacena las transacciones como activos del registro histórico, que se definen en el espacio de nombres del sistema Hyperledger Composer.

- **Mozilla MIG**

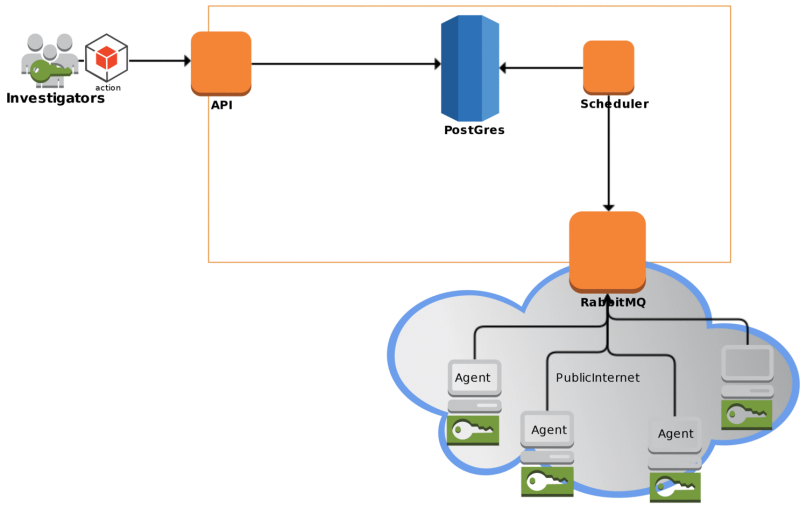
MIG es una plataforma para realizar investigación en puntos finales remotos. Permite a los investigadores obtener información de gran cantidad de sistemas en paralelo, lo que acelera la investigación de incidentes.
Además de la escalabilidad, MIG está diseñado para proporcionar primitivas de seguridad sólidas como:

1. El control de acceso se asegura al requerir firmas de GPG en todas las acciones. Las acciones sensibles también pueden solicitar firmas de múltiples investigadores. Un atacante que tome el servidor central podrá leer datos no confidenciales, pero no podrá enviar acciones a los agentes. Las claves GPG son guardadas de forma segura por sus investigadores.
2. La privacidad se respeta, nunca recuperando datos sin procesar de los puntos finales. Cuando MIG se ejecuta en computadoras portátiles o teléfonos, los

usuarios finales pueden solicitar informes sobre las operaciones realizadas en sus dispositivos. La regla de 2 hombres para acciones sensibles también evita que los investigadores deshonestos invadan la privacidad. La confiabilidad está incorporada. Ningún componente es crítico. Si un agente falla, intentará recuperarse y volver a conectarse a la plataforma por tiempo indefinido. Si la plataforma falla, una nueva plataforma se puede reconstruir rápidamente sin copias de seguridad.

En la Figura 3-6 se muestra la arquitectura básica de Mozilla MIG y todos los componentes que se deben temer en cuenta a la hora de la implementación de esta tecnología.

Figura 3-6 Arquitectura MIG



Autor: Mozilla MIG

3.3.3 Prototipo

Las siguientes instrucciones son necesarias para obtener las herramientas de desarrollo de Hyperledger fabric y Hyperledger composer.

- **Instale las herramientas CLI**

La herramienta más importante es composer-cli, que contiene todas las operaciones esenciales, por lo que primero lo instalaremos. A continuación, se muestran la serie de

pasos que hay que seguir para la instalación.

1. Instalación de paquete por medio de NPM y nodejs CLI:

   npm install -g composer-cli@0.19

2. Instalación de utilidad para ejecutar un servidor REST en su máquina para exponer las redes como API RESTful.

   npm install -g composer-rest-server@0.19

3. Instalación de utilidad útil para generar activos de aplicaciones:

   npm install -g generator-hyperledger-composer@0.19

4. Instalacion de Yeoman, el cual es una herramienta para generar aplicaciones

   npm install -g yo

- **Instalación de Hyperledger Fabric**

En este paso nos permite tener una red blockchain de manera local de Hyperledger Fabric.

1. En el directorio ~/fabric-dev-servers, se descarga el archivo .tar.gz que contiene las herramientas para instalar Hyperledger Fabric:

   mkdir ~/fabric-dev-servers && cd ~/fabric-dev-servers
   curl -O https://raw.githubusercontent.com/hyperledger/composer-tools/master/packages/fabric-dev-servers/fabric-dev-servers.tar.gz
   tar -xvf fabric-dev-servers.tar.gz

2. Luego se utilizan los scripts que acaba de descargar y extraer para descargar un tiempo de ejecución local de Hyperledger Fabric v1.1:

cd ~/fabric-dev-servers

export FABRIC_VERSION=hlfv11

./downloadFabric.sh

- **Arrancar y detener Hyperledger Fabric**

La primera vez que se inicie la red de blockchain, lo primero que se ejecuta es el script de inicio y luego generar una tarjeta PeerAdmin:

cd ~/fabric-dev-servers
export FABRIC_VERSION=hlfv11
./startFabric.sh
./createPeerAdminCard.sh

Existen scripts para iniciar y detener la ejecución con ~/fabric-dev-servers/stopFabric.sh, y volver a iniciarlo con ~/fabric-dev-servers/startFabric.sh.

- **Desarrollo de prototipo**

Después de instalar los requisitos previos y el entorno de desarrollo, se debe ejecutar ./startFabric.sh y ./createPeerAdminCard.sh

1. **Generando el esqueleto de la aplicación.**

Para generar el esqueleto usando Yeoman, se debe abrir el terminal y escriba el siguiente comando:

yo hyperledger-composer

Ahora, disparará una serie de preguntas. Siga las opciones que se muestran en la siguiente figura:

Figura 3-7 Generación esqueleto de aplicación

```
~/workspace/blockchain/fabric/itm-tesis
$ yo hyperledger-composer
Welcome to the Hyperledger Composer project generator
? Please select the type of project: Business Network
You can run this generator using: 'yo hyperledger-composer:businessnetwork'
Welcome to the business network generator
? Business network name: itm-tesis-network
? Description: Red blockchain para tesis de maestría - Manuel Ramírez
? Author name:  Manuel Ramírez
? Author email: manuelramirez38853@correo.itm.edu.co
? License: Apache-2.0
? Namespace: model
? Do you want to generate an empty template network? No: generate a populated sample network
   create package.json
   create README.md
   create models/model.cto
   create permissions.acl
   create .eslintrc.yml
   create features/sample.feature
   create features/support/index.js
   create test/logic.js
   create lib/logic.js
```

Autor: Construcción propia

Ahora, esta es la página principal donde definimos nuestro modelo. Los archivos de modelo, los archivos de script, los archivos de control de acceso y los archivos de consulta se pueden agregar a la red de blockchain.

Se definió el siguiente modelo el cual representa los actores que están involucrados en el prototipo. Esto está escrito en lenguaje de modelado de composer, según Figura 3-8.

Figura 3-8 Definición de modelo

model.cto

```
namespace org.hyperledger_composer.scms
asset Ehr identified by ehrId {
 o String ehrId
 o String nombre
 o String cedula
 o String fechaNacimiento
 o String telefono
 o String direccion
 o String tipoSangre
 o String sexo
 o String alergias
 o String enCasoEmergencia
 --> Participant owner
 --> Participant issuer
}
participant Paciente identified by email {
 o String email
 o String nombre
 o String cedula
 o String type
}
participant Medico identified by email {
 o String email
 o String nombre
 o String cedula
 o String type
}
participant Enfermera identified by email {
 o String email
 o String nombre
 o String cedula
 o String type
}
transaction MoveEhr {
 --> Ehr ehr
 --> Participant issuer
 --> Participant newOwner
}
```

Autor: Construcción propia

Los participantes para que interactúan en la solución son, el paciente, el médico y la enfermera, los cuales se identifican por su correo electrónico. El activo llamado Ehr que se identifica con ehrId. Creamos una transacción llamada MoveEhr.

La lógica principal de nuestro modelo se encuentra establecido en la Figura 3-9.

Figura 3-9 Lógica de modelo

logic.js

```
/**
 *
 * @param {org.hyperledger_composer.scms.MoveEhr} moveEhr
 * @transaction
 */
async function MoveEhr(moveEhr) { // eslint-disable-line no-unused-vars
    moveEhr.ehr.issuer = moveEhr.ehr.owner;
    moveEhr.ehr.owner = moveEhr.newOwner;
    const assetRegistry = await getAssetRegistry('org.hyperledger_composer.scms.Ehr');
    await assetRegistry.update(moveEhr.ehr);
}
```

Autor: Construcción propia

El siguiente archivo enumera todos los controles de acceso que todos tienen.

Figura 3-10 Control de accesos

permissions.acl

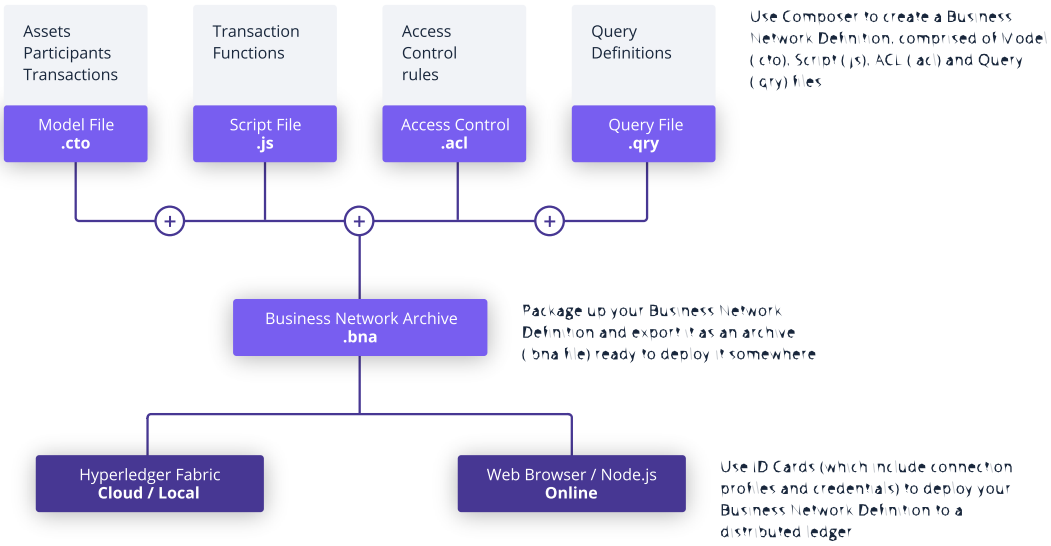
```
rule Default {
 description: "Allow all participants access to all resources"
 participant: "ANY"
 operation: ALL
 resource: "org.hyperledger_composer.scms.*"
 action: ALLOW
}
rule SystemACL {
 description: "System ACL to permit all access"
 participant: "org.hyperledger.composer.system.Participant"
 operation: ALL
 resource: "org.hyperledger.composer.system.**"
 action: ALLOW
}
rule NetworkAdminUser {
 description: "Grant business network administrators full access to user resources"
 participant: "org.hyperledger.composer.system.NetworkAdmin"
 operation: ALL
 resource: "**"
 action: ALLOW
}
rule NetworkAdminSystem {
 description: "Grant business network administrators full access to system resources"
 participant: "org.hyperledger.composer.system.NetworkAdmin"
 operation: ALL
 resource: "org.hyperledger.composer.system.**"
 action: ALLOW
}
```

Autor: Construcción propia

Creación del archivo Business Network Archive (BNA)

El archivo de red blockchain es un archivo que empaqueta de los archivos de modelo, archivo de script y archivo de control de acceso. La Figura 3-11 describe como está compuesto el archivo BNA.

Figura 3-11 Composición archivo BNA



Autor: Hyperledger fabric

Posteriormente, navegamos en la aplicación de bloque de pista en el terminal y escribimos el siguiente comando. Esto crea un archivo itm-tesis-network@0.0.1.bna.

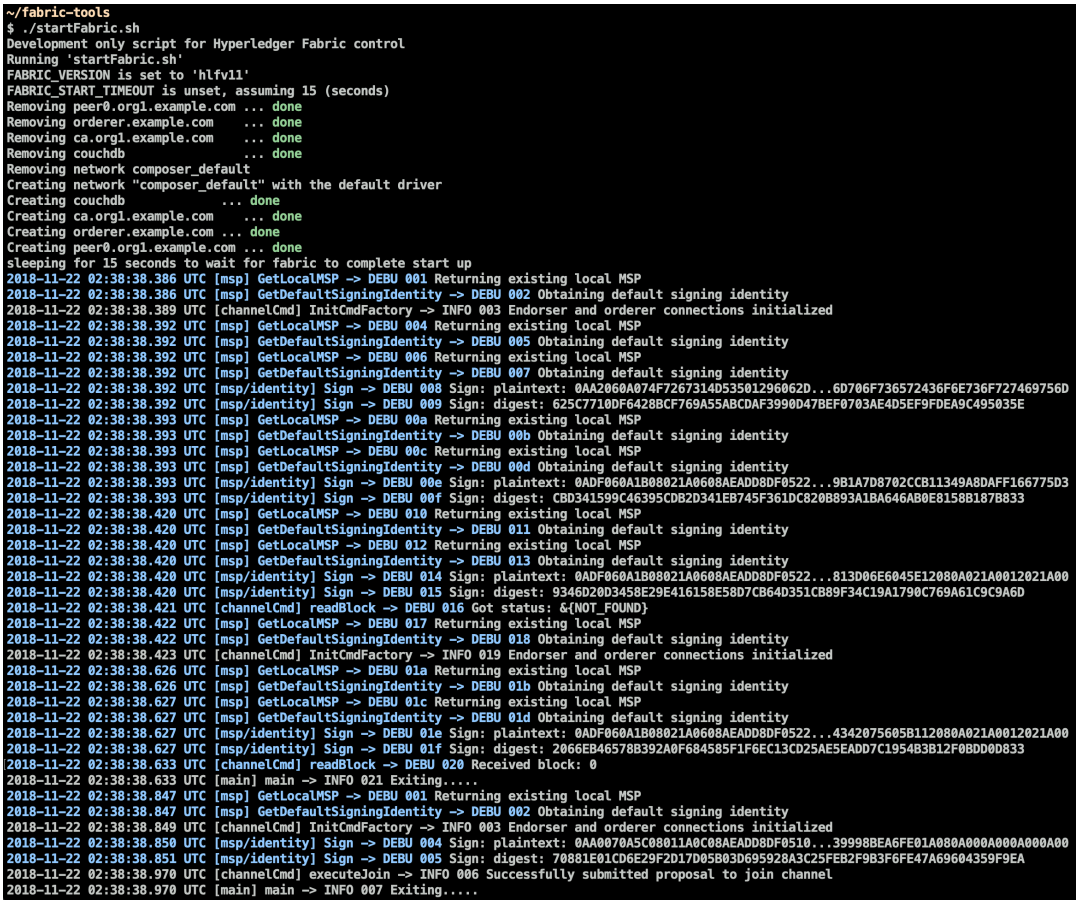
Figura 3-12 Creación de archivo BNA

```
~/workspace/blockchain/fabric/itm-tesis/itm-tesis-network
$ composer archive create -t dir -n .
Creating Business Network Archive


Looking for package.json of Business Network Definition
        Input directory: /Users/manalram/workspace/blockchain/fabric/itm-tesis/itm-tesis-network

Found:
        Description: Red blockchain para tesis de maestría - Manuel Ramírez
        Name: itm-tesis-network
        Identifier: itm-tesis-network@0.0.1

Written Business Network Definition Archive file to
        Output file: itm-tesis-network@0.0.1.bna

Command succeeded
```

Autor: Construcción propia

Para crear la red es necesario ejecutar el script que se muestra en la Figura 3-13.

Figura 3-13 Creación de red



Autor: Construcción propia

Como está representado en la (Figura 3-5) hay un administrador el cual es la persona que tiene todo el control sobre la red blockchain y por lo tanto administra los accesos y creación de los contratos que corren sobre esta. Para poder tener este perfil sobre la red blockchain se deben seguir los pasos establecidos en la Figura 3-14.

Figura 3-14 Creación de usuario administrador

```
~/fabric-tools
$ ./createPeerAdminCard.sh
Development only script for Hyperledger Fabric control
Running 'createPeerAdminCard.sh'
FABRIC_VERSION is set to 'hlfv11'
FABRIC_START_TIMEOUT is unset, assuming 15 (seconds)

Using composer-cli at v0.19.18

Successfully created business network card file to
        Output file: /tmp/PeerAdmin@hlfv1.card

Command succeeded


Successfully imported business network card
        Card file: /tmp/PeerAdmin@hlfv1.card
        Card name: PeerAdmin@hlfv1

Command succeeded

The following Business Network Cards are available:

Connection Profile: hlfv1
┌──────────────────┬──────────┬──────────────────┐
│ Card Name        │ UserId   │ Business Network │
├──────────────────┼──────────┼──────────────────┤
│ PeerAdmin@hlfv1  │ PeerAdmin│                  │
└──────────────────┴──────────┴──────────────────┘


Issue composer card list --card <Card Name> to get details a specific card

Command succeeded

Hyperledger Composer PeerAdmin card has been imported, host of fabric specified as 'localhost'
```

Autor: Construcción propia

Para instalar el Business Network Archive en la red Hyperledger Fabric, se debe ejecutar el comando establecido en la Figura 3-15 asociado al BNA generado en los pasos anteriores.

Figura 3-15 Instalación de usuario administrador

```
~/workspace/blockchain/fabric/itm-tesis/itm-tesis-network
$ composer network install --card PeerAdmin@hlfv1 --archiveFile itm-tesis-network@0.0.1.bna
✔ Installing business network. This may take a minute...
Successfully installed business network itm-tesis-network, version 0.0.1

Command succeeded
```

Autor: Construcción propia

Ahora se despliega la red de negocios.

Figura 3-16 Despliegue de red

```
~/workspace/blockchain/fabric/itm-tesis/itm-tesis-network
$ composer network start --networkName itm-tesis-network --networkVersion 0.0.1 --networkAdmin admin --networkAdminEnrollSecret adminpw --card PeerAdmin@hlfv1 --file
networkadmin.card
Starting business network itm-tesis-network at version 0.0.1

Processing these Network Admins:
        userName: admin

✔ Starting business network definition. This may take a minute...
Successfully created business network card:
        Filename: networkadmin.card

Command succeeded
```

Autor: Construcción propia

Luego de tener la red de negocios ejecutándose, se debe importar la identidad del administrador.

Figura 3-17 Importación de identidad

```
~/workspace/blockchain/fabric/itm-tesis/itm-tesis-network
$ composer card import --file networkadmin.card

Successfully imported business network card
        Card file: networkadmin.card
        Card name: admin@itm-tesis-network

Command succeeded
```

Autor: Construcción propia

Para verificar si la red de negocios se implementó con éxito o no, se ejecuta el siguiente comando.

Figura 3-18 Verificación de la red

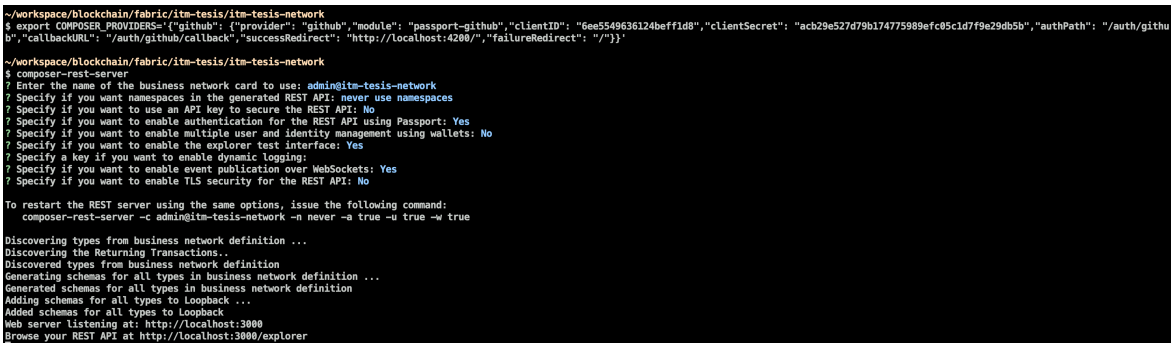
```
~/workspace/blockchain/fabric/itm-tesis/itm-tesis-network
$ composer network ping --card admin@itm-tesis-network
The connection to the network was successfully tested: itm-tesis-network
        Business network version: 0.0.1
        Composer runtime version: 0.19.18
        participant: org.hyperledger.composer.system.NetworkAdmin#admin
        identity: org.hyperledger.composer.system.Identity#5f36bc4de2b8a51e6baefd4c3a01e6e20b05015716c60b10a42c1673babc16e7

Command succeeded
```

Autor: Construcción propia

Ahora, comenzamos con la aplicación rest. En el front se está usando angular y para la capa aplicativa se está usado fabric. Todos los cambios realizados en la aplicación Angular se reflejan en el tejido Hyperledger y viceversa. La figura muestra una imagen más clara del flujo de nuestra aplicación.

Para esto se ejecuta el comando establecido en la Figura 3-19, solo hay que seguir los pasos para la creación de la estructura del proyecto.

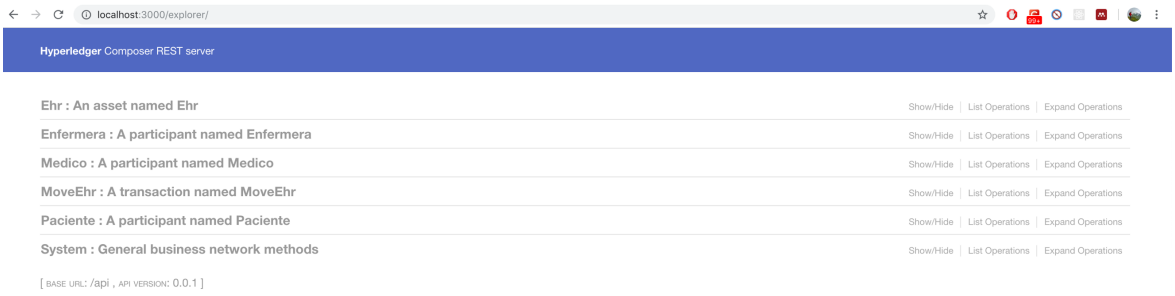
Figura 3-19 Ejecución de aplicación REST



Autor: Construcción propia

Para probar que la ejecución y que nuestro servidor rest está funcionando, hay que abrir un navegador y abrir la siguiente url http://localhost:3000/explorer.

Figura 3-20 Prueba de ejecución aplicación REST



Autor: Construcción propia

Para la creación del Front, hay que usar Yeoman con el plugin Hyperledger Composer.

Figura 3-21 Creación del FRONT

```
$ yo
? 'Allo Manuel! What would you like to do? Hyperledger Composer

Make sure you are in the directory you want to scaffold into.
This generator can also be run with: yo hyperledger-composer

Welcome to the Hyperledger Composer project generator
? Please select the type of project: Angular
You can run this generator using: 'yo hyperledger-composer:angular'
Welcome to the Hyperledger Composer Angular project generator
? Do you want to connect to a running Business Network? Yes
? Project name: tesis-app
? Description: Aplicación Tesis Manuel Ramírez
? Author name: Manuel Ramírez
? Author email: manuelramirez38853@correo.itm.edu.co
? License: Apache-2.0
? Name of the Business Network card: admin@itm-tesis-network
? Do you want to generate a new REST API or connect to an existing REST API?  Connect to an existing REST API
? REST server address: http://localhost
? REST server port: 3000
? Should namespaces be used in the generated REST API? Namespaces are not used
Created application!
Completed generation process
   create app.js
   create Dockerfile
   create e2e/app.e2e-spec.ts
   create e2e/app.po.ts
   create e2e/tsconfig.e2e.json
   create e2e/tsconfig.json
   create karma.conf.js
   create manifest.yml
   create package.json
   create protractor.conf.js
   create proxy.conf.js
   create README.md
   create src/app/app-routing.module.ts
   create src/app/app.component.css
   create src/app/app.component.html
   create src/app/app.component.spec.ts
   create src/app/app.component.ts
   create src/app/app.module.ts
   create src/app/asset/images/delete_noun_cc.svg
   create src/app/asset/images/edit_noun_cc.svg
   create src/app/asset/images/failed_noun_cc.svg
```

Autor: Construcción propia

Esto creará una carpeta llamada tesis-app en la carpeta principal.

cd tesis-app

npm start

Esto ejecutara el front, para poder acceder desde el navegador.

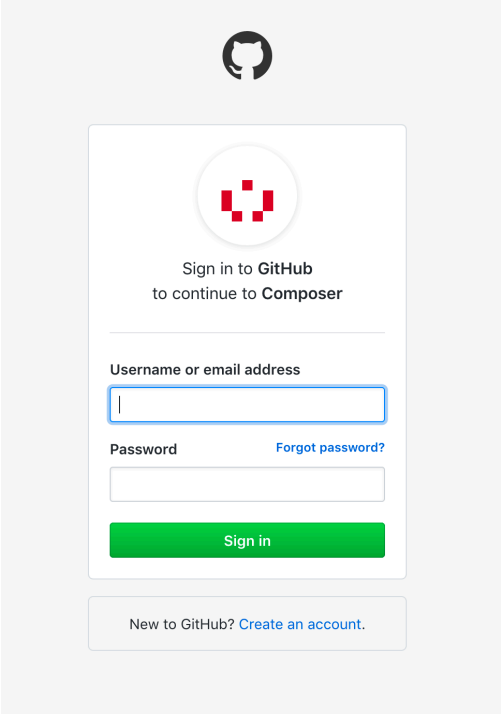
Figura 3-22 Ejecución del FRONT

```
~/workspace/blockchain/fabric/itm-tesis/itm-tesis-network/tesis-app
$ npm start

> tesis-app@0.0.1 start /Users/manalram/workspace/blockchain/fabric/itm-tesis/itm-tesis-network/tesis-app
> ng serve --proxy-config proxy.conf.js --host 0.0.0.0

** NG Live Development Server is running on http://0.0.0.0:4200 **
 10% building modules 4/4 modules 0 active[HPM] Proxy created: [ '/auth', '/api' ]  ->  http://localhost:3000
[HPM] Proxy created: /  ->  http://localhost:3000
Hash: 7ede5c50d6acbecd5152
Time: 11172ms
chunk    {0} polyfills.bundle.js, polyfills.bundle.js.map (polyfills) 270 kB {5} [initial] [rendered]
chunk    {1} main.bundle.js, main.bundle.js.map (main) 168 kB {4} [initial] [rendered]
chunk    {2} styles.bundle.js, styles.bundle.js.map (styles) 184 kB {5} [initial] [rendered]
chunk    {3} scripts.bundle.js, scripts.bundle.js.map (scripts) 440 kB {5} [initial] [rendered]
chunk    {4} vendor.bundle.js, vendor.bundle.js.map (vendor) 4.12 MB [initial] [rendered]
chunk    {5} inline.bundle.js, inline.bundle.js.map (inline) 0 bytes [entry] [rendered]
webpack: Compiled successfully.
```

Autor: Construcción propia

Para verlo funcionando hay que abrir http://localhost:4200/auth/github en su navegador y podrá interactuar con su modelo luego de loguearse y ser autorizado por la implantación de github. Esta se usó para facilidad en la simulación y no hacer una implementación propia, lo que contemplaría un tiempo considerable.

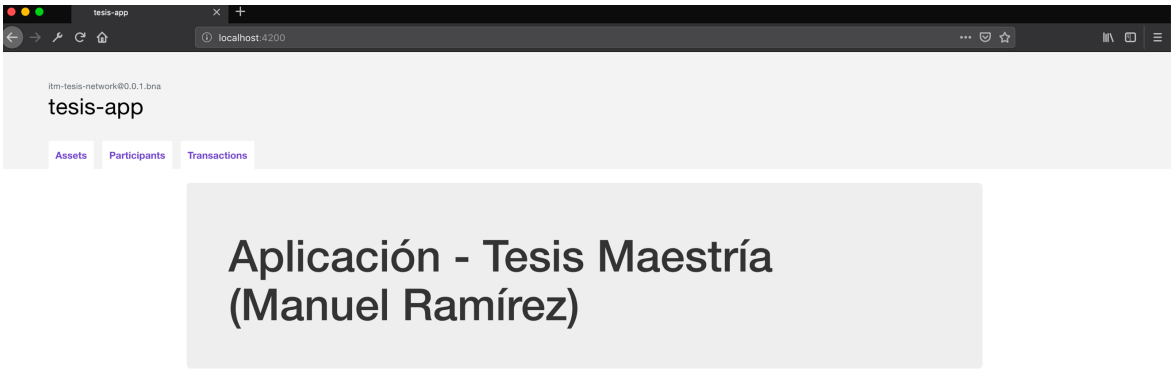
Figura 3-23 Pantalla de autenticación



Autor: Construcción propia

Luego que hay una autenticación exitosa, se puede proceder a usar la aplicación blockchain, por lo cual permite interactuar con todo el modelo planteado en la tesis.

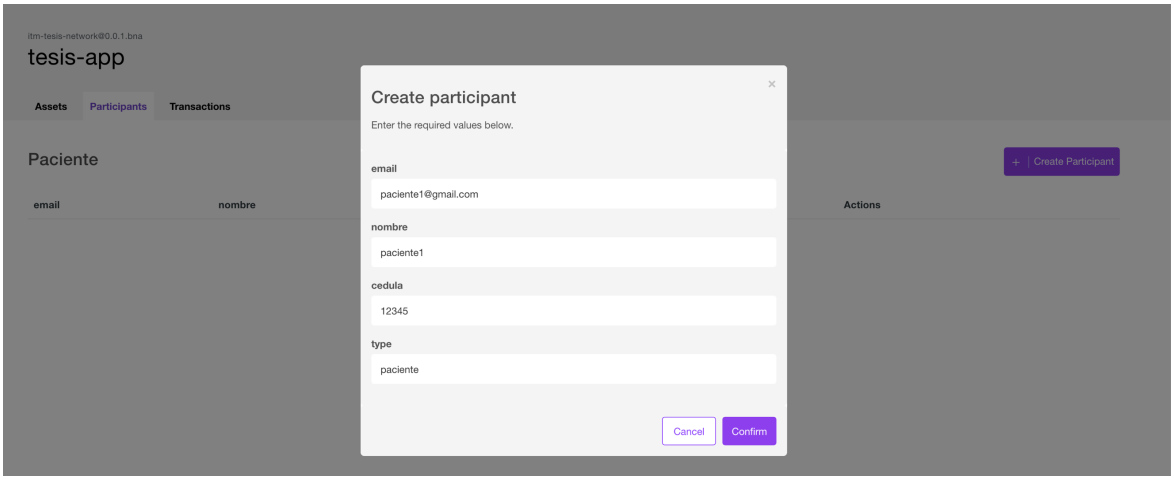
Figura 3-24 Pantalla inicial del prototipo



Autor: Construcción propia

Posterior al funcionamiento correcto de la aplicación, se procede a hacer las pruebas.

Figura 3-25 Creación de participante



Autor: Construcción propia

Como resultado se aprecia la creación del participante en la red blockchain, además que se pueden ejecutar las operaciones de modificación y borrado de registros.

Figura 3-26 Registro creado

Autor: Construcción propia

3.4 Pruebas

Esta sección describe el método utilizado para probar el prototipo. Describe los posibles casos de prueba para analizar qué tan bien se puede cumplir la expectativa de la declaración del problema. La sección también describe la configuración y ejecución de las pruebas de prototipos. Además, las medidas y los resultados se presentan junto con el análisis de los resultados y los aspectos de seguridad.

La prueba se configuró y ejecutó desde la perspectiva del proveedor de salud. La configuración y ejecución fue similar al entorno de prototipo. Esta configuración se ejecutó tres veces los casos de prueba para validar qué tan bien cumplimos con las expectativas de la declaración del problema y la necesidad de un prototipo.

La configuración de la prueba fue manual ya que requería varios disparadores manuales. Sin embargo, fue fácil visualizar y seguir los escenarios de autenticación, autorización, contabilidad con blockchain y análisis forense. Además, cuando se proporcionó una autenticación de usuario incorrecta (usuario falso) para el registro, se mostró un error. Por lo tanto, estos casos de uso demuestran que solo los usuarios autenticados y autorizados pueden acceder a los recursos de la red blockchain, y el proveedor de la entidad prestadora de salud pudo autenticar y autorizar a los usuarios con blockchain. Todas las transacciones fueron visibles en el explorer. Estas transacciones tenían hash id de usuario. Por lo tanto, fue difícil asociar qué usuario activó la transacción específica, dado lo anterior, se aseguró que tanto las entidades prestadoras de salud como los usuarios fueran anónimos en la red.

El prototipo propuesto en esta tesis es una prueba de concepto. Aunque hereda las propiedades predeterminadas de blockchain como el consenso descentralizado, las transacciones inmutables y la seguridad de los datos; no está distribuido y descentralizado, ya que se implementa en un nodo. Sin embargo, la configuración se puede implementar fácilmente en la red privada con múltiples nodos, esto hará que el prototipo descentralizado y distribuido.

Para el análisis forense, el primer paso, fue prepara el programa maligno que posteriormente se envía a las máquinas virtuales. El programa maligno fue elegido en función a la siguiente serie de características. Se debe ejecutar como un proceso en segundo plano para llevar a cabo sus actividades maliciosas, así mismo, persistir en el sistema, ya sea en algún lugar del sistema de archivos, la persistencia garantiza que el malware permanezca en el sistema después de un reinicio, así como la posibilidad de reiniciar el proceso de malware después de la terminación manual, además debe permitir conexiones externas, que se inician de forma saliente y que aceptan conexiones entrantes sin la interacción del usuario, estas conexiones salientes pueden indicar los datos que se están filtrando o el establecimiento de una conexión a un servidor. Entre los programas malignos evaluados tenemos, el troyano *retefe*, un programa maligno que instala una CA raíz en la máquina infectada y comienza a interceptar conexiones, así mismo el ransomware locky que encripta los archivos en el disco duro del usuario para solicitar el rescate de la clave de descifrado, también, el gusano Win32.Viking. Todos los programas malignos cumplen las características en una mayor o menor medida, por ejemplo, los tres programas malignos se ejecutan en segundo plano para llevar a cabo el comportamiento malicioso, así mismo persisten en el sistema, más precisamente el sistema de archivos, igualmente la característica de abrir conexiones lo hacen con un grado variable. Posteriormente a la selección de los programas malignos, estos se cargan en las máquinas, lo que permite que ciertos tipos de programa maligno infecten la máquina virtual en el momento del arranque o en el momento del inicio del sistema operativo, respectivamente. La herramienta forense MIG en tiempo real sondean los datos, lo que resulta en datos enviados a las máquinas virtuales infectadas. Tan pronto como los datos estén disponibles en MIG, se evalúan y se ponen a disposición del investigador.

Luego de realizar las pruebas nos da las siguientes conclusiones.

• Solo los usuarios autenticados y autorizados pueden acceder a los recursos de la red blockchain.
• El proveedor de servicios de salud puede autenticar y autorizar a los usuarios contra blockchain.
• Los usuarios de la entidad prestadora de salud pueden visualizar sus historias clínicas sin compartir detalle con terceros
• El proveedor de salud se autentica para ejecutar las transacciones en el blockchain.
• Los usuarios o proveedores son anónimos en la red.
• El prototipo hereda las debilidades genéricas de blockchain, como el contrato inteligente malicioso y el uso incorrecto de claves públicas.

3.4.1 Análisis de seguridad

Usando el prototipo, cualquier nodo en la red puede escribir su propio conjunto de contratos inteligentes, implementarse en la red y convertirse en una entidad prestadora de salud. Aunque este enfoque es seguro, transparente en comparación con la arquitectura cliente-servidor, no tiene protección contra contratos inteligentes maliciosos. El sistema prototipo podría engañar al usuario por servicios salud falsos. No hay ninguna especificación u organización para establecer las reglas para convertirse en proveedores de servicio de salud. Por lo tanto, los nodos defectuosos pueden implementar contratos defectuosos e intentar engañar al usuario con sus servicios falsos, ya que no hay un mecanismo para identificar qué proveedor de salud proporciona servicios de salud no falsos. Este problema se puede resolver formalizando primero un conjunto común de requisitos para convertirse en una entidad prestadora de servicios de salud y un conjunto común de especificaciones sobre cómo escribir e implementar un contrato inteligente para convertirse en entidad prestadora de servicios de salud. Además, estas especificaciones se implementarían en la cuenta de garantía y cada proveedor de salud debe registrarse en la cuenta de garantía, lo que garantizaría que se cumplan los requisitos del proveedor de salud. Si se cumplen los requisitos, el proveedor de servicios médicos puede ofrecer servicios, de lo contrario, el proveedor de servicios médicos no puede ofrecer ningún servicio. El prototipo actual asume que todos los usuarios son usuarios honestos. Sin embargo, en el mundo real, hay muchos usuarios malintencionados que, básicamente, podrían tomar la dirección pública del otro usuario y enviar una solicitud al proveedor de servicio de salud para registrarlo

como usuario. Además de los problemas anteriores, el sistema prototipo actual no tiene copia de seguridad ni sincronización de cuentas en varios dispositivos. Por lo tanto, si el hardware se corrompe o falla, los contratos y las cuentas no se pueden recuperar. Por lo tanto, para todas las entidades de salud y usuarios de estas entidades, es altamente recomendable utilizar el proveedor de la red principal, ya que los usuarios deben hacer una copia de seguridad y sincronizar sus cuentas en múltiples dispositivos. La herramienta MIG propuesto se utiliza en investigaciones ad-hoc y no para monitoreo permanente. Con respecto al programa maligno implementado se puede observar, los siguientes artefactos en el entorno del laboratorio:

• Si bien es posible analizar el contenido real de los archivos, la detección de archivos realmente modificados es más difícil debido a la falta de la línea de tiempo del archivo.
• No tener una línea de tiempo de archivos parece un poco problemático para obtener la mejor imagen de los cambios que tienen lugar en el sistema de archivos en general, aun así, pudimos detectar el programa maligno.
• Dado que el nombre de archivo que se genera es conocido, y el programa maligno genera un ejecutable que contiene cadenas de búsqueda para evitar la evasión de programa maligno, pudimos detectarlo utilizando MIG.

3.4.2 Discusión

La solución presentada en esta tesis puede ser implementada por un desarrollador individual para empresas pequeñas o empresas para proporcionar una solución tradicional. La solución requiere cambios y costos mínimos en el hardware, ya que funciona en el hardware existente y, aunque el proceso está saturado de CPU, no requiere varios servidores en comparación con las soluciones tradicional existentes. La solución por diseño es distribuida, descentralizada y tolerante a fallos, lo que disminuye los costos de implementación y mantenimiento.
A pesar de varias ventajas de esta solución sobre la solución tradicional existente, existen varias consideraciones que deben tenerse en cuenta antes de implementar la nueva solución en el entorno de producción por parte de la entidad prestadora de salud. Primero, esta solución requiere cambios arquitectónicos fundamentales en la solución tradicional existente, que es un cambio importante.

El proveedor de servicios de salud debe agregar soporte para la autenticación, autorización y contabilidad de blockchain a sus servicios existentes. El núcleo de blockchain se encuentra en un gran desarrollo, por lo que el proveedor de los servicios de salud debe actualizarse en consecuencia con los cambios de blockchain para evitar cualquier tiempo de inactividad en los sistemas de producción. Además, un núcleo de blockchain obsoleto podría ser vulnerable y las aplicaciones podrían terminar de ser hackeadas.

4. Conclusiones y recomendaciones

Esta sección resume el trabajo de maestría. También recomienda posibles trabajos futuros en esta área del conocimiento.

4.1 Conclusiones

La implementación de una solución completa descentralizada y segura con blockchain en general se encuentra en una fase muy temprana. Esta tesis ha propuesto una solución basada en autenticación con Github, hyperledger fabric y análisis forense con MIG. Dado lo anterior, se pudo proponer una metodología que contempla una solución al problema de la seguridad de los datos electrónicos médicos.

La arquitectura de la solución propuesta consta de 2 componentes principales. Contratos inteligentes y blockchain Hyperledger Fabric. Hyperledger composer es responsable de la autenticación del usuario contra Hyperledger fabric blockchain mediante la creación de una clave pública-privada. La clave pública se distribuye a través de la red de blockchain y la clave privada se mantiene en secreto con el usuario y está protegida por contraseña. Este par de claves actúa como la identidad del usuario donde la red puede verificar y validar la autenticidad del usuario mediante la clave pública del usuario. Los contratos inteligentes tienen la lógica central de la autorización del usuario y la lógica de asistencia de la autenticación, así como la contabilidad y la cancelación del registro del usuario. Los contratos a cargo son las entidades prestadoras de salud las que lo desarrollan y lo implementan en la cadena de bloques.
Finalmente, el blockchain de Hyperledger fabric es el núcleo del sistema que actúa como el backend. Asegura que todas las transacciones entre usuarios, proveedores y recursos se validen y verifiquen, y crea el bloque de transacciones que se agrega a la cadena de bloques una vez que la red alcanza el consenso.

Tan pronto como el bloque se agrega a blockchain, este cambio se vuelve permanente a la red y se transmite y se propaga a otros nodos. Este cambio no se puede deshacer ni duplicar. Por lo tanto, asegura que los usuarios son legítimos y autorizados. Las transacciones contractuales son inmortales, anónimas, distribuidas y descentralizadas. Estas transacciones pueden ser verificadas por cualquier persona en la red, pero no pueden ser desencriptadas por nadie más que el propietario.

Se ha implementado un prototipo para demostrar la viabilidad de la solución propuesta. Demuestra el conjunto de características necesarias mínimas para lograr la solución. Se implementan contratos inteligentes básicos. Estos contratos autentican y autorizan al usuario con la cadena de bloques. Solo los usuarios autenticados y autorizados pueden acceder a los recursos del sistema de salud y todas las transacciones se transmiten a la red. Las transacciones fueron inmutables una vez agregadas a blockchain. La solución se puede implementar y utilizar fácilmente desde pequeñas empresas hasta grandes empresas con el hardware existente a un costo mínimo. El mayor costo es escribir y mantener la lógica de los contratos por parte de los desarrolladores.

A través de esta investigación, se proporciona una posible solución para construir un sistema distribuido y descentralizado basado en blockchain. Esta propuesta de metodología tiene como objetivo proporcionar una solución más segura y más fácil en comparación con las soluciones tradicionales existentes con recursos de hardware existentes a costos mínimos, teniendo en cuenta la privacidad y la propiedad de los datos del usuario. Además, esta metodología no se puede hackear fácilmente y es fácil de usar, otra de las características de esta investigación fue la implementación de un sistema de análisis forense distribuido que es capaz de tratar con sistemas integrados, lo cual es un beneficio adicional que vale la pena mencionar, además que puede obtener en el tema de la verificación de archivos en caso de que el monitoreo detecte una generación de archivos nuevos, sospechosos o cambios. En el caso de una estructura de sistema más compleja que incluya sistemas integrados o hardware de gama baja, MIG simplemente es capaz de generar una imagen mucho más completa, ya que la información de estas fuentes se puede incorporar al análisis.

Este trabajo genera una metodología integral y sistémica, cumpliendo a la pertenencia de las empresas, no sólo viable, sino conveniente y efectiva, dando protección de datos electrónicos médicos, aplicado al almacenamiento, acceso y análisis forense de las

historias clínicas en Colombia y especificando los procedimientos que deben cumplirse en cada fase, promoviendo no sólo la reutilización y coherencia integral de la seguridad sino también fomentando la utilización de las mejores practicas

4.2 Recomendaciones

Finalmente, como prototipo, Hyperledger Fabric Blockchain es una tecnología que se comporta de manera adecuada. Debido a esto el objetivo de esta tesis era desarrollar y hacer una prueba de concepto, hay muchas características y mejoras que deben realizarse. De la misma manera, el entorno de prueba adecuado también podría usarse para realizar análisis más precisos de uso y costos, así mismo automatizar el proceso de desarrollo y ejecución.

Finalmente, el sistema podría probarse con una infraestructura real en la nube como AWS blockchain o Google IAAS para recursos reales en la nube y ejecutarse en la cadena principal de blockchain para encontrar el tiempo de ejecución real. Los costos reales de usar servicios en la nube como AWS podrían compararse y analizarse con este prototipo.

Bibliografía

[1] R. (EMC), “Cybercrime and the Healthcare Industry,” pp. 1–6, 2013.

[2] P. Sorokin, E. B. Estupiñán, P. Sorokin, and P. U. De Buenos, “¿ Historia clínica o historia cínica ? Aspectos éticos , legales y sociales implicados en el manejo de,” no. January, 2013.

[3] L. Gostin, J. Turek-Brezina, M. Powers, and R. Kozloff, “Privacy and security of health information in the emerging health care system,” *Health Matrix*, vol. 5, no. 1, 1995.

[4] B. García and M. Delgado Fernández, “Gestión y Generación de Conocimientos a partir de la información de patentes. Metodología.,” 2012.

[5] D. Liveri, A. Sarri, C. Skouloudi, and ENISA, *Security and Resilience in eHealth - Security Challenges and Risks*. .

[6] W. J. Curran, B. Stearns, and H. Kaplan, “Privacy, Confidentiality and Other Legal Considerations in the Establishment of a Centralized Health-Data System,” *N. Engl. J. Med.*, vol. 281, no. 5, pp. 241–248, 1969.

[7] A. Omotosho and J. Emuoyibofarhe, “A Criticism of the Current Security, Privacy and Accountability Issues in Electronic Health Records,” *Int. J. Appl. Inf. Syst.*, vol. 7, no. 8, 2014.

[8] R. C. Barrows and P. D. Clayton, “Privacy, confidentiality, and electronic medical records.,” *J. Am. Med. Inform. Assoc.*, vol. 3, no. 2, pp. 139–48, 1996.

[9] Min TIC, “Agenda Estratégica de Innovación - Nodo Salud,” *Sist. Investig. Desarro. e innovación. Minist. Tecnol. la Inf. y las Comun.*, pp. 2–57, 2014.

[10] Organización Panamericana de la Salud, *Registros médicos electrónicos en América Latina y el Caribe: Análisis sobre la situación actual y recomendaciones para la Región*. 2016.

[11] Congreso de Colombia, “Ley 1438 de 2011,” *Congr. Colomb.*, 2011.

[12] C. E. Rueda-Clausen Pinzón, “La historia clínica informatizada. Evaluación de los casos colombiano y español. (Spanish),” *MedUNAB*, vol. 9, no. 1, pp. 63–71, 2006.

[13] L. Michán, “CIENCIOMETRÍA, INFORMACIÓN E INFORMÁTICA EN CIENCIAS BIOLÓGICAS: ENFOQUE INTERDISCIPLINARIO PARA ESTUDIAR INTERDISCIPLINAS,” *Ludus Vitalis*, vol. 35, pp. 239–243, 2011.

[14] J. Ardanuy, “Breve introducción a la bibliometría,” 2012.

[15] F. Rezaeibagha, K. T. Win, and W. Susilo, “A systematic literature review on security and privacy of electronic health record systems : technical perspectives,” vol. 44, no. 3, pp. 1–16, 2015.

[16] N. R. Council, *For the Record*. Washington, D.C.: National Academies Press, 1997.

[17] F. Amato, G. De Pietro, M. Esposito, and N. Mazzocca, “An integrated framework for securing semi-structured health records,” *Knowledge-Based Syst.*, vol. 79, pp. 99–117, 2015.

[18] B. Chapter, D. Storage, A. Hamlin, E. Shen, and S. Yakoubov, *Cryptography for Big Data Security*. 2016.

[19] K. Häyrinen, K. Saranto, and P. Nykänen, “Definition, structure, content, use and impacts of electronic health records: A review of the research literature,” *Int. J. Med. Inform.*, vol. 77, no. 5, pp. 291–304, 2008.

[20] T. Miron-Scahtz and G. Elwyn, “To serve and protect? Electronic health records pose challenges for privacy, autonomy and person-centered medicine,” *Int. J. Pers. Cent. Med.*, vol. 1, no. 2, pp. 405–409, 2011.

[21] R. Hayward and C.-C. Chiang, “Parallelizing fully homomorphic encryption for a cloud environment,” *J. Appl. Res. Technol.*, vol. 13, pp. 245–252, 2015.

[22] A. J. Ikuomola and O. O. Arowolo, “Securing Patient Privacy in E-Health Cloud Using Homomorphic Encryption and Access Control,” *Int. J. Comput. Networks Commun. Secur.*, vol. 2, no. 1, pp. 15–21, 2014.

[23] G. Zyskind, O. Nathan, and A. “Sandy” Pentland, “Decentralizing Privacy:

Using Blockchain to Protect Personal Data," in *2015 IEEE Security and Privacy Workshops*, 2015, pp. 180–184.

[24] T. Neubauer and J. Heurix, "A methodology for the pseudonymization of medical data," *Int. J. Med. Inform.*, vol. 80, no. 3, pp. 190–204, 2011.

[25] A. Alabdulatif, I. Khalil, and V. Mai, "Protection of electronic health records (EHRs) in cloud," *Conf. Proc. ... Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. IEEE Eng. Med. Biol. Soc. Annu. Conf.*, vol. 2013, pp. 4191–4194, 2013.

[26] CACDS and CPhA, "Recommendations for the Implementation of Electronic Prescriptions in Canada," no. September, 2009.

[27] J. Calvillo-Arbizu, I. Roman-Martinez, and L. M. Roa-Romero, "Standardized access control mechanisms for protecting ISO 13606-based electronic health record systems," *2014 IEEE-EMBS Int. Conf. Biomed. Heal. Informatics, BHI 2014*, pp. 539–542, 2014.

[28] E. C. Cankaya and T. Kywe, "A Secure Healthcare System: From Design to Implementation," *Procedia Comput. Sci.*, vol. 62, no. Scse, pp. 203–212, 2015.

[29] D. Chen, L. Chen, X. Fan, L. He, S. Pan, and R. Hu, "Securing patient-centric personal health records sharing system in cloud computing," *China Commun.*, vol. 11, no. 13, pp. 121–127, 2014.

[30] J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. J. Peterson, and A. D. Rubin, "Securing Electronic Medical Records Using Attribute-Based Encryption On Mobile Devices," 2011.

[31] Congreso de Colombia, "Ley 23 de 1981," 1981.

[32] Presidencia de la República, "Decreto 3380," 1981.

[33] Ministerio de protección Social, "Resolución número 1448," 2006.

[34] Congreso de la República, "Ley 1122 de 2007," 2007.

[35] N. Carroll, M. Travers, and I. Richardson, "Evaluating multiple perspectives of a connected health ecosystem," 2016.

[36] K. L. Jena, *Modern approach to bibliometric studies*. SSDN Publishers & Distributors, 2012.

[37] Archivo General de la Nación, "Acuerdo 3 de 2015," 2015. .

[38] G. D. Flo´´rez, “La validez jurídica de los documentos electrónicos en Colombia a partir de sus evolución legislativa y jurisprudencial,” *Verba Iuris*, no. 31, p. 43, Jun. 2014.

[39] Congreso de la República, “Ley 527 de 1999,” 1999.

[40] N. P. Terry and L. P. Francis, “Ensuring the privacy and confidentiality of electronic health records,” *Univ. Ill. Law Rev.*, no. 2, pp. 681–736, 2007.

[41] E. AbuKhousa, N. Mohamed, and J. Al-Jaroodi, “e-Health Cloud: Opportunities and Challenges,” *Futur. Internet*, vol. 4, no. 4, pp. 621–645, 2012.

[42] Congreso de la República, “LEY 1753 DE 2015,” 2015. .

[43] P. de la República, “Decreto 2364 de 2012,” Nov. 2012.

[44] Congreso de la república, “Ley 1755 de 2015,” 2015. .

[45] C. Abraham, E. Nishihara, and M. Akiyama, “Transforming healthcare with information technology in Japan: A review of policy, people, and progress,” *Int. J. Med. Inform.*, vol. 80, no. 3, pp. 157–170, 2011.

[46] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, “Systematic mapping studies in software engineering,” *EASE’08 Proc. 12th Int. Conf. Eval. Assess. Softw. Eng.*, pp. 68–77, 2008.

[47] H. Zhang, M. A. Babar, and P. Tell, “Identifying relevant studies in software engineering,” *Inf. Softw. Technol.*, vol. 53, no. 6, pp. 625–637, 2011.

[48] M. Naveed *et al.*, “6 Privacy in the Genomic Era,” *ACM Comput. Surv. ACM Comput. Surv. Artic.*, vol. 48, no. 44, 2015.

[49] M. F. Ferdous and K. Sakamura, “A Secure and Flexible e-Health Access Control System with Provisions for Emergency Access Overrides and Delegation of Access Privileges,” no. January 2002, pp. 541–546, 2016.

[50] B. H. Gray, T. Bowden, I. Johansen, and S. Koch, “Electronic health records: an international perspective on ‘meaningful use’.,” *Issue Brief (Commonw. Fund)*, vol. 28, no. November, pp. 1–18, 2011.

[51] J. C. Forero Camacho and O. Bernal Acevedo, “Information systems in health sector in Colombia,” *Rev. Gerenc. y Políticas Salud*, vol. 10, no. 21,

pp. 85–100, 2008.

[52] E. Smith and J. H. Eloff, “Security in health-care information systems--current trends.,” *Int. J. Med. Inform.*, vol. 54, no. 1, pp. 39–54, 1999.

[53] M. Tsiknakis, D. G. Katehakis, and S. C. Orphanoudakis, “An open, component-based information infrastructure for integrated health information networks,” *Int. J. Med. Inform.*, vol. 68, no. 1–3, pp. 3–26, 2002.

[54] E. B??nes, P. Hasvold, E. Henriksen, and T. Stranden??s, “Risk analysis of information security in a mobile instant messaging and presence system for healthcare,” *Int. J. Med. Inform.*, vol. 76, no. 9, pp. 677–687, 2007.

[55] P. Vittorini, A. Tarquinio, and F. di Orio, “XML technologies for the Omaha System: A data model, a Java tool and several case studies supporting home healthcare,” *Comput. Methods Programs Biomed.*, vol. 93, no. 3, pp. 297–312, 2009.

[56] B. S. Elger *et al.*, “Strategies for health data exchange for secondary, cross-institutional clinical research,” *Comput. Methods Programs Biomed.*, vol. 99, no. 3, pp. 230–251, 2010.

[57] M. H. Hsu, Y. T. Yeh, C. Y. Chen, C. H. Liu, and C. T. Liu, “Online detection of potential duplicate medications and changes of physician behavior for outpatients visiting multiple hospitals using national health insurance smart cards in Taiwan,” *Int. J. Med. Inform.*, vol. 80, no. 3, pp. 181–189, 2011.

[58] S. Haas, S. Wohlgemuth, I. Echizen, N. Sonehara, and G. Müller, “Aspects of privacy for electronic health records,” *Int. J. Med. Inform.*, vol. 80, no. 2, pp. e26–e31, 2011.

[59] V. Patel, E. L. Abramson, A. Edwards, S. Malhotra, and R. Kaushal, “Physicians’ potential use and preferences related to health information exchange,” *Int. J. Med. Inform.*, vol. 80, no. 3, pp. 171–180, 2011.

[60] C. Quantin, D. O. Jaquet-Chiffelle, G. Coatrieux, E. Benzenine, and F. A. Allaert, “Medical record search engines, using pseudonymised patient identity: An alternative to centralised medical records,” *Int. J. Med. Inform.*, vol. 80, no. 2, pp. 6–11, 2011.

[61] C. C. Bennett, T. W. Doub, and R. Selove, “EHRs connect research and

practice: Where predictive modeling, artificial intelligence, and clinical decision support intersect," *Heal. Policy Technol.*, vol. 1, no. 2, pp. 105–114, 2012.

[62] X. Bai, R. Gopal, M. Nunez, and D. Zhdanov, "A decision methodology for managing operational efficiency and information disclosure risk in healthcare processes," *Decis. Support Syst.*, vol. 57, no. 1, pp. 406–416, 2014.

[63] C. D. Huang, R. S. Behara, and J. Goo, "Optimal information security investment in a Healthcare Information Exchange: An economic analysis," *Decis. Support Syst.*, vol. 61, no. 1, pp. 1–11, 2014.

[64] M. Gaynor, F. Yu, C. H. Andrus, S. Bradner, and J. Rawn, "A general framework for interoperability with applications to healthcare," *Heal. Policy Technol.*, vol. 3, no. 1, pp. 3–12, 2014.

[65] G. Comandé, L. Nocco, and V. Peigné, "An empirical study of healthcare providers and patients' perceptions of electronic health records," *Comput. Biol. Med.*, vol. 59, pp. 194–201, 2015.

[66] R. Karakis, I. Guler, I. Capraz, and E. Bilir, "A novel fuzzy logic-based image steganography method to ensure medical data security.," *Comput. Biol. Med.*, vol. 67, pp. 172–183, 2015.

[67] M. Anwar, J. Joshi, and J. Tan, "Anytime, anywhere access to secure, privacy-aware healthcare services: Issues, approaches and challenges," 2015.

[68] J. L. Fernández-Alemán, A. Sánchez-Henarejos, A. Toval, A. B. Sánchez-García, I. Hernández-Hernández, and L. Fernandez-Luque, "Analysis of health professional security behaviors in a real clinical setting: An empirical study," *Int. J. Med. Inform.*, vol. 84, no. 6, pp. 454–467, 2015.

[69] O. Ben-Assuli, "Electronic health records, adoption, quality of care, legal and privacy issues and their implementation in emergency departments," *Health Policy (New. York).*, vol. 119, no. 3, pp. 287–297, 2015.

[70] M. Lapke, C. Garcia, and D. Henderson, "The disconnect between

healthcare provider tasks and privacy requirements," *Heal. Policy Technol.*, 2016.

[71] J. L. Cardoso de Moraes, "A methodology based on openEHR archetypes and software agents for developing e-health applications reusing legacy systems," *Comput. Methods Programs Biomed.*, vol. 134, pp. 267–287, 2016.

[72] B. Riedl, V. Grascher, S. Fenz, and T. Neubauer, "Pseudonymization for improving the privacy in e-health applications," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 1–10, 2008.

[73] B. Regan, O. T. Pusatli, E. Lutton, and R. Athauda, "Securing an EHR in a health sector digital ecosystem," *2009 3rd IEEE Int. Conf. Digit. Ecosyst. Technol. DEST '09*, pp. 285–289, 2009.

[74] N. Dagdee and R. Vijaywargiya, "Credential Based Hybrid Access Control Methodology for Shared Electronic Health Records," *2009 Int. Conf. Inf. Manag. Eng.*, pp. 624–628, 2009.

[75] F. Amato, V. Casola, A. Mazzeo, and S. Romano, "A semantic based methodology to classify and protect sensitive data in medical records," *2010 6th Int. Conf. Inf. Assur. Secur. IAS 2010*, pp. 240–246, 2010.

[76] J. Barnickel, H. Karahan, and U. Meyer, "Security and privacy for mobile electronic health monitoring and recording systems," *2010 IEEE Int. Symp. "A World Wireless, Mob. Multimed. Networks,"* pp. 1–6, 2010.

[77] J. Heurix, M. Karlinger, and T. Neubauer, "Pseudonymization with metadata encryption for privacy-preserving searchable documents," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 3011–3020, 2011.

[78] A. Clarke and R. Steele, "Secure and reliable distributed health records: Achieving query assurance across repositories of encrypted health data," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 3021–3029, 2011.

[79] J. Mirkovic, H. Bryhni, and C. M. Ruland, "Secure Solution for Mobile Access to Patients Health Care Record," *2011 IEEE 13th Int. Conf. e-Health Networking, Appl. Serv.*, pp. 296–303, 2011.

[80] Rui Zhang, Jiqiang Liu, Zhen Han, and Ling Liu, "RBTBAC: Secure Access

and Management of EHR Data," *Inf. Soc. (i-Society), 2011 Int. Conf.*, pp. 494–499, 2011.

[81] Y. Han, J. W. Wang, Y. Li, and Y. X. Chen, "Information security of EHRs," *Proc. - 2012 4th Int. Conf. Multimed. Secur. MINES 2012*, pp. 896–899, 2012.

[82] S. Wang, X. Jiang, L. Ohno-Machado, L. Cui, S. Cheng, and H. Xiong, "Privacy-preserving biometric system for secure fingerprint authentication," *Proc. - 2012 IEEE 2nd Conf. Healthc. Informatics, Imaging Syst. Biol. HISB 2012*, vol. 2010, p. 128, 2012.

[83] T. Piliouras *et al.*, "Impacts of legislation on electronic health records systems and security implementation," *2012 IEEE Long Isl. Syst. Appl. Technol. Conf. LISAT 2012*, 2012.

[84] E. Bertino and J. Willemson, "Multiparty privacy protection for electronic health records," *2013 IEEE Glob. Commun. Conf.*, pp. 2730–2735, 2013.

[85] N. Ulltveit-moe, T. Gjøsæter, S. M. Assev, G. M. Køien, and V. Oleshchuk, "Privacy Handling for Critical Information Infrastructures."

[86] E. Frontoni, M. Baldi, P. Zingaretti, V. Landro, and P. Misericordia, "Security issues for data sharing and service interoperability in eHealth systems: The Nu.Sa. test bed," *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2014-Octob, no. October, 2014.

[87] D. B. Hoang and L. Chen, "Health records protection in cloud environment," *Proc. - 2014 IEEE 13th Int. Symp. Netw. Comput. Appl. NCA 2014*, pp. 85–90, 2014.

[88] S. Lakkaraju and D. Xu, "Integrated Modeling and Analysis of Attribute Based Access Control Policies and Workflows in Healthcare," *2014 Int. Conf. Trust. Syst. their Appl.*, pp. 36–43, 2014.

[89] M. Maffei, G. Malavolta, M. Reinert, and D. Schroder, "Privacy and access control for outsourced personal records," *Proc. - IEEE Symp. Secur. Priv.*, vol. 2015-July, pp. 341–358, 2015.

[90] Z. Huang, E. Ayday, J. Fellay, J. P. Hubaux, and A. Juels, "GenoGuard:

Protecting genomic data against brute-force attacks," *Proc. - IEEE Symp. Secur. Priv.*, vol. 2015-July, pp. 447–462, 2015.

[91] R. Chatterjee, J. Bonneau, A. Juels, and T. Ristenpart, "Cracking-resistant password vaults using natural language encoders," *Proc. - IEEE Symp. Secur. Priv.*, vol. 2015-July, pp. 481–498, 2015.

[92] L. Barman, M. T. Elgraini, J. L. Raisaro, J. P. Hubaux, and E. Ayday, "Privacy threats and practical solutions for genetic risk tests," *Proc. - 2015 IEEE Secur. Priv. Work. SPW 2015*, no. Mc, pp. 27–31, 2015.

[93] N. Mohammed, S. Barouti, D. Alhadidi, and R. Chen, "Secure and private management of healthcare databases for data mining," *Proc. - IEEE Symp. Comput. Med. Syst.*, vol. 2015-July, no. Section V, pp. 191–196, 2015.

[94] L. Bernardo Villa, I. Cabezas, and J. Cruz, "Historia Cl??nica Electr??nica como Servicio de Software en la Nube," *2015 10th Colomb. Comput. Conf. 10CCC 2015*, pp. 543–550, 2015.

[95] S. Sharma and V. Balasubramanian, "A biometric based authentication and encryption Framework for Sensor Health Data in Cloud," *Conf. Proc. - 6th Int. Conf. Inf. Technol. Multimed. UNITEN Cultiv. Creat. Enabling Technol. Through Internet Things, ICIMU 2014*, pp. 49–54, 2015.

[96] M. K. Debnath, S. Samet, and K. Vidyasankar, "A secure revocable personal health record system with policy-based fine-grained access control," *2015 13th Annu. Conf. Privacy, Secur. Trust. PST 2015*, pp. 109–116, 2015.

[97] N. Kahani, K. Elgazzar, and J. R. Cordy, "Authentication and Access Control in e-Health Systems in the Cloud," *2016 IEEE 2nd Int. Conf. Big Data Secur. Cloud (BigDataSecurity), IEEE Int. Conf. High Perform. Smart Comput. (HPSC), IEEE Int. Conf. Intell. Data Secur.*, pp. 13–23, 2016.

[98] D. Acharya and V. Kumar, "Security of MBAN based health records in mobile broadband environment," *Procedia Comput. Sci.*, vol. 5, pp. 539–545, 2011.

[99] J. L. Fernández-Alemán, I. C. Señor, P. ángel O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature

review," *J. Biomed. Inform.*, vol. 46, no. 3, pp. 541–562, 2013.

[100] A. Ghazvini and Z. Shukur, "Security Challenges and Success Factors of Electronic Healthcare System," *Procedia Technol.*, vol. 11, no. Iceei, pp. 212–219, 2013.

[101] D. Box and D. Pottas, "Improving Information Security Behaviour in the Healthcare Context," *Procedia Technol.*, vol. 9, pp. 1093–1103, 2013.

[102] J. W. Bos, K. Lauter, and M. Naehrig, "Private predictive analysis on encrypted medical data," *J. Biomed. Inform.*, vol. 50, pp. 234–243, 2014.

[103] A. Santos, J. Macedo, A. Costa, and M. J. Nicolau, "Internet of Things and Smart Objects for M-health Monitoring and Control," *Procedia Technol.*, vol. 16, pp. 1351–1360, 2014.

[104] Ş. Bahtiyar and M. U. Çağlayan, "Trust assessment of security for e-health systems," *Electron. Commer. Res. Appl.*, vol. 13, no. 3, pp. 164–177, 2014.

[105] Z. Li, C. H. Chu, and W. Yao, "A semantic authorization model for pervasive healthcare," *J. Netw. Comput. Appl.*, vol. 38, no. 1, pp. 76–87, 2014.

[106] T. Ermakova, B. Fabian, S. Kelkel, T. Wolff, and R. Zarnekow, "Antecedents of health information privacy concerns," *Procedia Comput. Sci.*, vol. 63, no. Icth, pp. 376–383, 2015.

[107] R. A. Meehan *et al.*, "Increasing EHR system usability through standards: Conformance criteria in the HL7 EHR-system functional model," *J. Biomed. Inform.*, vol. 63, pp. 169–173, 2016.

[108] S. Bhartiya, D. Mehrotra, and A. Girdhar, "Issues in Achieving Complete Interoperability while Sharing Electronic Health Records," *Procedia Comput. Sci.*, vol. 78, no. December 2015, pp. 192–198, 2016.

[109] H.-T. Wu, Y. Cheung, and J. Huang, "Reversible Data Hiding in Paillier Cryptosystem," *J. Vis. Commun. Image Represent.*, 2016.

[110] J. Sun, X. Zhu, C. Zhang, and Y. Fang, *Security and privacy for mobile health-Care (m-Health) systems*. Elsevier Inc., 2012.

[111] M. Ogburn, C. Turner, and P. Dahal, "Homomorphic encryption," *Procedia Comput. Sci.*, vol. 20, pp. 502–509, 2013.

[112] “MacBook Pro (15-inch, 2018) - Technical Specifications.” [Online]. Available: https://support.apple.com/kb/SP776?viewlocale=en_US&locale=en_US. [Accessed: 24-Nov-2018].